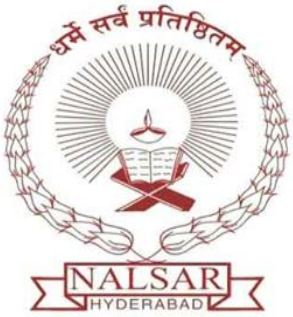


Centre for Aerospace & Defence Laws (CADL)

Directorate of Distance Education

NALSAR University of Law, Hyderabad

Course Material

M.A (MARITIME LAWS)

1.1.3. MARITIME SECURITY & SAFETY

Compiled by:

Prof. (Dr.) V. Balakista Reddy

Ms. Bangaru Laxmi Jasti

NALSAR University of Law, Hyderabad (Print 2021)
Re-Print 2023
(For private circulation only)

TABLE OF CONTENTS

MODULE-I

SAFETY AND SECURITY: AN INTRODUCTION

THE CONCEPTS OF RISK, SAFETY, AND SECURITY: A FUNDAMENTAL EXPLORATION AND UNDERSTANDING OF SIMILARITIES AND DIFFERENCES

Introduction

Risk and safety are often proposed as being antonyms, but more and more understanding grows that this is only partially true and not in line with the most modern, more encompassing views on risk and safety. Likewise, safety and security are often seen as being completely different fields of expertise and study, separated from each other, while other views might more underline the similarities that are to be found between the two concepts and how they can be regarded as being synonyms.

So, how do these concepts relate to each other? How can a contemporary and inclusive view on risk, safety, and security help in understanding and in dealing with the issues related to these concepts?

The Concepts of Risk, Safety, and Security

Perceptions and awareness regarding the concepts of safety, security, and risk have evolved in recent years from a narrow and specialist perspective to a more holistic view on, and approach toward the related issues. However, this understanding is not necessarily a common perspective.

The whole world comprehends what the words mean and in one′s own perception how they can be understood. However, when opening a discussion on what these concepts really are, and how one should study or deal with them, it is most likely to end up in ontological and semantic debates due to the different views, perceptions, and definitions that exist.

The Importance of Standardization and Commonly Agreed upon Definitions of Concepts

Science, including the domain of risk and safety, largely depends upon clear and commonly agreed upon definitions of concepts, and well-defined parameters, because having precise definitions of concepts and parameters allows for standardization, enhances communication, and allows for an unambiguous sharing of knowledge. Our ability to combine information from independent experiments depends on the use of standards analogous to manufacturing standards, needed for fitting parts from different manufacturers.

Synonyms and Antonyms

When studying in the field of safety and security science, it is hard to find unambiguous definitions and parameters that clearly link safety, security, and risk. After reviewing the safety science literature, it is clear that the question “what is safety” can be answered in many ways and that it is very hard to find a clear definition of its opposite.

As a consequence, the study of the concepts of risk, safety, and security shows that there is no truly commonly accepted and widely used semantic foundation to be used in Safety and Security Science. Likewise, such a study also confirms that there is a lack of standardization when it comes to defining the opposite, the antonyms that indicate a lack of safety or security.

Concept	Number of Hits	Concept	Number of Hits
Risk	4.770.000	Uncertainity	3.930.000
Safety	3.450.000	Unsafety	8.800
Security	3.290.000	Unsecurity	40.800
Accident	3.110.000	Insecurity	1.090.000
Incident	3.160.000	Mishap	77.500
Disaster	2.800.000	Catastrophe	899.000
Hazard	3.340.000	Danger	2.770.000
Injury	1.900.000	Loss	5.810.000

Table:1 Google Scholar search results - 27 March 2018

A perfect word to indicate a lack of safety would be “unsafety”, although it is little used in scientific literature, as is indicated in Table 1.

For the antonym of security, it is even more difficult to find a commonly used word covering the subject. For example, the Oxford living dictionary defines unsecurity as “uncertainty or anxiety about oneself”, “a lack of confidence”. Is this what people generally think of when talking about security issues in safety and security science today? It is sensible to use the word “unsecurity” instead.

A Semantic and Ontological Perspective on Safety and Security

Standard Definitions

While standard definitions for safety and security are lacking, this is not so for the concept of risk. Although regarding the concept of “risk” many opinions and definitions exist, an encompassing standardized definition is available. The International Organization for Standardization (ISO) defines risk as “the effect of uncertainty on objectives”.

Taking this definition as a reference makes it possible to define safety and security and their antonyms in a similar, unambiguous, and encompassing way. Safety in its broadest sense could then be defined as follows: “Safety is the condition/set of circumstances where the likelihood of negative effects on objectives is Low”.

Risk and safety—where safety needs to be understood in a broad perspective including security—are tightly related and the understanding of these two concepts have evolved in similar ways, expanding the view from a pure loss perspective toward a more encompassing view, including negative (loss) and positive (gain) effects. Also in safety science, the awareness rises that the domain of safety does not only cover the protection against loss (Safety-I), but also includes the condition of excellent performance in achieving and safeguarding objectives (Safety-II).

Today, risk, safety, and security are also linked to what one actually wants and how to get what one wants. However, it is this most obvious part, "the objectives", that is often forgotten in definitions, while the concept of objective is maybe the most important element in understanding the concepts of risk, safety, and security.

Linking and Differentiating Risk and Safety

What one "wants" can be considered as one′s "objectives", with the concept "objective" understood in its most encompassing way. The following comprehensive definition of the concept "objective" is proposed as a fundamental starting point for the comprehension of the concepts risk, safety, and security: "*Objectives are those matters, tangible and intangible, that individuals, organisations or society as a whole (as a group of individuals) want, need, pursue, try to obtain or aim for. Objectives can also be conditions, situations or possessions that have already been established or acquired and that are, or have been, maintained as a purpose, wanted state or needed condition, whether consciously and deliberately expressed or unconsciously and indeliberately present*".

Linking Risk and Safety

As such, based on the ISO definition of risk, the link between risk and safety can be seen as follows: risk, in order to exist, requires the presence of all three of the following elements: "objectives", "effects" that can affect those objectives, and "uncertainty" related to these elements. Safety (including security) mainly concerns the objectives and the effects that can affect these objectives. Understanding risk and safety (including security) then both requires the understanding of the objectives that matter, the possible effects that can affect these objectives (negative effects on objectives), the likelihood of occurrence of these effects, and the level of impact of these effects and the associated likelihood (likelihood is low).

Differentiating Risk and Safety

The only fundamental difference between risk and safety consists in the fact that risk deals with an uncertain future state, while safety is more concerned with determined, actual conditions. When these effects are positive, they enhance safety as they will support the objectives involved, while the negative effects degrade safety, or increase unsafety, as they subtract from the related objectives.

Quality of Perception

Irrespective of the actual conditions and future possible outcomes, risk, safety, and security will always vary from one individual to another due to variations in objectives and related values. As such, risk, safety, and security are constructs in people's minds. Every individual has different sets of objectives or values the same objectives differently, creating different perceptions of the same reality.

Furthermore, every individual has their own unique perception of reality, because reality will always need an interpretation and can only be perceived. Hence, there will always be a remaining level of uncertainty and residual lack of understanding related to risk, safety, and security, varying from one person to another. Safety science should, therefore, aim for the highest possible quality of perception, where the deviation between reality as it is and the perception of this reality is the lowest possible.

Constraints

Pursuing or safeguarding objectives will always be accompanied by the effects of uncertainty originating from a variety of risk sources. When managing risk, aiming for safety and security, and, therefore, has to identify the risk sources and their associated risks. Pursuing and safeguarding objectives requires certain level of risk not to be exceeded. These constraints are to be taken into account when managing risk and to be adhered to when safety is a concern.

Linking and Differentiating Safety and Security

So far, safety and security have been regarding in the same way. However, what are the common elements that make security the same as safety and what sets these two concepts apart?

A Distinction on the Level of "Effect"

In managing risk, risk professionals mainly try to determine the level of risk once risks have been identified. However, the assessment of the nature of risk is an important additional element to consider in managing risk and therefore, also in deterring and managing safety.

The level of risk can be understood as being the level of impact of the effects on objectives (negative and positive) in combination with their related level of uncertainty. It is often expressed in the form of a combination of probabilities and consequences. The nature of risk on the other hand is more linked to the sources of risk and how these risks emerge and develop. In ISO Guide 73, a risk source is defined as being an element that, alone or in combination, can give rise to risk. It is in the understanding of possible risk sources that the difference between safety and security can be found.

When continuing on the semantic foundation provided by ISO 31000 and ISO Guide 73, safety can be seen as "a condition or set of circumstances, where the likelihood of negative effects of uncertainty on objectives is low". When safety is regarded in a very general way, security then is just a sub-set of safety. Indeed, when the likelihood of negative effects of uncertainty on objectives is low, this also means that a secure(d) condition or set of circumstances exists.

A first (and obvious) distinction between safety and security can be discovered when looking at the "effects" of uncertainty on objectives, introducing the idea that effects can be regarded as being "intentional" or "unintentional" (accidental). When negative effects on objectives are "intentional", it is appropriate and correct to use the term security instead of speaking of safety. Consequently, it would also be inappropriate to use the term "security" when the effects of uncertainty involved are "unintentional". Terrorists, as an example, intend to cause damage and harm. They intentionally increase the likelihood of negative effects on the objectives of the groups of people or parts of society they want to terrorize. Likewise, criminals intentionally act against the laws meant to safeguard specific societal, organizational, or individual objectives. Security, therefore, can be defined as follows: "*Security is the condition/set of circumstances where the likelihood of intentional negative effects on objectives is low*".

A Distinction on the Level of "*Objectives"*

Another way to look at the difference between safety and security, on a more fundamental level, is to examine the concerned objectives. A typical aspect of a security setting is the involvement of multiple parties (with a minimum of two). Different perceptions come into play and accordingly also different objectives become involved. One of the parties will try to achieve,

maintain, and protect a set of objectives, whereas one or more opposing parties will have different opinions on those objectives, and they may intentionally try to affect these objectives in a negative way. When look- ing at security situations from this perspective, it becomes clear that security issues can be regarded as situations or sets of circumstances where different, non-aligned, objectives of stakeholders conflict with each other.

If we think of objectives as vectors, pointing in a defined direction, (non)alignment of objectives can be determined in a geometrical way, and the difference between safety and security can be determined by measuring the level of non-alignment of objectives of the different parties involved. Once the non-alignment of objectives becomes more than 90° (supposing fully aligned objectives are at a 0° deviation of each other), it is apparent that these objectives are conflicting and achieving the objective of one party will cause negative effects on the objectives of the other party. Therefore, one could argue that in security management, discovering the presence of different, opposing objectives is crucial.

A level of distinction between safety and security also can be found in the level of alignment of objectives of individuals, organizations, or societies. Building on the definition of security in the preceding section and including the alignment perspective, a definition for unsecurity can be proposed: "Unsecurity is the conditions/set of circumstances where the alignment of objectives is low and where the likelihood of intentional negative effects on objectives is high".

Terrorism, for example, is a very clear illustration of non-alignment of objectives, because many terrorist objectives are exactly opposite to the societal, organizational, and individual objectives they oppose.

A Distinction on the Level of "Uncertainty"

Last, but not least, a distinction on the level of uncertainty can be made. Safety science and safety management often depend on statistical data in order to develop theories and build safety measures. The nature of unintentional effects makes it so that the same events repeat themselves in different situations and circumstances. Furthermore, any individual can be taken into account for objectives that are very much aligned, such as keeping one′s physical integrity. This provides for a vast amount of data that can be used to build theories and measures, based on statistical instruments.

Unfortunately, in security issues, the intentional nature and the non-alignment of objectives lead to repeated attempts to invent new tactics and techniques to achieve the non-aligned objectives, making it much more difficult to build on statistical data to determine specific uncertainties. It also means that different tools can and must be used to determine levels of risk and safety/security, such as game theoretical models.

The similarities and distinctions between the discussed concepts can be imagined as follows. Risk emerges when objectives are present (conscious or unconscious, deliberate or indeliberate). Risk becomes a safety or unsafety concern when objectives are tied to a specific situation or set of circumstances containing specific risk sources, providing for possible effects of uncertainty on objectives. When more than one party is involved, conflicting objectives can develop, resulting in deliberate negative effects of uncertainty on objectives for either party, making safety issues become security issues.

Safety becomes security when conflicting objectives between different parties develop, because due to the conflict, negative effects become intentional and by their intentionality also, the nature of uncertainty changes.

Introduction to Security

International Security Studies (ISS) grew out of debates over how to protect the state against external and internal threats after the Second World War. Security became its watchword, both distinguishing ISS from earlier thinking and the disciplines of War Studies and Military History, and, as it evolved, serving as the linking concept connecting an increasingly diverse set of research programmes.

To delineate ISS is unfortunately not as straightforward an exercise as one might wish. The label 'international security 'was not adopted from the outset, but only gradually became accepted, and there is no universally agreed definition of what ISS comprises, and hence no accepted archive of 'ISS-documents 'that define our object of study. The composition of ISS has mainly been taken for granted, with the consequence that little self-reflection on what made up ISS or its boundaries has been produced. The absence of a universal definition of what makes up ISS means that ISS has at times become a site for disciplinary politics with different perspectives arguing that they should be included while others (usually different sorts of widening perspectives) should not.

The delineation of ISS is complicated by the fact that as time goes by we get a different perspective on what falls in and what does not. To paraphrase Foucault's genealogical understanding of history as always being told from the point of the present, the fact that we tell the story of ISS from a 2008 perspective means that we look at a field which has some strikingly different preoccupations, both substantive and epistemological, from those that dominated it in, say, 1972. And it would have been easier to delineate ISS had it always been explicitly centred on the concept of security. Unfortunately, this has not been the case. Indeed, after its first decade of explicit theoretical and conceptual innovation, the field's mainstream carried out its work without much conceptual reflection. During the 'golden age 'of Strategic Studies it would have been easy to think that 'strategy 'was the dominant concept, albeit strategy now dominated by civilian rather than military thinkers. Thus in 1983, Buzan could point out that security was an 'underdeveloped concept 'and 'seldom addressed in terms other than the policy interests of particular actors or groups, and the discussion has a heavy military emphasis'. 'Security 'is, about crucial political themes such as the state, authority, legitimacy, politics and sovereignty, but even today the majority of articles and books that fall within the discipline of ISS do not contain lengthy meta-theoretical or philosophical discussions, but speak from within an implicit position on the conceptual terrain.

Our solution to the problem of delineating ISS starts from understanding conceptual security debates as 'the product of an historical, cultural, and deeply political legacy', not as something that can be solved through references to 'empirical facts'. This means that we take the power of inclusion and exclusion seriously. We cast our net widely and include the work of those who self- identify as participants in ISS (mainly in terms of how they title their work, who they seem to regard as their appropriate audience and, up to a point, where they publish) regardless of whether all others who self-identify with the sub-field accept them as 'members 'or not.

Four questions that structure ISS:

There are four questions which have, either implicitly or explicitly, structured debates within ISS since the late 1940s. These questions can have different answers, but that is not to say that they are always explicitly discussed: a large part of the ISS literature simply takes particular answers/concepts as givens. The four questions are analytical lenses or tools through which to read the evolution of ISS; they are the deeper, substantial core that defines what 'international security 'is about and what brings the literature together. Explicit discussions usually happen when established approaches are contested and their answers cannot be taken for granted. Viewing ISS through these questions makes it clear that there are fundamental political and normative decisions involved in defining security and that this is what makes it one of the essentially contested concepts of modern social science. Security is always a 'hyphenated concept 'and always tied to a particular referent object, to internal/external locations, to one or more sectors and to a particular way of thinking about politics.

The first question is whether to privilege the state as the referent object. Security is about constituting something that needs to be secured: the nation, the state, the individual, the ethnic group, the environment or the planet itself. Whether in the form of 'national security', or later, as traditionalist 'international security', the nation/state was the analytical and normative referent object. 'International security 'was not about replacing the security of the state with the security of humanity, or the individual or minorities within or across state boundaries. Securing the state was seen instrumentally as the best way of protecting other referent objects. 'National security ' should thus, as many observers have pointed out, more appropriately have been labelled 'state security', yet, what the Cold War concept of 'national security 'entailed was more accurately a fusion of the security of the state and the security of the nation: the nation supported a powerful state which in turn reciprocated by loyally protecting its society's values and interests. To what extent this was a proper way of understanding the relationship between states and their nations, between governments, citizens and populations – that is, the question of 'what or whom should be the "referent object" for security? – 'has been one of the central lines of debate within ISS.

The second question is whether to include internal as well as external threats. Since security is tied into discussions about state sovereignty (whether as something to be protected or criticised), it is also about placing threats in relation to territorial boundaries. Wolfers famously described 'national security 'as 'an ambiguous symbol 'and he contrasted the post-Second World War political climate with the one of inter-war American economic depression, holding that the 'change from a welfare to a security interpretation of the symbol "national interest" is understandable. Today we are living under the impact of cold war and threats of external aggression rather than depression and social reform'. 'National security 'had shifted from a concern with domestic economic problems to external threats stemming from ideologically opposed, and thus presumed hostile, powers. As this shift became institutionalised, the concept of 'international security 'came to accompany, but not replace, 'national security', and was eventually more influential in giving the discipline its name, hence International rather than National Security Studies. This labelling concurred with the growing disciplinary status of International Relations, which was based on distinguishing inter-national from domestic politics, of which ISS was increasingly a sub-field. The internal/external dimension was partly re-opened as the Cold War ended and the overriding concern with the external threat of the Soviet Union disappeared from American and Western security discourses. Both IR and ISS faced mounting challenges from globalisation to blur, or even collapse completely, the inside/outside distinction.

The third question is whether to expand security beyond the military sector and the use of force. Since ISS was founded during the Cold War and the Cold War was so overwhelmingly about the military (conventional and nuclear) capabilities of foes, friends and Self, 'national security 'became almost synonymous with military security. This did not mean that other capabilities were not considered, the editors of International Security stressed, for instance, the need to incorporate economic vigour, governmental stability, energy supplies, science and technology, food and natural resources. These were, however, to be incorporated because they impacted on 'the use, threat, and control of force', and thus on military security, not because they were to be considered security issues in their own right. But this conception of security was not entirely uncontested. During the Cold War, Peace Researchers pointed to the necessity of granting equal priority to basic human needs and 'structural violence', and challenges to military security became an established part of ISS from the 1980s onwards as scholars called for the inclusion of environmental and economic security. Later a more general sectoral widening of security included societal, economic, environmental, health, development and gender.

The fourth question is whether to see security as inextricably tied to a dynamic of threats, dangers and urgency. 'National security 'developed in a political climate where the United States, and the West more broadly, understood themselves as threatened by a hostile opponent. As in Herz's (1950) famous formulation of the security dilemma, 'security 'had to do with attacks, subjection, domination and – when pushed to the extreme – annihilation. This would lead groups to acquire more capabilities, in the process rendering their opponent insecure and thus compelling both sides to engage in a 'vicious circle of security and power accumulation'. Security was about the extreme and exceptional, with those situations that would not just raise inconveniences, but could wipe out one's society. During the Cold War, this seemed rather common-sensical to the mainstream of ISS: the Soviet Union constituted a clear threat, and nuclear weapons were justified as a way to deter the Soviet Union from a first strike. As the debates over the expansion of the concept of security gained ground in the 1990s, this linkage of security to urgency, and to extreme and radical defence measures, was central. Some, most prominently the Copenhagen School, argued that the concept could be expanded as long as referent objects, threats and dangers were constituted with this logic of urgency and extreme measures. Critics countered that this understanding of security was itself linked to a particular Realist view of the state and international politics. In keeping with a longer critical and Liberal tradition, it was argued on normative grounds that politics could be different and that one's analytical framework should incorporate this possibility.

Security and its adjacent concepts

We have defined ISS as those approaches that self-define either with the label of ISS, or with some branch of Security Studies (Human Security, Critical Security Studies, the Copenhagen School of Security Studies, Constructivist Security Studies and so on), and held that ISS is organised around different responses to the four questions laid out above. A further way to both delineate and to get at the ways in which ISS has evolved is to understand the field as structured by a set of key concepts. Obviously, the central concept of ISS is 'security', but it is also the case that conceptually explicit discussions were few and far between after the first decade of the Cold War. Even those who challenged Strategic Studies and ISS generally did not go through the concept of security, but through the concept of peace or more concrete

discussions of disarmament, arms control, peace movements and world order. The concept of security was underdeveloped and unproblematised by those who used it, and an antagonistic concept to Peace Researchers insofar as it was located on the Realist, Strategic, mili- tary side of the political and academic battles. From the mid-1980s, as the Cold War unravelled, security became increasingly explicitly addressed and it became adopted by new and former critics of Strategic Studies. Security approaches thus appeared which fifteen years earlier would have been unlikely to adopt this label: Critical Security Studies (with key con- cepts of individual security and emancipation); the Copenhagen School of Security Studies based at the Copenhagen Peace Research Institute; and the International Peace Research Institute, Oslo (PRIO) based journal Bulletin of Peace Proposals changed its name to Security Dialogue. This certainly did not mean that 'security 'was an uncontested concept, in fact it became more contested than ever, but it showed that after the Cold War 'security 'became a concept which generated – and hence could unify – debates across perspectives previously opposed.

A delineation of what falls within ISS based religiously on an explicit discussion of the concept of security would as a consequence leave out the majority of the Cold War contestants. This in turn would make it difficult to explain the resurgence of widening approaches in the 1990s, as these grew out of Cold War Peace Research, Feminism, Poststructuralism and Critical Theory. To tell the story of Cold War ISS without incorporating the criticism it generated would unduly homogenise the academic and political terrain on which ISS was situated. What we suggest is thus to see 'security 'as supported by or conducted through three kinds of concepts: first, through complementary concepts, like 'strategy', 'deterrence', 'containment 'or 'humanitarianism', which point to a more specific and narrower set of questions; second, through parallel concepts, like 'power', 'sovereignty 'or 'identity', which take security into a broader, Political The- ory or wider IR frame of reference; and third, oppositional concepts which work through security, but argue that it should be replaced, such as by 'peace 'in Cold War Peace Research (see chapter 5) or 'risk 'or 'the exception 'in twenty-first-century widening debates. Figure 1.1 illustrates the three kinds of adjacent concepts and their relationship to the concept of security.

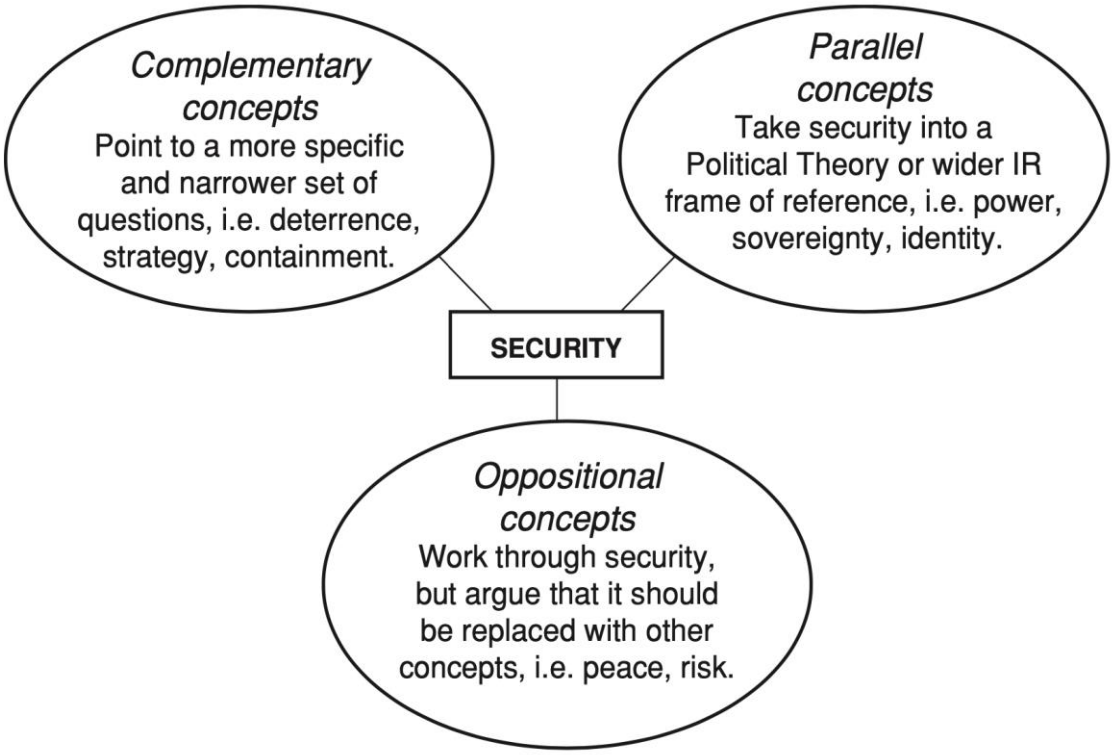


Figure 1.1. Security and its adjacent concepts

The advantage of the security plus three adjacent concepts framework is that it allows us to conduct a structured conceptual analysis, particularly of those literatures that do not explicitly link to debates over the concept of security in ISS. Literatures may be 'conceptually silent ' because they are adopting a taken-for-granted concept, are written in a rather straightforward empirical manner that downplays lengthy conceptual discussions, or because they come from other disciplines less reliant upon 'security 'debates. Even if an approach does not explicitly discuss its conceptualisation of security, the way it mobilises complementary, parallel or oppositional concepts allows us to see the river delta of ISS perspectives as engaged in the same meta-conversation about what 'security 'entails. An understanding of such conceptual points of engagement is, an important element in providing ISS with enough cohesion to make it an academic sub-field with a shared identity rather than a set of fragmented camps.

A different, but related, boundary-drawing question concerns literatures on security that are attached to prefixes not normally considered part of the ISS repertoire. Noteworthy examples include 'social security 'and 'computer security'. Social security is usually considered part of discussions of wealth, income distribution and domestic justice, not 'security proper'. Computer security is a technical term used by computer scientists referring to problems in computer hard- and software, some of them accidental bugs, others as outcomes of malicious outside attackers. The standard ISS reply is that such concepts lack the drama and urgency of 'national/international 'security, that they deal with domestic– individual questions in the case of social security and 'technical 'rather than political–military threats in the case of computer

security. In spite of a semantic similarity to (national) security, there is not a substantial, discursive resemblance.

This reply may be accurate in that these literatures do lack these characteristics and that they have historically not been considered part of ISS. But we should keep in mind that ISS is also a dynamic field that has expanded its legitimate contenders quite significantly in the past twenty years, and that what is considered to be part of it or not is not (solely) based on some static 'national/international security essence', but on how ISS evolves with its political environment. What academic and political actors man- age to get accepted as part of 'international security 'changes over time. Environmental security was not considered part of mainstream ISS in the early 1980s, yet it is hard to imagine it being excluded today. Such conceptual inclusion may be aided by the securitisation of hyphenated concepts, that is the constitution of something/somebody as radically threatening, as has been the case with health/disease security by prominent politicians or the media. Hyphenated securities might also make it onto the security agenda proper through conceptual analysis that explores and problematises the ways in which they are being excluded. A recent analysis by Neocleous (2006a) shows, for instance, how 'national security 'was tied to domestic economic concerns during the 1930s and that this discourse mobilised the same drama and urgency as 'national security 'did in the 1950s.

The disciplinary boundary of ISS

To see ISS as constituted through the questions and conceptual framework above still leaves the question of where ISS ends and other academic disciplines, particularly IR, begin. The boundary between ISS and IR is difficult to draw. In the early decades following the Second World War, the answer to this problem could have been given with some accuracy as: 'What distinguishes ISS from the general field of IR is its focus on the use of force in international relations. 'In the traditionalist perspective on ISS, 'use of force 'was and is primarily defined as 'state use of military force 'and the threats states face are predominantly military in kind. Yet even this apparently narrow framing implies potentially quite a broad scope. It is about war and the various ways in which military power can be deployed, but also about the foundations of military power (and thus, up to a point, about economics and the socio-political structures of the state), and about the causes of conflict in international relations that result in states and other actors creating, maintaining and sometimes using military power (thus potentially bringing in not just economic, but also environmental and identity issues). This type of ISS features the general dynamics of interaction amongst rival armed forces: arms racing, arms control, the impact of technological developments and suchlike. Because of its strong state-centrism and assumptions about power struggles, it can, at the risk of some simplification, be thought of as the specialist military– technical wing of the Realist approach to IR. In the UK literature this whole understanding and approach is often labelled Strategic Studies. By the 1970s, however, the simple 'use of force 'answer was becoming increasingly inaccurate. It remained true that the traditionalist position provided the foundational template, focusing on the international level and on threats that were about survival. But as the agenda of ISS began to widen towards the end of the Cold War, and more rapidly after it, the 'use of force 'answer became too narrow a description of what the field was about (at least for a large number of those participating in its debates). What increasingly distinguished ISS from IR was that it centred itself either on assumptions or on debates around and about the concept of international security.

Still there are inevitable overlaps between IR and ISS, particularly insofar as ISS has become more theoretically driven and that important IR debates simultaneously have evolved around security. As an example of the former, Waltzian Neorealism has been key to debates in the more theoretically informed parts of Realist Security Studies, particularly on how the polarity of the system impacts stability and grand strategy. There is, for instance, a rich literature on how to define polarity that is not strictly speaking about the concept of security as such, or how it may change in the light of shifting polarities, etc. One reason this literature does not explicitly discuss the concept of security is that it takes a conventional conception of security as national security for granted.

The overlaps between IR and ISS have also multiplied in that 'security 'has been selected as the arena for IR debates of a more general kind, noticeably over the status of Constructivist theory from the 1990s onwards. The programmatic statement of Conventional Constructivism in Katzenstein's The Culture of National Security explicitly adopted 'security 'as the 'hard case ' where Constructivist theories emphasising ideas, culture, norms and identity should stand trial in comparison with Neo- realist and Neoliberalist approaches. Yet there was no explicit discussion of 'security 'itself: what was contested were Realist explanations of state behaviour in the area of security, not whether the state should be the referent object, or whether the sector of concern should be the one of military and external threats.

Such works usually draw upon general IR literatures and debates, and there is therefore a link between telling the story of the evolution of ISS and the one of IR. Yet it should be kept in mind that our concern is with the evolution of ISS, not IR, and we will therefore not go extensively into IR literatures that have not addressed security or which have not been drawn upon explicitly by ISS. It should be stressed also that while IR is by far the main overarching discipline to ISS, it is not the only one to influence it: some of the first key thinkers on game theory, which influenced deterrence theory during the Cold War, were economists and physicists and other 'hard scientists 'explicitly engaged in debates over the nuclear condition. As conceptual debates started to take off in the 1980s and flourished in the 1990s, a series of sociologists, feminist theorists, philosophers, development theorists, anthropologists and media theorists have also joined the debates in ISS. Like the classical empires of old, ISS therefore does not have clearly defined borders. Instead, it has 'frontier zones 'where its debates blend into adjacent subjects, ranging from IR theory and International Political Economy (IPE), to foreign policy analysis and Political Theory. Since we cannot meaningfully cover both ISS and all of these frontier zones, we are often going to discuss the particular ISS engagements that bring in the frontier, while noting that there is a larger literature that those who wish to pursue a given theme should consult more thoroughly.

Even taking a broad view of what counts as ISS has not enabled us to avoid all the difficult decisions about inclusion and exclusion. This book is much longer than we or Cambridge University Press originally thought it would be, and space constraints have been a real issue. In seeking to identify the core of the subject, and to reflect the uniqueness of its civilian strategy character, we have favoured conceptual issues over operational ones. This means that we have largely excluded the large literature on intelligence, which comes up mainly in the context of imperfect information and strategy. We cover some aspects of military operations, but have not included the enormous literatures to be found in the many journals that are closely linked to the armed services, and which reflect professional military discourses. Turning to the boundary between ISS and Peace Research, we have included the literature dealing with substantial issues

and conceptual debates on ‘peace ’that either mirrors debates in ISS or directly challenges ISS perspectives, but not covered more distinct Peace Research concerns such as peace education or the substantial literature on the practical side of conflict resolution, including conflict mediation, dispute settlement and suchlike. Some will no doubt think these exclusions a mistake, and they may be right. Our judgement has been that with a few exceptions, these literatures exist in their own worlds, and have played only a marginal part in what we see as the great conversation of ISS.

THEORETICAL APPROACHES OF SECURITY

Traditional Approaches

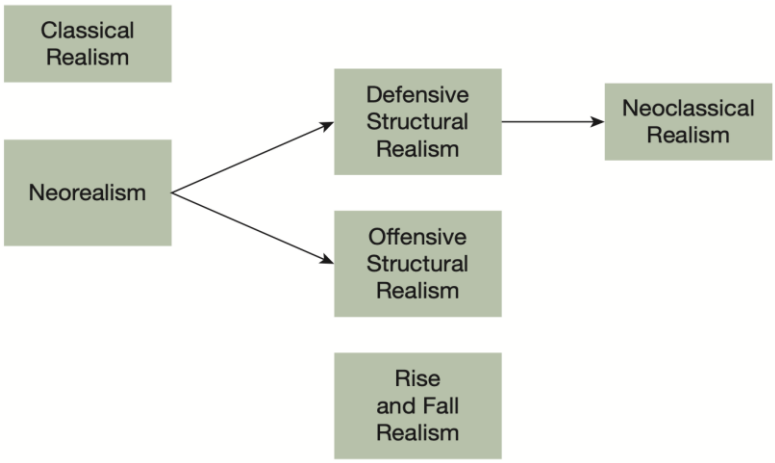


FIGURE 1.1 Six realist research programmes

1. Realisms:

Introduction:

The realist tradition has exercised an enormous influence over the field of security studies. Even its harshest critics would acknowledge that realist theories, with their focus on power, fear and anarchy, have provided centrally important explanations for armed conflict and war. This part discusses several different realist approaches to security studies. Although there are significant differences among variants of realism, they largely share the view that the character of relations among states has not altered. Where there is change, it tends to occur in repetitive patterns. State behaviour is driven by leaders ’flawed human nature or by an anarchic international system. Selfish human appetites for power, or the need to accumulate the wherewithal to be secure in a self-help world, explain the seemingly endless succession of wars and conquest. Accordingly, most realists take a pessimistic and prudential view of international relations.

In describing and appraising the realist tradition, it is customary to take a meta- theoretic approach that differentiates it from other approaches and that separates realist theories into distinct subgroups. Accordingly, accounts of twentieth-century realism typically distinguish political realist, liberal and other traditions, as well as describe different iterations of realist theory. As noted in Figure 1.1, this chapter distinguishes between six different variants of

realism – classical realism, neorealism and four flavours of contemporary realism: rise and fall, neoclassical, offensive structural and defensive structural realism. While this ordering is not intended to suggest a strict temporal or intellectual succession, classical realism is usually held to be the first of the twentieth-century realist research programmes.

Realists frequently argue that they draw on a long intellectual tradition and that realist themes can be found in important antiquarian works from Greece, Rome, India and China (e.g. Smith, M. 1986 and Garst 1989 for a contrasting view). They also suggest that humankind has, in most times and in most places, lived down to realism's very low expectations.

Classical realism

Classical realism is generally dated from 1939 and the publication of Edward Hallett Carr's The Twenty Year's Crisis. Classical realists are usually characterized as responding to then-dominant liberal approaches to international politics, although scholars disagree on how widespread liberalism was during the interwar years. Key works include those by Reinhold Niebuhr (1940), Martin Wight (1946), Hans Morgenthau (1948), George F. Kennan (1951) and Herbert Butterfield (1951, 1953). It was, however, Hans Morgenthau's Politics Among Nations: The Struggle for Power and Peace that became the undisputed standard bearer for political realism, going through six editions between 1948 and 1985.

According to classical realism, because the desire for more power is rooted in the flawed nature of humanity, states are continuously engaged in a struggle to increase their capabilities. The absence of the international equivalent of a state's government is a permissive condition that gives human appetites free rein. In short, classical realism explains armed conflict with reference to human failings. Wars are explained, for example, by particular aggressive statesmen, or by domestic political systems that give greedy parochial groups the opportunity to pursue self-serving expansionist foreign policies. For classical realists international politics can be characterized as evil: bad things happen because the people making foreign policy are sometimes bad (Spirtas 1996: 387–400).

Although not employing the formal mathematical modelling found in contem- porary rational choice theory, classical realism nevertheless posits that state behaviour can be understood as having rational microfoundations. As Morgenthau notes:

> *we put ourselves in the position of a statesman who must meet a certain problem of foreign policy under certain circumstances and we ask ourselves what the rational alternatives are from which a statesman may choose who must meet this problem under these circumstances (presuming always that he acts in a rational manner), and which of these rational alternatives this parti- cular statesman is likely to choose. It is the testing of this rational hypothesis against the actual facts and their consequences that gives theoretical meaning to the facts of international politics.*

State strategies are understood as having been decided rationally, after taking costs and benefits of different possible courses of action into account.

Neorealism

In 1979, Kenneth Waltz's Theory of International Politics replaced Morgenthau's 'Politics Among Nations' as the standard bearer for realists. Waltz argued that systems are composed of a

structure and their interacting units. Political structures are best conceptualized as having three elements: an ordering principle (anarchic or hierarchical), the character of the units (functionally alike or differentiated) and the distribution of capabilities. Two elements of the structure of the international system are said to be constant: the lack of an overarching authority means that its ordering principle is anarchy, and the principle of self-help means that all of the units (states) remain functionally alike. Accordingly, the only structural variable is the distribution of capabilities, with the main distinction falling between multipolar and bipolar systems.

Contrary to classical realism, neorealism excludes the internal make-up of different states when thinking about their foreign policy preferences. Unlike classical realists, Waltz's (1979: 91) theory is not based on leaders 'motivations and state characteristics as causal variables for international outcomes, except for the minimal assumption that states seek to survive.

In addition, whereas classical realism suggested that state strategies are selected rationally, Waltz is agnostic about which of several microfoundations explain state behaviour. State behaviour can be a product of competition among them, either because they calculate how to act to their best advantage or because those that do not exhibit such behaviour are selected out of the system. Alternatively, state behaviour can be a product of socialization: states can decide to follow norms because they calculate it is to their advantage, or because the norms become internalized.

Neorealism's minimal account of preferences and microfoundations means it makes only indeterminate behavioural predictions about foreign policy. Waltz nevertheless suggests that systemic processes will consistently produce convergent international outcomes. Waltz notes that in international politics the same depressingly familiar things happen over and over. This repetitiveness endures despite considerable differences in internal domestic political arrangements, both through time (contrast, for example, seventeenth- and nineteenth-century England) and space (contrast, for example, the United States and Germany in the 1930s). Waltz's purpose is to explain why similarly structured international systems all seem to be characterized by similar outcomes, even though their units (i.e. states) have different domestic political arrangements and particular parochial histories. Waltz concludes that it must be something peculiar to, and pervasive in, international politics that accounts for these commonalities. He therefore excludes as 'reductionist 'most assumptions about the units that make up the system – suggesting they must, at a minimum, seek their own survival.

By focusing only minor attention on unit-level variables, Waltz aims to separate out the persistent effects of the international system. A system can be said to exist:

> *'when (a) a set of units or elements is interconnected so that changes in some elements or their relations produce changes in other parts of the system; and (b) the entire system exhibits properties and behaviors that are different from those parts'*

Because systems are generative, the international political system is characterized by complex nonlinear relationships and unintended consequences. Outcomes are influenced by something more than simply the aggregation of individual states 'behaviour, with a tendency towards unintended and ironic outcomes. Neorealists therefore see international politics as tragic, rather than as being driven by the aggressive behaviour of revisionist states. The international political outcomes that Waltz predicts include that multipolar systems will be less stable than bipolar systems; that interdependence will be lower in bipolarity than multipolarity;

and that, regardless of unit behaviour, hegemony by any single state is unlikely or even impossible.

Waltz's Theory of International Politics proved to be a remarkably influential volume, spinning-off new debates and giving new impetus to existing disagreements. For example, the book began a debate over whether relative gains concerns impede cooperation among states, and added momentum to the extant question of whether bipolar or multipolar international systems are more war-prone.

Partly because of its popularity, and partly because of its rejection of competing theories, Waltz's Theory of International Politics became a prominent target. As time went by, detractors chipped away at the book's dominance (e.g. Keohane 1986). Neorealism's decline in the 1990s was amplified by international events that seemed to provide strong support for alternative approaches. The Soviet Union's voluntary retrenchment and subsequent demise; the continuation of Western European integration in the absence of American–Soviet competition; the wave of democratization and economic liberalization throughout the former Soviet Union, Eastern Europe and the developing world; and the improbability of war between the great powers all made realism seem outdated (Jervis 2002). Not surprisingly, after the 9/11 attacks on the United States, political realism enjoyed a resurgence. It is, however, ironic that this was at least partly owed to transnational terrorist networks motivated by religious extremism, actors and appetites that both lie well outside neorealism's traditional domain.

Excluding neorealism, there are at least four contemporary strands of political realism: rise and fall realism, neoclassical realism, defensive structural realism and offensive structural realism. All four take the view that international relations are characterized by an endless and inescapable succession of wars and conquest. The four variants can be differentiated by the fundamental constitutive and heuristic assumptions that they share. Briefly, these four realisms differ on the sources of state preferences – the mix of human desire for power and/or the need to accumulate the power necessary to be secure in a self-help world – while agreeing that rational calculation is the microfoundation that translates those preferences into behaviour.

Defensive structural realism

Defensive structural realism developed out of neorealism but is distinct from it. Defensive structural realism shares neorealism's minimal assumptions about state motivations, suggesting that states seek security in an anarchic international system – the main threat to their well-being comes from other states (Glaser 2003; Walt 2002).

There are three main differences between neorealism and defensive structural realism. First, whereas neorealism allows for multiple microfoundations to explain state behaviour, defensive structural realism relies solely on rational choice. Second, defensive structural realism adds the offence–defence balance as a variable. This is a composite variable combining a variety of different factors that make conquest harder or easier. Defensive structural realists argue that prevailing technologies or geographical circumstances often favour defence, seized resources do not cumulate easily with those already possessed by the metro- pole, dominoes do not fall, and power is difficult to project at a distance. Accordingly, in a world in which conquest is hard it may not take too much balancing to offset revisionist behaviour. Third, combining rationality and an offence–defence balance that favours defence, defensive structural realists predict that states should support the status quo. Expansion is rarely structurally mandated, and balancing is

the appropriate response to threatening concentrations of power. Rationalism and an offence–defence balance that favours defence means that states balance, and balances result.

Perhaps the best-known variant of defensive structural realism is Stephen Walt's 'balance of threat 'theory. According to Walt, 'in anarchy, states form alliances to protect themselves. Their conduct is determined by the threats they perceive and the power of others is merely one element in their calculations '. Walt suggests that states estimate threats posed by other states by their relative power, proximity and intentions and the offence–defence balance. The resulting dyadic balancing explains the absence of hegemony in the system:

> *Together, these four factors explain why potential hegemons like Napoleonic France, Wilhelmine Germany, and Nazi Germany eventually faced over- whelming coalitions: each of these states was a great power lying in close proximity to others, and each combined large offensive capabilities with extremely aggressive aims.*

Because balancing is pervasive, Walt concludes that revisionist and aggressive behaviour is self-defeating, and 'status quo states can take a relatively sanguine view of threats. . . . In a balancing world, policies that convey restraint and benevolence are best '.

One difficult problem for defensive structural realism is that the research programme is better suited to investigating structurally constrained responses to revisionism, rather than where that expansionist behaviour comes from. To explain how armed conflict arises in the first place, defensive structural realists must either appeal to domestic-level factors (which are outside of their theory) or argue that extreme security dilemma dynamics make states behave as if they were revisionists. Steps taken by states seeking to preserve the status quo are ambiguous and are often indistinguishable from preparations to launch offensive strikes. 'Threatened 'states respond, leading to a spiralling of mutual aggression that all would have preferred to avoid. This is international relations as tragedy, not evil: bad things happen because states are placed in difficult situations.

Defensive structural realism has some difficulty in relying on security dilemma dynamics to explain war, however. First, it is not easy to see how, in the absence of pervasive domestic-level pathologies, revisionist behaviour can be innocently initiated in a world characterized by status quo states, defence-dominance and balancing. Because increments in capabilities can be easily countered, defensive structural realism suggests that a state's attempt to make itself more secure by increasing its power is ultimately futile.

Second, defensive structural realists contend that states routinely signal their benign intentions to their peers, thus mitigating the uncertainty that drives the security dilemma. States can reveal their peaceful intentions to others by reducing their arsenals, by limiting the size of their armed forces or by investing in arms that are good for defence and deterrence but provide little offensive utility. Through these so-called 'costly signals', states can avoid the action–reaction spirals of the security dilemma that produce arms races and war.

Hence, defensive structural realists suggest that the world is made up of states that seek an 'appropriate 'amount of power and signal to their peers that they intend no harm. If states do seek hegemony, it must be due to domestically generated preferences; seeking superior power is not a rational response to external systemic pressures.

Offensive structural realism

Offensive structural realists, in contrast, argue that states face an uncertain international environment in which any state might use its power to harm another. Under such circumstances, relative capabilities are of overriding importance, and security requires acquiring as much power compared to other states as possible. The stopping power of water means that the most a state can hope for is to be a regional hegemon, and for there to be no other regional hegemons elsewhere in the world.

John Mearsheimer's theory of offensive structural realism makes five assumptions: the international system is anarchic; great powers inherently possess some offensive military capability, and accordingly can damage each other; states can never be certain about other states ' intentions; survival is the primary goal of great powers; and great powers are rational actors. From these assumptions, Mearsheimer deduces that great powers fear each other, that they can rely only on themselves for their security and that the best strategy for states to ensure their survival is maximization of relative power.

Mearsheimer argues that security requires the acquisition of as much power relative to other states as possible and that increasing capabilities can improve a state's security without triggering a countervailing response. Careful timing by revisionists, buckpassing by potential targets, and information asymmetries all allow the would-be hegemon to succeed. Power maximization is not necessarily self-defeating, and hence states can rationally aim for regional hegemony.

Although states will take any increment of power that they can get away with, Mearsheimer does not predict that states are 'mindless aggressors so bent on gaining power that they charge headlong into losing wars or pursue Pyrrhic victories'. States are sophisticated relative power maximizers that try 'to figure out when to raise and when to fold' . By expanding against weakness or indecision and pulling back when faced by strength and determination, a sophisticated power maximizer reaches regional hegemony by using a combination of brains and brawn.

Mearsheimer argues that ultimate safety comes only from being the most powerful state in the system. However, the 'stopping power of water 'makes such global hegemony all but impossible, except through attaining an implausible nuclear superiority. The second best, and much more likely, objective is to achieve regional hegemony, the dominance of the area in which the great power is located. Finally, even in the absence of either type of hegemony, states try to maximize both their wealth and their military capabilities for fighting land battles. In order to gain resources, states resort to war, blackmail, baiting states into making war on each other while standing aside, and engaging competitors in long and costly conflicts. When acting to forestall other states 'expansion, a great power can either try to inveigle a third party into coping with the threat (i.e. buck-pass) or balance against the threat themselves. While buckpassing is often preferred as the lower cost strategy, balancing becomes more likely (all things being equal) the more proximate the menacing state and the greater its relative capabilities.

In addition to moving Mearsheimer's focus to the regional level, the introduction of the stopping power of water also leads to different predictions of state behaviour depending on where it is located. While the theory applies to great powers in general, Mearsheimer distinguishes between different kinds: continental and island great powers, and regional

hegemons. A continental great power will seek regional hegemony but, when it is unable to achieve this dominance, such a state will still maximize its relative power to the extent possible. An insular state, 'the only great power on a large body of land that is surrounded on all sides by water ', will balance against the rising states rather than try to be a regional hegemon itself. Accordingly, states such as the United Kingdom act as offshore balancers, intervening only when a continental power is near to achieving primacy. The third kind of great power in Mearsheimer's theory is a regional hegemon such as the United States. A regional hegemon is a status quo state that will seek to defend the current favourable distribution of capabilities.

Mearsheimer's theory provides a structural explanation of great-power war, suggesting that 'the main causes . . . are located in the architecture of the international system. What matters most is the number of great powers and how much power each controls '. Great-power wars are least likely in bipolarity, where the system only contains two great powers, because there are fewer potential conflict dyads; imbalances of power are much less likely; and miscalculations leading to failures of deterrence are less common. While multipolarity is, in general, more war-prone than bipolarity, some multipolar power configurations are more dangerous than others. Great-power wars are most likely when multipolar systems are unbalanced, that is, when there is a marked difference in capabilities between the first and second states in the system, such that the most powerful possesses the means to bid for hegemony. Mearsheimer hypothesizes that the three possible system architectures range from unbalanced multipolarity's war-proneness to bipolarity's peacefulness, with balanced multipolarity falling somewhere in between.

Rise and fall realism

Rise and fall realism emerged as a powerful alternative to the balance of power theories that dominated International Relations scholarship during the 1950s. A.F.K. Organski's classic 1958 volume, World Politics, challenged the popular belief that power parity is a virtue in international relations by insisting that throughout history 'world peace has coincided with periods of unchallenged supremacy of power, whereas the periods of approximate balance have been the periods of war '. Organski's claim that hegemony is the foundation for peace, while balance is often associated with war, has since become a central theme of rise and fall realism.

In particular, this research programme emphasizes that war between major powers is least likely when the international system is dominated by a single state and when there is an absence of rising challengers vying for system leadership. Given its privileged position, the dominant state is capable of shaping the rules and practices of the international system in such a way as to satisfy its selfish interests. Stability is a product of this hegemonic order, as states that are dissatisfied with the status quo lack the capabilities to change it. However, as power becomes more evenly matched, war over system leadership is likely to occur. When two or more states approach power parity, the declining hegemon may rationally calculate the need for preventive war in order to preserve its status as the world's top power. In the absence of a preventive attack, a dissatisfied rising challenger could initiate a war in an attempt to capture the top spot and all of the benefits that go along with it.

Rise and fall realism depicts the course of human history, or some significant portion of it, as the successive rise and fall of great powers. In order to explain this historical trend, it pays particular attention to the mechanisms that cause states to grow at different rates and at different times. In contrast to neorealism, rise and fall realists contend that differential growth rates are mainly caused by processes internal to states, including the timing of industrialization, social

formation and type of economic system, bureaucratic politics and productivity, and military, economic and technological innovation. Since these dynamics are not at work in all states at the same time or to the same extent, rather than grow simultaneously, states tend to rise and fall in relation to one another. Thus, internal developments and the timing of their onset produce the periods of transition from one system leader to the next, which are often marked by war.

The rise and fall research programme has spawned a number of theories to explain differential growth patterns and the onset of major power war, including debates over (1) whether it is the rising challenger or the declining hegemon that initiates war; (2) what specific internal processes drive differential growth; and (3) whether the theory is applicable across time and space, or limited to a period of history or a particular region of the world.

While continuing to emphasize the onset of major power war, rise and fall realists have extended their scope to other important aspects of international relations. For example, Douglas Lemke has applied power transition theory to dyads other than those involving states directly contesting for system leadership and Dale Copeland (2014) has shown how relative power shifts deter states from participating in trade agreements. Moreover, adding alliances to the calculation of differential growth and security concerns and polarity to theories of great power competition, rise and fall realists have enriched explanations of power trends and war.

Neoclassical realism

Neoclassical realism suggests that what states do depends in large part on influences located at the domestic level of analysis. Neoclassical realism employs a 'transmission belt ' approach to foreign policy, which illustrates how systemic pressures are filtered through variables at the unit level to produce specific foreign policy decisions.

While neoclassical realists agree that the distribution of capabilities is a good starting point for the analysis of state behaviour, they contend that the international system rarely provides states with clear information on which to base foreign policy decisions. Systemic threats and opportunities are not easily identifiable and there are numerous policy options available to decision makers for meeting strategic goals. Given these challenges, variables at the unit level often intervene between systemic pressures and state behaviour to determine the precise nature and direction of a state's foreign economic and military policy.

Neoclassical realists have incorporated a large number of unit-level variables into their theories of foreign policy decision-making. Critics contend that these variables are often chosen in an ad hoc manner to explain particular historical cases, which limits the theoretical coherence and explanatory power of the research programme. In response, neoclassical realists contend that how a state reacts to systemic imperatives is largely shaped by the perceptions of its leaders, the culture of its military, bureaucracy and society, the nature of its domestic political institutions and the ability of its state apparatus to extract and mobilize domestic resources to achieve foreign policy goals.

Randall Schweller's (2006) theory of 'under-balancing 'provides a good example of how neoclassical realists incorporate unit-level variables into theories of foreign policy. Schweller starts from the structural realist position that state behaviour is primarily driven by the relative distribution of material power in the international system. He notes, however, that exactly how states choose to react to threatening accumulations of power depends on the degree to which

they embody structural realism's unitary actor assumption. When systemic pressures are transmitted through states that are unified at the elite and societal levels, decision makers find it easy to recognize threats and carry out appropriate balancing strategies to counter them. When states are fragmented, however, leaders often find it difficult to come to an agreement on the nature of a threat and how best to deal with it. Furthermore, divided states often lack the extractive capacity to mobilize the resources from society that are necessary for restoring a balance of power. According to Schweller, both France and Britain were fragmented states prior to the Second World War, and this explains why they both under-reacted to the threat posed by a rising Germany.

2. Liberalisms:

Introduction:

The liberal tradition in thinking about security dates as far back as the philosopher Immanuel Kant, who emphasized the importance of 'republican 'constitutions in producing peace. His pamphlet Perpetual Peace contains a peace plan and may fairly be called the first liberal tract on the subject. But liberal security has been elaborated by different schools within a developing tradition of liberal thought. Andrew Moravcsik (2001) has distinguished between ideational, commercial and republican liberalism following Michael Doyle (1998), who distinguished international, commercial and ideological liberalism, each with rather different implications for security planning; and Zacher and Matthews (1995) have identified four different tendencies in liberal security thought. Each reflects upon a family of loosely knit concepts, containing in some cases rather opposed approaches. Kant believed that trade was likely to engender conflict, while later, 'commercial 'liberals saw in trade a beneficial and beneficent development. Republican liberals argue that peace is rooted in the liberalism of the liberal state – the internal approach – while neo-liberal institutionalists emphasize the role of international institutions, which could ameliorate conflict from without.

This parts provides an overview of the major positions on security within liberal thought. The first section outlines traditional/Kantian liberalism. The second section introduces liberal economic thought regarding peace and war and the ideas of 'douce commerce'. The third section describes the democratic peace thesis and reviews the major discussions on the idea that liberal states do not fight wars with other liberal states.

Traditional or Kantian liberalism

Immanuel Kant was an Enlightenment philosopher (some would say the greatest Enlightenment philosopher), often noted for his approach to ethics. (Kant argued that moral choices were guided by an inner sense of duty – when individuals behaved according to duty, they were being moral.) But he was not only an ethicist; he philosophized the 'good state 'as well as its international relations. According to Kant, the only justifiable form of government was republican government, a condition of constitutional rule where even monarchs ruled according to the law. Moreover, the test of good laws was their 'universalizability – 'the test of universal applicability. The only laws that deserved the name of 'law 'were those one could wish everyone (including oneself) obeyed. Such laws became 'categorical imperatives'; they were directly binding, and monarchs as well as ordinary citizens were subject to them.

Kant argued that republican states were ‘peace producers’; that is, they were more inclined to peaceful behaviour than other sorts of states. He attributed this to habits of consultation; a citizenry that had to be consulted before going to war would be unlikely to endorse war easily. He also attributed it to the legal foundations of the republican state because he believed a state built on law was less likely to endorse lawless behaviour in international relations.

But being republican was not sufficient to ensure world peace. According to Kant – and it was the critical argument of Perpetual Peace – the situation of international relations, its lawless condition, unstable power balances and especially the ever- present possibility of war endangered the republican state and made it difficult for liberal political orders to maintain their republican or liberal condition. Hence, he argued, it was the duty of the republican state to strive towards law regulated inter- national relations; they could not merely be liberal in themselves.

A critical part of Kant’s argument, which initiated the debate between liberals and ‘realists’, was his critique of the concept of the ‘balance of power’: he refuted the argument, becoming prevalent in his day, that the balance of power was a peace- keeper. The idea of conscious balancing was fallacious, he argued, since ‘It is the desire of every state, or of its ruler, to arrive at a condition of perpetual peace by conquering the whole world, if that were possible ’, a view shared by some leading realists (e.g. Mearsheimer 2001). As to the automatic operations of such a balance, he held Rousseau’s view that such tendencies did indeed exist. Rousseau argued that states were naturally pushed into watching one another and adjusting their power accordingly, usually through alliances. How- ever, this practice resulted merely in ‘ceaseless agitation ’and not in peace.

Kant’s peace programme consisted of two parts. There were the ‘preliminary articles – ’the initial conditions that had to be established before even republican states could make much contribution to a more peaceful international environment. These included the abolition of standing armies, non-interference in the affairs of other states, the outlawing of espionage, incitement to treason and assassination as instruments of diplomacy, and an end to imperial ventures. These had to be abolished by a majority of states, non-liberal as well as liberal, to end the condition Hobbes had described as ‘the war of all against all’. There were then the three definitive articles, which provided the actual foundations for peace:

1. The civil constitution of every state should be republican.

2. The law of nations shall be founded on a federation of free states.

3. The law of world citizenship shall be limited to conditions of universal hospitality.

Spreading republican constitutions meant, in effect, generalizing the striving for peace, since, according to Kant, striving for peace was part of the natural orientation of the republican state. The ‘federation of free states ’would provide, in effect, a type of collective security system; and the provision of ‘universal hospitality ’would, in Michael Howard’s formulation, ‘gradually create a sense of cosmopolitan community’. Kant distinguished between the end of war and the establishment of positive peace, and his plan made peace ‘more than a merely pious aspiration’. Accordingly, he can properly be regarded as the ‘inventor of peace ’.

During the nineteenth century, liberals tended to emphasize only Kant’s views that liberalism inclined to peace. Through most of the nineteenth century, the liberal approach to

peace consisted of critiques of the ancient regime, and promised that peace would automatically follow the overthrow of autocracy and the establishment of constitutional regimes. According to Raymond Aron (1978), nineteenth-century liberals had no peace plan. With the outbreak of the First World War, however, the emphasis changed. Then, the dangers that Kant had foreseen for liberalism in a dangerous international environment were rediscovered and liberal thinkers turned from internal reform towards emphasizing arbitration, the development of inter- national law and an international court, to protect liberalism from without. When the League of Nations failed, moreover, some would go so far as to recommend either the abolition of, or severe restrictions upon, state sovereignty.

Douce commerce

According to Moravcsik, 'commercial liberalism 'focuses on 'incentives created by opportunities for trans-border economic transactions '. This contemporary formulation attempts to make specific the causal mechanisms behind the inclination of economically liberal states to prefer peace to conflict. According to Moravcsik, 'trade is generally a less costly means of accumulating wealth than war, sanctions or other coercive means '. But it is not the only theory – other commercial liberals stress the structure of a liberal economy, not merely the preferences of individual economic actors.

The origins of modern commercial liberalism lie in the liberal critique of mercantilism, the aggressive economic policies recommended to, and to a degree practised by, the autocrats of the ancient regime. Mercantilist doctrine advised doing all to increase the amount of bullion held by a country, in an environment where bullion was believed to be a fixed quantum. The economic philosophes (called physiocrats) such as François Quesnay and Victor de Mirabeau identified a structural proclivity in mercantilism towards trade wars and territorial conquests. If your own nation was to be wealthy, it could only be so by making others poorer. Tariff walls were needed to protect the prosperity of domestic producers from the 'attacks 'of foreign competitors. Subsidies were required for export producers so that they could 'seize 'the wealth of others in foreign markets. Resources in foreign lands had to be militarily 'captured 'to keep them out of the hands of commercial rivals. The effect of generalizing mercantilism was made explicit by Voltaire in 1764: 'It is clear that a country cannot gain unless another loses and it cannot prevail without making others miserable. '

The physiocrats argued that giving up mercantilism and allowing freedom to trade would civilize the citizens of a nation, facilitating a peaceful coexistence among fellow citizens and guaranteeing the rule of law. Commerce and international trade would exercise a restraining force on tyrannical and arbitrary leadership. Finally, inter- national trade would incline nations to peace. Montesquieu first presented all three arguments in De L'Esprit des Lois.

The explicit association between non-mercantilist, open trading orders and peace was, however, not French but a British development. It first appeared in Adam Smith's Wealth of Nations in 1776, where he argued that 'the hidden hand', besides increasing wealth, also promoted a lessening of economic hostilities. But even earlier, Smith's Scottish colleague and friend David Hume in his 1736 Treatise of Human Nature had proposed that a division of labour and trade benefited all participants, and David Ricardo (1817) formulated the theory of comparative advantage. According to Ricardo, wealth accrued in the degree to which states concentrated production in areas where they had 'comparative advantage 'and traded for other

products. Ricardo's theory underpinned the notion of a benevolent division of labour as well as the idea that trade was non-hostile competition.

The nineteenth-century 'commercial liberals 'developed these ideas into doctrine. Liberal trade doctrine, or the theory of douce commerce, held that trade among states, like trade among individuals, was mutually beneficial. All men would gain through participation in a global division of labour – a way of life in which they offered to each other the various products in the production of which they specialized. Market competition was not conflict, they argued, but rather peaceful cooperation: each producer helped to improve the quality of life for all through the production and sale of superior and less expensive products than the ones offered by his market rivals. The market was civil society and peace; economic policy in the hands of governments was conflict and war.

Commercial liberalism also took on a sociological aspect. James Mill described the British Empire as 'a vast system of outdoor relief for the upper classes'. Joseph Schumpeter in the twentieth century agreed that conquest and imperialism had economically favoured the old aristocratic elites, and argued that the social changes accompanying capitalism made modern states inherently peaceful, since they led to the decline of the aristocratic class.

The only formal non-liberal nineteenth-century riposte to the commercial liberals (that is, the only argument one could credit with some respect) was the mid-nineteenth-century idea of protecting infant industries. The German nationalist Jahn argued that because of the time lag between developed and developing countries, there was an argument for initial protection for 'infant 'industry, but even then only until it could compete in an open market. In the twentieth century, under the pressure of the Great Depression, liberals would also argue that there was some justification for protecting economies from storms in the world economy, but again temporary measures only. (The liberal tendency came to be to improve international regimes so that storms could be avoided or ridden out without closures.) There also developed a more refined critique of the argument that everyone benefited through trade. This made it clear that the wealth accruing through opening economic exchange did not automatically benefit everyone in society; this depended on social policies that, among other things, deliberately fostered the skills that would allow individuals to participate in market economies.

During the twentieth century, the initial successes of Nazism, government-directed labour programmes and the much-vaunted 'Soviet model 'led the commercial liberals to focus on government involvement in the economy and on protectionist ideologies. Indeed, twentieth-century commercial liberals spoke less of economy than of ideology, attacking ideas of economic closure and planning that derived from 'scientific socialism 'and economic nationalism. The most famous of these is Friedrich Hayek's Road to Serfdom, but it had many echoes, especially in Central Europe. During the 1930s, the German economist Wilhelm Röpke declared that the 'genuinely liberal principle 'required 'the widest possible separation of the two spheres of government and economy'. He recommended the largest possible 'depoliticization 'of the economic sphere. In 1936, the Swiss economist and political scientist William Rappard (the Rappard Chateau that houses the World Trade Organization in Geneva is named after him) in a lecture entitled 'The Common Menace of Economic and Military Armaments 'identified 'economic armaments 'with all of the legislative and administrative devices governments use to politically influence imports and exports as well as the allocation of commodities. Rappard

argued that a new world order of peace and prosperity would only come about when governments exited from control of the economy.

The notion that economic openness produces a more peaceful international posture has become the subject of close empirical examination. In 1997, Oneal and Russett (1997) declared that the 'the classical liberals were right 'in their study of the record in the post-war period. Similarly, Mansfield and Pollins (2001) summarized a large body of empirical work that, for the most part, supports the thesis. There are various exceptions and qualifications that are seen to limit the circumstances under which economic interdependence results in conflict reduction. Stephen van Evera (1994) has argued that the more diversified and complex the existing transnational commercial ties and productions structures the less cost-effective coercion is likely to be. By extension, the less diverse the production structure of a country and the more it is characterized by monopolies, the more fragile will be the inclination to peace.

Moving beyond economic interdependence to the issue of economic freedom within states, Erik Gartzke (2005) has found empirical evidence that economic freedom (as measured by the Fraser Institute Economic Freedom Index) is about 50 times more effective than democracy in reducing violent conflict. Gartzke's conclusions are critical for the direction of liberal reforms, since they imply that it is less important what sort of political regime a country has than its degree of economic freedom.

The policy prescriptions enjoined by the commercial liberals – often called 'economic disarmament – 'focus on limiting the power of governments to impose trade restraints, primarily through international regulation. Foreign exchanges were to be open; tariffs were to be reduced to the minimum and quotas and other quantitative restrictions positively forbidden. Governments were to pledge themselves to open tariff borders, to abolish quotas and to allow currencies to move in line with market forces. These policy prescriptions were immensely influential in the architecture of the newly established international economic organizations, set up at the end of the Second World War.

Recently, the literature on globalization has suggested that globalization, in its aspect as unfettered free trade on a global scale, is a peace producer. Graham Allison has opined that 'global networks, particularly in economics, create demands by powerful players for predictability in interactions and thus for rules of the game that become, in effect, elements of international law'.

The democratic peace thesis

The 'democratic peace 'thesis is the argument that liberal states do not fight wars against other liberal states. It was first enunciated in a keynote article by Michael Doyle in the journal Philosophy and Public Affairs. Doyle argued that there was a difference in liberal practice towards other liberal societies and liberal practice towards non-liberal societies. Among liberal societies, liberalism had produced a cooperative foundation such that 'constitutionally liberal states have yet to engage in war with one another.' Doyle based his findings on David Singer's Correlates of War Project (COW) at Michigan University and the COW's list of wars since 1816. Using the list, Doyle observed that almost no liberal states had fought wars against other liberal states, and that in the two instances in which it seemed that liberal states had fought against other arguably liberal states, liberalism had only recently been established. Doyle

sourced the tendency in Kant's 'three preconditions'; namely republican constitutions, collective security arrangements and civic hospitality, in which Doyle included free trade.

The specific causes of the 'liberal peace 'have become the subject of robust research and discussion. The two major contending theories focus on liberal institutions and liberal ideology, respectively. Liberal institutions include the broad franchise of liberal states and the need to ensure broad popular support; the division of powers in democratic states, which produces checks and balances; and the electoral cycle, which makes liberal leadership cautious and prone to avoid risk. But liberal institutions would tend to inhibit all wars, whereas liberal states have fought robust wars against non-liberal states. The other contender, which can explain the difference, is liberal ideology or 'culture'. According to the liberal culture argument, liberal states tend to trust other liberal states and to expect to resolve conflict through discussion and compromise. But, equally, they distrust non-liberal states. The major argument for liberal culture has been put forward by John M. Owen, who suggests that, 'Ideologically, liberals trust those states they consider fellow liberal democracies and see no reason to fight them. They view those states they consider illiberal with suspicion, and sometimes believe that the national interest requires war with them '.

Since Doyle first produced his findings, the theory has developed two variants: one maintains that democracies are more peaceful than non-democracies, that is, that they are more pacific generally. This is sometimes referred to as the monadic variant. The other maintains that liberal states are not necessarily more peaceful than non-liberal states but that they eschew the use of force in relation to other democracies; that is, the use of force depends on the recipient's form of government. In the later variant, sometimes called the dyadic variant, a few have argued that democracies may be even more robust in the use of force than non-democracies, owing partially to the ideological nature of democratic wars and partially to the fact that liberal democracies are generally strong states with a large wealth base.

From the security point of view, the recommendations of democratic peace theory are clear – in the final analysis, security depends on encouraging liberal institutions and a security policy must have as its long-term goal the spread of liberalism. In the short term, it must protect liberalism, including liberal tendencies in non-liberal states. Doyle himself argues that where liberalism has been deficient 'is in preserving its [liberalism's] basic preconditions under changing international circumstances '. The route to peace is to encourage democratic systems, the universal respect for human rights and the development of civil society.

But such a conclusion depends on an untroubled and robust correlation between the democratic nature of a state and a peaceful inclination, at least towards other liberal states, and it is not entirely clear that such a direct correlation exists. Chris Brown (1992) has pointed out that liberal states have, during the period that many states became liberal, faced determined enmity from non-liberal states. The fact that liberal states have faced enemies of liberalism distorts the historical record; we do not know how they may have diverged in the absence of such an enmity. It may also be that in a world of diverse states in situations of conflict; that is, in an anarchical society, liberal states make more reliable allies – they do not fight one another because they ally with one another. (This is called the liberal alliance thesis and is compatible with realist approaches.) There is also the not insignificant fact that the majority of liberal states are locked into economic integration, via the European Union (a fact that may support the douce commerce variant). Finally, the democratic transition phenomenon may be a statistical aberration. David

Spiro (1996), for instance, has argued that historically there have not been many liberal states, and that most states do not fight wars against one another anyway. The fact that liberal states have not fought wars against one another may not be statistically significant.

As to whether liberal states are more intrinsically peaceful than other states, this is perhaps even more contentious. Kant, for his part, seemed to support the monadic theory; he claimed not only that republics would be at peace with each other but that republican government is more pacific than other forms of government. But the empirical work is indeterminate since it has so far concentrated on traditional state-to-state wars and has ignored interventions – intervention could also be considered an intrinsically hostile act involving the use of force outside of one's borders. Recent 'liberal 'attempts to bring non-liberal states to liberal democracy (in Iraq, for example) have raised fears that, far from being a recipe for peace, liberal foreign policy may have its own tendencies towards war. This 'dark side of liberalism 'has occupied much of the resent research, which has turned to the conditions which may lead liberal states to fight wars.

Despite some hesitations from the academy, the theory that democracies do not fight wars against other democracies has been immensely influential in public policy. For example, it underpinned President Clinton's A National Security Strategy for a New Century (US 1998); it was also extensively used to support the neo-conservative case for war in Iraq and has guided post-war reconstruction in insisting on a broadly inclusive post-war government in Iraq and an early move to self-government with elections. The democratic transition thesis has also come to dominate the peace- building programme of the UN. Michael Barnett (2006) has been critical of what he calls the 'civil society 'model for post-war reconstruction, since it places emphasis on mobilizing social forces in often unstable and divided societies, when more attention should be placed on building state capacity and strengthening governmental powers.

The association between war, democracy and rights, prevalent in the immediate aftermath of the Second World War, has also been revived. Founded upon the principles of territorial integrity and state sovereignty, the UN has recently begun to shift towards an emphasis on the rights of human beings as being at least as important as the rights of states in the international realm. In a discussion on the relevance of the Security Council, UN Secretary-General Kofi Annan clearly indicated that 'the last right of states cannot and must not be the right to enslave, persecute or torture their own citizens'. In fact, rather than rally around sovereignty as its sole governing idea, the Security Council should 'unite behind the principle that massive and systematic violations of human rights conducted against an entire people cannot be allowed to stand'.

3. Constructivisms:

Constructivism has become an increasingly prominent theoretical approach to international relations since its emergence in the 1980s. Drawing on insights from the cognate discipline of sociology in particular, constructivists argue that the world is constituted socially through intersubjective interaction, that agents and structures are mutually constituted and that ideational factors such as norms and identity are central to the constitution and dynamics of world politics. It is less a theory of international relations or security, however, than a broader social theory that then informs how we might approach the study of security.

Constructivism: central tenets

Constructivism, a term first elaborated by Nicholas Onuf in his groundbreaking book World of Our Making in 1989, is a broad theoretical approach to the study of international relations that has been applied to a range of issues, from political economy to international organization and security. Despite attention to security issues, however, the extent to which constructivists have developed a theory of international security is limited. This distinguishes constructivists from critical theorists (with their conception of security defined as a commitment to emancipation) and realists (whose theory of world politics as a whole orients around a concern with achieving security in an inherently dangerous world). A prominent realist criticism is that constructivism has generally eschewed a focus on the power politics of security and focused instead on the development of benign norms for managing interstate competition and institutionalizing broader forms of political community.

Such a portrayal is little more than a caricature of constructivism. Constructivists argue that their approach enables a more sophisticated and complete understanding of dynamics traditionally associated with realist approaches to security, including the nature of power (Barnett and Duvall 2005), the security dilemma and the balance of power. Crucially, as Friedrich Kratochwil (1993) and Alexander Wendt (1992) have argued, constructivist approaches are therefore better able to understand periods of structural change enabled by strategic actors in world politics, most prominently the end of the Cold War. This places such approaches in a particularly strong position relative to structuralist theories such as neorealism that assume state interests are determined by the nature of the international system itself.

Security as social construction

If there is a shared conception of security within constructivist thought, it is that security is a social construction. For constructivists, this applies to the meaning of the concept itself, to definitions of the community and its values in need of protection, to perceptions of threats and to the types of actions that are viewed as legitimate in pursuing security.

As Karin Fierke has argued, 'to construct something is an act which brings into being a subject or object that otherwise would not exist'. This does not necessarily mean that there is no such thing as 'security 'or that security is devoid of meaning. Drawing on Arnold Wolfers's (1952) classic definition, security could be understood as the preservation of a group's core values, for example. But such a broad definition of security tells us little about who the group itself is, what its core values are, where threats to those values may come from and how the preservation or advancement of these values might be achieved. For constructivists, answers to these questions vary across different historical and political contexts and develop through social interaction between actors. And it is the answers to these questions – articulated and negotiated in a particular social and historical context through social interaction – that ultimately define security, bringing it into being for particular actors in world politics. Constructivists therefore tend to avoid advancing universal and abstract definitions of security, focusing instead on how security is given meaning in practice.

For constructivists, social construction extends also to the dynamics that influence the meaning and practice of security. Constructivists therefore emphasize the importance of ideational factors that help determine these conceptions, practices and dynamics of security, factors generally neglected in realist accounts of inter- national politics. As Barry Buzan and

Lene Hansen note, this has largely focused on norms at the international level and the role of identity at the domestic level.

4. Critical theory:

Although the origins of critical security studies as a distinct school of thought go back to the early 1990s, the ideas and struggles it feeds upon have been around for much longer. Citizens, social groups and movements, intellectuals and activists have long called for thinking beyond the Cold War categories that restricted ways of 'thinking 'about and practising security. Examples include the Non-Aligned Movement, whose underlying principle reminded the world that there existed insecurities other than the United States–Soviet Union standoff; the calls for a new international economic order in the 1970s, which underscored that the North–South tension was of no less significance for world politics than East–West rivalry; contributors to the World Order Models Project who during the 1960s and 1970s outlined visions of alternative and sustainable world orders; the 'Alternative Defence 'school that helped transform security relations across 'Europe 'during the 1980s through informing various social movements including the US-based 'Freeze', the UK- based CND (Campaign for Nuclear Disarmament) and END (European Nuclear Disarmament); the disciples of Mahatma Gandhi who sought non-violent ways of practising security and contributed to academic peace research; women's movements that have pointed to the 'arms vs. butter 'dilemma as a cause of disproportionate suffering for women; feminist scholars who have underlined the relationship between the personal, the political and the international; and students of North/South and 'Third World ' security who turned on its head the prevalent assumption that the inside/domestic realm was one of security whereas the outside/foreign realm was one of insecurity by pointing to the ways in which 'national security projects 'imported from (and supported by) the 'West 'have had a mixed record in the rest of the world.

In the years of euphoria that followed the end of the Cold War, the contributions of these groups were often forgotten not only by those who claimed victory on the part of the Ronald Reagan administration in the United States (to the neglect of a variety of other factors and actors that helped to bring the Cold War to an end) but also by the more theoretically oriented students of critical security studies who approached the task of rethinking security on mostly metatheoretical grounds, thereby failing to challenge existing ways of 'thinking 'about and 'doing 'security. The 11 September 2001 attacks and other al-Qa'ida-linked bombings that shook various parts of the world were tantamount to a wake-up call in more ways than one. For students of security studies who were sceptical of the contributions of critical perspectives, 9/11 served as a reminder that prevalent approaches to security are far from being able to account for let alone address the world's current insecurities. For students of critical security studies, 9/11 underscored the need to engage directly with issues related to war and peace, hard and soft power and state and non-state actors in world politics. It is in this context that the call for rethinking security (in theory and in practice) has gained new urgency.

Critical theory:

It was Robert W. Cox who familiarized students of international relations with the ideas of the Italian political theorist and activist Antonio Gramsci (1891–1937), most notably through his distinction between 'critical theory' and 'problem-solving theory'. The distinction between the two rests on the purpose for which theory is built. Whereas critical theory 'stands apart from the prevailing order and asks how that order came about', problem-solving theory is content with

fixing glitches in the prevailing system so as to make 'existing relationships and institutions work smoothly'. The labels used for the two strands of theorizing often confuse readers into thinking that 'critical theory' is not interested in solving problems but merely presents a critique and/or a utopia. This is a misnomer. 'Critical theory' does engage with present problems but without losing sight of the historical processes that have produced them, and proposes alternatives that are 'feasible transformations of the existing world'.

Another source of inspiration for critical scholars is the Frankfurt School theorist Max Horkheimer (1895–1973), who drew an important distinction between 'critical theory' and 'traditional theory'. According to Horkheimer, traditional theory is defined by its reification of ideas into institutions, which are then represented as immutable 'facts of life' that have to be lived with – all the while denying the role played by theory and the theorist. In contrast, critical theory rejects such rigid distinctions between subject and object and observer and observed and lays bare the role played by theories and theorists throughout the process of reification. Pointing to the role played by certain actors in bringing about the existing order of things (i.e. denaturalizing the present which some analysts take as pregiven) opens up room for human agency to come up with solutions that go beyond mere 'problem-solving' within the parameters of the existing order.

In security studies, 'traditional' and 'critical' approaches differ most notably in their treatment of the state. Traditional security studies views the world from a state-centric (if not statist) perspective. In contrast, critical security scholars have argued that states are a means and not the ends of security policy, and hence they should be decentred in scholarly studies as well as in policy practice. Proponents of traditional approaches to security, however, have brushed aside such concerns and continued to point to the centrality of the roles states play in contemporary world politics. On closer inspection, however, this traditional (realist) argument turns out to be rather unrealistic. As Wyn Jones (1999: 96) has pointed out,

> *Although no one can doubt the elegant simplicity of this position, crucial questions remain: Is the realist's statism analytically useful? Can the internal politics of the state be ignored, thus allowing analysts to concentrate their attentions on the determining influence of the international realm of necessity?*

The failure of traditional accounts to capture the end of the Cold War – in terms of how and when it happened – attests to their limited analytical value. The roles played by ideas and transnational movements in helping to bring the Cold War to an end were not visible to those who looked through the state-centric lens of traditional security studies.

Although the end of the Cold War underscored the inadequacy of theoretical frameworks that fail to take into account transnational and subnational factors, traditional approaches to security soon returned to business as usual. Even the 9/11 attacks, which reminded the world of the increasingly influential role that non-state actors play in world politics, seem to have made only a minor impact on the traditional approach, which has included such actors in its analysis but failed to change the way it approaches actor–system dynamics. Part of the problem is that post-9/11 security studies treats non-state actors in a way that is reminiscent of how structural realists treat states – that is, as unitary actors the behaviour of which can be understood without becoming curious about their internal dynamics and the transnational factors that help shape those dynamics.

Viewed as such, traditional security studies fails not only by the standards set by critical theory but also according to its own standards. Comparing outcomes with stated objectives is what Hegel meant by his concept of 'immanent critique' (also employed by Frankfurt School scholars). This type of critique re-evaluates a position from its own standpoint (as opposed to some externally imposed criteria) to reveal its shortcomings. The aim of critique, however, is not only to deconstruct but also to reconstruct. As Stamnes has shown in her study of UN peace operations, whereas the deconstructive task involves uncovering 'unfulfilled potential for change inherent in an organization of, or arrangement within, society', the reconstructive task 'makes possible a choice between the various alternatives – it points out potentialities for emancipatory change'.

The 'Aberystwyth School' of critical security studies

Ken Booth (1997: 106) laid out the rationale for critical security studies as follows:

> *security is what we make of it. It is an epiphenomenon intersubjectively created. Different world views and discourses about politics deliver different views and discourses about security. New thinking about security is not simply a matter of broadening the subject matter (widening the agenda of issues beyond the merely military). It is possible – as Buzan (1991) has shown above all – to expand 'international security studies' and still remain within a neorealist framework and approach.*

The first analytical move made by the 'Aberystwyth School' of critical security studies is to deepen our understanding of security. This reveals the politics behind scholarly concepts and policy agendas, which allows analysts to decentre states and consider other referent objects above and below the state level, such as individual humans and planet Earth. The second move is to broaden our understanding of security in order to consider a range of insecurities faced by an array of referent objects. In this sense, students of critical security studies do not 'securitize' issues, but 'politicize security'. They do this to reveal the political and constitutive character of security thinking and to point to 'men's and women's experiences of threat' so as to be able to decentre the military and state-focused threats that dominate traditional security agendas. This stance is at odds with the Copenhagen School, which calls for 'desecuritization' out of a fear that those issues that are labelled as 'security' concerns will be captured by state elites and addressed through the application of zero-sum military and/or police practices, which may not necessarily help address human insecurities. Critical scholars, while sympathetic to those concerns, prefer to hold on to 'security' as a concept for scholarly studies while scrutinizing its use in practice.

The divide between the two schools on this issue (whether to seek 'desecuritization' or to use 'security' for raising and addressing the concerns of referents other than the state/regime) is not one of 'objectivist' vs. 'constitutive' understandings of theory, since both approaches understand theorizing as 'a form of practice'. Whereas the Copenhagen School makes a case for 'desecuritization' (taking issues outside the security agenda and addressing them through 'normal' political processes), the Aberystwyth School retheorizes security as a 'derivative concept' and calls for 'politicizing security'.

The Aberystwyth School prefers 'politicizing security' as opposed to 'desecuritization' for three main reasons. The first reason is strategic. Desecuritization, they argue, would amount to leaving security as a tool with a high level of mobilization capacity in the hands of state elites who have not, so far, proven to be sensitive towards the security concerns of referents other than

the state and/or regime. While the Copenhagen School calls for desecuritization for exactly this reason, the Aberystwyth School turns that argument around and asks: 'are existential threats to security simply to be abandoned to traditional, zero-sum, militarized forms of thought and action?'. Politicizing security thus facilitates questioning of how state elites use security and the merits of policies based on zero- sum, statist and militaristic understandings.

The second argument is ethico-political. The fact that security has traditionally been about the state and its concerns does not mean that it has to remain that way. When defined by state elites, 'security' could include anything and everything depending on their policy agenda. Depending on the historico-political context, security agendas of states may indeed translate into zero-sum, militarist, statist and, at times, dehumanizing practices. But when 'security' is defined by other actors such as environmental or humanitarian NGOs, it may be more likely to be conceived globally and practised locally with an eye on the negative future implications of current thinking and practices. Of course, some actors are more capable of voicing their insecurities than others. Nevertheless, opportunities remain to open up room for dialogue, debate and dissent. From this perspective, the role of the scholar is to amplify the voices of those who otherwise go unheard.

The third argument is analytical. Ultimately, the question of whether it is 'desecuritization' or 'politicizing security' that would help address those concerns is one that 'must be answered empirically, historically, discursively'. Empirical evidence suggests that the framing of HIV/AIDS as a global security issue has been of immense help in addressing its pernicious effects in Africa. By contrast, the way in which diseases such as Ebola are represented as threatening to (national) security often serves to feed regressive policy and ideas of the developing world as a source of threat. Representing migration to Western Europe in alarmist language, meanwhile, has generally rendered 'constructive political and social engagement with the dangerous outsider(s) more difficult'. In other settings, regressive asylum policy has been challenged precisely on security grounds, with advocates calling for recognition of the human security of vulnerable populations escaping persecution.

Securitization:

Securitization theory was developed through a number of works, culminating in the 1998 book by Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: a New Framework for Analysis (hereafter referred to as Security). It grew partly out of Buzan and Wæver's earlier work on regional security complexes, as well as Buzan's People, States, and Fear (originally published in 1983).

At the end of the Cold War, scholars in security studies were divided to a point where some justifiably considered the field to be in crisis. On one side, 'wideners' called for expanding the concept of security beyond military-political threats to the state, to take in new threats in areas such as environmental security and human security. On the other side, 'traditionalists' feared that endless expansion of the concept of security would potentially make it meaningless. For example, Stephen Walt claimed that security studies should focus on 'the phenomenon of war', arguing that expanding security studies to include non-military phenomena would destroy the 'intellectual coherence' of the field.

Securitization theory responded to changes in the international system that intensified with the end of the Cold War, developing a new framework for security analysis that tried to satisfy

both traditionalists and wideners. Instead of equating security simply with military threats to the state, Security identified a wider security agenda that also included more traditional security threats. Drawing on Buzan's (1991) earlier work, Buzan et al. (1998: vii) argued that 'security is a particular type of politics' that occurs not just in the traditional military sector but also in four other sectors: the political, economic, environmental and societal sectors. At the same time, they defined the meaning of security narrowly, as relating to issues of survival and existential threat, to retain the focus of the traditional security studies research agenda. This opened up the possibility that a range of issues could potentially be conceived and approached as security issues (a position advocated by wideners), while retaining a core focus on issues of survival and on the role of powerful political actors such as national leaders in addressing these issues, speaking to the concerns of traditionalists who wanted a more narrowly defined research agenda. So the Copenhagen School tried to satisfy both wideners and traditionalists, developing a new agenda for security studies.

The key to this approach was its development of the concept and theory of securitization, that is, understanding how issues become security threats. Drawing on J.L. Austin's language theory, Copenhagen School theorists argued that security has a special quality. Speaking security is not just speaking: security is a 'speech act'. A security speech act is 'performative', not descriptive: to utter security is 'to do it'. This makes security a very particular type of language: like saying 'I do' at a wedding, making a promise or naming a ship, the saying in itself does something. These utterances are not descriptive; they are acts in themselves:

> *the process of securitization is what in language theory is called a speech act. It is not interesting as a sign referring to something more real; it is the utterance itself that is the act. By saying the words, something is done*.

The next step in the Copenhagen School's approach was to argue that threats can be real or perceived, but they were not interested in determining the political significance of particular threats. Instead, they suggested that, ultimately, security arguments are always about the future, they are always hypothetical, so we cannot apply 'objective standards of securityness'. Thus, what matters is not whether or not a threat is real; what matters is that 'when states or nations securitize an issue – "correctly" or not – it is a political fact that has consequences, because this securitization will cause the actor to operate in a different mode than he or she would have otherwise'.

Following this logic, 'something is a security problem when the elites declare it to be so'. The most important factor here is not the uttering of the word security but the use of a particular type of political logic that defines security: 'the designation of an existential threat requiring emergency action or special measures and the acceptance of that designation by a significant audience'. Here, '"security" is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics'.

For the Copenhagen School, security is equated with survival, and therefore it has an essential quality: 'In security discourse, an issue is dramatized and presented as an issue of supreme priority; thus, by labelling it as security, an agent claims a need for and a right to treat it by extraordinary means'. Securitization therefore occurs when an actor designates an issue as an existential threat to something, and the audience accepts this designation, all of which is heavily dependent on the external context. The latter refers to factors outside the securitizing move itself, which affect the likelihood of its acceptance – such as the timing, whether or not the threat

seems a realistic threat in the eyes of the audience, the position of the securitizing actor and so on. Once an issue has been successfully securitized, it can be treated differently; securitization enables emergency measures and tends to lead to 'threat, defense, and often state-centred solutions'. As a result, the Copenhagen School argued that most issues are best desecuritized – moved out of the security sphere.

This means that sometimes securitization occurs in cases where the word 'security' is not used, for example in matters of defence, where securitization is institutionalized. At other times the word 'security' is used outside of this logic. At least in theory, securitization can 'never only be imposed': for the Copenhagen School, the success of securitization ultimately lies with the relevant audience for the speech act. It is they who decide whether or not to accept the designation of something as an existential threat to something that is valued. A successful securitizing move enables emergency measures; these measures do not have to be taken but they do have to be possible.

A range of factors affect the potential success of securitization: the Copenhagen School calls these 'facilitating conditions', and they come in two categories -

1

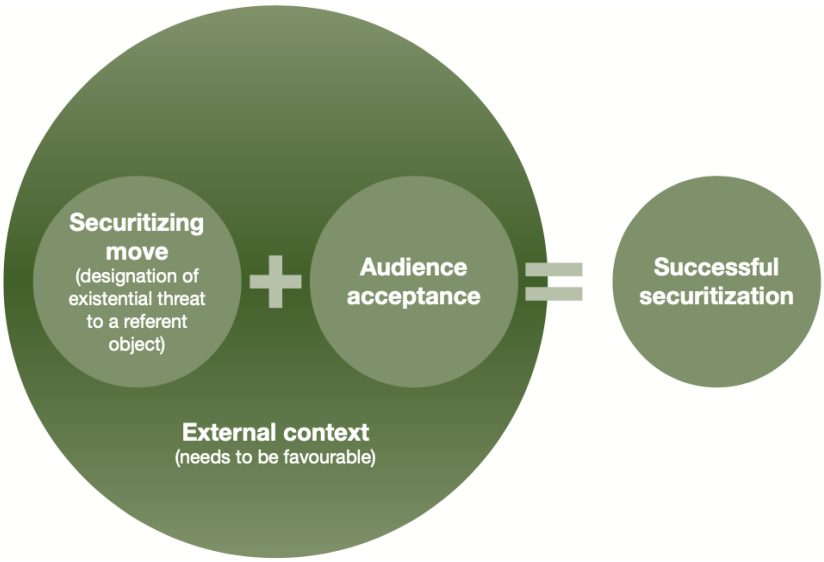


FIGURE 7.1 Successful securitization

'Internal, linguistic grammatical'.

2 'External, contextual and social'.

The first primarily concerns the speech act itself and the extent to which it follows the logic and grammar of security, creating a narrative that includes a clear existential threat. The second, external category includes the general circumstances of the act: both the securitizing actor and their position in society (for example, are they in a position of authority? Are they imbued with legitimacy?) and the threat itself (is it realistic and believable?). All of these factors affect the likelihood of the audience accepting the attempted securitizing move. If and when the audience accepts the securitizing move, then the issue ceases to be a part of normal politics and is moved into the sphere of security, where it can be treated with extraordinary means.

For the Copenhagen School, public issues exist on a spectrum that ranges from non-politicized (not dealt with by the state) to politicized (part of public policy) to securitized. Securitized issues are moved out of the sphere of regular politics, because they have been presented as existential threats 'requiring emergency measures and justifying actions outside the normal bounds of political procedure'. Here, '"security" is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics'. Securitization is therefore both an extreme form of politicization and its opposite, because it moves the issue out of the open debate that characterizes the sphere of politics and politicization for the Copenhagen School.

The distinction that the Copenhagen School makes between politics and security, where each sphere is characterized by a very particular form of politics (open democratic debate in the case of regular politics, and a closing down of debate and enabling of emergency measures in the case of security politics), leads them to make very particular conclusions about the desirability of securitization. Because they associate the politics of security with emergency threat-defence politics, they argue that 'security should be seen as negative, as a failure to deal with issues as normal politics'; this in turn makes desecuritization 'the optimal long-range option':

> *when considering securitizing moves . . . one has to weigh the always prob- lematic side effects of applying a mind-set of security against the possible advantages of focus, attention, and mobilization. Thus, although in the abstract desecuritization is the ideal, in specific situations one can choose securitization – only one should not believe this is an innocent reflection of the issue being a security threat; it is always a political choice to securitize or to accept a securitization.*

According to Buzan et al., security analysts should study 'who can "do" or "speak" security successfully, on what issues, under what conditions, and with what effects?'. They therefore place heavy emphasis on language and representation:

> *the way to study securitization is to study discourse and political constellations: when does an argument with this particular rhetorical and semiotic structure achieve sufficient effect to make an audience tolerate violations of rules that would otherwise have to be obeyed? If by means of an argument about the priority and urgency of an existential threat the securitizing actor has managed to break free of procedures or rules he or she would otherwise be bound by, we are witnessing a case of securitization.*

Securitization theory was developed as a constructivist analytical framework, but it has since grown and expanded and has been used by realists and liberals as well as critical theorists and poststructuralists. The simplicity of the central idea – the process of securitization – makes it fluid and adaptable, and it has become an influential approach in security studies. In this volume, securitization is included in the critical approaches section, though the extent to which it is considered critical depends on who is asked. In its origins, it has much in common with critical theory inasmuch as it also arose from discontent with mainstream approaches. The Copenhagen School itself emphasizes methodological pluralism. Indeed, a footnote in Security notes that while some of it might be seen as fitting the label of 'critical security studies . . . we have no prior commitment to antistate or antirealist positions'.

USE OF FORCE AND SELF-DEFENCE

History of the law on the use of force

For centuries, states have resorted to force in their international relations in order to achieve particular, desired aims. The use of violence has proved to be an accepted, although tragic in its consequences, method of resolving disputes between states. States reserved the right to wage war without any internationally agreed regulatory framework. Nevertheless, over time, the concepts of 'just and unjust war' emerged. The distinction between the two can be traced back to ancient Rome and the Fetials (*fetiales*), a group of priests who were responsible for maintaining peaceful internal and external relations and who gave rise to fetial law (*ius fetiale*) – religious law regarding the process of creation, interpretation and application of treaties and regulations on the declaration of war. The concept of 'just war' has changed over centuries.

Roman law of war and peace

Deliberations about war were expected to pass through these priests, who would seek a judgment of the gods about the justice of the proposed course of action. If it was decided that a grave breach of the peace had in fact occurred, such that a just war would be warranted, the fetials would first approach the guilty city to demand redress. If, after a certain period of time, no satisfaction was given, war could begin. (...) Declarations of war were cast in form of a lawsuit, in which the verdict transmitted by the fetials was meant to decide on the question whether the war could be rightly waged. Whether or not a war should be waged (to enforce a verdict) would then be the matter for a new decision, to be rendered by the king, the senate, or even (in later periods) the entire people.

The doctrine of 'just war' was further influenced by Christian theologians such as St. Augustine and St. Thomas Aquinas, the latter famously stated in Summa Theologica that the three criteria for just war are:

1. it should be waged by a sovereign authority (prohibition of waging a private war)

2. it must have a just cause (punishment of wrongdoers)

3. a just cause must be accompanied by the right intention.

Together with the rise of independent states in Europe, the doctrine began to evolve. In light of the growing number of sovereign states, wars started to be seen and defined as a state of legal affairs rather than a matter of subjective moral judgment. States no longer found themselves in a position to judge if another state's reason for resorting to force was just or not. This approach was supported by the rise of positivism, which strongly focused on the idea of sovereignty and by the Peace of Westphalia 1648, which established the European system of the balance of power. This system survived in Europe until the beginning of the twentieth century, effectively coming to an end with the outbreak of the First World War.

In the aftermath of the First World War efforts were made to rebuild international relations between states through the establishment and operation of an international institution which would play a central role in ensuring that such acts of aggression would not occur again. The League of Nations (LON) was created in 1919 with a view to achieving this aim. Under the 1919 Covenant of the League of Nations, member states were required to submit any inter-state

disputes for arbitration or seek other forms of judicial settlement at the League's Council. However, the Covenant did not in fact revoke the right of states to resort to war, although it subjected this provision to some limitations. In 1928, another attempt at the legal regulation of the use of force was made, in the form of the General Treaty for Renunciation of War as an Instrument of National Policy, more commonly referred to as the Kellogg–Briand Pact. Parties to this treaty declared that they 'condemn recourse to war' and agreed to 'renounce it, as an instrument of national policy in their relations with one another' (Article 1).

The outbreak of the Second World War in 1939 once again marked the end of peaceful international relations. The tragic events of this international conflict led to the adoption of the Charter of the United Nations (UN Charter) in 1945 resulting in the development of a framework, aimed at regulating the use of force by members of the international community. That system remains in force.

The post-1945 legal framework

The current legal framework regulating the use of force in international law is enshrined in the UN Charter. The maintenance of international peace and security is the primary purpose of the UN (Article 1(1) UN Charter). This includes:

prevention and removal of threats to the peace, [...] the suppression of acts of aggression or other breaches of the peace, [...] and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.

Therefore, as a general rule of international law, the use of force is prohibited.

The illegality of the use of force

Although states have resorted to the use of force in international relations on multiple occasions, there have been only two cases in which the International Court of Justice (ICJ) has found that there had been a violation of the prohibition of the use of force:

> *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v The United States of America) ICJ Rep 1986*
>
> *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) ICJ Rep 2005.*

The UN Charter further provides that:

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*

It is noticed from the wording of Article 2(4), prohibited acts include both the threat of force and the use of it.

It is important to remember that the prohibition on the use of force is not absolute. As the wording of Article 2(4) suggests, the force is permissible in circumstances consistent with the purposes of the UN. Chapter VII of the UN Charter ('Action with Respect to Threats to the

Peace, Breaches of the Peace, and Acts of Aggression'), outlines when a state can resort to the use of military force against other states. Force may be used against another state when:

1. such an act is authorised by the UN Security Council as part of collective security mechanism

2. a state is acting in self-defence.

The use of force authorised by the UN Security Council

The UN Security Council plays a major role in the global collective security system by deciding whether force may be used against other states. Should a situation that threatens international peace and security occur, it is within the Security Council's mandate to 'determine the existence of any threat to the peace, [...] or act of aggression' as well as to 'make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42' (Article 39 UN Charter). In such a situation, a state (or group of states) does not act unilaterally (as in the case of self-defence), but rather states act collectively by resorting to force acting under the authority of the international organisations (e.g. the UN Security Council).

The use of force in Libya

UN Security Council Resolution 1973 of 17 March 2011 is an example of the authorisation of the use of force by the UN Security Council. On the 17 February 2011, soon after the outbreak of protests in Egypt and Tunisia, which marked the beginning of 'The Arab Spring', Libyans in Benghazi joined in peaceful protests against the oppressive rule of Colonel Muammar Gaddafi. They demanded that he step down after 42 years of ruling Libya and called for an open, democratic and inclusive Libya. They demanded the end of an era of oppression and gross human rights violations in the country, such as those committed in 1996 in the Abu Salim prison. The response of Gaddafi to this protest with armed violence against civilian protesters ignited a civil war between the government forces in support of Gaddafi and the opposition armed forces formed by the rebels.

On 17 March 2011, the UN Security Council, acting under Chapter VII of the UN Charter, adopted Resolution 1973 authorising member states 'to take all necessary measures […] to protect civilians and civilian populated areas under threat of attack in the Libyan Arab Jamahiriya, including Benghazi, while excluding a foreign occupation force of any form on any part of Libyan territory.'

The use of force in self-defence

States may legitimately resort to the use of armed force in self-defence (Article 51 UN Charter). But what is the meaning of 'self-defence'?

Self-defence is a lawful reaction to the 'armed attack' against the territorial integrity of a state, which also diminishes its political independence (acts forbidden in Article 2(4) UN Charter). By executing the right to use force in self-defence, states are conducting a unilateral act.

The traditional meaning of the right to self-defence originates from the Caroline case; these principles were accepted by the British Government at the time and formed a part of customary international law.

The Caroline case (1837)

This case sets out a customary international law definition of the right to self-defence. It originates from a dispute between the British Government and the US Secretary of State regarding the destruction of an American vessel in an American port by British subjects. The reason behind this act was the use of the vessel to transport munitions and groups of Americans, who were conducting attacks on the Canadian territory. The US Government declared that the attack on the vessel constituted an attack against the American territory. The British Government responded by claiming the right to self-defence. The subsequent diplomatic correspondence between the parties contained an outline of the key elements for legitimate self-defence. The US Secretary of State, Daniel Webster, emphasised that for the self-defence to be lawful in international law, the British Government must prove the:

1. necessity of self-defence, instant, overwhelming, leaving no choice of means and no moment for deliberation

2. and that assuming such a necessity existed at the time

3. the act justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it.

The customary nature of the right to use force in self-defence was further confirmed by the International Court of Justice (ICJ) in the Nicaragua Case (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America ICJ Rep 1986). This is one of the key judgments in international law.

Criteria for self-defence

In order to lawfully exercise the right to self-defence, a state must be able to demonstrate that it has been a victim of an armed attack. The burden of proof in such a case lies with the state seeking to justify the use of force in self-defence. Nevertheless, not all attacks will constitute an armed attack for the purposes of Article 51: only the most grave forms of attack will qualify (Nicaragua Case, para.191).

Furthermore, the ICJ held in the Nicaragua Case (Merits) that ‘self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it’ (para. 176). This statement sets out two important principles in international law concerning the use of force: the principle of proportionality and the principle of necessity. In this context, proportionality means that the response to an armed attack must be reflective of the scope, nature and gravity of the attack itself. On the other hand, the principle of necessity guards against the use of measures which are excessive and not necessary in response to an armed attack.

The meaning of ‘armed attack’ causes significant controversy in international law. In the Nicaragua Case and in Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Advisory Opinion ICJ Rep 2004, the ICJ rejected the idea that an armed attack may include ‘not only acts by armed bands where such acts occur on a significant scale

but also assistance to rebels in the form of the provision of weapons or logistical or other support'(Nicaragua Case, para.195). In other words, it is necessary to show that an armed attack is attributable to a state.

In the Nicaragua Case, Judge Higgins strongly opposed this view and argued that the act involving the use of force from actors other than a state, such as groups of insurgents or terrorist groups, may give rise to the exercise of the right of self-defence by the attacked state. This statement highlights a very contentious issue in modern international relations, namely the use of force in self-defence against non-state actors.

Self-defence against non-state actors

The law on the use of force is traditionally designed to regulate the legality of armed force between states. This reflected the reality of the aftermath of the Second World War and the efforts of the international community to prevent such conflict from recurring in future. However, over the past few decades, states have increasingly been subjected to attacks by non-state entities. This raises questions about the adequacy of the traditional legal framework on the use of force in modern armed conflicts. The key questions are:

- When (if at all) may a state lawfully use force against non-state actors?
- May states exercise pre-emptive self-defence in anticipation of attack?

These questions attracted great international attention in the aftermath of the terrorist attacks on the World Trade Centre on 11 September 2001 (the '9/11' attacks) carried out by members of the al-Qaeda network.

Soon after the 9/11 attacks, the UN Security Council issued Resolution 1373 of 28 September 2001. The language of this resolution may suggest an almost unlimited mandate to use force against terrorist groups. It reads:

> *Acting under Chapter VII of the Charter of the United Nations, [...]*
>
> *2. Decides also that all states shall:*
>
> *(b) Take the necessary steps to prevent the commission of terrorist acts [...].*

In addition, the UN Security Council established a Counter-Terrorism Committee, mandated with the implementation of the resolution.

Although there were instances of the use of force against non-state actors prior to 2001, the 9/11 attacks urged discussion about the right to pre-emptive self-defence in international law. Following the attacks, the Bush Administration in the USA adopted a security strategy, based on the right to pre-emptive self-defence. The doctrine of pre-emptive self-defence assumes the right to use force without international authorisation in order to prevent the development of a possible future attack by another state. The USA's National Security Strategy (US Government, 2002) used the term of pre-emptive self-defence, particularly with reference to terrorist attacks:

The war against terrorists of global reach is a global enterprise of uncertain duration.

[...]

And, as a matter of common sense and self-defence, America will act against such emerging threats before they are fully formed.

The idea of pre-emptive self-defence is extremely controversial, as it goes against the core principles of international law regulating the use of force. The UN Charter allows for the use of force only in extreme circumstances, as a means of last resort, once all peaceful means have been exhausted. Furthermore, the use of force against another state in circumstances where there is a lack of an armed attack in the first place questions the necessity and proportionality of an attack carried out by a state which acts on the basis of 'pre-emptive self-defence'.

The ICJ has not yet commented on the existence of a right to use force against non-state actors, nor the right to pre-emptive self-defence.

COLLECTIVE SECURITY

Balance of Power has lost its relevance as a device of power management and Collective Security has gained recognition as a modern device of power management which can enable the international community to meet a crisis situations.

Meaning of Collective Security:

Collective Security is a device of crisis management which postulates a commitment on the part of all the nations to collectively meet an aggression that may be committed by any state against another.

War or aggression is viewed as a breach of international peace and security and collective security stands for collective action by all the nations in defence of peace.

Collective security stands for meeting any war or aggression by the creation of a global preponderance of power of all nations against the aggression.

Collective Security is also regarded as a deterrent against aggression in so far as it lays down that the collective power of all nations will be used to repel aggression or war against any state.

It is based on the principle, ′Aggression against any one member of the international community is an aggression against international peace and security. As such it has to be met by the collective efforts of all the nations′.

Definition of Collective Security:

(1) "Collective Security is machinery for joint action in order to prevent or counter any attack against an established international order." —George Schwarzenberger

(2) "Collective Security clearly implies collective measures for dealing with threats to peace." — Palmer and Perkins

(3) “In essence, Collective Security is an arrangement among states in which all promise, in the event any member of the system engages in certain prohibited acts (war and aggression) against another member, to come to latter′s assistance.” —Schleicher

In simple words, Collective Security system guarantees the security of each state of the world against any war or aggression which may be committed by any state against any other state. It is like an insurance system in which all the nations are bound to protect the victim of an aggression or war by neutralizing the aggression or war against the victim.

Nature of Collective Security:

Collective Security stands for preserving security through collective actions. Its two key elements are:

(1) Security is the chief goal of all the nations. Presently the security of each nation stands inseparably linked up with the security of all other nations. National security is a part of the international security. Any attack on the security of a nation is in fact an attack on the security of all the nations. Hence, it is the responsibility of all the nations to defend the security of the victim nation.

(2) The term ′collective′, as a part of the concept of collective security, refers to the method by which security is to be defended in the event of any war or aggression against the security of any nation. The power of the aggressor has to be met with by the collective power of all the nations. All the nations are required to create an international preponderance of power for negating the aggression or for ending a war.

The underlying principle of Collective Security has been ′**One for All and All for One**′. Aggression or war against any one nation is a war against all the nations. Therefore all the nations are to act collectively against every War/Aggression.

Main Features/Characteristics of Collective Security:

(1) A Device of Power Management:

Collective Security is a device of power management or crisis management. It seeks to preserve international peace through crisis management in the event of any war or aggression in the world.

(2) It accepts Universality of Aggression:

Collective Security accepts that violations of the security of a nation are bound to occur and that wars and aggressions cannot be totally eliminated from international relations.

(3) All Nations are committed to pool their power for ending Aggression:

Collective Security believes that in the event of a violation of international peace by any aggression in any part of the world, all the nations are committed to pool their power and resources for taking effective steps against every aggression for restoring international peace.

(4) Global Preponderance of Power:

Collective Security stands for the creation of a universal or global preponderance of power involving all the nations for the maintenance of international peace and security. Under it all the nations are ready to defend international peace and security through collective military action against aggression.

(5) Admits the presence of an International Organisation:

Collective Security presupposes the existence of an international organisation under whose flag a global preponderance of power is created for ending the aggression.

(6) Collective Security System is a Deterrent against War:

Collective Security can be an effective deterrent against a state with aggressive designs. Under this system each nation knows that any aggression against another nation shall be met by the collective power of all other nations. As such no nation tries to commit aggression and war because it knows that such an action will invite collective security action against it. This realization acts as a deterrent against any war or aggression.

(7) Aggression/war is the enemy and not the State which commits it:

Finally, Collective Security regards ′aggression′ or ′war′ as the enemy and not the state which may resort to war or aggression. A collective security action is limited to the elimination of war, aggression or threat of war or aggression. It does not stand for the elimination of the state which commits aggression. Its sole concern is to get the aggression vacated, to prevent the aggressor to gain out of its aggression, to restore the health of the victim of aggression, and to restore international peace and security.

As such Collective Security stands for securing international peace and security through collective efforts of all the nations. Security is the common objective of all the nations and it has to be secured through collective efforts of all.

Ideal Conditions for the Success of Collective Security:

Collective Security system can successfully operate when the following conditions are present in the international system:

1. Agreement on the definition of Aggression.

2. More broad based and more powerful United Nations.

3. More powerful role of UN Security Council and strong commitment of its permanent members in favour of collective security of international peace and security.

4. Existence of a permanent international peace keeping force.

5. An established procedure for termination of every collective security action.

6. Popularization of peaceful means of conflict resolution.

7. Sustainable socio-economic development of all the nations.

8. Strengthening of peaceful means of crisis-management and international peacekeeping.

Difference between Collective Security and Collective Defence in International System:

Collective Defence refers to the organisation of collective machinery for meeting any aggression by the enemy against any member of the collective defence system.

A collective defence arrangement is made by a group of nations who have a common perception of threat to their security from a common enemy.

Usually, a collective defence system is organised as an alliance involving a regional defence system. It covers only the members of the collective defence system. As against this, Collective Security stands for a universal system in which all states of the world, without any discrimination, undertake to meet any aggression anywhere in the system, and against any aggressor. It is designed to act as a deterrent against any aggression against any nation.

Dissimilarities between Collective Security and Collective Defence:

(1) Collective Defence is a limited or group system, whereas Collective Security is a global system. Collective Defence is a limited arrangement. It involves only some states who come forward to join hands against a common enemy. Collective Security is a global system. It involves all the states of the world.

(2) In Collective Defence possible threat is known not in Collective Security. In Collective Defence threat to security is known, in Collective Security threat to security is sudden. Any war or aggression by any one state against any other state is covered under the system of collective security

(3) In Collective Defence enemy is known in advance, Collective Security the enemy is every aggressor. In Collective Defence enemy is known in advance, but not in Collective Security.

(4) Collective Defence admits Advance Planning, Collective Security does not.

Advance planning is possible in Collective Defence because the enemy is known in advance. In Collective Security it is not possible because no state is the target. In comes into operation when any aggression or war or threat of war and aggression is committed by any member of the international community. As such Collective Defence is something very different from Collective security.

UN Collective Security System:

During this last decade of the 20th century, the Collective Security System began acting as a popular and useful device for the preservation of international peace and security.

The Charter of the United Nations regards the preservation of international peace and security as its most major objective. In this Charter "International Peace and Security" have been used 32 times. In its very first article, while stating the purposes of the United Nations, it makes the preservation of international peace and security as the first priority. It lays down a collective security system for this purpose.

Collective Security system has been laid down in Chapter VII of the U.N. Charter and its title reads: "***Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression."*** It contain 13 Articles, from Art. 39 to 51, which together provide for a collective system for preserving international peace and security.

The UN Security Council has been assigned the responsibility and power to initiate collective security action for meeting any threat to international peace by a war or aggression.

Art. 39 makes it the responsibility of the Security Council to determine the existence of any threat to the peace, breach of peace, or act of aggression and to decide about measures that are to be taken for managing crisis for restoring international peace and security.

Art 40 lays down that as the first step towards preventing the aggravation of the situation involving a threat to or breach of international peace and security, the Security Council can take provisional measures like cease fire, and call upon the concerned parties to comply with these.

Art. 41 refers to the enforcement actions, other than the collective military action. The Security Council can recommend to the members of the United Nations for compelling the concerned parties to end the violation of peace and security. It can recommend sanctions against the state involved in aggression.

Art. 42 empowers the Security Council to take military action for securing or maintaining international peace and security.

Art. 43 makes it the responsibility of all the members of the United Nations to contribute their support, efforts, resources and forces for raising the Collective Security force that may have to be raised when Security Council decides to undertake action under Article 42.

The next four Articles of the U.N. Charter (44-47) lay down the procedure for raising, maintaining and using the U.N. Peace Keeping Force for Collective Security force.

Art. 48 states, "The action required to carry out the decision of the Security Council for the maintenance of international peace and security shall be taken by all the members of the United Nations, or by some of them, as the Security Council may determine."

Article 49 asserts that: "The members of the United Nations shall join in affording mutual assistance in-carrying out measures decided upon by the Security Council."

Arts 50 lays down the ways in which non-member states can adjust their policies and actions towards the decision that may be taken up by the Security Council under Articles 41 and 42.

Art. 51, however, accepts the right of the states "to individual or collective self-defence if an armed attack occurs against a member, until the Security Council has taken the measures necessary to maintain international peace and security."

With all these provisions, Chapter VII of the U.N. Charter lays down the Collective Security system for preservation of international peace and security.

Since 1945, the Collective Security system has been tried in a number of cases. It was used for the first time for meeting the Korean Crisis of 1950.

Collective Security in Korean War:

North Korea invaded South Korea on the night of 24-25th June 1950. The Security Council, in the absence of the USSR, decided on June 25 and 27, 1950 to take enforcement action against the aggressor, North Korea. It held that North Korean attack on South Korea constituted a breach of peace and called for an immediate withdrawal of North Korean forces from South Korea.

However, when North Korea failed to comply with these directives and the Security Council found it essential to order collective security military action under the UN Charter Chapter VII. The response of the members to the Security Council resolutions was quite favourable as 53 countries expressed their willingness to support the Collective Security action.

On July 7, 1950, the Security Council set up a unified command under the UN flag and requested the member states to provide military assistance. In the first instance the U.S.A., the U.K., Australia, New Zealand came forward to induct small naval and air units into the "peace operation" in Korea. Later on, by early 1951, sixteen more countries came forward to offer their armed forces which were placed under the UN unified UN command. Thus the U.N.O. was successful in raising a U.N. collective force for repelling aggression.

However, the U.N. Collective Security operations in Korea became highly complicated when Communist China intervened in the Korean war for protecting the interests of North Korea. This development made the Collective Security operations in Korea very problematic because many states expressed their hesitation towards continued collective security operations in Korea as they felt that these could lead to an escalation of war.

The decision of the commander of the UN forces in Korea, to cross the 38th Parallel (Boundary between South Korea and North Korea) for repelling the aggression was sharply criticized by several states as a decision designed to punish communist China. This led to complications which made the Korean crisis almost a dispute between the communist and capitalist countries. The Chinese decision to pursue its intervention and the US decision to halt the march of communism into South Korea made things worst. Consequently, attempts were made to secure a peaceful resolution of conflict.

On 3rd November 1950, the **UN General Assembly adopted the Uniting for Peace Resolution** which was designed to give over- riding powers to the UN General Assembly. The resolution empowered the General Assembly to over- ride by 2/3rd majority any failure on the part of veto bound Security Council in respect of determining the aggressor, the nature of aggression against peace and the enforcement action that might be taken for preserving or retiring international peace and security.

The Uniting for Peace resolution was intended to give additional teeth to the Collective Security system. However, in actual practice it failed to produce the desired effect. The (erstwhile) Soviet Union became more apprehensive about a possible anti-communist stance of the General Assembly. It also made the USA apprehensive about the outcome of the Korean crisis. However, several members felt that this resolution constituted a bold attempt to strengthen the UN attempts at crisis management in the event of a war or aggression for restoring international peace and security.

Its immediate result on the Korean war was almost negligible. By January 1951, the Korean war got stabilized. Under considerable pressure from the United States, the UN General Assembly adopted a resolution on 1st February 1951, charging China of engaging in aggression in Korea. A committee was set up as a matter of urgency "to consider additional measures to be employed to meet this aggression and to report thereupon to the General Assembly."

The same resolution authorized the President of the Assembly to establish Good Offices Committee to explore further the possibilities of a peaceful settlement. Consequently, Collective

Security action and other activities aimed at securing peace in Korea were initiated after the passing of these resolutions. The face of Korean war now changed rapidly and by June 1951, the frontier was stabilized at the 38th Parallel.

Ultimately, an armistice was arranged on a Soviet proposal of June 23, 1951. Thus the Korean war ended and with this, the first attempt of the United Nations to end aggression against peace through collective security action got completed. However, the success in Korean crisis came not only due to the efforts of the UN but also due to the efforts of various nations who came forward to keep the Korean War limited.

After the Korean experience, Collective Security system underwent a second major test at the time of **Suez crisis of 1956**. But the results were secured less due to the action of the United Nations and more due to the Soviet threat to Britain, France and Israel.

However, in Congo, the U.N. Peace Force did a good job in restoring peace in this strife torn country. Even at the time of Hungarian crisis of 1956, (Erstwhile) USSR was compelled to respond favorably to the pressure from the U.N. against its interferences in the internal affairs of Hungary.

However, during the period 1956-90 Collective Security system under the United Nations failed to work successfully in securing international peace and security because of several factors. The cold war between the two super powers, the bipolarity in international relations, the inability of the General Assembly to act under the Uniting for Peace Resolution, and the changed nature of aggression and war, all combined to prevent the operationalization of Collective Security system during this period. The Lebanon crisis, the Iran-Iraq War and several other local wars kept on going and the UN failed to act.

However, during this last decade of the 20th century, the Collective Security System began acting as a popular and useful device for the preservation of international peace and security. It was successfully operationalized to meet the Iraqi aggression and occupation of Kuwait.

To meet the violations of international peace and security resulting from the Iraqi act of aggression, the UN Security Council first called upon Iraq to vacate aggression, and when it failed to comply with, enforced economic sanctions against Iraq. UN Security Council later on decided to take military action, i.e. Collective Security action against Iraq. A UN peace keeping force was raised under the US leadership and to which 42 countries contributed their armed contingents.

On 17th January 1991, Collective Security war against Iraq was initiated and within few days Iraq′s resistance was neutralized and liberation of Kuwait was secured. Collective Security war was successfully made to secure international peace and security and to negate Iraq′s aggression.

However, this exercise was successful primarily due to the keen interest taken by the USA and the inability or unwillingness on the part of the other four permanent members of Security Council to oppose the former. The internal troubles of the (erstwhile) the USSR compelled it to support the US sponsored decisions and policies. Further the decision to continue sanctions against, Iraq even after the end of its aggression against Kuwait reflected the problems involved in keeping a collective security war limited and confined.

After the collapse of the Soviet Union, Russia became its successor state. Its economic dependence upon the USA and some other Western countries began compelling it to accommodate the US view point in the UNO and other international fora. China also began feeling isolated after the collapse of socialist regimes in the USSR and other socialist-states of Europe.

The changed international scenario of the post-cold war, the post-USSR and the Post-Warsaw bloc international system, made the decision-making by the US security Council easier.

New development gave a new strength of the operationalization of Collective Security. In one form or another, the UN Collective Security operations for preserving peace and security began operating in as many as 20 different places. In 2001 war against Afghanistan′s Al Qaeda′s terrorist regime was made under the UN Charter.

However in 2003 the USA decided to go to a war against Iraq in the name of eliminating weapons of mass destruction (WMD). Such a US action came as a source of erosion of the UN Security Council′s role in international relations as the UN has not given its sanctions to such a war. This should have been prevented.

Presently, Collective Security system is being operationalized in more than 20 different places. The Collective Security System has been gaining a new credibility in contemporary international relations. Preservation of international peace and security as well as securing of development through cooperation at all levels of international relations can be described as the two major objectives of our generation. Collective Security of peace and collective efforts for development stand accepted as the two means for attaining these objectives.

As a device of crisis management through power-management and as a means of securing international peace and security, Collective Security has been the object of severe criticism.

Criticism Against Collective Security:

1. It is Idealistic in Nature and Scope:

The concept of Collective Security is based upon certain idealistic assumptions which make its operationalization difficult.

For example:

(1) It assumes that there can be a complete international understanding regarding the nature of all threats or aggressions against international peace and security.

(2) It is assumed that all nations could and would come forward to name the aggressor and to take up collective security actions against the aggressor.

(3) The concept of “collectivity” meaning, “All acting for one and all” is basically an idealistic concept since it ignores the fact; all nations are not active in international relations. Nor can all the nations be expected to join a collective security action.

2. At times it is not possible to identify the Aggressor:

Another major defect of the Collective Security system is that it wrongly assumes that in the event of an aggression against any nation, the aggressor and the nature of its aggression can be really and easily identified. In practice, it is very difficult to determine and name the aggressor as well as to identify the nature of aggression. Often the aggressor acts in the name of self-defence and justifies its aggression as a defensive action.

3. Admits War as a means:

Collective Security is self-negating in so far as it first denounces war or aggression as an illegal activity and then indirectly accepts that wars and aggressions are bound to remain present in international relations. It wrongly believes the most effective way to deal with such situations is to undertake a collective security war.

4. Rules out ˈNeutralityˈ in times of War:

The concept of Collective Security makes it an international obligation of all the nations to pool their resources and undertake collective action in the event of an aggression. It, as such, rules out neutrality. Many nations often prefer to remain away from war. It makes Collective Security war an international obligation and wrongly assumes that all nations are willing to participate in such a war.

5. A Limited Concept:

The concept of Collective Security, as laid down in the U.N. Charter, has two inherent limitations. It accepts the right of the states to undertake war as a measure of self-defence against any aggression. In practice this provision gives a legal basis to an aggression or war in the name of action in self-defence.

Secondly, it admits the right of the nations to establish regional defence pacts and organisations for protecting their security. It admits regional security systems as devices for preserving peace and security. The working of regional security systems has in-fact been a source of strain upon international peace and security.

6. Absence of a Permanent International Peace Keeping Force:

Another major limitation of the Collective Security system is the absence of a permanent peace keeping force. It is only after a decision of the Security Council to take military action against an aggressor is taken that the constitution of a collective security military force in initiated. This process is so slow and difficult that it takes a long time to raise the force and press it into service. The time-gap between the date of aggression and the date on which the United Nations is actually able to send its peace keeping force for restoring peace is very big, and the aggressor gets all the time needed for reaping the fruits of aggression.

7. Lack of provisions for the termination of Collective Security Action:

Another drawback of the U.N. Collective Security System is that whereas elaborate provisions have been laid down for implementing the system, no provision has been made regarding the method of terminating the Collective Security action.

8. Dependence on Powerful States:

One of the basic principles of Collective Security is that all the states should have an equal say in arriving at collective security decisions. In actual operation, it fails to work on the principle of equality. Powerful states always dominate collective security decisions and actions. In fact, only the powerful states can play an effective role in executing a collective security action. At times the powerful state are reluctant to put their power behind a collective security action which does not strictly conform to their national interests.

9. Dangerous:

Some critics hold the view the Collective Security system is a dangerous system as it can transform a local war into a global war involving all the nations. On the basis of these points critics describe the collective security system as an idealistic and limited system.

Justification of Collective Security System:

However, despite these points of criticism and recognized weaknesses of the Collective Security system, it cannot be denied that the system has not been totally meaningless and without positive features. It has brought into vision the idea and possibility of collective steps for the preservation of world peace through crisis management in the event of a war. The chances for a more purposeful and successful use of Collective Security in this post-cold war world have brightened. Currently it is being operationalized in several different parts of the world.

Collective Security constitutes a modern device of crisis management. All the members of community of nations are expected to act and save the humankind from the scourge of war and aggression and to use the collective security system for this purpose.

MODULE-II

INTRODUCTION TO MARITIME SECURITY

INTRODUCTION: MARITIME SECURITY[1]

While the sea has traditionally been a space that states have used to project their power – military, economic, and political – it has only been in recent years that maritime security has become a key issue of interest to policymakers and academics, notably following key incidents such as the attack on the Achille Lauro in 1985 and the 9/11 attacks in the United States of America (US) in 2001. The sea is now recognised as an integral part of international security agendas due to its geopolitical importance. Geopolitics, which references the intersection between geography and political processes and imperatives, and geostrategy, the area of geopolitics that addresses strategy (Van Rooyen 2011,p. 6), are important lenses through which states now view the world's oceans.

From the most basic perspective, states rely on the 'freedoms of the sea' to be able to conduct trade given that the vast majority of the world's trade (around 90%) traverses the seas, and are increasingly drawing on their rights to exploit sea resources for their economic development. These both encompass economic imperatives, but of course states also have political imperatives in this space. From a political point of view, states have traditionally used their access to the sea and ability to travel its length and breadth as a means to expand their empires and spheres of influence. Thus, in order to protect these interests, the security of the seas follows naturally as an issue of importance.

This module will seek to lay the foundation for the volume it introduces by explaining the importance of the sea as a geostrategic space, while also introducing concepts of maritime security, and indeed Maritime Security as a field of study. In so doing it should become clear why the issues that this volume explores have become areas of interest for policymakers in particular; an interest to which academic research has also responded.

A Brief History of Maritime Security

A good starting point to contextualise how maritime security and maritime geostrategy has been shaped, is to consider briefly their historical origins. Amirell (2016) provides a fascinating overview of what he describes as four phases of the historical development of maritime security studies and policy-making. The first phase runs from 1450 to 1600, a period during which the Bull Romanus Pontifex – a document issued by Pope Nicholas V in 1455 – ruled that Portugal essentially had sovereignty over all seas south of the conquered territory of Guinea, including both those that were known to man at that time as well as those that were yet to be discovered. Sailing the seas, trading, and fishing required a license from Portugal's king along with the payment of a tribute. Amirell (2016, p. 278) notes that "subsequent treaties and writings pertaining to maritime security agreed about the need to provide law and order at sea, even

[1] Lisa Otto, Introducing Maritime Security: The Sea as a Geostrategic Space, Global Challenges in Maritime Security: An Introduction, Advanced Sciences and Technologies for Security Applications, Springer Nature Switzerland, 2020

though there was disagreement about the moral and legal basis for the different claims to sovereignty, jurisdiction, the right to exploit natural resources and the right to sail and trade in distant waters". What followed was the Treaty of Tordesillas which gave Spain maritime powers and sovereign rights alongside Portugal by drawing a demarcation line through the Atlantic.

In the second phase – the period 1600–1850 – a decline in the maritime power of Portugal and Spain, and the rise and increasing importance of trading companies, defines the maritime security regime. It is in this context, with the expansion of Dutch trade, notably through the Dutch East India Company, that Hugo Grotius in 1609 writes Mare Liberum. His text rejects state-based claims of sovereignty and jurisdiction over the seas, advances the notion of freedom of navigation, and for rights for all to sail, trade and fish throughout the seas. This argument "came by and large to prevail until modern times and eventually developed to become the cornerstone of international maritime law". Indeed, in this period trading companies made sizeable profits as a result of the freedom of navigation as Dutch sea lines of communication (SLOCs) traced out the contours of several continents including Europe, Africa, and Asia.

In the period 1850–1990, the third phase, Amirell (2016, pp. 279–281) describes how power shifted and responsibility reverted to states as trading companies declined in the wake of the increasing cost of protection. Alongside this, imperialist states in Europe were on the rise and Great Britain became the "dominating global maritime power", while others like France, the Netherlands, and the US began playing increasingly important roles. This was particularly so following the opening of the Suez Canal, which granted easier access for European imperial powers to their colonies in Africa and Asia. Amirell (2016, pp. 279–281) contends that Europeans and North Americans saw themselves as the harbingers "of civilisation" and "the provision of maritime security… was a key aspect of the global civilising project". Combatting piracy and conducting operations against the slave trade were key elements of the project of securing the seas. In the meanwhile, significant technological advances were made that allowed for a global maritime security regime to exist and be supported by capacitated navies. Thus, by the twentieth century there were few sea-based threats to the economic and political interests of imperialists. These improvements in security at sea "led to the widespread notion that security… was the generic condition of sea travel".

In the post-Cold War era, which is the fourth phase that Amirell (2016, p. 281) describes, three main developments shifted maritime security conditions. First was the international détente at the end of the Cold War, that resulted in a reduction of naval capacity and as great a visible presence of naval power. Secondly, states saw their shorelines be extended with the adoption of Exclusive Economic Zones (EEZs) – an area that extends 200 nautical miles from the territorial sea baseline – which gave responsibility for these swathes of sea to the littoral state. Finally, states again saw their power decline in relation to private actors, and these private actors began taking up a greater role in the provision of public goods that would usually be within the remit of the state, including security, particularly as the responses of global navies to threats such as Somali piracy were deemed insufficient. It is during this period that Rogers (2010, p. 4) contends that

the US navy gained far greater prominence, allowing the country to develop itself as a global superpower by constructing maritime theatres that facilitated a rapid power projection that was intended to stave off hostility from enemies, notably the Soviet Union.

Amirell (2016, pp. 281–282) concludes on a somewhat ambivalent note, unsure as to whether these developments suggest a next phase characterised by greater private responsibility in the realm of maritime security, or whether China's growing presence in the East and South China Seas alongside a "more assertive position" suggests that state power continues to loom large. Indeed, China has been at work since the 1960s to create its 'String of Pearls' in the seas bordering the Asian and Middle Eastern landmass, which Khurana (2008, p. 1) describes as "nodes of influence". Another point for consideration here is that, although the US is ceding space to other powers as the world becomes more multipolar, it continues to hold a significant maritime presence with over 500 military installations flecked across its areas of influence and interest, of which the navy forms a strong component. The United Kingdom (UK) also has a number of naval bases around the world, including in Cyprus, the Falkland Islands, Diego Garcia, Singapore, and Bahrain.

This historical overview gives context to how the sea has been seen as space where power can be asserted and projected, as well as to how the key laws and concepts pertaining to the sea that are now accepted came to be so.

The Sea as a Geostrategic Space

Geopolitics is earlier explained as the intersection between geography and political processes and imperatives, and can be further understood as "an approach to studying contemporary international affairs that is anchored in the study of history, geography and culture". Germond (2015, pp. 137–138) expands, explaining that geopolitics can be seen in reference to "state's zones of interest or influence and how they clash with each other's", with states thus factoring geographical factors into their strategic thinking, developing 'geo-strategies' to guide their policymaking in relevance to international affairs and security.

Indeed, Granieri (2015, p. 493) harks back to The Influence of Sea Power on History 1660–1783, the work of Captain Alfred Thayer Mahan, to explain that the control of the seas played a crucial role in Britain's ability to rise as a world power. Mahan's work, published in 1890, holds that the ability to conduct commerce at sea was crucial for dominance on the international stage, with Granieri further arguing that sea power and the success of navies provides an explanation for "how some powers had risen while others had failed". This sentiment continues to ring true today as the sea remains linked to economic and security imperatives for states. Rogers (2010, p. 3) avers that sea power still matters because, "when wedded to a well-thought-out maritime geostrategy, [it] facilitates the application of maritime assets… to gain influence over particular and geographically sensitive spaces on the global map".

The Chinese String of Pearls is perhaps the best example with which to explain maritime geostrategy. Brewster (2017, pp. 270–272) notes that control over access to the Indian Ocean has long been securitised: given that the ocean is enclosed on three sides by Africa, the Middle East and the Indian subcontinent, and the Asian island states, with only a few entry points from other oceans such as the Red Sea, the Andaman Sea, the South China Sea (SCS), the Java Sea and so on, those states who then control these so-called 'chokepoints' can grant or deny access to the Indian Ocean for others, thus accruing a "strategic premium". Khurana (2008, pp. 1–2) demonstrates the strategic importance for China being compounded by the fact that, at the time of his writing, 30% of Chinese sea trade transited the Indian Ocean, while 77% of oil imports also traversed this space on the way from Africa and West Asia. A decade later, China still accounts for some of the largest containerized imports and exports, with the SCS, and access from there to the Indian Ocean to the west, and the Pacific Ocean to the east being critical, with US$3.37 trillion of trade passing through the SCS, the largest proportion of which belongs to China. To add to this, the SCS may be home to significant oil and gas resources, which has led to contestation over territorial claims of a number of islands in this area, with estimates for oil reserves around the Spratly Islands being between 100 and 200 billion barrels, and gas reserves being estimated to be 266 and 2000 trillion cubic feet. Moreover, as the world population grows, and the ability to secure food sources grows in importance, the SCS offers another attractive prospect: it offers "exceptionally favourable conditions for a fertile marine ecosystem". Successful claims over these islands allow for the establishment of EEZs, which then forms part of that country's sovereign territory. This has led China to consolidate its presence in the region, while also sparking controversy and heightening tensions with rivals through the development of a number of man-made islands in contested areas of the SCS. But, this is certainly not a new development; China identified the importance of the Indian Ocean and SCS decades ago. The String of Pearls essentially refers to military and commercial assets that China has throughout this region or can leverage due to friendly relations with key countries. This then forms a "wide distribution network to protect the transportation of resources from countries around the Indian Ocean to China's factories and provide Beijing with a foothold in the Indian Ocean". Dabas (2017) lists the following as elements of this strategy:

• Maintaining friendly relations with Malaysia and Singapore, particularly because its rival India has a "strategic hold" on the Malacca Strait;

• A presence in Myanmar's Kyaukpyu port, to which it has commercial access and may use for military purposes in times of war;

• A military base on the Coco Islands in the north eastern Bay of Bengal, reportedly being built by China;

• Investment in Bangladesh's Chittagong port, with negotiations for a naval base near here being ongoing;

• The development of the port in Hambantota, Sri Lanka, which is controlled by a Chinese company, with China also having intentions of negotiating a naval base in Sri Lanka; and

• Maintaining its close allegiance with Pakistan, particularly in countering India, with reports of a naval base here too.

Khurana (2008, p. 3) quotes You Ji, an expert on the Chinese navy, who says that China is employing a strategy of making its "presence felt through building a credible naval presence". Moreover, "there exist many uncertain factors in the security environment along China's borders, especially in the maritime dimension", which threaten the country's economic development, which it deems to be dependent upon the sea. This explains why China feels it necessary to project power outward into the Indian Ocean and surrounding seas.

China has complemented its String of Pearls with its One Belt One Road initiative – a plan to create overland linkages between the Eurasian hinterland, characterized by sometimes treacherous terrain, and the ocean – given an appreciation that land-based pathways also play an important role in accessing the seas.

As such, the example of the String of Pearls illustrates quite clearly how the sea can also be factored into geostrategy, and be used to advance an array of interests of a particular state. This case demonstrates this on a reasonably grand scale, but the reality is that the sea can be a geostrategic space for states not projecting power to this magnitude, having implications for the smallest of littoral states. Even those that do not have coastlines may view the sea as an important space given that their goods must also reach port in order to be exported, and likewise rely on seaports for arriving imports. The battle for South Sudan's access to the sea for the export of its oil resources is an apt example to show how non-littoral states can be impacted by sea-based geopolitics.

Maritime Security as a Field of Study

Before coming to what maritime security is, it may be useful consider what security itself is first. Buzan (1983, pp. 4–5), perhaps the most renowned security scholar, classifies security as a contested concept, but notes that an underlying theme emerges when analysing the perspectives of the likes of Jervis, Bull, Ashley, Booth and Beaton; that is: that security bound to the level of states is not adequate. In later works, Buzan, along with Wæver and de Wilde (1998, p. 21), sees security in international relations as being tied to the traditions of power politics, with international security issues thus becoming such when they pose "an existential threat to a designated referent object (traditionally, but not necessarily, the state)". They (Buzan et al. 1998, pp. 22–23) go on to examine the nature of an existential threat across various levels of analysis and sectors. Stone (2009, pp. 3–6) explains that Buzan offers three levels of analysis: individuals, states and international systems, and sees security threats emerging in five linked sectors: military, political, economic, societal and environmental. All of these concerns can coalesce at sea.

Much as maritime security has, in practice, a history spanning hundreds of years, and much as people have theorised about the meaning and value of the sea to mankind, particularly the laws that should pertain to it, actual scholarship around maritime security itself and what that constitutes is relatively nascent. Germond (2015, p. 138) describes the expression as being one that is recent, gaining prominence in the 1990s and 2000s. Maritime security has, thus far, largely been understood from realist and liberalist points of view, which see the sea as a theatre for power rivalries and projection, while other theoretical perspectives have had a lesser impact on debate around maritime security, but the concept itself remains new and contested (Bueger and Edmunds 2017, pp. 1295–1296). Till highlighted a need for clarity in what the study of Maritime Security would entail going forward, noting the challenge of this, given that the concept of maritime security entails a vast range of issues. Rahman (2009, p. 29) attempts to situate maritime security within broader concepts of security. He says that while maritime security may be seen to reflect wider conceptual debates on security, Security Studies literature does not confirm it as an independent dimension of security. Amirell (2016, pp. 284–285) makes a similar observation, arguing that Maritime Security studies has few academic institutions dedicated to it, does not have dedicated journals, and is not institutionalised as a field of study. Rahman (2009, p. 29) concludes that many established concepts of security may have maritime elements; for example, maritime environmental security, maritime border protection, comprehensive maritime security, and so on.

But can maritime security not be defined in its own right? This is exactly the question that Christian Bueger sets out to answer in his now well-cited Marine Policy article. In this piece, Bueger (2015, pp. 159–160) describes maritime security as being a buzzword that has drawn attention to a new set of challenges and threats located in the maritime domain, for which support is rallied. In this context, one might argue that maritime security should simply be the absence of these threats. But, Bueger criticises this approach, considering it insufficient. He takes a similar view to proponents of 'good order at sea', which provides a positive end-state rather than a negative peace, but also does not clarify what good order should be or whose order it should be. Bueger's article sets out to address the dearth of consensus by offering what Mudrić (2015, pp. 5–6) understands as being three underpinning frameworks from which to start better understanding maritime security. Indeed, Bueger (2015, pp. 160–161) uses semiotics, the securitisation framework, and security practice theory to establish a matrix in which maritime security relates four concepts to one another: the marine environment, economic development, national security, and human security.

Within this he is able to situate what might be called policy objectives of marine safety, blue economy, sea power, and resilience. Further, it allows him to position numerous of the challenges broadly considered to fall under the umbrella of maritime security – indeed many of which are discussed in this volume – which fall in various locations relative to the four framing concepts he begins with. Bueger includes: accidents at sea, pollution, smuggling, terrorist acts, climate change, piracy, illegal, unreported and unregulated (IUU) fishing, arms proliferation,

inter-state disputes, and human trafficking. This is illustrated below in Bueger's Maritime Security matrix (Bueger 2015, p. 161) (Table 1.1).

Following on from this Bueger and Edmunds (2017, pp. 1300–1301) continue Bueger's earlier theorisation of security at sea, describing four characteristics of the maritime security agenda:

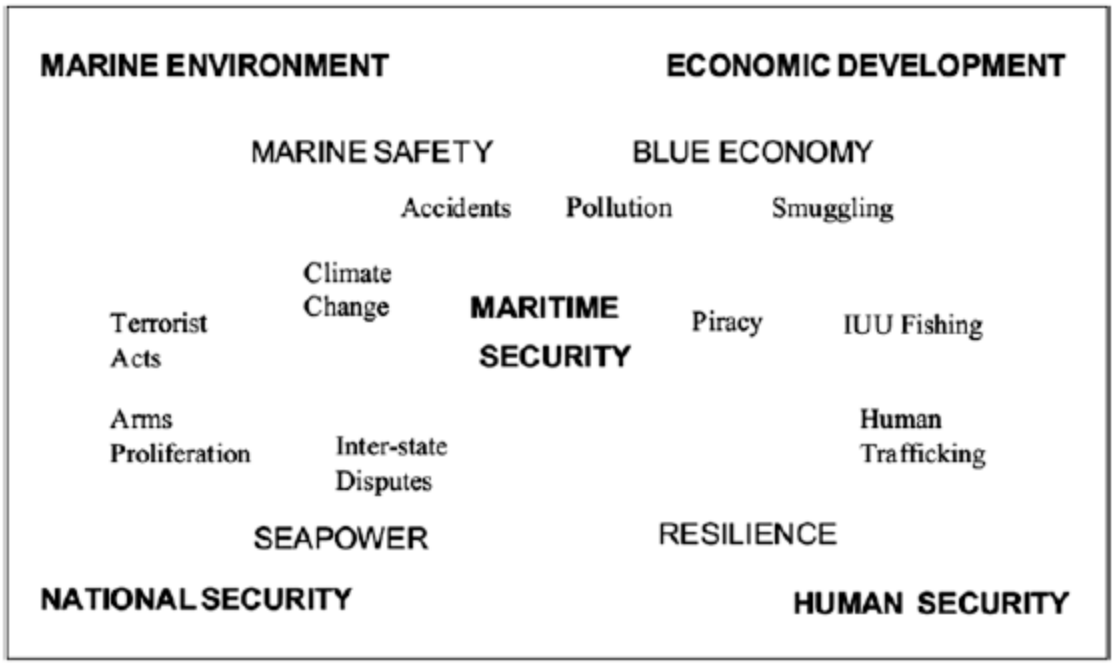
• one, the interconnected nature of maritime security challenges;

• two, the liminality of maritime security – that is, that most maritime security problems cannot be understood nor addressed without a consideration of their linkages to challenges on land;

• three, the transnational nature of maritime security given that the sovereignty of the high seas is shared, with jurisdiction there being international in theory, but also varying depending on the given circumstances pertaining to a threat or incident; and

• four, that, by extension, the maritime domain is essentially cross-jurisdictional.

Table 1.1 Bueger's Maritime Security Matrix



It should also be noted that maritime security is not merely a concern for littoral states or the international community at large in terms of access to the sea as a common space, but is also of concern to landlocked states, given the transnational nature of threats to the maritime domain which also, at some point, meet with land. Moreover, access to sea ports for the purpose of trade is imperative for all nations.

Amirell (2016, p. 284) suggests that Maritime Security is not an academic protodiscipline as yet, but it can be argued that maritime security studies may yet evolve into one. Since the time of his

writing, more journals have emerged that deal more closely with maritime security, while, as Mudrić (2016, p. 6) notes, a number of academic research centres have also engaged in what he describes as the pioneering venture of defining this emerging field. Examples includes the University of Cardiff and the University of Coventry in the UK, the Maritime Security Programme at the Nanyang Technological University in Singapore, whereas in South Africa the University of Stellenbosch has also placed a clear research focus on maritime security. Moreover, as highlighted by Bueger (2015), maritime security continues to edge closer to the centre from the periphery of issues on both domestic and global agendas, as indicated by the flurry of maritime security strategies that have been developed over the last decade at a state-level for those such as the UK, the US, China, Japan and Brazil, as well as those of regional institutions including most regional economic communities in Africa, the African Union, and the European Union.

It is evident that interest in matters relating to maritime security is growing among states, policy-makers, and academics alike, and that more work needs to be done to institutionalise Maritime Security as a field of study. Given the broad range of subjects that Maritime Security covers, it often draws together scholars and policy-makers with convergent interests but different academic and institutional backgrounds. This volume is intended thus to contribute in some way to this institutionalisation, and act as an introductory and foundational text for those, wherever they may come from, interested in Maritime Security.

What is maritime security?

It must be observed that a challenge exists in defining the term "maritime security." This is due to the diverse nature of the field which encompasses many different subject areas.

The term "maritime security" is now generally accepted and widely used by the international community. Despite this fact, there still exists no universal legal definition for the term under international law. In fact, IMO also fails to provide its own specific definition of maritime security.

However within the IMO context a distinction is made between the terms "maritime security" and "maritime safety." These IMO responsibilities, i.e. maritime security and maritime safety, are considered to be complimentary regimes essentially serving the same aim which is to ensure the protection of ships, passengers, crew, cargo and the marine environment. However despite sharing a common goal, the two regimes have distinguishing features; whereas maritime safety is primarily concerned with providing a defense against accidents at sea, maritime security deals with providing a defense against willful and unlawful acts against ships. Therefore, the distinction between the two terms lies in the willfulness of the act performed.

Klein observes that the distinction between the two terms has often been blurred. This is especially true considering the fact that the same word has often used to describe both "safety" and "security" in other languages, notably French and Spanish.[2]

A well-established definition of maritime security is provided by Hawkes who describes maritime security as:

"those measures employed by owners, operators, and administrators of vessels, port facilities, offshore installations, and other marine organizations or establishments to protect against threats, seizure, sabotage, piracy, pilferage, annoyance or surprise."[3]

From an analysis of this definition, one may conclude that implementing a successful maritime security regime requires a combined effort of action from different international, public and private entities, all of whom would benefit from improving international maritime security.

In the absence of an internationally-recognized definition, maritime security has been defined differently according to the context and the way it is being used. Klein confirms this fact as she suggests that the term is hardly ever defined in a categorical manner, but tends to have a more "context specific meaning." For example, from a military point of view, maritime security is concerned with protecting a State's freedom from any threats to national interest. On the other hand, for shipping operators, maritime security is more focused on the safety and security of maritime transport, where operators wish to ensure a safe journey for cargo and crew free from any kind of criminal activity.[4]

In light of the above, it may be said that an act against maritime security is one which uses the sea or ships in a manner that is unlawful, with the result that it threatens the security of a coastal state or vessels, persons, property or the marine environment. However as is seen in this study threats against maritime security are ever evolving, and consequently a precise definition would have to take into account the changing circumstances of international life.

In this regard therefore, it is extremely useful to pay particular attention to the analysis of the UN Secretary General in his 2008 Report on the Oceans and the Law of the Sea. In this Report Mr. Ban Ki-Moon also confirms the "context-specific meaning" of the term "maritime security":

[2] Natalie Klein, Maritime Security and the Law of the Sea (Oxford University Press 2011) 8.
[3] Kenneth Hawkes, Maritime Security (Cornell Maritime Press 1989) 9.
[4] Natalie Klein, Joanna Mossop and Donald Rothwell (eds), Maritime Securin, International Law and Policy Perspectives from Australia and New Zealand (Routledge 2010) 5.

“There is no universally accepted definition of the term "maritime security." Much like the concept of ‘national security,’ it may differ in meaning, depending on the context and the users.”[5]

However in the same Report, he recognizes the following seven important threats to maritime security;

1. Piracy and armed robbery against ships;

2. Terrorist acts involving shipping, offshore installations and other maritime interests;

3. Illicit trafficking in arms and weapons of mass destruction;

4. Illicit traffic in narcotic drugs and psychotropic substances;

5. Smuggling and trafficking of persons by sea;

6. Illegal, unreported and unregulated fishing; and

7. Intentional and unlawful damage to the marine environment.

One may note that the list of threats provided above in the 2008 Report embraces various concerns presented by different maritime stake holders including shipping operators, law enforcement officials and even maritime security analysts.

The Maritime Security regime

1. Suppression of Unlawful Acts

The Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) Convention and Protocol was designed to fill voids in international law necessary to combat other threats to human life and security of navigation and commerce at sea not fully prescribed under UNCLOS. It requires states to pass legislation making unlawful piratical and terrorist acts against navigation serious criminal offenses under their national laws. The SUA framework came in two waves.

(1) SUA Framework 1988

First are the 1988 Convention and Protocol. Under this legislation, states have an obligation to establish jurisdiction to extradite or prosecute violators even if the alleged offenses were committed outside their physical territory.

Unlike the UNCLOS definition of piracy, which only applies on the high seas and therefore only allows security responses on the high seas, the SUA framework criminalizes piracy-like offenses

[5] Secretary-General of the United Nations, Report of the Secretary General on Oceans and the Law of the Sea, 10 March 2008, UN Doc. A/63/63, para.39.

against vessels which have journeyed out of the territorial sea or are scheduled to transit beyond the territorial sea. Yet a major gap in the 1988 SUA framework is that it only granted flag states the necessary jurisdiction to respond to threats against vessels that flew their particular flag.

(2) SUA Framework 2005

In 2005 the 1988 SUA Convention and Protocol were amended to become the 2005 SUA Convention and the 2005 SUA Protocol. The 2005 SUA framework contains three new categories of offenses.

i. Using a ship as a weapon or as a means for committing terrorist acts.

ii. Proliferation of weapons of mass destruction (WMD) on the high seas.

iii. Transporting a person alleged to have committed an offense under other UN anti-terrorism conventions.

In addition, the 2005 SUA framework broadened state jurisdiction to include not only the flag state but also third states. Thus, the SUA frameworks further the extent of criminalizing acts against navigation beyond UNCLOS, increasing states' legal latitude to prevent attacks and pursue violators in maritime zones shore side of the High Seas. Examining the SUA framework from the broadest perspective, it is evident that it provides an agreement condemning maritime threats, acknowledging that countermeasures must be taken in shoreward maritime zones, including but not exclusively limited to private ship borne responses to threat mitigation. Standards and guidelines for private responses have been created via the necessary channels in IMO such as SOLAS, described below, as well as in soft law implemented by the industry.

2. SOLAS

The Safety of Life at Sea (SOLAS) Convention, first developed to increase safety aboard ocean-going vessels after the *Titanic* disaster, has grown since 1914 into the most thorough of all marine safety conventions. Its main purpose is to establish minimum standards for the construction, equipment and operation of ships, compatible with their safety. It is enforced by flag states and port state control measures.

Many coastal states have taken additional steps to clarify the relationship between Master and privately contracted armed security personnel (PCASP), amending national legislation to reaffirm the Master's overall authority to authorize PCASP targeting, deployment and target engagement (specifically, weapons discharge of any-kind). In an effort to resolve this dispute, the largest international shipping association, the Baltic International Maritime Council (BIMCO), has released a commercial contract template, GUARDCON, which establishes this clear line of superiority with the ship's Master remaining in command at all times.

Despite the superiority of the Master being reaffirmed in SOLAS, by flag states, and even in many industry contracts between PCASP and ship owners/operators, many security providers affirm that in certain grave life-or-death situations, they would disobey a Master's call to stand down under their individual right to self-defense should they believe their life or the life of crew-members to be in danger.

SOLAS allows port states to prevent ships from sailing when serious deficiencies are found that may pose a danger to persons, property, or the environment. This can be extended to implementation of maritime security procedures within SOLAS and its family of regulations (ISPS, ISM, etc.) if PCASP, their behavior, or their equipment seems to be substandard and as a result poses a danger to those aboard the vessel or the general public.

3. The International Maritime Organization

The International Maritime Organization (IMO) is the principal international organization dealing with maritime affairs.

The fascinating history of IMO began after World War II. In 1946 the United Maritime Consultative Council was set up to tackle any difficulties that may have arisen in the effort to resume regular peacetime activities, and also to encourage maritime trade as one of such activities.

During this time the establishment of a permanent intergovernmental organization in the field of shipping was becoming a clear necessity. UMCC member States recommended the United Nations Economic and Social Council to convene a conference, whose aim would be to set up an Intergovernmental Maritime Consultative Organization (IMCO). The recommendation also included a draft convention which would establish such an international body as a specialized agency of the UN. Governments were then invited to attend the UN Maritime Conference in Geneva in February 1948 in order to evaluate the establishment of such a body within the UN's framework. This was no easy task; in fact the Conference was concluded after seventeen days of intensive debate. Finally, 6 March 1948 marked the adoption of the Convention on the International-Governmental Maritime Consultative Organization which formally established IMCO. By the mid-1970s the Organization was no longer merely consultative and this was a main reason for the IMCO later being renamed the International Maritime Organization in May 1982.

The Organization focused its attention on matters such as maritime traffic. In the year 1972, the Convention on International Regulations for Preventing Collisions at Sea[6] (COLREGs) which aimed at improving navigational safety and also concerned the organization of traffic separation schemes for vessels was adopted.

[6] The Convention on International Regulations for Preventing Collisions at Sea, London, 20 October 1972.

IMO's role in Maritime Security: Despite there being no mention of maritime security as a function in IMO's formal mandate, IMO has always had a responsibility to ensure that transport and travel by sea is as safe as possible. In light of the recent terrorist activities around the world, IMO has had to take action to combat unlawful acts which threaten the safety of international shipping. The Organization now describes maritime security as an intricate part of its responsibilities.

IMO has played an important role in building a multi-faceted regime to ensure the safety and security of shipping, and also the prevention of marine pollution from ships. In particular over the years IMO has worked towards providing a source of international rules regulating maritime security.

4. Law of the Sea Convention

The LOSC is the foremost international legal instrument for realizing collaborative approaches to maritime security.[7] Maritime security supports an international order that is maintained through rule of law, and relies upon clear regulation of, and adherence to, the principles of both customary and formal international law, judicial decisions, other protocols, customs, and legal scholarship. Balancing issues of state sovereignty and collective interest, the Convention supports broad issues of security explicitly and implicitly, prescribing specific enforcement and jurisdiction requirements for states. The Convention provides a legal framework through which states organize their military and law enforcement assets to spread safety and security through international networks and coalitions.

The Convention specifically identifies only certain types of transnational crime that affect maritime security, but there are many varieties and combinations of criminal activity that affect security and safety from the high seas to internal waters. The Convention provides a strong framework and multilateral efforts to deter and defeat criminal activity in all maritime zones will result in a more secure, safer operating environment for all.

Maritime Safety and Security within Sustainable Ocean Economy / Blue Economy Governance Processes[8]

Ocean economic development is strongly linked to maritime safety and maritime security (Voyer et al. 2018), which are often defined in relation to perceived or potential threats in the maritime domain. Such threats include boundary disputes, terrorism, piracy, human, narcotic or illicit goods trafficking, arms trafficking, illegal fishing and other environmental crimes, or maritime accidents and disasters. Colgan (2018) noted that the safety and security services are essential to the adequate functioning of any economy, whilst Voyer et al. (2018) reported that maritime

[7] James Kraska, "Grasping 'The Influence of Law on Sea Power,'" SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, June 20, 2009).

[8] K. P. Findlay, Oceans and Blue Economies; L. Otto (ed.), Global Challenges in Maritime Security, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-34630-0_2

security is both an enabler of the blue economy (through economic asset and revenue protection) and a source of economic development and growth as a sector within blue economies. Ocean management strategies to ensure sustainability and social inclusion require both the enforcement and compliance monitoring of laws and regulations and a secure maritime environment, which provides the precondition for managing marine resources. Turton et al. (2007) in advancing Fallenmark's 'Trialogue model' of ecosystem governance, accent the trias politicas role of governments in the development of legislation and regulations, the implementation, compliance monitoring and enforcement of regulations, and the associated adjudication processes. Colgan (2018) reports these as the setting of appropriate limits, the development of policies to ensure compliance within such limits and the enforcement of such policies and identifies information, co-ordination and participation as central to successful management.

The question then remains as to how to achieve sustainable and equitable governance across the three social, economic and environmental domains, particularly where social equity and resource use clashes with resource sustainability and require increased regulation compliance monitoring and enforcement. Sustainable ocean governance has been advanced in a number of different forms, including for example, Integrated Coastal and Ocean Management (ICOM or alternatively, Integrated Coastal Zone Management (ICZM), or Integrated Coastal and Marine Area Management (IMCAM)), all of which generally have the Ecosystem Approach (EA), the Ecosystem Based Approach (EBA) or Ecosystem Based Management (EBM), at their core. A typical definition of EBM acknowledges the complexity and interspecies relationship within ecological systems, but definitions also account for social and governance objectives, with the latter aspects broadening the range of definitions. The Ecosystem Approach is defined by the Convention on Biological Diversity (CBD) as "a strategy for the integrated management of land, water, and living resources that promotes conservation and sustainable use in an equitable way". The Convention for the Conservation of Antarctic Marine Living Resources (2001), narrowly describes EA as management taking into account "all the delicate and complex relationships between organisms (of all sizes) and physical processes (such as currents and sea temperature) that constitute the Antarctic marine ecosystem". Long et al. (2015) report that EBM is generally viewed as a strategy that manages the human activities influencing ecosystems, considering such impacts in management decisions. Importantly, the EA considers the functional relationships and processes within ecosystems, the flows from systems to human benefits as ecosystem services, the use of adaptive management practices in policy cycles, management actions at multiple scales, and inter-sectoral cooperation within ecosystem management. Underpinning the process are the needs for balancing resources and resource use of ocean economies through adequate governance approaches that include domain awareness in both the marine biophysical realm and the maritime human resource-use realm.

Overarching ocean governance processes that incorporate the sustainability and equity considerations of a blue economy model can be viewed as a series of sequential steps towards the development of effective policies capable of adapting to changes and opportunities as these arise.

It should be noted that such governance instruments are often required across multi-sectoral use (and associated authority aspects) in that in many countries ocean use is highly sectoral with government departments / authorities tasked with different ocean management responsibilities (and each often with their own sectoral mandates). These sequential steps include the following aspects:

1. The development of knowledge economies, ocean systems monitoring and research. Ocean governance as either a process or a product requires informed decision-making that in turn depends on relevant information derived through dedicated ocean system monitoring and research programmes across each of the environmental (and ecological) science, social science and economic science domains. Integral within these programmes are a) the resources and human and technological capacity (including increasingly remote-sensing and robotic technological capacity in fourth industrial revolution backdrops) to undertake the required research and monitoring; b) the needs for data systems that can accommodate and process high volumes of data; and c) the capacity to translate data to information to knowledge to wisdom. It is critical that such knowledge creation frameworks go beyond empirical academic knowledge and extend to experiential and indigenous knowledge systems.

2. Standards Development. The use of the knowledge and wisdom derived from adequate research and monitoring to develop standards and metrics against which decisions can be made. Such standards and metrics may, for example, relate to biophysical criteria standards, ecological and conservation status assessments or social criteria.

3. Marine Spatial Planning (MSP). MSP can be viewed as a means to a rational organisation of the use of marine space and the interactions between its users, so as to both balance developmental demands with the need to protect the environment, and to achieve social and economic objectives in an open and planned way. Within area-based EBM frameworks that primarily focus on specific ecosystems and the range of activities impacting them within particular space, MSP aims at “analysing three-dimensional and highly dynamic marine spaces and allocation of these to specific users so as to achieve the ecological, economic, and social objectives that are usually specified through the political process”. However, MSP incorporates processes that range from simple mapping to identify conflicts to more comprehensive planning processes that require trade-off valuations across domains and several shortcomings in MSP case studies have been identified.

4. Representative Marine Protected Area (MPA) allocation. It is particularly important that representative systems are protected so as to a) advance the conservation of biodiversity and ecosystems leading to potentially enhanced ecosystem services values in SESs; b) ensure the potential role as benchmarks of the impacts of anthropogenic stressors in unprotected areas; c) enhance ecosystem resilience to combat indirect global influences and impacts; and d) ensure the safeguarding against scientific uncertainty and management failure. Representative MPAs can be defined as “any area of the intertidal or sub-tidal terrain, together with its overlying water and

associated flora, fauna, historical, and cultural features, which has been reserved by law or other effective means to protect part or all of the enclosed environment" (Kelleher 1996) or as defined by the IUCN "a clearly defined geographical space, recognised, dedicated and managed, through legal or other effective means, to achieve the long-term conservation of nature with associated ecosystem services and cultural values". Through protection of both species and their habitats, MPAs advance ecosystem-based approaches to both biodiversity conservation and extractive management, as distinct from the historic and more traditional focus on single species management practices. Recent MPA advancement has been boosted by international conservation targets including those resulting from the World Summit on Sustainable Development; the Convention on Biological Diversity and the CBD Aichi Biodiversity Targets, particularly Target 11.

5. Legislation and regulation, compliance monitoring and enforcement including marine domain awareness Surveillance and remote sensing. Regardless of the governance regulations, enforcement and compliance monitoring remains a critical aspect of governance structures. The goods and service benefits of oceans or blue economies arise as both rival and non-rival excludable or non-excludable goods so that competition for access to common pool resources means that they are susceptible to overharvesting and destruction. However, such over-use as embodied in (Hardin 1968) Hardin's 'tragedy of the commons' has been counter-argued in that communities manage shared natural resources through the establishment of 'self-governance' regulations that limit overuse. It is however imperative that adequate monitoring and governance instruments are in place in offshore (and relatively invisible) resource uses. Inherent in the compliance monitoring and enforcement are the aspects of safety and security in marine and maritime domain awareness to limit value loss across a range of activities in the ocean domain.

6. Capacity Development. Ocean governance is critically dependent on both technological and human capacity across the range of the above disciplines, and Attri (2018) has identified that capacity development in ocean governance in many developing countries is weak.

7. Adaptive Management and Policy Cycles. Integral within ocean governance processes is the need for review and adaptive management within policy cycles. Such adaptive management is particularly important in light of ocean change (e.g. increasing global temperature, altered regional weather patterns, rising sea levels, acidifying oceans, altered nutrient loads and altered ocean circulation) manifested through the human impacts of climate change, ocean acidification, unsustainable extraction, habitat modification or pollution loading.

Illegal, Unreported and Unregulated (IUU) Fishing as a Maritime Security Concern[9]

The functional nature of the IUU fishing concept has permitted its adoption in official narratives that are not always concerned with matters of fishery conservation, though its inclusion in national maritime security policies has often been met with resistance. Yet, recent developments

[9] Mercedes Rosello, Illegal, Unreported and Unregulated (IUU) Fishing as a Maritime Security Concern

in security strategies at the national and regional levels suggest a progressive broadening in understandings of maritime security, towards a framework that is more responsive to the risks associated with IUU fishing. Scholars increasingly regard maritime security to be inclusive of economic and environmental resilience considerations, and of the role of non-state actors involved in marine fisheries in the causation and perpetuation of risks. The association between maritime security and IUU fishing broadly responds to two types of distinct but interdependent considerations, namely impacts on human communities, and operational synergies with crime.

Impacts on Human Communities

IUU fishing impacts can be difficult to discern from the effects of legal fishing, but they are thought to be severe. Indiscriminate and unmanaged harvesting of ocean living resources, particularly if already under pressure from regulated fishing, may pose a considerable threat to stocks. When IUU fishing activities include highly destructive fishing gears, they may cause a high incidence of mortality of target as well as non-target species, which can be aggravated when gear is discarded at sea. Literature by non-governmental organisations suggests that over 85% of global commercial stocks may be at risk of IUU fishing, with 54% at high risk, throughout all ocean areas. Economically, IUU fishing is believed to exact a heavy cost. In 2015, the FAO commenced a review of existing cost assessments, highlighting multiple areas of uncertainty, partly due to the imprecise nature of IUU fishing as an interpretive lens (Poseidon Aquatic Resource Management 2016). An influential 2009 study has suggested that the global costs inflicted by IUU fishing each year could range between US$10 and US$23.5 billion, which is equivalent to between 11 and 26 million tonnes of seafood. It is unclear whether these estimations accurately reflect the state of affairs today, though international actors generally accept the lower end of the range as a valid indication. The majority of the costs of IUU fishing are born by the exclusive economic zones (EEZs) of coastal states, which contain most ocean taxa. Over-harvesting of EEZ stock can have significant detrimental effect on the security of affected fishing economies. In particular, when artisanal and other small-scale fisheries are disrupted, their higher contribution to employment means work and food security may be impacted. It is thought that the impacts caused by illegal fishing may increase the susceptibility of affected individuals to engage in piracy and other unlawful activities in communities lacking economic resilience. Least developed nations are amongst the most vulnerable to fluctuations in catch availability, due to the fact that ability to plan and execute adaptation in the face of resource scarcity may be diminished by a lack of capacity. A lack of availability of commercially valuable highly migratory species such as tuna, can be particularly damaging to small island states with a high dependency on the harvesting or processing of such fishery products.

Operational Synergies with Crime

IUU fishing is not only characterised by infractions of fisheries conservation and management obligations: IUU fishing operations have been documented to have operational synergies with a broad range of criminal activities. Vessel operations such as ‘transhipment’, the practice of

transferring cargo from one vessel to another, facilitates the blurring of traceability in fishery products, also providing opportunities for transferring non-fishery cargo (Chapsos and Hamilton 2018). Crimes associated with IUU fishing are diverse, and can include documentary fraud, tax evasion, drug smuggling, people smuggling and crew exploitation. Human trafficking has been linked to the Gulf of Thailand, where large-scale economic migration patterns from less developed neighbouring states into Thailand and its large fishing industry have led to significant problems of labour abuse in the fisheries sector. As Thailand has begun developing its domestic legal framework and policies, practices of workforce abuse have nevertheless been identified in fishing vessels flying the flag of other states. Reports of human trafficking are not limited to specific geographies or stages of development, with cases having been documented also in developed states. Links have been established between IUU fishing and drug trafficking routes between South America and Europe. Further, IUU fishing has been associated with corruption, particularly when governance structures are fragile. The interconnectivity of IUU fishing and associated criminal practices, and their impacts on human communities are increasingly being understood as significant from a security perspective. The UN General Assembly (2001) has referred to IUU fishing as 'one of the most severe problems currently affecting world fisheries and the sustainability of marine living resources (…)'. Yet, research increasingly supports the view that the ramifications and impacts of IUU fishing are complex and far-reaching, transcending the fishery management context in which the term was first coined.

Multilateral Cooperation and Securitisation

The practices of individual states can be significant in catalysing effective trends to combat IUU fishing, but the need for multilevel cooperation in transnational matters is widely acknowledged. Indeed, the often transnational nature of IUU fishing activity means that multilateral institutional approaches may be better placed to address deficiencies in vessel activity regulation, monitoring, and enforcement. Significant efforts are being made at the global level to address existing weaknesses in governance. Since the 1990s, concerns over IUU fishing have been debated in the forum of the United Nations General Assembly (UNGA). A resolution upon destructive fishing practices was adopted by the UNGA in 1991, which became upheld by a large number of states. The adoption of three multilateral fisheries treaties addressing regulatory issues that are essential to IUU fishing control was conducted under the auspices of the UN Food and Agriculture Organization. Significantly, the FAO has promoted the adoption of a Global Record of Fishing Vessels, Refrigerated Transport Vessels and Supply Vessels. The Global Record serves as a shared vessel data repository that can support State coordination in combatting IUU fishing, as well as wider coordination with the information held by RFMOs (FAO 2016). In addition, another international organisation with an information remit, Interpol, has also been engaged by its member states for the coordination of law enforcement in matters concerning maritime crime that is transnational in nature, and which frequently involves IUU fishing activities.

In the marine space, resource distribution and geopolitical diversity calls for the added specificity and flexibility of regional approaches. Some regional organisations have developed securitisation

policy narratives, in which IUU fishing has been explicitly identified as a risk. Examples include declarations by the European Union (EU) and the African Union (AU), both of which have identified IUU fishing as an eradication objective in their marine security strategies, with the AU in particular identifying IUU fishing as a range of activities akin to criminal acts (African Union, African Integrated maritime Strategy, Addis Ababa 2014). Finally, nowhere is the need for regional approaches to cooperation and coordination more pressing than in regions where IUU fishing has become a complex security risk, combining largescale depressors of human security, and transcending in significance the criminality and food security concerns previously outlined. In particular, in the South China Sea, where fishing has been an important pillar for the food security of the States in the region, IUU fishing has been a persistent threat (Teh et al. 2017). Its prevalence and impacts have been exacerbated by expansionist efforts by China in securing marine resources to an increasing distance from its landmass, combined with sovereignty disputes over maritime features in the area. Fishing vessels have become involved in numerous incidents, exponentially increasing security concerns.

Enhancing Security via Regional Resource Management Fora

Regional responses to IUU fishing typically take place in the RFMO fora, where states converge regularly to take important decisions concerning resource utilization and management, and vessel operations. The authority of RFMOs has been progressively affirmed through growing international support. They often establish conservation and management measures (CMMs) that include operational restrictions and associated controls. CMMs are varied in nature, comprised by heterogeneous technical rules, guidelines and procedures that have the objective of managing harvesting activities. Rules have to be internalised by member states so that they can issue appropriate rules and regulations, ensure compliance by their vessels, and take enforcement action where appropriate. Beyond this, RFMOs are sites of recurrent formal and informal processes of consultation and review, and their governance remit has the potential to reach beyond the establishment of fisheries CMMs, to touch upon mechanisms of coordination that can be security relevant. These include mechanisms for the recording and disclosure of operational information, identification of infractions and publication of related black lists, and cooperation via complementary surveillance and inspection activities.

RFMOs typically require access to fishery management data held by states, in conformity with international law, and with their own internal legal frameworks. State duties extend into matters of compliance, evaluation and verification, via processes under which member States report to the internal institutions of the organization. Typically, States report to the RFMO operational and management information, including effort and catch data, in particular formats, and some RFMOs also mandate the reporting of transshipment data. Although the quality of RFMO CMMs and other rules varies, as does compliance among the member states, collectively RFMO measures make a valuable contribution to IUU fishing control, particularly as RFMO duties reach States with large fleets that have not always ratified important global fishery treaties. Being based to a great extent on information reporting and sharing, the performance of RFMOs

largely depends on integration of the relevant data, and the epistemic quality of information disclosures made by states. Resulting RFMO expertise concentration and ability to coordinate regulatory and compliance efforts in their respective management areas confer onto these organisations a unique strategic potential. It is precisely in the regions where security is most fragile, such as the South China Sea, and where existing regional arrangements fall short of the capabilities of an RFMO, that their absence might be felt most keenly.

Enhancing Security Through Port Cooperation

In recognition of the economic nature of industrial fishing operations, there has been an increase in IUU fishing control approaches involving port measures. Although coastal states have powers of detention and enforcement under the UN Convention on the Law of the Sea (UNCLOS) (1982) within their EEZs, IUU fishing activities carried out in the high seas fall beyond the jurisdiction of coastal states. The IPOA IUU contains guidance for states interested in developing extraterritorial port based mechanisms (paragraphs 52–64), setting out a number of regulatory options that states may adopt when foreign fishing vessels seek admission for fuelling, victualing, transhipping, or landing fish cargo (paragraph 53). This has served to complement and reinforce the traditional flag state controls over fishing vessels in respect of high seas activities. At least in part, the IPOA IUU reflects provisions contained in a number of international legal frameworks and consolidated State practice affording authority to port States to carry out inspections, and to act alongside flag states to ensure IUU fishing activities are identified and addressed.

Fisheries-specific international treaties have made an invaluable contribution in respect of extraterritorial standards of conduct that may inform port controls. The United Nations Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks (usually referred to as the Fish Stocks Agreement) sets out a typology of conducts to which it refers as ‘serious violations’. Significantly, it includes references to conducts that might be seen as possible criminality indicators, such as falsifying documentation regarding the identity or registration of a fishing vessel, and concealing or manipulating evidence. The 2009 Port State Measures Agreement enables verification through inspection of critical information, such as may be found in vessel and authorisation documents, and vessel monitoring and surveillance data. These measures are contemplated in respect of vessels, upon which port states may effectively offload the burden of proof, so that investigations and certain consequences of presumed non-compliance are no longer dependent solely on flag states. IUU fishing activities could take effect in any part of the ocean, where member states of RFMOs may call on the port state for assistance. However, more stringent extraterritorial enforcement measures, such as detention, are restricted to offences committed in the EEZ, and otherwise do not appear to be supported by international practice, beyond certain exceptional instances.

RFMOs have had a significant role in promoting the coordination and enhancement of port controls. Insofar as measures of this nature might be operationalised in a manner that may result in them acting as barriers to trade to the detriment of specific states, compliance with the rules of the international organisation established to regulate global trade, the World Trade Organization (WTO), is required. In line with those requirements, a number of RFMOs have elaborated catch documentation schemes (CDS), which operate as statistical tools able to record and clarify the traceability of certain types of catch. Beyond the critically important function of introducing transparency to the product supply chain, the CDS has another advantage: it is able to identify certain governance flaws by the flag states that regulate the relevant fishing vessels. Following the success of the measures adopted by some RFMOs, the EU in 2008 adopted a different and more comprehensive mechanism, a regulation establishing market measures in order to combat IUU fishing, named Council Regulation (EC) 1005/2008 (the IUU Regulation), which entered into force in January 2010, and related legislation, whereby processes for the identification of the IUU origin of seafood products destined to EU markets are established. The IUU Regulation applies port state measures to vessels harvesting marine living resources destined to EU ports to be sold. An empirical data collection system for the purposes of identifying and verifying IUU fishing trade flow operates under the IUU Regulation via a specially designed catch certificate, conditioning the sale of wild seafood to EU markets to the completion of a standardised form, including identification details of the harvesting vessel. Data concerning suspected IUU fishing operations has to be validated by each individual vessel's flag state, which results in the provision of critical evidence on possible breaches of flag state obligations. Where the flag state fails to verify compliance, it may be identified as non-cooperating, and receive a trading suspension of all fishery products originating from that state. The IUU Regulation has therefore had the consequence of enhancing port inspections with regard to IUU fishing activities in designated ports across the EU, as well as driving the need to prioritise fishing vessel regulation among the many States that sell seafood to the EU.

Maritime Security and Right of Innocent Passage

UNCLOS and customary international law recognize three important navigational regimes which are vital for the maintenance of maritime security;

1) Innocent passage which applies in the territorial sea and archipelagic waters;

2) Transit passage which applies to straits used for international navigation; and

3) Archipelagic sea lanes passage which applies to archipelagic waters.

Each of these regimes attempts to strike a balance between two important competing interests. On the one hand, there exist the interests of coastal States that wish to extend their maritime jurisdiction, not just for economic but also for security reasons; and on the other hand, the interests of States who strive far as possible to maintain freedom of navigation and overflight.

There may be certain situations where this delicate balance is upset, as in the case of the passage of foreign warships and their security ramifications when passing through the territorial sea of another State.

A coastal State or archipelagic State is interested in protecting its own national interests and sovereignty and will attempt to prevent foreign vessels from causing any prejudice to its security. In this sense, such States may be justified in placing certain limitations on the navigational rights of foreign vessels. Conversely, as correctly pointed out by Bateman, major maritime States might view these restrictions as having a negative impact on their own maritime security, in particular their naval mobility and defense operations.

Right of Transit Passage: Most coastal States had extended their territorial seas to twelve nautical miles, while a few claimed maritime jurisdictions up to 200 nautical miles. Consequently, many of the world's straits-which are of vital importance to international navigation and trade-would form part of the territorial sea and are therefore subject to the sovereignty of coastal States concerned. In order to avoid restricting the freedom of navigation in these areas, UNCLOS provides that in straits used for international navigation, the sovereignty of the coastal State is preserved, subject to the right of transit passage.

This right grants foreign vessels freedom of navigation solely for the purpose of continuous and expeditious transit of the strait. Moreover, bordering straits may not impede or suspend such transit passage as in the case of innocent passage. However, the limitation placed on the sovereignty of bordering States is balanced with the obligation of foreign vessels exercising the right of transit passage to respect *inter alia* the security interests of bordering strait States. Therefore, foreign vessels are to refrain from any use of threat or force in any manner in violation of the principles of international law found in the UN Charter.

PASSAGE OF WARSHIPS

I. Right of innocent passage: Conceptual discussion

The right of innocent passage has been recognized at a universal scale.[10] The right is in the context of territorial waters of a State. The distinction between the internal waters and the territorial water needs to be established. The internal waters of a State constitute "the landward side of the baseline of the territorial sea form part of the internal waters of the State."[11]

The definition of the right of innocent passage is to be found in Article 18 of the United Nations Convention on the Law of the Sea, 1982 which stipulates that:

[10] Shabtai Rosenne, League of Nations Conference for the Codification of International Law, vol 4 (Oceana Publications 1975) 1412.

[11] United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16November 1994) 1833 UNTS 3 (UNCLOS) article 8(1).

"Passage means navigation through the territorial sea for the purpose of: (a) traversing that sea without entering internal waters or calling at a roadstead or port facility outside internal waters; or (b) proceeding to or from internal waters or a call at such roadstead or port facility".[12]

A. Conditions to enjoy the right of innocent passage.

The Convention imposes certain conditions on the passage, namely that it has to be continuous and expeditious, the underwater vehicles must navigate on the surface and show their flag and the activity carried on by the vessel should not be prohibited by the UNCLOS.

1. Continuity.

Due speed is expected from foreign vessels entering the territorial sea of a State, always in accordance with the capacity of the vessel and the navigational conditions and regulations.

The condition of the continuity of the navigational route of the vessel may be overridden only in the case that "anchoring or stopping are incidental to ordinary navigation" as well as when *force majeure* has rendered anchoring or stopping necessary and imperative for the safety of the crew on board.

2. Underwater vehicles must navigate on the surface and show their flag.

Another condition upon which the right of innocent passage lies relates to underwater vehicles and submarines. These vehicles are expected to navigate on the surface and to show their flag according to Article 20. Submerged navigation is considered to be suspicious taking into account the purpose of the submarines to navigate without being detected and collect intelligence; hence the purpose of non-innocence is lost.

However, not complying with this prerequisite will not instantly give rise to the use of force from the part of the coastal State. What is expected to be attempted first is to force the submarine to leave the foreign sovereign territory.

3. Activity should not be prohibited by the UNCLOS.

If the foreign vessel is indulged in an activity which is prohibited under the UNCLOS, then such a vessel cannot demand a right of innocent passage and the coastal state has the right to deny innocent passage to such vessels. For instance, the use of any kind of weapons is strictly prohibited and will remove the right of the vessels to innocent passage.

Article 19 paragraph 2 of UNCLOS enumerates some of the activities which shall be considered to fall outside the scope of the concept of innocent passage. This enumeration is only an indication and thus not exhaustive. This is derived from the wording of the last provision of the

[12] United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16November 1994) 1833 UNTS 3 (UNCLOS) article 18(1).

article which refers to “any other activity not having a direct bearing on passage” which leaves space for acts being subject to subjective interpretation.

However, it is presumed that in cases where the coastal State has doubts regarding the passage of a foreign vessel it shall provide the vessel with the benefit of the doubt and hence a presumption of innocence, by giving it the possibility to make clear what its real intentions are. In this way, unnecessary actions can be avoided.

The coastal state can suspend the right of innocent passage to foreign vessels. Suspension though shall not be discriminatory against foreign ships and shall only be enforced for the sake of the security of the coastal State. Fishing activities, research and survey activities, polluting activities, spying activities are all included in the prohibitive list of UNCLOS. It is estimated that the violation of the scope of Article 19 will *ipso facto* deprive a passage of its innocent character contrary to the violation of the law of the coastal State.

B. Is the right to innocent passage absolute in nature?

Notably, not all parts of the territorial sea may be used for the purposes of innocent passage. The coastal State retains the right to request from foreign vessels to navigate through designated areas (sea lanes and traffic separation schemes). Hence the right is not absolute. When designating the specific areas, the coastal State shall show due respect to the IMO recommendations, the density of the traffic as well as the characteristics of particular ships and channels.

One of the purposes of the UN is “to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace.” UNCLOS could not deviate from the foundational principle of the UN and accordingly provide that innocent passage shall mean the passage which is “not prejudicial to the peace, good order or security of the coastal State.”

However, anything that might deem to endanger the peace and security of the coastal State will be conceived as a hostile activity and will not fall under the concept of “innocent passage”.

II. Passage of Warships: Conceptual discussion

The definition of warships is to be found in Article 29 defines a warship as “a ship belonging to the armed forces of a state bearing the external marks, distinguishing such ships of its nationality, under the command of an officer…”

Following this definition, any vessels belonging to rebel movements and used for warfare are not considered warships.

UNCLOS also secures the immunity of warships but it is quite unclear as to the actions that a coastal State can take against warships which do not comply with its rules and regulations.

A. Do warships enjoy the right of innocent passage?

The international literature is divided on the issue. No explicit, express reference is made in UNCLOS stating that warships fall under the category of those vessels which enjoy the right of innocent passage. Likewise, no explicit provision excludes them from exercising this right. It can be presumed that warships were intended to fall under Article 17 since no distinction was made by the drafters.

The view that since conventional law does not regulate this strongly debated issue, customary international law applies is the most commonly accepted in state practice. Jessup also supported that "as a general principle, the right of innocent passage requires no supporting argument or citation of authority; it is firmly established in international law."

Moreover, it is accepted so far that submarines, which are obliged to navigate on the surface as a prerequisite, are for military services hence they can benefit from the right of innocent passage.

Some states have officially declared that warships indeed enjoy the right of innocent passage such as the United States and the Russian Federation through a bilateral 1989 Uniform Interpretation of Norms of International Law Governing Innocent Passage, as would make sense since both constitute the two biggest naval powers in the world. However, undoubtedly the absence of conclusive conventional provisions has led to different interpretations with regards to the innocent passage of warships.

B. Why are commentators against the right of innocent passage for warships?

Several commentators have been against this privilege for warships due to the simple fact that warships have on board several weapon mechanisms. This is their equipment and "unlike the situation of merchant vessels, in the case of warships there is no commercial interest involved and there may be danger at times to the nation whose waters are being used."

Maritime Security and Military Activities

Maritime security is both multi-dimensional and multifaceted. It involves both military and non-military issues. These include naval threats and challenges (military security issues), arms trafficking and narco terrorism as well as piracy (non-military security issues) along with shipping, fishing, seabed minerals and offshore oil and natural gas resources, vulnerability of sea lanes of communications (SLOCs) and illegal immigration. Moreover maritime security also includes environmental protection, nuclear issues, ballistic missile defense and maritime management as the seas are indivisible.

Furthermore, a general but well-structured definition of terrorism is contained in the International Convention for the Suppression of the Financing of Terrorism: "Any ... act intended to cause death or serious bodily injury to a civilian, or any other person not taking part in hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context,

is to intimidate a population or to compel a government or an international organization to do so or to abstain from doing any act."

From a maritime context, these definitions could be applied to acts of piracy; acts of violence of a general nature not necessarily confined to piracy against a ship, its crew or passengers; acts using a ship as a weapon of destruction against navigational and public safety; acts of sabotage using the high seas or territorial waters of a nation to support and sustain terrorism; using the sea as a platform to launch attacks against States, persons or property; and transport of weapons over the seas for terrorism purposes.

Whilst the 1982 United Nations Convention on the Law of the Sea is concerned with maritime security law, the Convention has had problems coping with contemporary maritime security threats such as terrorism or the proliferation of weapons of mass destruction. Moreover, the Convention also fails to adequately deal with certain maritime security threats that have come to the forefront in the last 30 years, such as crimes against the safety of navigation.

The first modern act of modern maritime terrorism

On January 22, 1961, the Portuguese cruise ship SANTA MARIA was captured by a Portuguese rebel group in the Caribbean Sea off the coast of Venezuela. The goal of the rebels was to protest the brutal dictatorship of Portugal's Antonio Salazar. Sadly, the SANTA MARIA's third mate was killed when the cruise ship was overrun. After the SANTA MARIA was surrounded by vessels of the U.S. Navy and the events became headline news around the world, the rebels surrendered on February 2, 1961, and were granted political asylum in Brazil. If we accept the definition of terrorism as premeditated, "politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine [state] agents,"[13] then this was probably the first modem act of maritime terrorism.

MILITARY ACTIVITIES BEYOND THE TERRITORIAL SEA

I. Military activities in the Exclusive Economic Zone.

As defined by the Treaty, the EEZ "is an area beyond and adjacent to the territorial sea," which "shall not extend beyond 200 nautical miles from the baselines from which the breadth of the territorial sea is measured." It is not a part of the high seas, although high-seas like freedom exist there with respect to navigation. EEZ claims extract approximately 30 to 36 per cent of the world's oceans from waters traditionally considered high seas.

[13] Raphael Perl, Terrorism, the Future, and U.S. Foreign Policy, Congressional Research Service Issue Brief for Congress, Order Code IB95112, at 4 (Apr. 11, 2003), available at

http://www.fas.org/irp/crs/IB95112.pdf (last visited May 13, 2005).

Today, military activities by foreign nations in the Exclusive Economic Zones of other nations are becoming more and more frequent for a number of reasons: the accelerating pace of globalization; the tremendous increase in world trade; the rise in the size and quality of the navies of many nations; and technological advances that allow navies to exploit oceanic areas.

A. Are military activities permitted in the Exclusive Economic Zone?

Along with this increase in military activity has come increasing contention over the scope of rights to military activities within the EEZ. Whether and to what extent high seas freedoms of navigation and associated uses exist for warships and aircraft in the EEZ has been the subject of a fair amount of discussion in academic literature.

Some have argued that it is vague, ambiguous and difficult to conclusively determine just what the UNCLOS means with respect to naval activities in the EEZ. According to one commentator, "The uncertainty [in the Convention] is nowhere so striking as in the area of military uses of the EEZ."[14]

Article 58 states, in part, that "Articles 88 to 115 and other pertinent rules of international law apply to the exclusive economic zone in so far as they are not incompatible with this Part." Article 88 of the Convention states: "The high seas shall be reserved for peaceful purposes." Thus, the interplay of these two Articles reserves the exclusive economic zone, like the high seas, for peaceful purposes. The question then becomes: Does the reservation of the *sui genris* exclusive economic zone for peaceful purposes prohibit previously lawful naval maneuvers and operations in these waters? As to this question, the Convention is silent.

Although it is clear that maritime powers intended and some say it was the "general understanding" of the Convention to permit, as a matter of right, military uses in the exclusive economic zone. But some coastal States persistently objected to that view. Brazil, for example, like the United States, was part of the Casteneda-Vindenes Group. In a declaration made upon signing the Convention, Brazil insisted that "the provisions of the Convention do not authorize other States to carry out military exercises or manoeuvres within the exclusive economic zone, particularly when these activities involve the use of weapons or explosives, without the prior knowledge and consent of the coastal State." Recent Brazilian domestic law implements this view.

Furthermore, these dissenters can argue that the issue of military uses was never formally discussed at the Conference, despite efforts of a number of countries to bring it to the surface. Indeed, it was the United States which foreclosed explicit discussions on "any specific limitation on military activities," arguing that "such a complex task could quickly bring to an end current efforts to negotiate a law of the sea convention." While contending that the term "peaceful

[14] Boleslaw A. Boczek, Peacetime Military Activities in the Exclusive Economic Zone of Third Countries, 19 OCEAN DEV. & INT'L. L. 445, 458 (1988);

purposes" did not preclude military activities generally, the United States suggested "limitations on military activities would require the negotiation of a detailed arms control agreement."

The apparent exclusion of the subject from formal negotiations, combined with the "remarkable" silence of the Convention "on legal questions connected with military uses" ' (a silence that might logically follow from exclusion of the subject in negotiations), render suspect, to some, the conclusion that military uses were intended to be permitted under the Convention regime.

1. Contentions of the commentators in support of the military activities in the Exclusive Economic Zone.

Article 56 of UNCLOS specifically limits coastal State sovereign rights in the EEZ to the seabed, its subsoil and the waters superjacent to the seabed, with one exception—the coastal State also has exclusive rights over the production of energy from the winds. It is pertinent to note here that the coastal State has sovereign rights over the seabed and subsoil but not on the sea itself. Consequently, argument may be formulated that since coastal state do not exercise any sovereign rights over the sea beyond the territorial limits, therefore it cannot regulate or restrict the military activities in the Exclusive Economic Zone.

It is also important to recognize that UNCLOS does place some restraints on military activities at sea. However, none of these limitations apply in the EEZ. Article 19 of the Convention restricts certain military activities in foreign territorial seas for ships engaged in innocent passage, such as threat or use of force, use of weapons, intelligence gathering, acts of propaganda, launching and landing of aircraft and other military devices, military surveys and intentionally interfering with communication systems. Article 52 applies the same limitations to archipelagic waters. Submarines and other underwater vehicles engaged in innocent passage in foreign territorial seas and archipelagic waters must navigate on the surface and show their flag. Articles 39 and 54 prohibit the threat or use of force when ships are engaged in transit passage or Archipelagic Sea Lanes Passage (ASLP), and Articles 40 and 54 prohibit survey activities for ships engaged in transit passage or ASLP. Similar restrictions are not found in Part V of UNCLOS and therefore do not apply to warships, military aircraft and other sovereign immune ships and aircraft operating in or over the EEZ.

Within the EEZ, all States enjoy high seas freedoms of "navigation and overflight . . . laying of submarine cables and pipelines and other internationally lawful uses of the seas related to those freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and which are compatible with the other provisions of the Convention."

These "other internationally lawful uses of the seas" may be undertaken without coastal State notice or consent and include a broad range of military activities such as: intelligence, surveillance and reconnaissance (ISR) operations; military marine data collection and naval oceanographic surveys; war games and military exercises; bunkering and underway replenishment; testing and use of weapons; aircraft carrier flight operations and submarine

operations; acoustic and sonar operations; naval control and protection of shipping; establishment and maintenance of military-related artificial installations; ballistic missile defense operations and ballistic missile test support; maritime interdiction operations (e.g., visit, board, search and seizure); conventional and ballistic missile testing; belligerent rights in naval warfare (e.g., right of visit and search); strategic arms control verification; maritime security operations (e.g., counter-terrorism and counter-proliferation); and sea control.

2. Contentions of the commentators against the military activities in the Exclusive Economic Zone.

Some commentators opine that the Convention explicitly limits warship operation in the EEZ by the obligation to have due regard to the rights and duties of the coastal State.

In its EEZ, the coastal State has certain "sovereign rights" with respect to natural resources, and "jurisdiction" over the establishment and use of artificial islands, installations and structures, over marine scientific research, and over the protection and preservation of the marine environment." These provisions might preclude naval activities that potentially interfere with or harm these coastal State interests. A frequently cited example is that of a weapons exercise, test or placement, such as the use of mines that might potentially harm a natural resource.

One commentator has stated that the Convention may justify a coastal State in "prohibiting a military activity which caused ecological harm."

3. State Practice.

A small number of strategically placed countries interpret the UNCLOS to prohibit naval activities and maneuvers in the EEZ without their prior permission. Eighteen States purport to regulate or prohibit foreign military activities in the EEZ. These States include: Bangladesh, Brazil, Burma (Myanmar), Cape Verde, China, India, Indonesia, Iran, Kenya, Malaysia, Maldives, Mauritius, North Korea, Pakistan, Philippines, Portugal, Thailand, and Uruguay.

Additionally, even though Article 3 of the Convention limits the breadth of the territorial sea to 12 nm, seven coastal States—Benin (200 nm), the Congo (200 nm), Ecuador (200 nm), Liberia (200 nm), Peru (200 nm), Somalia (200 nm) and Togo (30 nm)—claim a territorial sea in excess of 12 nm that also purports to deny or restrict foreign-flagged military activities.

Others, such as Thailand, Italy, Germany, the Netherlands, the United Kingdom, and the United States, disagree.

The **United States** interpretation of the Convention is this:

"All States continue to enjoy in the EEZ, traditional high seas freedoms of navigation and over-flight and tie laying of submarine cables and pipe- lines, and other internationally lawful uses of the sea related to those freedoms, which remain qualitatively and quantitatively the same as those

freedoms when exercised seaward of the zone. Military operations, exercises and activities have always been regarded as internationally lawful uses of the sea. The right to conduct such activities will continue to be enjoyed by all States in the exclusive economic zone."[15]

Internationally lawful uses of the sea related to high seas freedoms of navigation and over flight historically included military operations. The vast weight of authority confirms that this is the proper interpretation. Under this light, the Commander's Handbook states that "Warships and military aircraft enjoy the high seas freedoms of navigation and overflight and other internationally lawful uses of the sea related to those freedoms, in and over the EEZ..."

The United States view of the law is not universally accepted. **Uruguay**, for example, takes the position that the Convention does not explicitly permit the same range of uses associated with warship operation in the EEZ as are permitted on the high seas. **Brazil** has enacted domestic legislation that states: "In the exclusive economic zone, military maneouvres, in particular those involving the use of weapons or explosives, may only be carried out by other States with the consent of the Brazilian Government."

Furthermore, **Iran** flatly prohibited "foreign military activities and practices" within its EEZ. Similarly, **India, Malaysia, and Pakistan** have all made claims that would restrict naval activities in their EEZs without prior permission.

B. What kind of constraints States put on foreign military activities in the Exclusive Economic Zone?

Coastal State constraints on foreign military activities in the EEZ vary from State-to-State and include:

- restrictions on "non-peaceful uses" of the EEZ without consent, such as weapons exercises;
- limitations on military marine data collection (military surveys) and hydrographic surveys without prior notice and/or consent;
- requirements for prior notice and/or consent for transits by nuclear-powered vessels or ships carrying hazardous and dangerous goods, such as oil, chemicals, noxious liquids, and radioactive material;
- limiting warship transits to innocent passage;
- prohibitions on ISR operations (intelligence collection) and photography;

[15] Warren Christopher, United States of America Statement in Right of Reply (Mar. 8, 1983) 17 THIRD CONFERENCE ON THE LAW OF THE SEA, OFFICIAL RECORDS 244, U.N. Sales No. E.83.V.3 (1984) reprinted in ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS (NWP 1-14M/MCWP5-2.1/COMDTPUB 5800.1) at 1- 25, 1-27 to 1-28 (1997).

- requiring warships to place weapons in an inoperative position prior to entering the contiguous zone;
- restrictions on navigation and overflight through the EEZ;
- prohibitions on conducting flight operations (launching and recovery of aircraft) in the contiguous zone;
- requiring submarines to navigate on the surface and show their flag in the contiguous zone;
- requirements for prior permission for warships to enter the contiguous zone or EEZ;
- asserting security jurisdiction in the contiguous zone or EEZ;
- application of domestic environmental laws and regulations; and
- requirements that military and other State aircraft file flight plans prior to transiting the EEZ.

States that purport to limit military marine data collection (surveillance operations and oceanographic surveys) in the EEZ argue that such operations are akin to MSR and are therefore subject to coastal State control. That argument is clearly flawed. Although UNCLOS does not define MSR or hydrographic surveys, the Convention clearly differentiates between MSR, surveys, and military activities in various articles. Hence, intention of the drafters could be discerned regarding differentiation between military marine data collection and MSR.

C. Do military activities in the Exclusive Economic Zone violate the "Peaceful Purpose" provisions of the UNCLOS?

A corollary argument made be some States, including China, is that military activities are inconsistent with the peaceful purposes provision of UNCLOS. Again, this position is not supported by State practice, a plain reading of UNCLOS or other applicable international instruments. Article 301 of the Convention calls on States to "refrain from any threat or use of force against the territorial integrity or political independence of any State …"

The language is identical to text in Article 2(4) of the UN Charter on the prohibition of armed aggression in the relations among States. UNCLOS, however, makes a clear distinction between "threat or use of force" on the one hand, and other military-related activities, on the other. Article 19(2)(a) repeats the language of Article 301, prohibiting ships in innocent passage from engaging in "any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State." The remaining subparagraphs of Article 19(2) restrict other military activities in the territorial sea: (b) any exercise or practice with weapons of any kind; (c) any act aimed at collecting information to the prejudice of the defense or security of the coastal

State; (d) any act of propaganda aimed at affecting the defense or security of the coastal State; (e) the launching, landing or taking on board of any aircraft; (f) the launching, landing or taking on board of any military device; . . . . (j) the carrying out of research or survey activities; k) any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State.

The distinction in Article 19 between "threat or use of force" from other types of military activities clearly demonstrates that UNCLOS does not automatically equate use of force with these other military acts.

The "peaceful purposes" language originally was derived from the text of UN General Assembly Resolution 2749 (1970), which declared that the sea-bed beyond the limits of national jurisdiction was reserved exclusively for peaceful purposes. A group of developing nations proposed that the original version of Article 301 be included in Article 88, which provides that "the high seas shall be reserved for peaceful purposes." That proposal was not adopted, however, and the text was reintroduced separately as a new article. An effort to include the new Article 301 in the EEZ section of the Convention (Part V) was also defeated "by maritime States on the ground that security matters should not be considered within the EEZ regime."

As the negotiations of the Convention continued, some developing States took the position that the text of Articles 88 and 301 would prohibit all military activities in the oceans. Ecuador, for example, argued that "the use of the ocean space for exclusively peaceful purposes must mean complete demilitarization and the exclusion from it of all military activities." Maritime States opposed such a strict interpretation of the "peaceful purposes" language, asserting that the test of whether an activity was considered "peaceful" was determined by the UN Charter and other obligations of international law.

It is logical to interpret the "peaceful purposes" clauses as prohibiting only those activities which are not consistent with the UN Charter. It may be concluded accordingly that the peaceful purposes…clauses in Articles 88 and 301 do not prohibit all military activities on the high seas and in EEZs, but only those that threaten or use force in a manner inconsistent with the UN Charter.[16]

Thus, the determination of whether an activity is "peaceful" is made under Article 2(4) of the UN Charter. Successive U.S. administrations have maintained the position that the "peaceful purposes" provisions can only be read in conjunction with the general body of international law, including Article 2(4) and the inherent right of individual and collective self-defense, as reflected in Article 51 of the UN Charter. To accept that all military activities are, by their nature, inconsistent with the "peaceful purposes," would mean that nations could not operate military

[16] Moritaka Hayashi, Military and Intelligence Gathering Activities in the EEZ: Definition of Key Terms, 29 MARINE POLICY 123–37 (2005).

vessels or aircraft, not just in the EEZ, but also the high seas. Such a conclusion, however, is at odds with decisions of the UN Security Council, which indicate that "military activities consistent with the principles of international law embodied in Article 2(4) and Article 51 of the Charter of the United Nations…are not prohibited by the Convention on the Law of the Sea." The International Court of Justice has similarly ruled that naval maneuvers conducted by the United States from 1982 to 1985 off the coast of Nicaragua during the U.S.-backed counter-revolution against the Sandinista government did not constitute a threat or use of force against Nicaragua.

Also, the Security Council has likewise determined that peacetime intelligence collection is not considered a "threat or use of force against the sovereignty, territorial integrity or political independence of the coastal state…in violation of the Charter of the United Nations." Following the shoot down of an American U-2 spy plane near Sverdlovsk in1960, an effort by the Soviet Union to have a Security Council resolution adopted that would have labelled the U-2 flights as "acts of aggression" under the Charter failed by a vote of 7 to 2 (with 2 abstentions), thereby confirming that peacetime intelligence collection is consistent with the UN Charter.64 The San Remo Manual on the Law of Armed Conflicts at Sea similarly rejects the interpretation that all military activities are inconsistent with the "peaceful purposes" provisions of the Convention. According to the Manual, armed conflict at sea can take place on the high seas, as well as in the EEZ of a neutral State. The only limitation is that belligerents must "have due regard for the resource rights and duties of the coastal State" in the EEZ.

D. What are the remedies available to the coastal State if it is of the view that the foreign vessel is carrying out a non-peaceful activity or a prohibited activity?

Even if the coastal State is of the opinion that the foreign vessel in its territorial waters is carrying out a non-peaceful activity or a prohibited activity under the UNCLOS, it does not ipso facto gives it the right to use force against the vessel. The only explicit action is to "require it to leave its territorial waters".

It should be noted that the responsibility of the flag state for the reimbursement of any damage caused by the non-compliance is also unambiguous under UNCLOS.

E. North Korea's Military Zone.

North Korea has one of the most expansive and illegal claims in the EEZ. On August 1, 1977, North Korea announced that it was establishing a "military zone"—"50 miles from the starting line of the territorial waters in the East Sea and to the boundary line of the economic sea zone in the West Sea." The zone was purportedly established to safeguard the North Korean EEZ and defend the "nation's interests and sovereignty." Foreign military ships and aircraft are prohibited from entering the zone, and "civilian ships and civilian planes (excluding fishing boats) are allowed to navigate or fly only with appropriate prior agreement or approval." Civilian ships and aircraft that have been granted access to the zone may not, however, engage in "acts for military

purposes or acts infringing upon the economic interests." Taking photographs and collecting marine data is also strictly prohibited.

In effect, North Korea treats the waters and airspace contained within the military zone as internal waters and national airspace, respectively. Such a claim is clearly inconsistent with UNCLOS, Parts II (territorial sea and contiguous zone), III (EEZ), and VII (high seas), as well as the Chicago Convention, Articles 1–3 and 9.

II. Military activities on the high seas.

According to Article 88 of the UNCLOS, the high seas shall be reserved for peaceful purposes. Additionally, Article 301 provides that States Parties shall refrain from any threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the principles of international law embodied in the Charter of the United Nations. The question is often raised as to whether such provisions limit military activities on the high seas.

It is important to understand as to whether and to what extent the provisions of the UNCLOS, and in particular Article 88, restrict military activities on the high seas.

The "peaceful purposes" provision has also been used in other multinational treaties. Based upon those multilateral treaties, the position is often put forward that the peaceful use clause in the LOS Convention has to be understood generally as a prohibition of any military activity.

The terms "peaceful use" or "for peaceful purposes" as used in international conventions are, in general, highly ambiguous, leaving aside for the moment the fact that Article 301 of the UNCLOS has to be regarded as an attempt to clarify the meaning of this clause.

The peaceful use clause may be interpreted as a prohibition of any military activities, or of only aggressive activities in the sense of Article 2, paragraph 4, of the United Nations Charter. A clear interpretation of this term in the former sense is found, for example, in the Antarctic Treaty. It preserves a non-militarized status of Antarctica by prescribing in Article I that the continent be used for peaceful purposes only. This general clause is further specified by the Article's prohibition (the list not being exhaustive) of "any measure of a military nature, such as the establishment of military bases and fortifications, the carrying out of military maneuvers, as well as the testing of any type of weapons." As an exemption from the general provision, the Article allows the use of military personnel and equipment "for scientific research or for any other peaceful purpose." This exemption proves that the peaceful purposes clause in the Antarctic Treaty has to be understood as excluding all military activities.

Having referred to those international treaties using the phrase "peaceful" in the sense of nonmilitary, one should mention the Outer Space Treaty as a counter-example, one where the same clause has been used in the meaning of "non-aggressive." This interpretation, however, is

not undisputed. There is a clear difference of opinion among states regarding the correct interpretation of the term “peaceful” as used in Article IV of the Outer Space Treaty. Some refer it to have the same meaning as “non-aggressive” and some refer it to have the same meaning as “non-military.”

Hence, the way the peaceful use clause is used in other international treaties does not give a clear answer as to its meaning under the UNCLOS.

Therefore, full clarity on the exact content of the peaceful use clause can be achieved by evaluating the impact of Article 301 of the UNCLOS on the interpretation of Article 88. The legislative history of Article 301 again casts very little light on the intentions of its drafters.

Article 301 is clearly modeled along the lines of Article 2, paragraph 4 of the UN Charter. Apart from differences that are clearly of a drafting nature, one distinction has to be stated. Instead of the term “or in any manner inconsistent with the purposes of the United Nations,” Article 301 uses the phrase "or in any other manner inconsistent with the principles of international law embodied in the Charter of the United Nations.” This difference highlights that Article 301 refers not only to Chapter I of the UN Charter (Purposes and Principles) but to other parts too, such as Chapter VII, which includes Article 51 (right of self-defense).

In conclusion, Article 88, considered in the light of Article 301, does not impose any obligations upon States exceeding those of Article 2, paragraph 4, of the UN Charter.

A. Legality of establishment of marine exclusion zones.

Whether a party to a conflict may establish maritime zones of war or zones of exclusion from which shipping is totally or partially excluded, thus limiting freedom of navigation and overflight.

Some instances of establishment of marine exclusion zones on high seas:

- The system of maritime exclusion zones was first introduced in the Russo-Japanese War by Japan, in an effort to control the navigation of neutral Powers in specified areas.
- In the First World War, the United Kingdom proclaimed the North Sea to be a military area within which exceptional measures would be taken.
- In the Second World War, the United Kingdom declared exclusion zones, which were effected by means of mine fields.
- In 1915 Germany declared that all maritime spaces surrounding the British Isles constituted a war zone in which any enemy merchant vessel would be sunk by submarines, even if it was not possible to save the crew or passengers. The exclusion zones declared by Germany were of a different nature; in these all shipping would be

attacked on sight. The International Military Tribunal of Nuremberg declared the establishment of the latter zones to constitute a war crime.

- More recent examples of the establishment of war zones were the two proclamations of the United Kingdom in 1982 establishing a "maritime exclusion zone" around the Falkland Islands, which had been occupied by Argentine forces.

It is worth considering whether the UNCLOS limits the establishment of exclusion zones beyond existing restrictions recognized under the international law of war.

Pursuant to Article 88, paragraph 1, of the UNCLOS, the ships of all States (not only of States Parties) enjoy the right of freedom of navigation. However, the right to freedom of navigation is not unrestricted. It is to be used with due regard to the interests of other States in their exercise of the freedom of the high seas, which includes respect for military activities. Even in times of war, the freedom of navigation cannot be regarded as suspended between States which are not parties to the conflict. Accordingly, the establishment of exclusion zones is restricted. The freedom of navigation requires that limitations imposed upon shipping by the establishment of exclusion zones-and the same applies to overflight-have to be kept to the minimum necessary. Neither the limitations imposed upon shipping in these zones (nor their duration) nor the rights of military ships therein may exceed what is strictly necessary (principle of necessity and proportionality) for the protection of the security of the party to the conflict having established the zone. In consequence thereof, the range of military activities is limited, and they may not be directed indiscriminately against military and nonmilitary targets. Only under such preconditions and with proper notification may one characterize marine exclusion zones as a valid limitation on the freedom of navigation and overflight.

B. Legality of emplacing of sea mines.

Mines have frequently been used as a means of sea warfare, and although they are considered indispensable, attempts have been made to restrict their use. In this respect, one should refer to the 1907 Hague Convention on Mine Warfare at Sea (which, however, has not entered into force).

The **International Court of Justice** has dealt with the emplacement of sea mines twice. In the **Corfu Channel** Case, it stated:

“The obligation incumbent upon the Albanian authorities consisted in notifying, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in warning the approaching British warships of the imminent danger to which the minefields exposed them. Such obligations are based, not on the Hague Convention of 1907, No. VIII, which is applicable in time of war, but on certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war, the principle of the

freedom of maritime communication; and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."

In the **Nicaragua** Case, it argued along the same lines:

"In peacetime for one State to lay mines in the internal or territorial waters of another is an unlawful act; but in addition, if a State lays mines in any waters whatever in which the vessels of another States have rights of access or passage, and fails to give any warning or notification whatsoever, in disregard of the security of peaceful shipping, it commits a breach of the principles of humanitarian law underlying the specific provisions of Convention No. VIII of 1907."

The State emplacing sea mines is faced with obligations to safeguard the interests and rights of third States, was confirmed by Judge Schwebel in his Dissenting Opinion in the **Nicaragua** Case.[17]

The interests and rights of third States in the maintenance of the freedom of navigation have to be balanced against the security interests of the belligerent parties. The principle of the freedom of navigation requires that the emplacement of minefields meets the conditions of the principles of necessity and proportionality. Minefields must not amount to a blockage of navigation to and from ports of nonbelligerent States, the national occupation of areas of the sea, or the unnecessary abolishment of the freedom of navigation for ships of non-belligerent States.

Generally speaking, States emplacing minefields are under an obligation to take every precaution to secure the safety of shipping of nonbelligerent States. Only to the extent that the emplacement of mines leaves room for a safe passage of ships of nonbelligerent States, the minefields are appropriately published, and the fields are kept under permanent surveillance and meet the applicable international rules on marine warfare may the resulting restrictions on the freedom of navigation be justified.

Sea mines may result in a negative change of the marine environment to the extent that they constitute a hindrance to marine activities in the respective area. In this context, note should be taken of the fact that Article 192 of the UNCLOS obliges all States to protect and to preserve the marine environment. Might this obligate States concerned to remove sea mines? This possibility deserves further consideration.

C. Legality of nuclear tests.

The question of the legality of the nuclear tests on the high seas is now decades old. At the very outset two questions emerge. First, are nuclear tests explosions on the high seas illegal? Second,

[17] 1986 I.C.J. 266, 368.

if so, what amount of international liability attaches to a state engaging in such nuclear experimentation?

This question of legality of nuclear tests on the high seas arose when the America tested hydrogen bombs in the “Pacific Proving Grounds.”

Two schools of thought emerged. It was argued by some that the test explosions were contrary to the laws of humanity and to the law of nations. Others, however, sought to justify the tests as necessary steps in the defense of the “free world.”

This question was also referred to the International Court of Justice in the Nuclear Tests Cases. The complaint was made by Australia, New Zealand and the Republic of Fiji, against France, for the latter's nuclear testing over the Pacific Ocean.

Specifically, the legality of nuclear test explosions on the high seas turns upon three principal issues: (1) whether such testing may be deemed in violation of the freedom of the high seas; (2) whether the proven adverse ecological effects of such testing render it violative of international customary and conventional anti-pollution law; and (3) whether such testing is currently proscribed by multilateral nonproliferation treaties and other legal instruments for international disarmament.

Article 2 of the 1958 Convention made “the high seas open to all nations” and declared that “no state may validly purport to subject any part of them to its sovereignty.” The high seas freedoms, enjoyment of which is made expressly subject to conventional and other rules of international law, comprise, inter alia: freedom of navigation, freedom of fishing, freedom to lay submarine cables and pipelines, and freedom of overflight.

Nuclear test explosions on the high seas violate the doctrine of the freedom of the high seas, inasmuch as they interfere with two of its most crucial incidents: the freedoms of navigation and of fishing.

Furthermore, article 2 of the 1958 Convention makes it clear that any other right within its scope “shall be exercised by all states with reasonable regard to the interests of other states in their exercise of the freedom of the high seas.” As nuclear test explosions can only proceed safely after excluding totally other users of the seas, they can hardly be accorded the character of reasonable use.

MODULE-III

INTELLIGENCE GATHERING & INFORMATION SHARING

MARITIME DOMAIN AREA AWARENESS

A. Maritime Domain Awareness as a Form of Intelligence.

The first step in considering the role of intelligence in maritime security law enforcement operations is, obviously enough, to consider what is meant by intelligence. Here, Colby's observations remain helpful:

"There are no limits to the types and sources of information which may be useful. The processing of intelligence refers to the treatment accorded the raw data which has been collected. It generally includes appraisal of the relevance of the information, as well as editing and cataloguing in forms useful to decision-makers. These tasks vary enormously in complexity, depending in large measure on the amount and quality of data requested and actually collected."[18]

One topic considered in passing in this article will be the sharing of information between intelligence and law enforcement agencies. However, while such information may-and sometimes does-play a role in real cases where maritime law enforcement action is taken, it is obviously not the only or even necessarily the best source of actionable intelligence in maritime law enforcement. A critical concept remains maritime domain awareness (MDA). The International Maritime Organization (IMO) definition of MDA is "the effective understanding of any activity associated with the maritime environment that could impact upon…security, safety, economy or the environment."

This definition appears to draw heavily on the wording of the 2004 U.S. Maritime Security Policy directive. While MDA is originally a U.S. concept, Australia, Canada, the European Union and the Philippines (among others) all have MDA policies." MDA is basically about knowing who is doing what, where. A simple example is provided by Seychelles efforts to secure their exclusive economic zone (EEZ) (formidably large compared to their land territory) against piracy. By fitting all Seychellois fishing vessels with automatic identification systems, and improving radar coverage across their EEZ, the Seychellois Coast Guard was able to identify vessels in its EEZ that were not Seychellois fishing vessels and send one of its limited number of cutters to investigate and verify that the vessel was not a threat. However, MDA is not always this simple.

B. Maritime Domain Awareness and International Law

While MDA is a simple enough concept, delivering it in a manner consistent with international law is not free from difficulty. First, there may be questions regarding the intelligence uses to which information gathered in maritime law enforcement operations may be put. Second, States

[18] Jonathan E. Colby, The Devloping International Law on Gathering and Sharing Security Intelligence, 1 YALE STUDIES IN WORLD PUBLIC ORDER 49, 53 (1974) (quoted in NATALIE KLEIN, MARITIME SECURITY AND THE LAW OF THE SEA 211 (2012)).

may desire information about vessels transiting off their coasts that they have no obvious power to demand under the UN Convention on the Law of the Sea (UNCLOS) absent further international cooperative mechanisms being established.

As a key example of the latter, in 2004 Australia declared its intention to create a 1,000 nautical mile (nm) "Maritime Information Zone" within which it proposed that any passing vessel would be "required to provide details of cargo, destination, crew, port of call, [and] likely arrival [time] at port." The Australian Prime Minister was further reported as saying the Defence Force "will be able to intercept and board ships and do 'whatever it takes' to get the information they need."" Though clearly able to make the provision of such information a condition of entry for vessels intending to enter an Australian port, Australia had no obvious authority to demand such information from vessels merely transiting within 1,000 nm, let alone intercept them using defense personnel to demand information. In addition, the Australian government declared an intention "to identify all vessels, other than day recreational boats" upon their entry to its EEZ." Within months protests from Indonesia and New Zealand saw Australia rebrand its initiative the "Australian Maritime Information System" and stress that information would be sought from shipping on "a wholly voluntary basis" underpinned by "cooperative international arrangements.""

Unsurprisingly, Australia was already actively involved in efforts to establish a cooperative international system for greater exchange of shipping information at the IMO. In 2006 after four years of work, and in an initiative largely spearheaded by the United States and the United Kingdom, the IMO Maritime Safety Committee reached agreement on a long-range identification and tracking (LRIT) system, to be implemented as Regulation 19-1 of the International Convention for the Safety of Life at Sea (SOLAS). Its implementation under SOLAS obviously has the effect of making it binding on SOLAS State parties through the tacit acceptance procedure. The regulation entered into force in July 2009. The LRIT system's essential features are as follows:

- Vessels covered by the regulation must automatically transmit every six hours the ship's identity, position (expressed in latitude and longitude) and "the date and time of the position provided;

- all covered vessels "must transmit ... LRIT data to the data centre nominated by its flag State" and the LRIT regulations “allow flag States to receive LRIT information from ships flying their flag” wherever they are worldwide and

- contracting SOLAS governments must “elect either to create a National LRIT Data Centre, or participate in a Regional or Cooperative [LRIT] Data Centre.”

LRIT Data Centres may request information of each other through the International Data Exchange. Using this mechanism, port States are "entitled to receive [LRIT] information about ships which have indicated their intention to enter a port facility . . . or a place under the

jurisdiction of that [State], irrespective of where such ships [are] . . . provided they are not located" within another SOLAS party's internal waters. Correspondingly, a coastal State is "entitled to receive [LRIT] information about ships…navigating within... 1,000 nautical miles of its coast provided such ships are not located" within another SOLAS party's internal waters.

Thus, despite the skepticism with which the Australian Maritime Information Zone proposal was initially received; the final LRIT system strongly resembles what Australia had proposed. Nor was Australia alone in seeking information about vessels transiting waters off its coasts. During IMO negotiations in 2005, the United States suggested coastal States should be able to request LRIT information about vessels within 2,000 nm of their coasts. The following year, Norway suggested 1,200 nm.

As at 9 March 2012, 97 out of 161 parties to the International Convention for the Safety of Life at Sea were part of the system and 66 data centres for long-range identification and tracking of ships were connected to the Exchange.

Nonetheless, as an MDA tool the LRIT system is far from perfect. It contains rather "pedantic" restrictions on the ability to request information about ships present within another State party's baselines. More problematically it permits flag States to opt out entirely from providing information where requests are made on security grounds." Another weakness of the system is that it applies only to passenger ships, cargo ships of at least 300 gross tons and mobile offshore drilling units." It therefore does not apply to cargo ships under 300 tons nor to fishing vessels or small privately-owned recreational craft. It is precisely such small vessels that pose the greater security threat: "While safety, security, and stewardship regimes are increasingly being developed for larger vessels on the sea, many smaller vessels, including most fishing vessels, tugs, and recreational vessels, are not covered by these regimes and remain largely anonymous."

As the U.S. Department of Homeland Security has noted, “Small vessels are. . . readily vulnerable to potential exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, aliens, and other contraband, and other criminals.” Small vessels have also been successfully employed overseas by terrorists to deliver Waterborne Improvised Explosive Devices (WBIEDs). Further, the scale of the challenge posed by small boats is immense, as the United States alone has “nearly 13 million registered ... recreational vessels, 82,000fishingvessels, and 100,000 other commercial small vessels.” LRIT information will thus be of no use in relation to the frequent use of small boats for smuggling (especially of drugs and migrants) and the increasing use of fishing vessels in transnational organized criminal activity. Terrorist organizations may also use small boats in attacks on land targets, as was the case for some of the terrorists involved in the 2008 Mumbai attacks.

Intelligence Gathering as a Military Activity

States routinely engage in intelligence activities, as generally understood to mean gathering information for national security, military, or police purposes, often in a covert manner and with

questionable effectiveness of legislative attention and control. Yet even acts that receive legislative approval may be unlawful. In international relations certain rules and restrictions cannot be set aside. Even if governments tend to portray situations as emergencies and emphasize the need to take extralegal measures in "ticking time-bomb" scenarios, serious breaches of law must have legal consequences in the interest of public welfare and the protection of individual victims.

Military intelligence is a military discipline that uses information collection and analysis approaches to provide guidance and direction to assist commanders in their decisions. This aim is achieved by providing an assessment of data from a range of sources, directed towards the commanders' mission requirements or responding to questions as part of operational or campaign planning. To provide an analysis, the commander's information requirements are first identified, which are then incorporated into intelligence collection, analysis, and dissemination.

Intelligence activities are conducted at all levels, from tactical to strategic, in peacetime, the period of transition to war, and during a war itself. Most governments maintain a military intelligence capability to provide analytical and information collection personnel in both specialist units and from other arms and services. The military and civilian intelligence capabilities collaborate to inform the spectrum of political and military activities.

I. INTELLIGENCE GATHERING IN INTERNATIONAL LAW

As Jonathan Colby wrote in 1974,

"There are no limits to the types and sources of information which may be useful. The processing of intelligence refers to the treatment accorded the raw data which has been collected. It generally includes appraisal of the relevance of the information, as well as editing and cataloguing in forms useful to decision-makers. These tasks vary enormously in complexity, depending in large measure on the amount and quality of data requested and actually collected."[19]

The task of intelligence gathering is particularly challenging in the marine environment, not only due to the vastness of the oceans, but also because of the diverse legal nature of the maritime zones. As for the methods employed, they vary, inevitably following relevant technological advancements. In an earlier era, Roach and Smith noted, "military surveys can include oceanographic, marine geological, geophysical, chemical, biological and acoustic data. Equipment used can include fathometers, swath bottom mappers, side scan sonars, bottom grab and coring systems, current meters and profilers." Today, they may involve surface vessels and

[19] Jonathan E. Colby, The Developing International Law on Gathering and Sharing Security Intelligence, 1 YALE STUDIES IN WORLD PUBLIC ORDER 49, 53 (1974).

submarines, as well as remotely operated vehicles, autonomous underwater vehicles (AUVs), seabed landers and even satellites and other earth observation systems, such as radars.

With respect to the legal regime governing intelligence gathering, Natalie Klein rightly posits, "Laws relating to the collection and dissemination of information as a matter of international law come from a range of sources and this remains true in the law of the sea more specifically."[20] Indeed, as Dieter Fleck has written, "intelligence activities as such may not be wrongful under present international law, but the wrongfulness may derive from additional conditions, such as illegal intervention, breach of foreign sovereignty, or common crimes committed in the course of espionage acts."[21]

Under the law of the sea, intelligence gathering may violate coastal State rights over the territorial sea, since it is presumed to be non-innocent passage as set forth in Article 19(2)(c)." However, intelligence gathering within the EEZ may qualify as a legal activity under the freedom of the high seas preserved in Article 87. The lawfulness of the act will depend on the nature of the intelligence gathering itself and the context in which it takes place. When it comes to where States are permitted to engage in intelligence gathering, the most controversial maritime zone is the EEZ, as demonstrated by the considerable legal literature addressing this topic.

Further, many of the international incidents concerning intelligence gathering, such as those involving the USNS Impeccable and a U.S. Navy EP-3 aircraft, had occurred in the EEZ.

It is true that some intelligence gathering activities bear a close resemblance to marine scientific research (MSR), which is largely regulated by the Law of the Sea Convention, even though it does not define MSR. As Sam Bateman notes,

"There is a tendency in practice to use the term "marine scientific research" loosely when referring to all kinds of data collection (research) conducted at sea. However, not all data collection conducted at sea necessarily comes within the scope of the marine scientific research regime established by Part XIII of UNCLOS.[22]

Bateman persuasively argues that a distinction should be made between marine scientific research and hydrographic survey and military survey activities. Major maritime powers, such as the United States and Australia, adhere to this distinction, while the United Kingdom astutely posits that "while the means of data collection used in MDG [military data gathering] may sometimes be the same as that used in Marine Scientific Research (MSR), information from such activities, regardless of the security classification, is intended primarily for military use and is not released to the scientific community." Without further dwelling upon this controversial issue,

[20] NATALIE KLEIN, MARITIME SECURITY AND THE LAW OF THE SEA 211 (2011).
[21] Dieter Fleck, Individual and State Responsibility for Intelligence Gathering, 28 MICHIGAN JOURNAL OF INTERNATIONAL LAW 687, 707 (2007).
[22] Sam Bateman, Hydrographic Surveying in the EEZ: Differences and Overlaps with Marine Scientific Research, 29 MARINE POLICY 163, 164 (2005).

this position, that the distinction between MSR and MDG lies in the application of the data, and not in the process of the data gathering itself, appears to be on a firm legal ground. Moreover, this position aligns with the overall tenor of the Convention not to include military matters within its regulatory scope.

II. WHEN IS INTELLIGENCE GATHERING ILLEGAL?

No general norm exists in international law expressly prohibiting or limiting acts of intelligence gathering. On the contrary, even in the case of espionage-a "consciously deceitful collection of information, ordered by a government.., accomplished by humans unauthorized by the target to do the collection" 2-spies receive a certain minimum protection under the law of armed conflict. The 1907 Hague Regulations Respecting the Laws and Customs of War on Land confirm that the employment of measures necessary for obtaining information about the enemy is generally permissible. Belligerent espionage is not a violation of the laws of war. For purposes of national punishment, a person can only be considered a spy "when, acting clandestinely or on false pretences, he obtains or endeavors to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party."

The Regulations expressly require trials before punishment, and they even exclude criminal prosecution for previous acts of espionage of spies who, after rejoining the army to which they belong, are subsequently captured by the enemy. The 1977 Protocol Additional to the Geneva Conventions and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I) reaffirms these principles and extends them to residents of occupied territory.

Yet acts of intelligence gathering committed by civilians in an armed conflict during a concrete and coordinated military operation would not be protected by the laws of war and would be objects of legitimate attack, if these civilians' actions amounted to direct participation in hostilities. This applies, for instance, to transmission of tactical intelligence to attacking forces or instruction and assistance given to troops with regard to the execution of a concrete military operation. Conversely, activities that may support the conduct of hostilities but fall short of participation in a concrete and coordinated military operation would not deprive these civilians of legal protection against attack.

The late Richard Baxter provides the classical answer to the question of whether espionage is legally, or at least morally or politically, prohibited. He states there is "virtual unanimity of opinion that while the morality of espionage may vary from case to case, some, and probably all, spies in an armed conflict do not violate international law. A distinction may, of course, be made with respect to espionage other than in time of war, for such conduct is of doubtful compatibility with the requirements of law governing the peaceful intercourse of states." The fact that no explicit treaty norms address peacetime espionage is paradoxical in light of the enormous amount of intelligence activities and their relevance for international relations between states.

The question of the legality of peacetime espionage has no easy answer. In the recent past, many arguments for the legality of certain acts of intelligence gathering arose in the context of East-West confrontation during the Cold War, for instance outside an armed conflict when peaceful cooperation was largely unrealistic. Today, such arguments are not altogether unattractive. Yet in the present world of complex interdependencies, another approach should be taken. Strict adherence to the dichotomy between war and peace would be ineffective and counterproductive for establishing peace and security. Also, the revolution in the transparent flow of information during recent decades has diminished the relevance of covert action and clandestine methods to the security intelligence function. Secret sources today are in constant competition with publicly available information, and they are often less reliable.

The need to improve the effectiveness of intelligence gathering given existing terrorist threats has led to increased international cooperation under increasingly transparent procedures." At the same time, the need to augment professional support for better intelligence evaluation is evident.

Where states have restructured national intelligence services in the course of such activities, the transparency requirements of national courts raise difficult questions.

Seen in this context, covert operations might pose more problems than solutions. Furthermore, intelligence operations have revealed new areas in which the law appears inadequate. Activities that fall within the category of "information warfare"-such as spreading false information or even sabotaging computer networks-are one example. Some even claim such activities change the rules governing military operations in armed conflict and also affect international relations in peacetime.

The International Court of Justice (ICJ) has not taken a position on the issue of peacetime espionage, although it has had the opportunity to do so on a few occasions. In the **Teheran Hostages case** the Iranian Foreign Minister referred to alleged espionage and interference in Iran by the United States in its embassy in Teheran. The Court did not accept this as a justification for Iran's conduct, and thus it failed as a defense to the United States' claims “because diplomatic law itself provides the necessary means of defense against, and sanction for, illicit activities by members of diplomatic or consular missions.” As the Court explained, "means" under diplomatic law could include "that a diplomatic agent caught in the act of committing an assault or other offence" may, “on occasion, be briefly arrested by the police of the receiving State in order to prevent the commission of the particular crime.” Problematic for Iran was that it “did not ... employ the remedies placed at its disposal by diplomatic law.”

In the **Nicaragua case**, close logistics, intelligence, and material support by the United States to the contras was central to the Nicaraguan claims. The Court drew attention to the Friendly Relations Declaration, which mandates that "no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the r6gime of another State, or interfere in civil strife of another State. It even emphasized the

importance of this declaration and the fact that the United States actively supported its development and adoption. The judgment of the Court, however, concentrated on the threat or use of force as well as on violations of international humanitarian law, and it did not endorse Nicaragua's view of subversive activities by the United States as indirect means of coercion and intimidation.

Legal scholars often take a fatalist position on the phenomenon of intelligence gathering. They mostly conclude that covert action must be taken for granted. Some even try to deny state responsibility in this context, relying on the fact that spies are not official agents of states for the purpose of international relations, and indeed, if they are caught abroad, the capturing state can severely punish and expel them. This denial of state responsibility may meet realistic expectations in an imperfect world, as a spy is concealing his or her activity as an agent of a state. Yet peacetime rules of international law may be seen as including an implicit prohibition on subversive activities, as reflected in the Friendly Relations Declaration. Such an understanding may be based on the principle of nonintervention in the political independence of any other state and its internal affairs, which includes a prohibition on "indirect or subversive intervention involving secret activity," if "a jungle world which places a premium on skills in subversion, infiltration, espionage, guerrilla warfare, nibbling aggression, and other forms of intervention" is to be avoided. The illegality of covert action may also have other bases, such as unauthorized entry into a foreign state's airspace or territory, illegal exercise of jurisdiction on foreign territory, attempts to destabilize the government of another state," and common crimes, such as bribery, blackmail, unlawful entry into residences, or a breach of data protection laws committed in the course of such acts. Such activities can never be justified under customary law because they are gross violations of commonly accepted legal principles. The fact that they are committed through clandestine action offers a strong argument against the existence of any alleged opinio juris covering such conduct in international relations between states. Hence it is unacceptable to conclude, as many have, that legal arguments can neither condemn nor justify covert action in peacetime. The opposite is true, and among the various legal disciplines involved in any thorough assessment, international law has an important role to play. Legal arguments may not only support prohibitions or limitations of certain activities of intelligence gathering, they may also advocate for self-restraint in the interest of confidence-building and stable peace.

As many covert acts have a human rights dimension, they may be illegal under the 1966 International Covenant on Civil and Political Rights or regional human rights conventions. Intelligence agencies do not take this aspect seriously enough. They often consider it sufficient to balance human rights violations against the positive intelligence their agents supply or will likely supply. Yet human rights instruments are of particular political and forensic significance. Extraordinary rendition for human intelligence gathering is a case in point, as the forced transfer of people for the purpose of conducting interrogation has often proven counterproductive and it frequently raises the concerns of human rights bodies, civil society, states, and international organizations. It must also be considered that intelligence objectives do not justify the derogation

of human rights. While it may be doubtful whether states involved in espionage activities themselves could convincingly support a legal prohibition on espionage by other states under the equitable principle of "clean hands," the situation is different in the case of human rights violations. Here, the owner of the right is not the state but the individual victim, and the state has an obligation to protect its citizens.

Special treaty regimes may contain specific restrictions for intelligence gathering. In this context, disputed commitments on the use of outer space for exclusively peaceful purposes, different interpretations of the exact meaning of innocent passage through the territorial sea of a foreign coastal state, and certain voluntary restrictions as part of regional confidence and security building measures could provide elements for further legal development. Where such specific restrictions apply, they may be of continued relevance in the event of an armed conflict.

In this respect, the current work of the International Law Commission can be expected to offer new insight and widely acceptable results, so that Articles 24 and 29 through 31 of the Hague Regulations and Article 46 of Additional Protocol II may not be the last word for regulating relevant activities in armed conflicts. This is of practical significance for the application of human rights obligations of a state conducting military operations in situations where it exercises jurisdiction. It is particularly relevant for peace operations that include elements of peace enforcement and must apply international humanitarian law.

III. INTELLIGENCE GATHERING IN THE EXCLUSIVE ECONOMIC ZONE.

One of the most controversial questions arising from the adoption of the United Nations Convention on the Law of the Sea' is whether the coastal State can control the gathering of intelligence by other States within its exclusive economic zone. Many scholars have attempted to answer this question.[23] Currently, the majority position is that "such intelligence-gathering activities by foreign States in the coastal State's EEZ are exercises of the freedom of navigation and are not subject to the coastal State's jurisdiction.'" However, in the absence of an authoritative judicial ruling on the matter, and with numerous States, including China,' fervently challenging this position, this issue remains very much contested.

Equally important is the question of whether a coastal State may interfere with the navigational and overflight rights of other States in the EEZ in the course of intelligence gathering for maritime security purposes. As Klein observes, "a critical element to protecting maritime security is ensuring that states have the necessary information at their disposal to take

[23] See, e.g., Mark J. Valencia, Introduction: Military and Intelligence Gathering Activities in the Exclusive Economic Zones: Consensus and Disagreement II, 29 MARINE POLICY 97 (2005); Moritaka Hayashi, Military and Intelligence Gathering Activities in the EEZ: Definition of Key Terms, 29 MARINE POLICY 123 (2005); Stuart Kaye, Freedom of Navigation, Surveillance and Security: Legal Issues Surrounding the Collection of Intelligence from beyond the Littoral, 24 AUSTRALIAN YEARBOOK OF INTERNATIONAL LAW 93 (2005); Jon M. Van Dyke, Military Ships and Planes Operating in the Exclusive Economic Zone of Another Country, 28 MARINE POLICY 29 (2004); Desmond Ball, Intelligence Collection Operations and EEZs: The Implications of New Technology, 32 MARINE POLICY 67 (2008).

preventative or responsive action."[24] Threats to maritime security include a host of activities pertaining not only to national security, but, increasingly, also to transnational organized crime at sea. In that regard, it is sufficient to note that the UN Secretary-General in his 2008 Report on Oceans and the Law of the Sea identified seven specific "threats to maritime security," all of which may involve criminal organizations.

Therefore, it comes as no surprise that the need for intelligence gathering beyond the littoral ranks high in the maritime security policy of many coastal States. For example, one of the main U.S. policy initiatives in relation to intelligence gathering since 9/11 has been the creation of maritime domain awareness (MDA) system, which seeks to generate and use information concerning vessels, crews and cargos. According to the U.S. National Plan to Achieve Maritime Domain Awareness, "MDA is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the US." To this end, the United States indicates MDA should include the institution of worldwide standards for broadcasts of vessel position and identification and automated tools to discern patterns of suspicious behavior and potential security threats.

Other States and regional organizations have developed their own strategies in handling information on maritime security. Australia and New Zealand, in light of the large expanses of their EEZs and search and rescue regions, have adopted similar MDA policies. Further, on December 14, 2004, Australian Prime Minister John Howard promulgated the Maritime Identification Zone (MIZ) as part of Australia's effort to strengthen its offshore maritime security." The creation of this zone, which extended one thousand nautical miles from Australia's coastline, was to enable Australian authorities to identify vessels, including their crew, cargo and journey, seeking to enter Australian ports. The air defense identification zones, maintained by the United States and other nations, serve a similar purpose. In the U.S. example, this zone can extend three hundred miles out to sea in some places and requires both civilian and military aircraft to identify themselves and to follow the directions of U.S. authorities.

IV. INTELLIGENCE GATHERING BY COASTAL STATES

The importance of intelligence gathering is evident in both law enforcement efforts and military operations, and recent developments to enhancing maritime security is replete with mechanisms of information gathering and sharing. Maritime domain awareness policies, the designation of maritime or aerial identification zones and the use of satellite systems to track and monitor vessels share the same purpose-to increase awareness of the marine environment and any activity therein that may amount to a threat to the security of the coastal State. This is especially true for coastal States operating in their EEZs given the economic considerations and contiguity with the territorial sea. As such, this Part examines unilateral and multilateral efforts to improve the collection of information in relation to the movement of ships. In particular, it focuses on

[24] NATALIE KLEIN, MARITIME SECURITY AND THE LAW OF THE SEA 211 (2011).

maritime identification zones, such as the Australian Maritime Identification System and various satellite-based tracking systems.

A. Maritime Identification Zones

As stated above, several States have promulgated maritime or aerial identification zones to improve intelligence gathering concerning the movement of vessels or aircraft for maritime security purposes. Examples include the Air Identification Zone (ADIZ) of the United States established in 1950; the Japanese ADIZ promulgated in 1969 and of course, the East China Sea Air Defense Identification Zone established by China in 2013. However, the most infamous and the identification zone that will serve as the focus of our analysis is the Australian Maritime Identification Zone (MIZ) promulgated on December 14, 2004 by Prime Minister John Howard, as part of Australia's effort to strengthen its offshore maritime security. The MIZ, extending one thousand nautical miles from Australia's coastline, was established to identify vessels, including their crew, cargo and journey, seeking to enter Australian ports. The provision of this information was viewed as a means of enhancing the effectiveness of civil and military maritime surveillance, particularly in protecting offshore oil and gas facilities in the Australian EEZ. In the MIZ, information would not only be sought from port-bound vessels entering this zone, but would also aim "to identify all vessels, other than day recreational boats" entering the EEZ. As initially envisaged, vessels not complying with the request to provide information would be subject to interdiction."

It was no surprise that Australia's claim to such interdiction authority raised serious concerns as to the legality of the MIZ under international law. Eventually, Australia reformulated the MIZ into the Australian Maritime Identification System (AMIS). Under the AMIS, ships would be requested to provide information on a voluntary basis and the new system would be based on cooperative international arrangements, particularly with neighboring States. It must be noted, however, that Australian maritime control initiatives did not stop with AMIS, but revived in 2013 with Operation Sovereign Borders, which targets the influx of migrants by sea through various measures, including interdiction operations based, apparently at least in part, on intelligence.

As far as the legality of these measures in the EEZ is concerned, there is no reference in the Law of the Sea Convention to maritime identification zones. Under the Convention, coastal States may establish a contiguous zone extending up to twenty-four nautical miles from its baselines in which they may exercise the control of vessels necessary to prevent violations of certain laws and regulations.

In the EEZ, arguably, any identification process by the coastal State should be linked with the exercise of its sovereign rights and jurisdiction over the conservation of living resources, the protection of offshore platforms and the marine environment. Interestingly, in relation to the protection of the marine environment, Article 220(3) provides that

“[w]here there are clear grounds for believing that a vessel navigating in the exclusive economic zone ... has, in the exclusive economic zone, committed a violation of applicable international rules and standards for the prevention, reduction and control of pollution from vessels or laws and regulations of that State conforming and giving effect to such rules and standards, that State may require the vessel to give information regarding its identity and port of registry, its last and its next port of call and other relevant information required to establish whether a violation has occurred.”

Thus, it specifies the information that may be requested, and in Article 220(4), requires States to adopt laws and regulations and take other measures so vessels flying their flag comply with requests for this information. While this provision is limited in its application to conduct impacting the marine environment, any request of information that is linked with the exercise of sovereign rights and jurisdiction of the coastal State over its natural resources in the EEZ would be consistent with the rebuttable presumption in favor of the coastal State discussed above, and would meet the due regard obligation set forth in Article 56(2).

Moreover, in examining the legality of such intelligence activities in the EEZ, recourse may be had to other applicable rules of international law.

First, the coastal State, in this case Australia, is entitled to request information from vessels seeking to enter its ports under customary international law and under the authority of the 2004 amendments to the International Convention for the Safety of Life at Sea (SOLAS) and the International Security and Port Security Code (ISPS Code).

Second, information could also be requested for vessels in the EEZ under the customary right of approach.”

Since "other pertinent rules of international law" apply to the EEZ pursuant to Article 58(2), it is arguable that the customary right of all States to enquire about the identity of foreign-flagged vessels on the high seas equally applies thereto and may be exercised not only by Australian warships, but also by those of other States.

Indeed, even though the international law of the sea does not permit interference with the navigation of foreign-flagged vessels on the high seas except in exceptional circumstances, the same does not hold true for other monitoring measures. For example, according to Oppenheim's International Law, “it is a universally recognized customary rule of international law that warships of all nations, in order to maintain the safety of the high seas, have the power to require suspicious private vessels on the high seas to show their flag.” This right of approach, or reconnaissance, is limited to verifying the ship's right to fly its flag." This, an approaching warship may request an encountered vessel to show its colors, which are prima facie evidence of its nationality. It is submitted here that the customary right of approach in principle, has remained intact in the twenty-first century, albeit its implementation has been significantly modified due to technological changes. As one commentator describes:

“in its exercise of the customary "right of approach," a warship may intercept a vessel, inspect it from a safe distance to determine its name, flag, and home port, receive and review any data the vessel may be emitting from its automatic identification system (AIS) or long range identification and tracking (LRIT) equipment, perhaps scan other electromagnetic emissions if so equipped, and finally hail it on the radio.”

It follows from the foregoing that the mere request of information by Australia or any other State establishing similar identification zones would not be in dissonance with international law. On the contrary, it may be founded on more than one legal basis. What would clearly be in dissonance is any interdiction operation based solely on the denial of the requested vessel to provide the relevant information. As Natalie Klein rightly observes,

“There is no exception to flag State authority on the high seas that would permit the right of visit to enforce a coastal State requirement to provide information in pursuit of that State's maritime security policies.”

The sole exception to this rule appears to be if the vessel has failed to provide information concerning marine pollution in the EEZ, as found in Article 220(5).

Of course, if there are other suspicions regarding the vessel, for example, that it may be engaging in illegal fishing activities or that it is without nationality, the coastal State may use other legal bases to intercept the vessel.

In sum, even though maritime identification zones are not provided for in the Law of the Sea Convention, the coastal State may request information from foreign vessels in its EEZ under certain circumstances and in relation to certain activities. Such information would be confined to the identity of the vessel, its next port of call and its activities that may be related to the suspicious conduct in question. Any further enforcement measures must be specifically warranted by the Convention, since the mere refusal to provide this information does not trigger these measures.

B. Earth Observation Systems

It is an increasingly common practice of coastal States to employ earth observation systems, including satellites, radars or drones, to monitor vessels and their activities in an effort to prevent threats to maritime security. Such monitoring and surveillance measures are a key part of intelligence gathering in the EEZ. Examples include the automatic identification system (AIS) and the long-range identification and tracking (LRIT) system established by the International Maritime Organization (IMO) and the European Border Surveillance System (EUROSUR) established by the European Union (EU).

The IMO adopted AIS in 2000 as part of a revised Chapter V of SOLAS. It requires ships to carry AIS capable of providing information about the vessel, such as identity, location, course

and speed, to other vessels and coastal authorities. The regulation requires AIS to be fitted aboard all ships of three hundred gross tonnages and upwards engaged on international voyages, cargo ships of five hundred gross tonnages and upwards not engaged on international voyages and all passenger ships, irrespective of size.

The IMO further revised SOLAS to increase the tools available to States to learn about vessels in the surrounding waters by adopting Regulation 19-1 in 2006. Regulation 19-1, which entered into force in July 2009, requires ships to transmit information automatically, through a satellite-based system, disclosing the identity of the ship, its position and the date and time of the position." This information is to be received for "security and other purposes as agreed" by the IMO," such as marine environment protection.

Similar to AIS, it applies to vessels engaged on international voyages and encompasses passenger ships, cargo ships of three hundred gross tonnage and upwards and mobile offshore drilling units.'

In addition to AIS and the LRIT system, there are vessel monitoring systems (VMS) that have been developed and installed by some States and shipping companies. These systems are used in marine accident investigations, search and rescue, safety of navigation and pollution prevention. The type of information collected may include the course of the vessel, its speed, draft, and estimated time of arrival and departure from various positions. The use of VMS has also become an important means of deriving information about the location of fishing vessels, to which LRIT regulations do not usually apply because of their smaller size. Accordingly, many regional fisheries management organizations have introduced VMS as a means of enhancing surveillance and enforcement.

In 2013, the European Council adopted a regulation establishing EUROSUR. Its aim is to reinforce control of the external borders of the EU States. In particular, EUROSUR establishes a mechanism for member States' authorities carrying out border surveillance activities to share operational information and to cooperate with each other and with other EU agencies, such as the European Border and Coast Guard Agency (formerly known as FRONTEX). Its objectives are reduction of the number of irregular migrants entering the EU undetected and enhanced internal security by preventing cross-border crime, such as trafficking in human beings and narcotics smuggling. Clearly, the surveillance of maritime borders is facilitated by the use of modern technologies such as satellites.

In discussing whether the Russian authorities fulfilled the requirement of sending "a visual or auditory signal to stop" to the Greenpeace vessel, **Arctic Sunrise**, as dictated by the right of hot pursuit under Article 111, the tribunal stated,

“Given the large areas that now must be policed by coastal States and the availability of more reliable advanced technology (sea-bed sensors, satellite surveillance, over-the-horizon radar, unmanned aerial vehicles), it would not make sense to limit valid orders to stop to those given by

an enforcement craft within the proximity required for an audio or visual signal that makes no use of radio communication."

Such an evolutionary interpretation of the Convention's hot pursuit provisions is certainly welcome, as it takes into account contemporary technological advancements and the practice of States. However, no broader conclusions can be drawn from this finding. The tribunal alluded to satellites, along with other devices, such as radars and UAVs, solely to substantiate its argument that in the twenty-first century, law enforcement agencies may also lawfully use radio communication in lieu of "a visual or auditory signal" under Article 111.

Can this argument also be interpreted as allowing the coastal State to use these specific means to give signals to stop? Possibly yes, in the view of the author, if there are secure channels of communication providing safeguards to ensure the signal comes from competent authorities of the coastal State and that the vessel is aware of the existence of these channels.

The question in the context of our inquiry, however, is broader than the use of such systems in the course of hot pursuit and concerns the legality of such methods for intelligence gathering in the EEZ. Evidently, to the extent that these measures are incorporated in treaties like SOLAS, there is no doubt that they are part of the "pertinent rules of international law" that apply to the EEZ under Article 58(2). But even besides the authority provided by SOLAS, it stands to reason that the use of earth observation systems, including radars, satellites and drones, by the coastal State in its EEZ would comply with the international law of the sea, either pursuant to Articles 56 and 59 or under the customary right of approach.

Specifically, as long as coastal States police their EEZ to safeguard their exercise of sovereign rights therein or to protect the marine environment, these acts would clearly accord with the rebuttable presumption in favor of the coastal State. Even if we have recourse to the abstract formula of Article 59, it is submitted that "equity" and the "importance of the interests involved to the parties" would considerably favor the coastal State.

On the other hand, as permitted under the customary right of approach, every State, including the coastal State, may request some basic information regarding the vessels exercising the freedom of navigation. States can do this by sending their warships and other duly authorized vessels to approach the vessel concerned or through observation systems, like AIS and vessel monitoring systems (VMS). As stated above, the intention of the right of approach has traditionally been to inquire the identity of vessels on the high seas. In modern times, there is no need to approach the vessel physically to complete this act, as States can achieve the same result by using earth observation systems. The rationale, however, remains the same.

That said, it is one thing to request information on the flag, the name or the course of the vessel concerned and another to interfere with its navigation, board and search it. For the latter actions, there must be another legal basis found in the provisions of the Convention concerning the EEZ

or the high seas by reference to Article 58(2), as well as the default rule of the consent of the flag State.

A further, extremely relevant question concerns the level of information that coastal States may request in the exercise of the right of approach, either in its traditional form or in its contemporary manifestations. Certainly, earth observation systems have limits on what they can actually see and discern.

Nonetheless, it is the present author's view that the intelligence that may be collected or requested is confined to that information needed for the "*police generale*" of the EEZ. This data may include the vessel's nationality and documentation number, its current position and its course, as well as the next port of call, especially if they are fishing vessels and are bound to a port of the coastal State. However, any further information concerning the internal matters of the vessel, including information relating to its crew and cargo, falls within the remit of flag-State jurisdiction and may not be requested solely under the right of approach. Such a request would undermine the freedom of navigation safeguarded in Article 58, as well as shift the presumption from favoring the coastal State to favoring other States and their *jus communicationis*, as discussed in Part III.

To conclude, the use of earth observation systems, with their advantages and inherent limitations, will increase and will inevitably challenge the traditional contours of policing of the seas, including the EEZ. It rests upon State practice and future judicial opinions to discern how to accommodate such advancements with the legal regime of the EEZ and the freedom of navigation of other States.

V. INTELLIGENCE GATHERING BY OTHER STATES IN THE EEZ

It is a truism that most scholarly writings have been devoted not to whether the coastal State may engage in intelligence gathering in the EEZ, but the inverse question: whether other States may engage in intelligence gathering in a foreign EEZ. Several recent incidents in various EEZs, political tension in contested areas such as Southeast Asia and the importance that naval powers ascribe to military intelligence gathering have all fueled this debate.

In particular, questions arise as to the contours of the rights of coastal States and the freedom of navigation enjoyed by other States. As Natalie Klein observes,

"the lack of legal clarity has become especially problematic as technological advances have not only improved the range and accuracy of both weaponry and intelligence collection, but also changed the very art of both warfare and intelligence gathering."

In this regard, Hayashi describes potential intelligence activities as follows:

"Other signals intelligence activities intercept naval radar and emitters, thus enabling the location, identification and tracking of surface ships as well as the planning and preparation of

electronic or missile attacks against them. These activities appear to involve far greater interference with the communication and defense systems of the targeted coastal State than any traditional passive intelligence gathering activities conducted from outside national territory."

The law of the sea does not provide a straightforward answer concerning the permissibility of intelligence gathering activities in the EEZ. While Article 19(2)(c) defines intelligence gathering in the territorial sea as non-innocent passage, there is no corresponding provision in the Convention that addresses intelligence gathering in the EEZ. Hence, a contrano, one can presume that since this activity is not prohibited, it is permitted. Indeed, the preponderant view is that intelligence gathering is one of the "other internationally lawful uses of the sea" related to the freedoms set forth in Article 58. For example, Hayashi notes, "traditionally, intelligence gathering activities have been regarded as part of the exercise of freedom of the high seas and therefore, through Article 58(1), is lawful in the EEZ as well."

Similarly, Rauch has argued that the freedom of navigation associated with the "operation of ships" allows for a range of internationally lawful military activities, including intelligence gathering and surveillance."

Assuming that intelligence gathering is associated with the freedom of navigation enjoyed by other States in foreign EEZs, the rebuttable presumption would favor its permissibility. However, as discussed in the previous Part, this is just a rebuttable presumption, which is subject to the legal regime of the EEZ, the Convention, and other pertinent rules of international law.

In turn, this point raises the question of when the presumption may be rebutted or qualified.

It is obvious that the gathering and sharing of intelligence would be unlawful if it interfered with the exercise of the coastal State's sovereign rights and jurisdiction. This outcome would be evident where information gathering undermined the existing sovereign rights of coastal States. More broadly, it could be argued that any intelligence gathering, having as its purpose the economic benefit of other States would violate the due regard requirement in Article 58(3), at least as that requirement has been construed in the Chagos Marine Protected Area and the South China Sea arbitrations.

An example of such intelligence gathering would be the incidental-and perhaps intentional-collection of information related to the natural resources of the EEZ, such as a survey involving the acquisition of seismic data that could be used to locate oil and gas exploratory wells. Such an acquisition could occur in the course of a marine scientific research project that had already received the requisite consent by the coastal State under Article 246(2). Here, the collection of such information would amount to an unjustifiable interference with the sovereign rights of the coastal State under Article 77, as preserved under Article 246(7), as well as under Article 56 in conjunction with Article 58(3).

A second example in which military intelligence gathering by third States in the EEZ would not be permitted is when such activities constituted unlawful conduct as "the threat or use of force" contrary to Article 2(4) of the UN Charter, and, more particularly, to Article 301 of the Law of the Sea Convention. As Article 301 states:

“In exercising their rights and performing their duties under this Convention, States Parties shall refrain from any threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the principles of international law embodied in the Charter of the United Nations.”

This provision echoes, but is not identical to Article 2(4) of the UN Charter. Nonetheless, Article 2(4) may serve as the interpretative yardstick for incidents falling within the scope of Article 301.

It is true that international courts and tribunals have been very reluctant to find a "threat or use of force." An arbitration tribunal did make such a finding in a 2007 award arising from a dispute between Guyana and Suriname.

Here, sailors on two Surinamese gunboats asked the operators of a Guyanese-licensed drilling rig in a contested maritime area to leave the rig within twelve hours. The tribunal concluded these activities amounted to an illegal threat of the use of force, rather than a law enforcement activity.

In general, to constitute a threat of the use of force, the act in question must involve a considerable degree of coercion against the coastal State.

Thus, the act of intelligence gathering, without any further activities, would fall short of reaching the threshold of either Article 301 or Article 2(4). The act would need to be accompanied by other coercive measures to substantiate impermissible intelligence gathering. As an example, Bateman suggests that “typically this would be the case if the research or data collection were being undertaken to support contingency plans for military operations against the coastal State.”

As such, it is evident that the threshold for establishing such a violation is particularly high.

Another instance in which intelligence gathering by other States within the EEZ would violate the law of the sea is when that State's activities amount to an abuse of right, in this case the right of navigation and the associated right to collect information in a foreign EEZ Article 300 of the Convention addresses good faith and abuse of right, stating: “States Parties shall fulfill in good faith the obligations assumed under this Convention and shall exercise the rights, jurisdiction and freedoms recognized in this Convention in a manner which would not constitute an abuse of right.”

According to the Virginia Commentary, “it would appear that the parameters of the notion as enunciated in Article 300 and applicable to the whole Convention…concern the unnecessary or

arbitrary exercise of rights, jurisdiction and freedoms or the misuse of powers by such a State Party."

Having assumed that intelligence gathering is a freedom reserved under Article 58(1), it may still result in abusive conduct, such as when it is conducted arbitrarily or unaligned with a purpose associated with the jus communicationis. That said, abuse of right has proven a very elusive concept, scarcely referred to in international case law, and very difficult to substantiate in practice.

In sum, notwithstanding that some scholars disagree, intelligence gathering in foreign EEZs is a lawful use of the seas associated with the freedoms reserved for other States in coastal State EEZs. While this presumption is rebuttable, few examples arise that do not favor this presumption, and for those that do, it is often the underlying conduct, rather than the intelligence gathering itself that violates the law of the sea and international law generally.

VI. INTELLIGENCE COLLECTION AND VISIT, BOARD, SEARCH AND SEIZURE (VBSS) OPERATIONS

A. VBSS Operations on the High Seas

Useful law enforcement intelligence can be gathered in the course of a VBSS operation." In particular, boarding a vessel suspected of one crime may reveal evidence of another crime. Thus, it was not uncommon for counter piracy patrols off Somalia during VBSS operations to find that hidden below decks aboard suspect vessels was not a crew of pirates, but a human cargo of irregular migrants seeking to be smuggled into Yemen.co The frustrating result was that migrant smugglers were often let go because the counter piracy missions lacked a mandate to deal with migrant smuggling off the African coast, even though some of the same navies were engaged in interdicting migrant smugglers in the Mediterranean."

While this was ultimately a problem of mandate, not legal authority, it does raise the broader question of whether there are distinct legal limitations on what naval forces and maritime agencies can do with information gathered in the course of VBSS operations. Unsurprisingly, the issue turns on the zone in which one operates. The high seas are for present purposes the most pertinent case (though other zones are discussed briefly below).

In respect of the high seas, a controversy is provided by the extent of authority conferred under UNCLOS Article 110, which governs the conduct of VBSS operations in cases of reasonable suspicion that a vessel is engaged in piracy, the slave trade, unauthorized broadcasting or is without nationality.

Such an operation is intended to be conducted in sequence. Under Article 110(3), a warship may "send a boat under the command of an officer to the suspected ship." The boarding party is to first inspect the ship's documents to "verify the ship's right to fly its flag." Then, "if suspicion

remains ... it may proceed to a further examination on board the ship, which must be carried out with all possible consideration." The question that arises is whether the information found in the course of such an "examination" is limited by the original purposes of the boarding.

The conventional view is that at least some forms of wider use are prohibited. 62 The foundational text relied upon to posit this view is normally the commentaries of the International Law Commission to the 1956 draft Articles on the Law of the Sea. With regard to the equivalent provision to Article 110, the Commission stated:

If the examination of the merchant ship's papers does not allay the suspicions [giving rise to the rights of boarding], a further examination may be made on board the ship. Such examination must in no circumstances be used for purposes other than those which warranted stopping the vessel. Hence the boarding party must be under the command of an officer responsible for the conduct of his men.

The same point is made in the highly regarded Virginia Commentary, which tracks closely to the language used by the Commission:

"If suspicion remains after examination of the ship's papers, the boarding party may proceed to a further examination on board the ship. Such further examination is not to be used for purposes other than those which warranted stopping the ship, and is to be carried out with all possible consideration."

Given that international lawyers normally take the pronouncements of the International Law Commission as authoritative, how is this limitation to be construed? Wendel suggests a potentially broad construction. Consider the interception of a vessel that displayed no flag or identifying markings.

These facts could justify boarding and inspection on grounds of suspected statelessness. Wendel argues, however, that the right to verify nationality in such cases cannot justify inspection of the hold or cargo, as the only relevant material will be the vessel's papers. If the papers resolve the issue, no further search should occur. This, in Wendel's view, raises questions regarding the legality of continuing to conduct a search of the hold in cases such as the So San incident in which a vessel suspected of conveying Scud missiles from North Korea to Yemen bore no external markings of nationality, but attempted to claim Cambodian nationality verbally." Setting aside the fact that the So San interdiction occurred with the consent of the ostensible flag State (which had authority under international law to authorize the search), Wendel's general point is not unfair. We must return, however, to the text of Article 110(2), which states that "if suspicion remains after the documents have been checked; [the boarding State] may proceed to a further examination."

The right of "further examination" appears to be a general one. Even if narrowly construed by reference to the original suspicion, as Wendel would have it, where inadequate papers have been

presented and the relevant suspicion is one of statelessness, inspection of the hold may reveal information such as a main beam number capable of assisting in the vessel's identification.'

To some, however, all of this is beside the point. The question at hand is not whether a VBSS operation can be conducted on a pretext (i.e., statelessness) in order to conduct a search with an ulterior motive. This would be open to an allegation of abuse of right (UNCLOS Article 300). Rather, the question is what can one do with information uncovered in the course of a legitimate VBSS operation that might be generally relevant to broader questions of maritime security, or indeed that might provide evidence of specific criminal conduct, going beyond the original suspicions giving rise to a right of boarding.

Indeed, at least one treaty concerning maritime security, the 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, imposes such a duty on a boarding State granted flag State permission to board and inspect a vessel at sea.

The Protocol details a range of terrorism offenses, suspicion of which might justify boarding and inspection of a vessel. Generally such a boarding by a "requesting party" may only follow a request for and receipt of flag State consent, unless the flag State has waived that requirement under the treaty.

For VBSS operations the Protocol provides:

“When evidence of conduct [prescribed under the Protocol] is found as the result of any boarding…the flag State may authorize the requesting Party to detain the ship, cargo and persons on board pending receipt of disposition instructions from the flag State. The requesting Party shall promptly inform the flag State of the results of a boarding, search, and detention conducted pursuant to this article. The requesting Part shall also promptly inform the flag State of the discovery of evidence of illegal conduct that is not subject to this Convention.

Admittedly, other than this text there seems to be relatively little positive law dealing with the question of whether wider use can be made of evidence of other illegal conduct discovered aboard. One could attempt to invoke the so-called Lotus presumption in support of the conclusion that wider use is permitted in order to argue that anything not expressly prohibited is, in fact, permitted. The proposition, as usually stated, is too broad to be meaningfully applied and presumes international law to consist largely of prohibitions rather than positive or facilitative rules. The better question is whether there any identifiable obligations of international law that would be breached if one were to make wider use of information found during a VBSS operation. It is submitted that such obligations are in practice rather hard to find.

One could attempt to argue that wider use of information discovered somehow violates the principle of exclusive jurisdiction of the flag State, but one would have to state the principle at a very high level of generality for that result to follow.

As this author has argued elsewhere," the regulatory jurisdiction (i.e., prescriptive jurisdiction) is by no means completely exclusive and other States remain free to attach consequences to the actions of, for example, their nationals aboard foreign vessels on the high seas. At best, the principle of "exclusive" flag State jurisdiction confers prima fade immunity from physical interference on the high seas (enforcement jurisdiction) subject to exceptions provided by UNCLOS, other treaties or flag State consent. The rule of exclusive flag State jurisdiction is thus heavily qualified, and is by its very nature derogable. This does not seem compatible with the idea that it contains by necessary inference an otherwise unstated blanket prohibition against wider use of information discovered aboard a vessel on the high seas subject to a legal VBSS operation. Indeed, one might argue that positive obligations upon States to cooperate to suppress various illicit activities at sea mitigates in favor of the sharing of information where possible. Such obligations of cooperation exist with regard to, inter alia, piracy," maritime drug smuggling, or unauthorized high seas radio broadcasting,"' the enforcement of internationally agreed fisheries conservation measures and the prevention of migrant smuggling by sea.

B. VBSS in Waters under National Jurisdiction

There are numerous good studies of the practical limitations international law may place upon VBSS operations in waters under national jurisdiction.

The territorial sea of up to 12 nm is plainly a zone of sovereign jurisdiction over which coastal States have law enforcement jurisdiction, subject to innocent passage. What this means in practice has been debated. Some see innocent passage as conferring an absolute immunity from VBSS, unless non-innocence" is made out on one of the specified grounds. Others have long pointed to the ambiguity of UNCLOS and the Geneva Convention on the Territorial Sea on this point. Both conventions proclaim that a coastal State "should not" exercise criminal jurisdiction over "a foreign ship passing through the territorial sea" unless one of the categories of non-innocent passage are made out. Views differed as to whether that practice evidenced a restriction on powers of enforcement in the territorial sea (i.e., a limitation upon sovereignty) or simply evidenced comity (i.e., plenary sovereignty, usually exercised with restraint)." The debate is far from resolved, but the only clear prohibitions on law enforcement in the territorial sea concern sovereign immune vessels and crimes "committed before the ship entered the territorial sea" where the vessel in question is simply passing through the territorial sea without entering internal waters.

Conversely, the extent of law enforcement power in the contiguous zone may provide less authority than commonly thought to conduct VBSS operations.

Within a contiguous zone (extending up to a further 12 nm seaward from the territorial sea), "states have limited powers" under UNCLOS Article 33 to enforce "customs, fiscal, sanitary and immigration laws." UNCLOS allows coastal States only to exercise "control" (not sovereignty or jurisdiction) either to prevent infringement of the specified laws within the State's territory or

territorial sea or to punish acts already committed within its territory or territorial sea." Shearer argues that the connotations of control limit preventive enforcement action to "inspections and warnings," rather than arresting vessels. Some authorities, and in particular U.S. commentators, treat Article 33 as allowing plenary criminal law enforcement for violations of the specified subject matters up to the outer limit of the zone.

This approach fails to give separate meanings to “prevent” and “punish.”

The power to "punish" is conditioned upon criminal acts having occurred within a State's territory or territorial sea." By analogy with the doctrine of hot pursuit, this appears to be an express extension of an otherwise impermissible jurisdiction. The condition limiting the exercise of jurisdiction to '"punish" would be redundant if relevant criminal laws were continuously enforceable up to the outer limit of the zone. The claim, for example, that "if the U.S. Intelligence Community levies terrorism threat reporting [i.e., the vessel is allegedly carrying terrorism-related material or personnel] against a ship anywhere within 24 nautical miles of the United States coast, it would be subject to United States jurisdiction is absurd unless the facts of the case disclose a close link to a customs or immigration violation that has actually occurred. If such a violation is merely threatened, permissible measures may be constrained to visit and inspection.

Finally, in the 200 nm EEZ, coastal States enjoy a limited bundle of sovereign rights and subject matter jurisdiction. They have “sovereign rights for the purpose of exploring and exploiting, conserving and managing the natural resources, whether living or non-living…and with regard to other activities for the economic exploitation and exploration of the zone.”

Under this jurisdiction, the coastal State may also conduct activities pertaining to "artificial islands, installations and structures," marine scientific research and "the protection and preservation of the marine environment." In exercising its sovereign rights the coastal State may "take such measures, including boarding, inspection, arrest and judicial proceedings" as are necessary to enforce its laws with respect to those rights." Curiously, there are no express enforcement provisions in UNCLOS regarding "artificial structures and marine scientific research," but it is not questioned that, for example, a State's criminal law may in principle extend to vessels that violate laws applicable in a safety zone around an artificial structure. In protecting the marine environment, the coastal State enjoys power to regulate dumping under Article 211(5), to conduct boarding and inspection of vessels causing or threatening "significant pollution of the marine environment" and to arrest and institute proceedings against vessels in pollution incidents that on "clear objective evidence" have caused "major damage or threat of major damage" under Articles 220(5) and 220(6).

As regards both the contiguous zone and EEZ, it would be an abuse of right to use such a power of inspection intentionally to gain intelligence not related to the subject matters over which rights or jurisdiction have been granted to a coastal State; however, wider use of any information

discovered in the course of such a boarding should be permitted for the reasons discussed above in relation to the high seas. Thus, it is hard to see what significant restrictions international law might place upon the use a coastal State could make of law enforcement intelligence gleaned through a lawful VBSS operation in waters under national jurisdiction. One question might be whether VBSS operations can be conducted in international straits subject to the regime of transit passage, under which vessels enjoying such a right "shall not be impeded." There is, however, not space to consider this point further in the present article.

Monitoring the movement of ships and seafarers

In the framework of the International Convention of Safety of Life At Sea (SOLAS 1974), the International Maritime Organization (IMO) has introduced the Long-Range Identification and Tracking system (LRIT) which aims to obtain ship identity and location information in sufficient time to evaluate the security risk posed by a ship off its coast and to respond, if necessary, to mitigate risks. Apart from maritime security LRIT covers search and rescue, safety, and protection of the marine environment and is mandatory for all passenger ships, high speed craft, mobile offshore drilling units and cargo ships of over 300 gross tonnes. Every 6 hours ships are required to issue reports, which are received by satellites, and securely transferred to data centres which manage LRIT information on behalf of flag States.

There are a wide variety of vessel tracking systems including Vessel Monitoring Systems (VMS), Automatic Identification Systems (AISs) and LRIT which are designed to provide information about the ship to other ships and to coastal authorities automatically. This information should include the ship's identity, type, position, course, speed, navigational status and other safety-related information. These systems however require active cooperation of the vessels. Because VMS cannot be used to monitor vessels that do not have VMS on board or whose system is switched off or malfunctioning, the EU JRC and EU Fisheries Council have promoted the use of remote sensing as an additional control tool. Consequently a number of space-based satellite earth observation technologies are emerging which address communication and global positioning for ship traffic surveillance and the identification of security threats. Since these satellite technologies do not depend on the willingness of ships to cooperate, remote sensing overcomes the lack of independence of transponders and complements active detection systems with passive measurements for non cooperating ships.

A. Surveillance systems

A range of different surveillance techniques are typically used under this heading including visual sightings, still cameras, closed circuit television (CCTV), radar and infra red imaging. While the main limitation of such systems lies in the limited information that can be provided, they nevertheless play an important role in building up a maritime picture: (a) in cases where data is not provided under a reporting regime (whether deliberately or not); (b) in respect of

(typically smaller) vessels that are not subject to a reporting regime; and (c) due to their immediacy and, in some cases, greater accuracy.

Military surveillance systems

The gathering of surveillance data is inherent to the role of Europe's navies for defence purposes, which since 2001, includes defence against terrorism. Assessing what surveillance data is actually collected is a difficult task: the data itself is usually classified as is information about acquisition mechanisms. Nevertheless it is possible to surmise that maritime surveillance data is gathered through: (a) physical observation from military vessels and aircraft; (b) unmanned vehicles and drones; (c) remote sensing; (d) coastal radars; and (e) underwater sensors. As will be seen below Europe's navies typically also make use of civilian monitoring and surveillance data.

Sistema Integrado de Vigilancia Exterior (SIVE)

SIVE is a Spanish coastal surveillance system operated by the Guardia Civile. Originally designed to focus on small vessels carrying illegal immigrants it is used to detect, identify and intercept a range of illegal activities around Spain's maritime frontiers. It is based on a network of fixed stations and mobile units that make use of still cameras, CCTV, radar and infra-red sensors. The data (video images, radar tracks and infra-red images) are transferred by secure internet to provincial control centres. There is no specific legal basis for SIVE – it derives from the basic mandate of the Guardia Civile. At present the data is used only by the Guardia Civile.

Vessel traffic services (VTS)

VTS are shore based-systems which range from the provision of information messages to the extensive management of maritime traffic. There are two basic types of VTS: (a) port VTS which are concerned primarily with traffic management in/around a port; and (b) coastal VTS which deal with traffic passing through a specific area. Usually, on entering a VTS area the master of a ship must first report to the authority responsible for the VTS. He must then monitor a specific radio frequency for navigational or other warnings. The activities of a ship within a VTS area are, however, usually monitored by the VTS authority using radar, AIS and in some cases radio direction finders (RDF) and remote video cameras. In terms of international law the legal regime for VTS is contained in Regulation 12 of SOLAS supplemented by guidelines adopted pursuant to IMO Resolution A. 857(20) of 27 November 1997. At EC level, VTS is addressed in Articles 8 and 9(3) of the VTM Directive. The guidelines state that the purpose of VTS is to improve the safety and efficiency of navigation, safety at sea and the protection of the marine environment, offshore installations etc from possible adverse effects of maritime traffic.

CleanSeaNet

CleanSeaNet is a satellite-based monitoring system for marine oil spill detection and surveillance in European waters provided by the European Maritime Safety Agency (EMSA). EMSA obtains radar satellite images from a commercial satellite provider in response to requests from Member States.

B. Reporting regimes

Because reporting regimes impose a legal reporting obligation it is relatively easy to determine what legal rules apply as evidently this must be specified in law.

Vessel monitoring system (VMS)

In connection with the implementation of the common fisheries policy each Member State is required pursuant to the Control Regulation (EC) 1489/97 and the VMS Regulation (EC) 2244/2003 to establish a VMS whereby data relating to the identification, position, speed and course of its fishing vessels above 15 metres in length can be transmitted at all times by satellite to a fisheries monitoring centre (FMC). These data include three unique identification numbers: (a) the Community Fleet Register number of each vessel which in turn correlates with details contained in the national fishing boat registers that must be maintained by each Member State; (b) a national register number; and (c) the external or side number of the vessel. In addition, for most vessels, the radio call sign number will be unique. This data is collected to ensure the effective monitoring of the activities of fishing vessels. Each flag Member State is entitled to receive VMS data through its FMC. In addition a coastal Member State is entitled to receive data from the flag State FMC in respect of a foreign fishing vessel in its waters. The European Commission is also entitled to obtain remote on-line access on specific request. Practice as regards sharing of VMS data at national level beyond the FMC varies among Member States.

Automatic Identification System (AIS)

AIS are a ship-born mechanism that automatically provides for the exchange of data between ships as well as coastal stations. This data includes: (a) fixed data such as the unique maritime mobile service identity (MMSI), call sign and name, IMO number and details of the ship; (b) automatically generated dynamic navigational data including details of the ship's position, course and speed over ground and navigational status; and (c) manually entered voyage data. The rate of data exchange increases as a ship gains speed. The fitting of AIS is mandatory for all vessels of 300 gross tonnages and above on international voyages, cargo ships of 500 gross tonnages and above and passenger ships irrespective of size. Warships and government owned vessels are exempt. The basic obligation to fit and use AIS is imposed by Regulation 19 of Chapter 19 of the International Convention for the Safety of Life at Sea (SOLAS). Furthermore the Vessel Traffic Monitoring Directive 2002/59/EC (the 'VTM Directive') requires any ship calling at the port of a Member State to be fitted with AIS. The purposes of AIS include

promoting the safety of navigation, collision avoidance, enabling coastal States to obtain information about ships and their cargoes and as a VTS tool (see below). Implicit in the structure of AIS is that other vessels within transmission range are entitled to AIS data as are the monitoring stations of coastal States. Furthermore the VTM Directive provides for the exchange of AIS data between Member States. In addition, because AIS is transmitted un-encrypted over open frequencies, there is nothing to prevent anyone with suitable equipment from receiving it.

Long Range identification and Tracking of Ships (LRIT)

LRIT is a new long-range vessel monitoring system which also requires the periodic transmission of the name and course of vessels. However the data is transmitted only at six hourly intervals and the transmissions take place by satellite meaning that LRIT is a closed system. The legal basis for LRIT is contained in Regulation 19-1 of Chapter V of SOLAS which provides that the following, providing they are parties to SOLAS, are entitled to LRIT data: (a) the flag State at all times; (b) a port State where a ship has indicated its intention to enter a port in that State; and (c) a coastal State in respect of a ship within 1,000 nm of its coast (unless the ship is in the waters of its flag State). LRIT is not yet fully operational.

C. Indian Coastal and Maritime Security

India's long coastline presents a variety of security challenges including illegal landing of arms and explosives at isolated spots on the coast, infiltration/ex-filtration of anti-national elements, use of the sea and off shore islands for criminal activities, and smuggling of consumer and intermediate goods through sea routes. Absence of physical barriers on the coast and presence of vital industrial and defence installations near the coast also enhance the vulnerability of the coasts to illegal cross-border activities. In addition, the Indian Ocean Region is of strategic importance to India's security. A substantial part of India's external trade and energy supplies pass through this region. The security of India's island territories, in particular, the Andaman and Nicobar Islands, remains an important priority. Drug trafficking, sea-piracy and other clandestine activities such as gun running are emerging as new challenges to security management in the Indian Ocean region.

India's coastline and island territories

India has a coastline of 7,517 km, of which the mainland accounts for 5,422 km. The Lakshadweep coast extends for 132 km and the Andaman and Nicobar Islands have a coastline of 1,962 km. The Indian coastline is distributed among nine coastal states and four UTs, and almost the entire coast of India falls within the tropics. The nine coastal states are Gujarat, Maharashtra, Goa, Karnataka, Kerala, Tamil Nadu, Andhra Pradesh, Odisha and West Bengal. India also has large coastal wetlands, which cover an area of over 41,401 km², which is 27.13% of the total area covered by wetlands in India. India's inland wetlands, on the other hand, cover 1,05,649 km². Most cargo ships that sail between East Asia, America, Europe and Africa pass through Indian territorial waters. According to the Ministry of Shipping (MoS), around 95%

of India's trade by volume and 70% by value is done through maritime transport. Special economic zones (SEZs) are being developed in close proximity to several ports, thereby providing a logistical advantage to industries within these zones. The government has announced plans to develop 14 coastal economic zones (CEZs) in a phased manner for port-led development in all of the nine maritime states. According to the Maritime Zone Act, 1976, the maritime zones of India are divided into five Coast Guard regions, with the Indian Coast Guard (ICG) responsible for the enforcement of maritime zones. The five regions are North-West, West, East, North-East and Andaman and Nicobar, with the respective regional headquarters located at Gandhinagar, Mumbai, Chennai, Kolkata and Port Blair. The regions are further divided into twelve Coast Guard 'districts', one each for the nine coastal states on the mainland, two in the Andaman and Nicobar region and one at Kavaratti in the Lakshadweep and Minicoy Islands. In addition, there are Coast Guard Air Stations (CGASs) and Coast Guard Air Enclaves (CGAEs) for air operations from various locations along the coastline. There are presently 12 major ports and 200 notified minor and intermediate ports in India. The 200 non-major ports are in the following states: Maharashtra (48), Gujarat (42), Tamil Nadu (15), Karnataka (10), Kerala (17), Andhra Pradesh (12), Odisha (13), Goa (5), West Bengal (1), Daman and Diu (2), Lakshadweep (10), Pondicherry (2), and Andaman and Nicobar (23). Apart from five main fishing harbors, Mangalore (Karnataka), Kochi (Kerala), Chennai (Tamil Nadu), Vishakhapatnam (Andhra Pradesh) and Raichak in Kolkata (West Bengal), further, 23 minor fishing harbors and 95 fish-landing centres are designated to provide landing and berthing facilities to fishing craft. The coastal areas are safeguarded by the police forces of the respective coastal states and UTs, which have jurisdiction of up to 12 nautical miles (nm) from the coast. India, a traditionally maritime country with a rich maritime heritage, has an exclusive economic zone (EEZ) of 200 nm from its coast. India is currently seeking to extend its EEZ to 350 miles. The ICG and the Indian Navy have jurisdiction over the entire maritime zone up to 200 nm, including the 12 nm of territorial waters.

Security threats

India's long coastline poses a variety of security concerns:

• Landing of arms and explosives at isolated spots on the coast

• Infiltration/ex-filtration of anti-national elements

• Use of the sea and offshore islands for criminal activities • Smuggling of consumer and intermediate goods through sea routes, etc.

Indian Coast Guard

The ICG is a multi-mission organization that is responsible for coastal security in territorial waters, including areas to be patrolled by the coastal police. It is also responsible for maintaining maritime surveillance across India's two million sq. km EEZ, and contributes towards the

development and implementation of an effective security mechanism to combat seaborne threats. The security matrix of the ICG encompasses a host of operations and involves measures undertaken to address coastal security, offshore security, anti-terrorism, antipiracy and port security. The ICG also provides support to the Indian Navy to ensure the maritime security of the country. After the terror attacks in Mumbai in 2008, there has been a paradigm shift in the maritime security apparatus. Currently, there is an increased emphasis on surveillance, intelligence gathering and information sharing amongst the various stakeholders to ensure an effective response to any emerging situation. In February 2009, the ICG was additionally designated as the authority responsible for coastal security in territorial waters, including areas to be patrolled by the coastal police. The ICG is also responsible for overall coordination between the Central and state agencies in matters relating to coastal security. As part of coastal security mechanisms, a surveillance system called the Coastal Surveillance Network (CSN), comprising a chain of static sensors having radars, an automatic identification system (AIS), day/night cameras and metrological sensors has been established at 46 locations along the coastline and island territories by the ICG. In order to achieve near gap free surveillance of the entire coastline, 38 additional radar stations and eight mobile surveillance systems, apart from vessel traffic management system (VTMS) connectivity at the Gulf of Kutch and Gulf of Khambhat, are being installed under CSN Phase-II. The ICG has also promulgated standard operating procedures (SOPs) for ensuring coordination and cohesion amongst various agencies involved in coastal security. The ICG and marine police are working according to the 'hub-and-spoke' concept; the hub being the ICG stations and the spoke being the CPSs. To revalidate the coastal security mechanism and create awareness among the fishermen at sea, regular boarding operations are also being conducted to validate and check the credentials of the occupants of the vessels, including their identity cards and registration documents. Further, based on intelligence inputs, coastal security operations are conducted by the ICG in coordination with other stakeholders. Community interaction programmes (CIPs) are conducted periodically by the ICG for the fishermen and coastal populace in order to sensitize them to security and safety issues. In order to develop their capacity, the ICG has been imparting regular training to marine police personnel since 2006. Regular training programmes are conducted at the Coast Guard District Headquarters corresponding to the coastal states/UTs. In order to strengthen the capabilities of the ICG with regard to anti-smuggling and narcotics control, the Government of India has sanctioned the merger of the Customs Marine Organization (CMO) under the Department of Revenue with the ICG. In West Bengal earlier this year, the ICG commissioned a 27-m long high-speed interceptor boat C-424, which can reach a speed of 45 knots, for the further development of West Bengal's coastal security measures. Along with this new boat, West Bengal now has Coast Guard assets, including three fast patrol vessels, four hovercrafts, two interceptor boats, a radar station and an air cushion vessel (ACV) forward-operating base in Frazerganj.

In Andhra Pradesh, the ICG conducted 110 outreach programmes with the fishing community to sensitize them to the local government's coastal security undertakings. The fishermen were educated on search and rescue operations, precautionary measures during harsh weather, distress

alarms and proper documentation requirements. The programme was a product of the policies that the state is trying to develop for better communication and cooperation between the coastal security officials in Andhra Pradesh and the fishing/trading community. Keeping the 26/11 attacks in mind, the government has approved a 31,748 crore INR 'definitive five-year action programme' for the Coast Guard. The aim is to make the Coast Guard a 175-ship and 110-aircraft force by 2022 to plug the operational gaps and strengthen its capabilities to safeguard coastal security, island territories, offshore assets and the marine environment, as well as undertake anti-piracy, anti-smuggling, oil-spill and pollution-control operations. The Coast Guard currently operates 130 ships consisting of 60 offshore patrol vessels, fast-patrol vessels and pollution control vessels, 18 hovercrafts, and 52 smaller interceptor boats/crafts. The air assets consist of 39 Dornier maritime surveillance aircraft, 19 Chetak choppers and four Dhruv advanced light helicopters (ALHs). For future requirements, the Coast Guard has 65 ships and interceptor crafts/boats under construction and has planned the acquisition of 30 helicopters. Further, 16 indigenous Dhruv choppers have already been ordered from Hindustan Aeronautics Ltd, and the procurement of 14 twin-engine EC-725 tactical choppers from Airbus is in the final stages of approval. The force is also looking for six more maritime multi-mission surveillance aircraft and the establishment of five air stations/enclaves.

Border Security Force

Established in 1965, the Border Security Force (BSF) is a paramilitary force responsible for guarding India's land borders during peace time and preventing transnational crime. The BSF falls under the administrative control of the MHA. In order to thwart the landing of terrorists through sea routes, the BSF formed its first commando unit called Creek Crocodiles. The Creek Crocodile Commando unit is an elite commando force with 42 commandos responsible for manning 85 km of hostile creek area where India shares a border with Pakistan along the Rann of Kutch. The coastline is abundant with creeks that could be used by infiltrators to evade security forces and radars. As a result, the circumstances mandate difficult defensive requirements, especially during high tides and tough weather. Further, the lands are entirely submerged and poisonous snakes and scorpions are rampant. The BSF primarily patrols the three largest creeks in the region— namely Sir Creek, Kori Creek and Padala Creek. The Creek Crocodile Commandos are equipped with around six all terrain vehicles (ATVs) and 30 fast patrol boats, including four American-made fast attack craft (FAC).

International Ship and Port Facility Security Code

The International Ship and Port Facility Security (ISPS) Code is a comprehensive set of guidelines and regulations established for the security of ships and port facilities. Developed by the International Maritime Organization (IMO) in response to the 9/11 attacks, the code is constituted in the International Convention for the Safety of Life at Sea (SOLAS), an international maritime treaty. All 148 signatories of the treaty, including India, are required to comply with the ISPS Code. The purpose of the set of regulations is to establish a standardized

framework across international ports and ships, which then allows governments to efficiently evaluate risks and offset threats and vulnerabilities to shipping and port facilities through alterations to security levels and undertaking the security measures prescribed by the Code. Compliance with the ISPS Code falls within the spectrum of central programmes related to maritime security. The standardized regulations aim to:

• Monitor the access of unauthorized persons on port premises.

• Track cargo operations and detect security threats on vessels or on shore.

• Assign appropriate security levels to ships and establish various duties and functions within each security level. • Prescribe roles and responsibilities for port state officers and on-board officers to manage maritime security threats at an international level.

• Gather global data related to maritime security threats and results to tackle the same.

There are three security levels for ports within the ISPS Code, and each level consists of certain security undertakings that are mandatory for proper compliance.

1. Security level 1 (normal):

The ship or port facility operates normally. It mandates a set number of security measures to be active within the ports, which include compulsory pre-boarding checks, constant surveillance of 'no access' zones and coordinated supervision of cargo and minimum access to ships.

2. Security level 2 (heightened):

Level 2 stays active for as long as there is a substantial amount of risk present against the port/ship facility. It requires additional layers of security, over and above the minimum requirements, until the threat is mitigated. Security measures require deployment of additional personnel, limiting waterside access to the ship, establishing restricted areas, escorting visitors on board and conducting comprehensive searches on ships.

3. Security level 3 (exceptional):

Level 3 implies probable and imminent risk and requires maximum security for a limited time frame. Even if the specific target is unidentified, ports are expected to be ready to evacuate ships, limit access to a single point, suspend movement of any shipping traffic, suspend cargo and storage operations, and closely monitor personnel and vessels in the port facility.

INFORMATION SHARING AND LAW ENFORCEMENT

INFORMATION SHARING TO COMBAT MARITIME PIRACY

A. The Primary Legal Sources Underlying the Duty to Cooperate

Combating maritime piracy requires commitment and active engagement by states. As indicated by Mr. Helmut Tuerk, the honorable justice of the International Tribunal for the Law of the Sea, "the practice of piracy has been widespread over the centuries and continues to be a menace. As a result, every State not only has a right, but also a duty, to take action to curb piratical activities."

States are expected to take measures on both the domestic level for example, by criminalizing piratical acts and on the international level. The key element of the latter is international cooperation, whether directly among states or through the involvement of international organizations and other mechanisms created by states.

Indeed, international instruments repeatedly refer to the importance of international cooperation in the repression of maritime piracy. Thus, for example, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation ("SUA Convention") provides in Article 13 that state parties shall cooperate in the prevention of the offences defined by that convention.

Similarly, the U.N. Security Council (UNSC), in its series of resolutions related to the threats of piracy and armed robbery at sea off the coast of Somalia (and more recently in the Gulf of Guinea), urged all states to cooperate with each other and with international organizations in combating acts of piracy and armed robbery at sea.

The importance of international and regional cooperation in this domain was also highlighted by the U.N. General Assembly in its resolutions on oceans and the law of the sea. Notably, Article 100 of UNCLOS, titled "Duty to cooperate in the repression of piracy," specifies that "all States shall cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State."

The duty to cooperate is at the core of the piracy section of UNCLOS. Indeed, it is the first provision of this section, thereby providing an appropriate benchmark as well as framework for the substantive provisions that follow. Moreover, while international cooperation is a common theme of UNCLOS, Article 100 is unique in two ways. First, it is the only provision in UNCLOS in which the title is the duty to cooperate. Secondly, it uses the strongest wording found in UNCLOS with regard to this obligation; namely, that all states shall cooperate "to the fullest possible extent."

Article 100 of UNCLOS contains the precise wording of Article 14 of the 1958 Geneva Convention on the High Seas (HSC), which in turn incorporated (again, verbatim) the

corresponding article adopted by the International Law- Commission (ILC) on the law of the sea. All of these provisions went beyond the proposal put together in the scholarly work known as the Harvard Research Draft, which later served as the basis for the discussions of piracy by the ILC and the negotiations of the piracy provisions in the HSC. Article 18 of the Harvard Research Draft provided that "the parties to this convention agree to make every expedient use of their powers to prevent piracy, separately and in co-operation." The commentary to this provision underscored that Article 18 imposes on states only "a general discretionary obligation to discourage piracy by exercising their rights of prevention and punishment as far as is expedient."

By establishing a duty to cooperate, UNCLOS and the HSC therefore send a clearer message than originally foreseen in the proposal of the Harvard Research Draft. Both UNCLOS and HSC, however, did not set out the precise obligations that fall within the scope of the general duty to cooperate, thereby leaving this provision open to interpretation with regard to the means that states should employ to sufficiently fulfill their obligation. At the very least, however, it is evident that inaction or failure to cooperate in response to piratical acts-where both the factual circumstances and the applicable legal framework allow for action and cooperation-cannot be reconciled with the duty as prescribed by Article 100. The ILC, in its above commentary, clearly stated that "any State having an opportunity of taking measures against piracy, and neglecting to do so, would be failing in a duty laid upon it by international law." Similarly, Mr. Jack Lang, the Special Adviser appointed by the U.N. Secretary General to address the legal issues related to piracy off the coast of Somalia, underscored that the degree of flexibility provided by the wording of Article 100 "should not be used as a pretext for failure to prosecute." Professor Rudiger Wolfrum, the honorable justice and former President of the International Tribunal for the Law of the Sea, echoed this approach, stating that "a ship entitled to intervene in cases of piracy may not, without good justification, turn a blind eye to such acts." Professor Wolfrum went a step further by asserting that "turning a blind eye to the activities of pirates is in itself an act of piracy," and by suggesting that states permitting piracy activities may be subject to countermeasures and also, theoretically, to an intervention by the UNSC.

B. The duty to share information as a specific obligation under the general duty to cooperate.

The concrete measures to be applied by states as part of their general duty to cooperate are determined based on the characteristics of the particular threat and the circumstances of each case. Whatever the specific measures are, however, there should be little doubt that information exchange is vital to ensure successful international cooperation in counter-piracy operations.

Indeed, the duty to share information can be identified as a particular obligation within the general duty to cooperate. This conclusion is supported by relevant international instruments. For example, the SUA Convention provides that "States Parties shall co-operate in the prevention of the offences set forth in article 3, particularly by…exchanging information in accordance with their national law."

As explained by Justice Tuerk in reference to that provision: “there is a duty for States Parties that have a reason to believe that an offense set forth in the SUA Convention will be committed to furnish as promptly as possible any relevant information to those States having established jurisdiction over such offenses.”

In addition, the UNSC resolutions related to the suppression of piracy and armed robbery at sea also urge all states to share information on acts related to piracy and armed robbery at sea. The U.N. General Assembly has also emphasized the importance of information sharing as part of international cooperation in addressing the problem of piracy.”

On the regional level, the need for information sharing as a means of promoting cooperation in the suppression of piracy was a prime motivator for Asian states in adopting the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (Re CAAP). A key feature of Re CAAP is the creation of an information sharing center, based in Singapore, whose role is to undertake the collection, collation, and analysis of information received from state parties and to ensure a flow of information between them. Similarly, the more recent sub-regional Codes of Conduct, adopted in 2009 in Djibouti and in 2013 in Cameroon, both inspired by Re CAAP, each provide that cooperation among the state parties shall include "sharing and reporting relevant information." The Codes of Conduct further provide for detailed obligations related to information sharing, such as the need to designate a national focal point to facilitate coordinated, timely, and effective flow of information.

The duty to exchange information related to the prevention and suppression of maritime piracy may also derive independently from the abovementioned principle of due diligence. This concept entails, inter alia, that states have a responsibility to forewarn other countries about potential threats by communicating relevant information and updating international police databases in a systematic and comprehensive fashion. The "responsibility to forewarn" is not a new notion under international law. For example, in the Corfu Channel case, the International Court of Justice pointed to the duty of states to notify and warn countries of an imminent danger based on certain general and well-recognized principles such as elementary considerations of humanity.

With the Corfu Channel case in mind, the obligation to forewarn was introduced into UNCLOS, where it is provided in Article 24(2) that “the coastal State shall give appropriate publicity to any danger to navigation, of which it has knowledge, within its territorial sea.”

It would be reasonable to contend that activities of a piratical nature pose a “danger to navigation” within the meaning of Article 24(2), thereby requiring the coastal state to warn other states of such known activity in its territorial waters. Beyond the territorial sea, the duty to forewarn is a corollary obligation of the duty to cooperate enshrined in Article 100 of UNCLOS, and by other relevant instruments, such as the SUA Convention and the abovementioned UNSC resolutions.

C. Scope of the Duty to Share Information and the "National Security" Exception

Frequently, the international instruments applicable to the suppression of piracy do not shed much light on the precise scope of the duty to share information. In the SUA Convention, the need to share information is mentioned, yet without further details.

Consequently, states are left to decide what precise information should be shared, how it is to be transmitted, and when it is to be delivered. Moreover, even when more detail on the duty to share information is provided, restrictions are often imposed due to national security, sovereignty, or commercial confidentiality concerns. Such restrictions are found in the SUA Convention (exchange of information "in accordance with national law"), as well as in Article 302 of UNCLOS, a general provision concerning the disclosure of information: "Nothing in this Convention shall be deemed to require a State Party, in the fulfillment of its obligations under this Convention, to supply information the disclosure of which is contrary to the essential interests of its security."

These restrictions-in particular, those based on the "national security" argument-can be used by states to justify their decision not to share information. Nonetheless, it is submitted that the implementation of laws and regulations that prevent or restrict the exchange of information should be done only as an exception to the general obligation to share information deriving from Article 100 and the due diligence principle. Thus, if a state possesses relevant data, and it neglects-or even refuses-to share it, it carries the burden of justifying such a position.

This approach is grounded in the wording of provisions such as the abovementioned Article 302 of UNCLOS, which allows non-disclosure of information only for purposes of protecting "essential interests of state security. It is further based on the fundamental principle under international law requiring states to fulfill their obligations in good faith. Indeed, if, as a matter of policy, a state refrains from sharing information related to the prevention and suppression of maritime piracy, it can hardly be argued that it fulfills its obligation to cooperate in good faith.

This conclusion is further supported by the nature of piracy as, in essence, an ordinary law crime. Accordingly, the type of information whose sharing is of importance for the purpose of combating maritime piracy would typically be that which is exchanged as a standard procedure among law enforcement authorities when countering crime: identification of suspects, modus operandi, etc. Thus, in general, the sharing of such information between the entities involved in counter-piracy operations (whether the navies or law enforcement agencies) is unlikely to compromise national security. It should therefore not be surprising that at least among law enforcement agencies and based on INTERPOL's practice following the creation of its Global Maritime Piracy Database, in the domain of maritime piracy; very few restrictions have been imposed by INTERPOL's member countries on information exchanged via the INTERPOL information system.

D. Data sharing mechanisms

A range of mechanisms currently exist for sharing maritime monitoring and surveillance data at national and international level. While some national level mechanisms enable the sharing of data among different agencies for a range of different purposes, at the international level such mechanisms are single purpose.

National data sharing mechanisms

The French SPATIONAV information system is designed to collect and compile data generated by a range of sensors to assist maritime operational centres in the performance of their duties. The principal partners are the Navy, the Directorate of Maritime Affairs and the Customs Department. SPATIONAV, which makes use of data provided by coastal observation stations and AIS, operates alongside another mechanism, TRAFIC 2000, which was developed to implement the VTM Directive. The primary role of TRAFIC 2000 is to provide the authorities responsible for maritime security the data necessary to assess risks to security, safety and the environment from vessels, including those carrying dangerous or polluting goods. The system is intended to be integrated with SafeSeaNet (see below). Finland has a well developed maritime data exchange mechanism the principal actors in which are the Navy, the Frontier Guard and the Maritime Administration. Pursuant to a 1993 inter-agency memorandum, AIS and VTS data, including data from the GOFREP reporting system are sent by the Maritime Administration to the Navy as are data gathered by the Frontier Guard from its patrol vessels and aircraft and sensors. This data is then compiled with the Navy's own classified data to create a real-time maritime picture. Data is then distributed to the two agencies in accordance with their needs. It is also supplied to a range of 'secondary' agencies including the environment ministry, customs, police and rescue service.

Regional AIS data sharing agreements

The HELCOM AIS Network enables the real time sharing of AIS data among the parties to the 1992 Helsinki Convention (Denmark, Estonia, EC, Finland, Germany, Latvia, Lithuania, Poland, Russia and Sweden) and Norway. The North Sea Data Exchange, developed with the assistance of INTERREG III undertakes a similar function for North Sea countries Norway, Sweden, Denmark, the Netherlands, Belgium and the UK and a similar network is currently planned for the Mediterranean.

SafeSeaNet

SafeSeaNet is a data exchange system, based on an index server, developed by EMSA to support the implementation of elements of the VTM Directive (relating to port, HAZMAT, ship and alert notifications). SafeSeaNet is not specifically referred to in the VTM Directive although some of the reporting requirements are. It is envisaged that SafeSeaNet, which is not yet fully operational will also be used to distribute LRIT data. One of the reasons for its slow implementation has

been concerns at the Member State level over data security and the lack of a clear and binding data policy for SafeSeaNet.

Commercial AIS data sharing mechanisms

Because, AIS data is unencrypted and broadcast over publicly available wavelengths, a number of commercial companies have successfully established web-based AIS data sharing mechanisms. The first such service, and one of the largest, is AIS Live which is owned by Lloyds Register Fairplay Limited. Access to this service is by subscription.

Finland/Sweden

Since 2006 the Swedish and Finnish navies have routinely exchanged their respective compiled maritime pictures on the basis of a 2005 memorandum of understanding. The data shared is classified and is safeguarded in accordance with applicable national legislation.

Maritime Analysis and Operations Centre – Narcotics (MAOC-N)

MAOC-N, which is based in Lisbon, is a law enforcement centre that coordinates the maritime interdiction of illegal drugs trafficked on the high seas. It was established in 2007 on the basis of an agreement between Ireland, the Netherlands, Spain, Italy, Portugal, France and the UK. Data is gathered from a range of sources including AIS and classified intelligence.

Virtual Maritime Traffic Centre (V-RMTC)

The V-RMTC is a virtual network connecting the operational centres of a number of navies that enables the sharing via internet of unclassified information on merchant shipping. Coordinated by the Italian Navy, it was established in 2006 pursuant to an Operational Agreement between some 15 countries with naval interests in the Mediterranean.

NATO – Marine Situational Awareness (MSA) Concept

NATO's Maritime Safety and Security Information System (MSSIS) is based around AIS data, provided by NATO-member States and a number of non-NATO States, which the location and movement of some 10,000 ships to be tracked each day. This data is then analyzed using a range of software analysis tools, some of which make use of commercial and open source databases, to identify potential anomalies. The analyzed data is then fed into NATO's Maritime Command and Control Information System which also includes intelligence data, classified data and the real-time location of NATO vessels.

Other planned data sharing mechanisms

On 13 February 2008 the European Commission adopted a communication on the creation of a European Border Surveillance System (EUROSUR) with the main purpose of preventing unauthorized border crossings, reducing the number of illegal immigrants losing their lives at

sea, and increasing the internal security of the EU. The communication proposes that in a first phase existing surveillance systems and mechanisms should be interlinked and streamlined and that a secure computerized communication network should be established in order to permit real-time data exchange 24 hours a day between centres in the Member States as well as FRONTEX. Phase 2 is concerned with the development and implementation of common tools and applications for border surveillance at EU level while Phase 3 will seek to integrate all existing sectoral systems which are reporting and monitoring traffic and activities in European waters into a broader network to allow border control authorities to take advantage of the integrated use of these various systems. Meanwhile the European Defence Agency (EDA) began work some two years ago on its Maritime Surveillance Project (MARSUR) in order to explore the needs and requirements for a purely European naval surveillance system.

MARITIME LAW ENFORCEMENT

A question that surfaced in past generations whether human rights apply on the water-is no longer the salient issue. Rather, courts, governments, and deployed naval forces are now confronting the issue of harmonizing human rights with the inherent challenges of high seas maritime law enforcement interdictions. It is an urgent issue today not just because of increased judicial attention or because certain terms that have no uniformly, internationally accepted definition are populating bilateral and multinational documents. It is an urgent issue because no consistent approach to harmonizing human rights obligations with operational exigencies necessary in maritime law enforcement exists.

Medvedyev v. France, a European Court of Human Rights case, highlights the struggle of balancing human rights obligations with maritime law enforcement operations.

To combat illicit high seas activity, maritime law enforcement could employ multiple distinct, intersecting, and complementary lines of effort: Action prior to an interdiction, right of approach/boarding, detention, and the assertion of jurisdiction.

Acquiring information that supports situational awareness prior to a boarding is a key enabler of effective maritime law enforcement. Such capabilities may include “radar, photo, audio and video monitoring…that supports the interception of radio and cellular phone communications, maybe e-mails.”

A maritime interdiction is fundamentally different from operations on land and includes unique environmental factors-such as unpredictable weather and sea state conditions-as well as other distinctive operational considerations. “Weather is more punishing on the open water because it comes from above and below,” according to a mariner, adding that severe weather on the high seas is similar to “experiencing an earthquake and a hurricane at the same time.” Issues for a boarding officer operating in this challenging environment could include safely inspecting containers on a moving platform, ensuring connectivity while on a vessel of interest, as well as inspecting the ship's crew, its cargo, and potentially, the vessel itself.

Interdictions present yet another layer of complexity if cargo, such as cocaine, is jettisoned, or if the vessel is scuttled or intentionally set on fire. Though uncommon, maritime law enforcement officers have been killed and seriously injured during boardings."

Other maritime law enforcement challenges include the frequent lack of back-up support and the ability of suspect vessels to evade detection because of their profile, low radar signature, or nighttime operations. Even after addressing operational (and potentially significant logistical, materiel, and medical) issues, legal considerations include: Resolving jurisdictional issues; ensuring an evidentiary chain of custody on a platform that may not have a secure storage space; obtaining witness statements and conducting other aspects of an investigation, possibly while underway; and determining whether to arrest or detain a suspect. Authorities must also identify the port to take suspects to, ensure prosecutorial interest (possibly while underway), and confirm the venue for prosecution.

Judicial recognition of the unique maritime operating environment and its distinctive response spectrum is crucial to effective maritime law enforcement and legal accountability.

A. Applicable Human Rights Law

Human rights law does not reside in one document but, rather, is drawn from multiple accords, regional and international instruments, judicial rulings, and national policy. "Soft law" adds yet another layer of complexity to developing human rights norms." This Part addresses institutions- primarily regional tribunals- and human rights provisions most operative in maritime law enforcement operations and discusses the United Nations (U.N.) system of protection of human rights. Identifying human rights obligations across an intricate array of instruments, multinational tribunals, and institutions represents the starting point for assessing how those obligations intersect with maritime law enforcement operations.

The U.N. Human Rights Council, along with its Universal Period Review process and various committees (e.g., the Human Rights Committee) that supervise numerous conventions are a relatively recent development. A 2006 U.N. General Assembly Resolution acknowledged and recognized "that peace and security, development and human rights are the pillars of the United Nations system and the foundations for collective security and well-being [and] that development, peace and security and human rights are interlinked and mutually reinforcing.

Authorities on human rights obligations include the Universal Declaration of Human Rights (UDHR), the Convention Relating to the Status of Refugees, the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the Convention against Torture and Cruel, Inhuman or Degrading Treatment or Punishment (CAT), among others. Other relevant instruments include the European Convention on Human Rights (ECHR), the American Convention on Human Rights (Pact of San Jose), the Africa Charter on Human and Peoples' Rights (Banjul Charter), the Arab Charter on Human Rights," and the ASEAN Human Rights Declaration.

In addition to multinational tribunals, domestic courts are also addressing human rights in prosecutions resulting from maritime law enforcement interdictions. Key considerations in judicial rulings in the maritime law environment include determining extraterritorial jurisdiction and interpreting, among others terms, deprivation of liberty, due process, promptness, wholly exceptional circumstances, humane treatment, right to life, and non-refoulement.

The current legal and judicial landscape, which includes multiple conventions and court rulings, represents a broad and uneven array of authorities that impose varying human rights considerations in maritime law enforcement in drug trafficking, piracy, maritime migration, and fisheries enforcement.

B. Drug Trafficking

Several cases have examined human rights in the context of maritime law enforcement operations that successfully interdicted drug traffickers. The most prominent case is **Medvedyev v. France**, where the European Court of Human Rights addressed human rights following a French court's conviction for drug trafficking. The Court ruled on two issues: The right to liberty and security, and promptness. Medvedvev involved crew members acting as traffickers plying the high seas on a Cambodian-flagged merchant ship (Winner) with the “intention of transferring [contraband] to speedboats off the Canary Islands for subsequent delivery to the coasts of Europe.” Responding to a French request, Cambodia authorized French authorities "to intercept, inspect and take legal action" against Winner.'" Because Cambodia was not a party to the Vienna Drug Convention," the French court correctly treated their consent as an ad hoc agreement."" French authorities subsequently interdicted Winner on the high seas, seized 100 kilograms of cocaine, and detained the crew (characterized as a "de facto restriction" on their movement) during their thirteen day voyage to Brest, France. "Because of its poor state of repair and the weather conditions, the ship was incapable of speeds faster than five knots."

A French court found the six suspects guilty of drug smuggling. The convicted traffickers then brought proceedings before the European Court of Human Rights challenging the legality of their detention at sea and the delay involved in bringing them before a court under ECHR articles 5(1) (the right to liberty and security) and 5(3) (the right to be brought promptly before a judge or other authorized officer).

The European Court of Human Rights first addressed whether Cambodia's diplomatic note provided France with authorization to intercept, inspect, and take legal action. The Court held that “the fate of the crew was not covered sufficiently clearly by the note and so it is not established that their deprivation of liberty was the subject of an agreement between the two States that could be considered to represent a 'clearly defined law' within the meaning of the Court's case-law.” Legal commentators have appropriately characterized this portion of the ruling as astonishing and inconsistent with the internationally recognized practice that a flag state may waive jurisdiction to enable a State conducting the interdiction to apply its laws to the

vessel. The ruling on ECHR 5(1)'s right to liberty and security inexplicably dismissed bilateral diplomacy, and instead, appeared to recognize only treaty-level obligations to "prevent the application of foreign law from being arbitrary."

A number of judges dissenting from the ECHR 5(1) holding sagely remarked, "[w]hen there is sufficient concurring evidence to suspect that a ship on the high seas, thousands of miles from the State thus authorized to board it, is engaged in international trafficking to which all countries want to put a stop, it is without a doubt legitimate not to place as narrow an interpretation on the legal basis as one would inside the territory of the State concerned."

Further, Medvedyev explicitly noted "the fight against drug trafficking on the high seas… undoubtedly presents special problems." However, because the court misinterpreted the legal ability of a flag state to waive jurisdiction under international law, its authoritative force is diminished.

Rigopoulos v. Spain is another European Court of Human Rights case that involved a challenge of promptness in a maritime law enforcement counter-drug trafficking operation. In this case, decided approximately eleven years before Medvedyev, a Spanish customs vessel interdiction of drug traffickers on the high seas led to a sixteen-day, 3000-nautical mile transit to Las Palmas (Grand Canary).

C. Fisheries Enforcement

The fishing industry is lucrative, multifaceted, and vulnerable to abuses. Areas examined include those with express guidance that are nevertheless not al-ways followed (imprisonment of fishermen and use of force), areas that pose enforcement and oversight challenges (illegal work conditions), and areas without any express guidance (vessel destruction as enforcement action).

Article 73(3) of the LOS Convention provides: "Coastal State penalties for violations of fisheries laws and regulations in the EEZ may not include imprisonment, in the absence of agreements to the contrary by the States concerned, or any other form of corporal punishment."

Despite this provision, a wide variety of measures have been enacted by coastal States to enforce their laws and regulations relating to fishing in the exclusive economic zone. Some of those measures continue to provide for imprisonment for violations of these laws and regulations despite the prohibition in article 73. Those provisions thus are not consistent with article 73.

A separate LOS Convention provision provides that "[a]rrested vessels and their crews shall be promptly released upon the posting of reasonable bond or other security." Some coastal States authorize imprisonment for fisheries violations if a bond or administrative penalty is not paid or authorize imprisonment for resisting arrest. An NGO study lamented that fishermen were being detained for as long as three years by India and Pakistan.

“The practice of apprehending each other's fishermen, along with their boats, has been followed by Pakistani and Indian forces since the time of the partition” However, as “there is no consolidated information about detained fishermen because it is not updated regularly,” the Asian Human Rights Commission recommended that “there should be a record somewhere, which consists of all the names of all the detained fishermen with their particulars including date of arrest & release and the address of the jail.”

In 2005, the Australian Human Rights Commission held that Australia violated the human rights of Indonesian fishermen detained on vessels in Darwin Harbour. Since 1988, the Commonwealth detained fishermen suspected of illegally operating in the Australian territorial sea and EEZ. For the most part, detained fishermen would remain aboard their vessels awaiting disposition, which generally included posting a financial bond that in some instances could take more than a month. The primary issue addressed by the Human Rights Commission was whether detention aboard a suspect's vessel violates ICCPR and national detention standards." ICCPR article 10(l) provides: "All persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person."

Some of the complaints raised by fishermen included poor bedding ("old foam mattresses with torn covers and one or two blankets and pillows"); a lack of fresh water; insufficient exercise time (one fisherman noted that they were only taken off their boats one day a week to play soccer); insufficient reading material (the same fisherman added: "we were given nothing to read on the boats"); and insufficient toilet/bathing facilities ("fishers go to the toilet on the boat by either defecating or urinating off the edge of the boat or through a hole cut in the deck of the vessel").

Australia explained in their response that:

“Fishers held in boat-based detention are provided with safety and hygiene products, toiletries, mattresses (suitable within the practical constraints of the limited spaces on boats and exposure to the environment), new clothing, lamp oil and kerosene to fuel stoves on arrival in Darwin Harbour. Further, each fisher is also provided with a blanket and, on arrival into Darwin Harbour, given an appropriate briefing. Tarpaulins for protection and cover during inclement weather and additional cooking and heating fuel are made available on request.”

The Commission held that:

The practice by the Commonwealth of detaining Indonesian fishers on their vessels in Darwin Harbour in the conditions and arrangements observed in June 2004 constitutes a breach of human rights under article 10(1) of the ICCPR, even for short periods of detention. Those conditions do not constitute humane conditions of detention as required by this article and are inconsistent with a number of Australia's regulations on detention.

The Commission also specifically held that “the sanitary and shower/ bathing arrangements in place on the vessels were not consistent with human rights .... Fishers were not able to shower or bath at a temperature suitable to the climate.”

Destruction of property-the intentional sinking of a ship-has sparked considerable attention in fisheries enforcement and other maritime law enforcement action. The inherent challenge is that there is no uniformly recognized standard for vessel destruction. The right to property is addressed in, among other instruments, Article 1 of the Protocol to the ECHR, though some human rights documents are silent on the issue. The ECHR provides: “Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.”

The intersection of vessel destruction and human rights begins with first identifying an operative human rights instrument and then determining the basis for government action: safety (e.g., the vessel posed a navigational hazard), enforcement of a U.N.S.C. Resolution (e.g., where the operative provisions provide explicit authority to destroy), or security (e.g., law enforcement action).

The LOS Convention does not expressly address intentional vessel destruction. LOS Convention Article 73(2), however, does address "prompt release" of a vessel and crew. ITLOS rulings on prompt release issues (in the context of enforcement action) highlight due process of law considerations and the need to allow for judicial recourse. The court in **Tominmaru** held, in part, that:

“A decision to confiscate eliminates the provisional character of the detention of the vessel rendering the procedure for its prompt release without object. Such a decision should not be taken in such a way as to prevent the ship owner from having recourse to available domestic judicial remedies, or as to prevent the flag State from resorting to the prompt release procedure set forth in the Convention; nor should it be taken through proceedings inconsistent with international standards of due process of law. In particular, a confiscation decided in unjustified haste would jeopardize the operation of article 292 of the Convention.”

D. Use of Force

Multilateral instruments and jurists recognize that force may be employed in maritime law enforcement and have forged standards for its use. The use of force, particularly deadly force, has the potential to trigger human rights considerations, even in instruments that do not expressly contain human rights provisions.

The ICCPR provides that “every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life.” The Pact of San Jose provides,

“every person has the right to have his life respected. This right shall be protected by law and…no one shall be arbitrarily deprived of his life.”

Similarly, the ECHR provides that “everyone's right to life shall be protected by law.” Deprivation of life shall not be regarded as inflicted in contravention of this Article when it results from the use of force which is no more than absolutely necessary.

Where actions in question involve maritime law enforcement, the ITLOS ruling in **M/V Saiga** represents the seminal case on the use force. M/V Saiga is particularly noteworthy, as no provision of the LOS Convention expressly addresses the use of force. The oil tanker Saiga, registered in Saint Vincent and the Grenadines, operated as a bunkering service in West Africa. Officers from Guinea fired on Saiga, boarded it, and arrested the crew approximately twenty-two miles from their coast. The Hamburg court held that "the use of force must be avoided as far as possible and, where force is unavoidable, it must not go beyond what is reasonable and necessary in the circumstances.

Considerations of humanity must apply in the law of the sea, as they do in other areas of international law.

Juno Trader involved a dispute before the ITLOS in 2004 regarding the detention of a fishing vessel and its crew for alleged illegal fishing in the EEZ of Guinea-Bissau. Judge Treves, in a separate opinion, wrote that “unnecessary use of force and violations of human rights and due process of law are elements that must also be taken into consideration in fixing a bond or guarantee that can be considered as reasonable.”

More recently, in the “**Enrica Lexie**” Incident order, ITLOS in 2015 reaffirmed “its view that the considerations of humanity must apply in the law of the sea as they do in other areas of international law.”

Two international instruments explicitly address use of force in a maritime law enforcement context, both articulating a necessary and reasonable standard where force cannot be avoided (as stated in Saiga). The 2005 SUA Protocols provides:

“When carrying out the authorized actions under this article, the use of force shall be avoided except when necessary to ensure the safety of its officials and persons on board, or where the officials are obstructed in the execution of the authorized actions. Any use of force pursuant to this article shall not exceed the minimum degree of force which is necessary and reasonable in the circumstances.”

And, the U.N. Fish Stocks Agreement provides an inspecting State shall ensure that its duly authorized inspectors “avoid the use of force except when and to the degree necessary to ensure the safety of the inspectors and where the inspectors are obstructed in the execution of their duty. The degree of force used shall not exceed that reasonably required in the circumstances.”

Generally accepted standards for the use of force in maritime law enforcement have developed over the past two decades. While not every scenario has been addressed-notably private sector oversight and the use of force during rescue operations- the existence of generally accepted standards supports consistent training, uniform employment, and importantly, compliance with human rights.

E. Navies Carrying Out Law Enforcement Activities

Since piracy takes place on the high seas, and often very far from the shore, combating piratical acts requires more than the typical police-prosecution cooperation, which is predominant in land-based ordinary law crimes such as theft or robbery. Notably, it calls for the involvement of navies as the front-line entities that both prevent attacks and gather relevant information to facilitate prosecution. In fact, in such operations, the navies exercise activities of a law enforcement nature. This unique feature in combating maritime piracy creates certain problems including those related to information exchange. The lead role taken by navies in combating piracy has also led the international community to overlook the role of law enforcement organizations and agencies, particularly during the early stages of combating piracy off the coast of Somalia. Thus, despite the fact that by the end of 2008 a shift towards a law enforcement paradigm was already underway, it was not until late November 2010 that the UNSC-already in its eleventh resolution related to piracy off the coast of Somalia made a clear reference to organizations such as INTERPOL and Europol operating in the counter-piracy field.

In Resolution 1950, the UNSC underlined the importance of continuing to enhance the collection, preservation, and transmission of evidence of acts of piracy to competent authorities; welcomed the ongoing work of the International Maritime Organization (IMO), INTERPOL, and industry groups to develop guidance to seafarers on preservation of crime scenes following acts of piracy; and urged states, in cooperation with INTERPOL and Europol, to further investigate international criminal networks involved in piracy off the coast of Somalia, including those responsible for illicit financing and facilitation. This rather late inclusion of the law enforcement angle in UNSC resolutions (and elsewhere) was particularly surprising, given that the guidelines for involving police forces in combating maritime piracy had already been put in place when the situation off the coast of Somalia began to deteriorate.

By not considering the potential in engaging the law enforcement community, a number of difficulties have emerged, particularly with regard to facilitating the prosecution of pirates, a task that typically falls within the expertise of law enforcement agencies. Naval forces do not necessarily have the tools or the expertise to gather and preserve the relevant evidence necessary for criminal proceedings. In addition, they generally do not have criminal databases where important data such as personal information on suspects, fingerprints, and DNA can be stored and compared with existing data. Such expertise and tools are at the core of law enforcement activities and international police cooperation. The relative lack of involvement of the police in

those early stages therefore created a gap, or a "missing link," between the navies operating off the coast of Somalia and the prosecution services.

The growing recognition of the need to engage all relevant actors, including the law enforcement community, as part of the holistic interdisciplinary paradigm, led to welcome changes in the mindset that guided the international community in the early stages of combating piracy off the coast of Somalia.

Thus, in addition to the abovementioned UNSC Resolution 1950, three noteworthy examples of the positive shift in approach are found in the following instruments. First, in UNSC Resolution 1976, the UNSC, acting under Chapter VII of the U.N. Charter: (1) invited states, individually or in cooperation with regional organizations, UNODC, and INTERPOL, to examine domestic procedures for the preservation of evidence and assist Somalia and other states in the region in strengthening their counter-piracy law enforcement capacities; (2) underlined the importance of continuing to enhance the collection, preservation, and transmission of evidence to competent authorities; and (3) urged states and international organizations to share evidence and information for anti-piracy law enforcement purposes with a view to ensuring effective prosecution. UNSC Resolution 2020 further highlighted the importance of sharing information with INTERPOL and Europol, including for the purposes of investigating those responsible for illicit financing and facilitation.

The second example is the amendment to the 2008 European Union Council Decision on Operation Atalanta, which is the European Union military operation off the coast of Somalia. The amended framework explicitly instructs Operation Atalanta to: (1) collect data including characteristics likely to assist in identification of piracy suspects such as fingerprints; and (2) circulate, via INTERPOL's channels, and check against INTERPOL's databases, personal data concerning suspects, including fingerprints and other identifiers (e.g., name, DOB, etc.).

A third example concerns the updates introduced in the fourth version of the Best Management Practices for Protection against Somalia Based Piracy. In the Best Management Practices for Protection against Somalia Based Piracy, produced and supported by a number of prominent players in the civil industry and naval forces, a specific chapter was added on cooperation with law enforcement authorities.

These three examples illustrate a positive shift in the strategic view of counter-piracy undertakings. Yet, certain complexities related to the exchange of information between navies and law enforcement entities had to be addressed. First, as a matter of normal procedure, navies tend to designate the data they collect as "classified information." This poses serious impediments with regard to the use of such data for the purpose of prosecution on the national level, as well as in the context of international collaboration with entities (i.e., countries or international organizations) that generally do not have access to classified information. As an example from INTERPOL’s practice, this issue had to be addressed during the discussions that

led to the conclusion of a pilot agreement on information sharing between NATO and INTERPOL.

To address this concern, it is advocated that while the implementation of classified information rules is justified in the operations of navies during wartime or in preparation for military activities, a different approach should govern the operations of naval forces when carrying out missions of a law enforcement nature such as counter-piracy activities. Thus, applying standard navy classification procedures in this context, and consequently withholding from law-enforcement agencies important information such as fingerprints of suspected pirates, can hardly serve the original purpose of classified information. Further, it does not correspond to the general obligation to share information in combating maritime piracy. Piracy-related information either should not be designated as "classified information" in the first place, or it should be declassified as standard procedure.

Sharing information in the other direction, specifically from law enforcement entities to the navies, also posed certain challenges. For example, in the context of INTERPOL's work, a question arose whether INTERPOL may cooperate with navies considering Article 3 of its Constitution, according to which "it is strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious or racial character." A plain reading of this provision could have led to the conclusion that INTERPOL must not share any information with the navies or organizations that operate off the coast of Somalia, such as NATO. INTERPOL nonetheless concluded that as long as the purpose and nature of the collaboration is confined to promoting international police cooperation, Article 3 does not prevent it from doing so. Based on this functional interpretation of Article 3 which permits, in principle, the flow of data from INTERPOL to the naval forces, INTERPOL shared information with the navies deployed in the Indian Ocean, such as a photo album of suspected pirates. The information contained in the photo album, gathered by INTERPOL from its member countries, can assist the navies in identifying Somali pirates, and it can potentially support a decision by the navy to detain suspects pending further investigations.

MODULE-IV

ARMED CONFLICT
&
NAVAL WARFARE

LAW OF THE SEA DURING ARMED CONFLICTS

The Second Geneva Convention applies in the first place in case of an international armed conflict that takes place wholly or partly at sea. Pursuant to Article 3 common to the four Conventions, fundamental protections also apply in the event of a non-international armed conflict at sea. While the meaning of the term 'sea' is central to determining the applicability of the Second Convention, the latter does not contain a definition of this term. It is commonly understood that the term 'sea' is used to distinguish the scope of application of the Second Convention from that of the First Convention, which applies on land. To avoid a protection gap between the two Conventions, the term 'sea' should be interpreted broadly. Thus, for the purpose of determining who deserves the protection of the Second Convention, the term 'sea' comprises not only salt water areas such as the high seas, exclusive economic zones, archipelagic waters, territorial waters and internal waters, but also other bodies of water such as lakes and rivers.

Once wounded, sick and shipwrecked members of the armed forces are put ashore, the Second Convention ceases to apply and these persons immediately benefit from protection under the First Convention. This principle applies regardless of the 'branch' of the armed forces a person belongs to: a member of the air force who is shipwrecked at sea is protected by the Second Convention, as much as a member of the navy who is wounded on land is protected by the First Convention.

Although persons cannot be simultaneously protected under the First and Second Conventions, they can benefit from the parallel application of the Second and Third Convention. When wounded, sick or shipwrecked members of the armed forces are cared for by medical personnel or on hospital ships of the enemy force, they "fall into enemy hands" and thus become prisoners of war, protected under the Third Convention. Until their recovery, and as long as they remain at sea, they continue to be protected under both the Second and Third Conventions. Wounded and sick prisoners of war who are put ashore are protected simultaneously by the First and Third Conventions. Once they are recovered, they remain protected under the Third Convention until their final release and repatriation.

Provisions of the Fourth Convention are also relevant in the event of an armed conflict at sea, for the protection of wounded, sick and shipwrecked civilians. The Fourth Convention requires, for example, that parties to the conflict assist the shipwrecked and protect them against pillage and ill-treatment, as far as military considerations allow. It also mandates the respect and protection of specially provided vessels on sea used to transport wounded and sick civilians, the infirm and maternity cases.

Moreover, Additional Protocol I, applicable to international armed conflicts, supplements the Second Convention. It provides several definitions relevant to enhanced protection for the wounded, sick and shipwrecked at sea. The Protocol also extends the protection of the Second

Convention to all civilians who are wounded, sick or shipwrecked, and to other medical ships and craft than those mentioned in the Second Convention.

Additional Protocol II, applicable to non-international armed conflicts, complements the provisions of Article 3 of the Convention. For example, it prescribes the search and collection of the wounded, sick and shipwrecked and their protection against pillage and ill-treatment.

Finally, it should be mentioned that customary humanitarian law also applies to warfare at sea. In this regard, special mention must be made of the 1994 San Remo Manual on International Law Applicable to Armed Conflicts at Sea, which, in its own words, is a "contemporary restatement – together with some progressive development - of the law applicable to armed conflicts at sea" and which "has been drafted by an international group of specialists in international law and naval experts".

In parallel to these other IHL sources; the Second Geneva Convention also interacts with other sources of international law regulating activities at sea. This includes the 1982 UNCLOS. The outbreak of an armed conflict at sea does not terminate or suspend the applicability of most provisions of UNCLOS; they remain in operation and apply simultaneously to the Second Geneva Convention during an armed conflict.

This complementarity is reflected in the updated Commentary on the Second Geneva Convention. The term 'warship', for example, used several times in the Second Convention, must be interpreted based on the definition provided for in Article 29 UNCLOS.

There are also a number of treaties adopted under the auspices of the IMO, in particular the Safety of Life at Sea (SOLAS) Convention and the Maritime Search and Rescue (SAR) Convention. With regard to those IMO treaties that do not expressly limit their scope of application by exempting warships, the question arises to what extent and how they apply during an armed conflict that takes place wholly or in part at sea. No clear answer to this question currently exists. Arguably, these IMO treaties are "multilateral law-making treaties" that, based on the International Law Commission's 2011 Draft Articles on the Effect of Armed Conflicts on Treaties, belong to the categories of treaties that may remain in operation during armed conflict, also when this takes place at sea.

Features of the Protective Scope of the Second Convention

There are certain substantive differences between the First and Second Geneva Conventions. These differences relate to the persons and objects protected under the respective Conventions.

1. Protection of the Shipwrecked

While the basic protection provided for in both Conventions is the same, the scope of persons covered by that protection in the Second Convention is adapted to warfare at sea. The Convention does not only protect the wounded and sick, but also the shipwrecked. Thus, the text

of common Article 3 is worded slightly differently in the Second Convention compared to the other three Conventions, which has been reflected in the updated Commentary. Whereas in the First, Third and Fourth Geneva Conventions reference is made only to the "wounded and sick", the Second Convention consistently refers to the "wounded, sick and shipwrecked". For the purpose of common Article 3, a 'shipwrecked' person is someone who, as a result of hostilities or their direct effects, is in peril at sea or in other waters and requires rescue. A person would also qualify as shipwrecked where, for example, hostilities adversely affect the ability of those who would normally rescue them to do so in fact. It should be noted that a person in such situations must not commit any hostile acts.

Likewise, Article 12 which establishes the general obligation for States to respect and protect in all circumstances, refers to the "wounded, sick and shipwrecked", whereas Article 12 in the First Convention only refers to the "wounded and sick".

2. Protection of Hospital Ships and Coastal Rescue Craft

Logically, the difference between the First and Second Conventions also extends to the objects that are protected. While ambulances and other land based medical transports are protected under the First Convention, medical transports used on water are protected under the Second Convention in equal measure. Recognizing an important means by which its obligations may be implemented, the Second Geneva Convention affords protection to hospital ships and coastal rescue craft, as well as to ships chartered for the transport of medical equipment and to medical aircraft.

The operation of hospital ships constitutes one way in which parties to the conflict can carry out their obligation to protect and care for the wounded, sick and shipwrecked at sea. To be able to fulfill this function, hospital ships enjoy special protection "at all times", and they may neither be attacked nor captured. The hospital ship's personnel and crew are likewise accorded special protection, owing to the vital role they play in the ship's performance of its humanitarian functions.

In order to benefit from special protection under the Second Convention, hospital ships must have been "built or equipped.., especially and solely with a view to assisting the wounded, sick and shipwrecked, to treating them and to transporting them". It follows that hospital ships may not serve any other than the said humanitarian purpose, and that they lose their protection if they are used to commit acts harmful to the enemy. As noted in the updated commentary on Article 22, it is their exclusively humanitarian function of impartially providing assistance to the protected persons that justifies their special protection, but parties to the conflict have the right to control and search hospital ships to verify that their use conforms to the provisions of the Convention. This far-reaching right has been inserted by States in the Geneva Conventions in order to counter the possibility that an enemy's hospital ship is being abused to further military operations.

At present, only a small number of States have military hospital ships, which are expensive to operate and maintain and difficult to protect against attack. The updated commentaries on Articles 33, as well as Articles 18 and 22, point out that one option available to parties seeking to comply with their obligations to respect and protect the shipwrecked, wounded and sick is to transform a merchant vessel into a hospital ship. It is important to note that once a merchant vessel has been transformed into a hospital ship by a party to the conflict, it may not "be put to any other use throughout the duration of hostilities".

The Second Convention regulates a variety of aspects pertaining to hospital ships. Two issues in particular have become topical since 1949. First, Article 34(2) refers, as an example of an 'act harmful to the enemy' (which may lead to a loss of protection) to the requirement that "hospital ships may not possess or use a secret code for their wireless or other means of communication". Thus, in principle none of the communication to and from the hospital ships may be encrypted, but must be sent in the open. Due to developments in communication technology, most prominently the use of satellites, encryption is now so common to the point of being unavoidable as available technology, and the rule has been challenged in a number of military manuals. This development leads the updated Commentary to conclude that "there is, therefore, a certain trend in international practice whereby the use of satellite communications does not constitute a violation of paragraph 2, even if messages and data are transmitted using encryption."

The second topical issue pertains to whether hospital ships may be armed, in particular whether they may be armed to the level of being able to defend themselves against incoming attacks (as opposed to relying on other vessels, in particular warships, to defend them). In principle, the arming of a hospital ships with weapons other than purely deflective means of defense (such as chaffs and flares) or other than light individual weapons could be considered an act harmful to the enemy, leading to a loss of protection.

Thus, in order to maintain their specially protected status under IHL, the Commentary considers that a Party to the conflict may not mount such weapons on a hospital ship.

In addition, the Second Convention affords protection to small craft used by the State or by officially recognized search and rescue organizations.

To qualify for protection under Article 27, coastal rescue craft must be employed by a State that is party to the conflict or by officially recognized lifeboat institutions of a party to the conflict. In the latter case, these institutions must be "officially recognized" for the craft to be protected. This means that the institution must have been approved or authorized by a government authority or other public body to perform coastal rescue functions.

Coastal rescue craft have long rendered assistance to those in distress at sea and might be the only vessels available for this purpose to the vast majority of States which do not have hospital ships. Yet, owing to their small size and speed, at the time of the adoption of the Second Convention, rescue craft were considered difficult to identify and were often suspected of

engaging in intelligence gathering for the enemy. As explained in the updated commentary on Article 27, this generated reluctance among States to grant them any special protection. The compromise embodied in the Convention is to give small craft special protection, but more limited than that afforded to hospital ships. Compared with the eleven articles dedicated to hospital ships, it only one deals with coastal rescue craft, namely Article 27.

Coastal rescue craft that satisfy the conditions for protection may not be attacked, captured or otherwise prevented from performing their humanitarian tasks. This protection extends "so far as operational requirements permit". By contrast, the protection afforded to hospital ships is stronger. They "may in no circumstances be attacked or captured, but shall at all times be respected and protected".

Hence, operational considerations by a reasonable commander may justify interference with rescue craft by, inter alia, preventing them from performing their humanitarian tasks in a given sea area. Since the reasonableness will, of course, depend on the prevailing circumstances, it is impossible to define the terms in an abstract manner. In this context, it is important to emphasize that this provision cannot be read in isolation from the rules of Additional Protocol I regulating the conduct of hostilities. Thus, coastal rescue craft may only be the object of an attack if they qualify as a 'military objective' in the sense of IHL.

Finally, there is no mention in the Convention of the status of the crew of coastal rescue craft.

With respect to the marking of hospital ships and coastal rescue craft, it is not constitutive of their protection but merely signals their protected status to the parties to the conflict. According to Article 43, all surfaces of the ship or craft shall be white and one or more dark red crosses shall be displayed on each side of the hull and on the horizontal surfaces. These traditional marking methods, presupposing close physical proximity to allow for visual confirmation of the marking, might not suffice to ensure the proper identification of protected vessels in view of contemporary techniques of naval warfare, such as long-fire and submarine capabilities. It is therefore significant that Article 43 encourages the parties to the conflict to conclude special agreements on the "most modern methods available to facilitate the identification of hospital ships". As noted in the updated commentary on Article 43, there is no reason why such agreements could not also be concluded for coastal rescue craft. Such agreements could be critical to ensure that protected vessels are effectively identified by parties to the conflict and given the protection to which they are entitled to be able to carry out their humanitarian work.

SUBSTANTIVE OBLIGATIONS UNDER THE SECOND GENEVA CONVENTION

Further to the central obligation on the parties to an armed conflict that takes place at sea to respect and protect the wounded, sick and shipwrecked, and to treat them humanely in all circumstances, the Second Convention sets out a number of additional obligations intended to ensure that this core obligation is fulfilled. This includes the obligation to take all possible measures to search for and collect the wounded, sick, shipwrecked and dead at sea.

To achieve the protective purpose of the Second Convention, it is paramount that the parties to the armed conflict, after each engagement, take all possible measures to search for and collect casualties. The parties might be the only actors sufficiently close to the victims to search for and collect them." Article 18 of the Convention thus requires the parties, after each engagement and without delay, to take all possible measures to search for and collect the wounded, sick, shipwrecked and dead at sea, without discriminating between their own and enemy personnel. The good faith interpretation and implementation of this provision is of critical importance in order to achieve the objectives of the Second Convention.

The obligation to "take all possible measures" is an obligation of conduct to be carried out with due diligence." All possible measures must be taken "after each engagement" and "without delay". In this respect, Article 18 differs from the parallel provision in the First Convention, which requires its obligations to be carried out "at all times, and particularly after an engagement". As the updated commentary on Article 18 explains, the different wording reflects the fact that the conditions of warfare at sea, compared to those on land, might make it impossible to carry out search and rescue activities "at all times".

What constitutes "possible measures" in any given case is inherently context-specific. Each organ of the "Party to the conflict" - entity to which the obligation applies - has an obligation, at his or her own level, to assess in good faith which measures are possible.

Moreover, the updated commentary on Article 18 takes into account the fact that advances in technology and scientific knowledge may influence what measures a party to the conflict can, in practice, take in any given case.

Advances in methods of naval warfare since 1949 have resulted in ever longer-distance attack capabilities. A vessel that has launched a weapon from a considerable distance against an enemy warship or aircraft might not be able to implement itself "without delay" any of the obligations contemplated on the basis of Article 18, since it is not physically present in the vicinity of the casualties, and thus not in the possibility of undertaking any. Still, that vessel remains under an obligation to consider what measures are possible in light of the circumstances. This includes considering whether it is possible to take measures such as disclosing the geographic location of the attacked vessel or aircraft with as much precision as possible, not only to its land based authorities but also to enemy and neutral vessels or impartial humanitarian organizations capable of conducting search and rescue operations.

In this regard, the availability of new technology such as satellites and unmanned aerial platforms can enable a more accurate assessment of the number and location of the shipwrecked, wounded, sick and dead without requiring physical proximity to the attacked vessel or aircraft.

The commentary on Article 18 also describes certain advances in technology and scientific knowledge pertinent to the obligation to search for the dead at sea. There have been considerable developments in underwater technology since 1949 that permit locating and retrieving dead

bodies at sea, including remotely operated vehicles with cameras. Moreover, scientific research in marine taphonomy has led to enhanced understanding of the factors that affect human remains in water. The fact that bodies cannot be seen with the naked eye immediately after an engagement no longer means that none can be recovered. The extent to which a party has access to such technology and knowledge may therefore affect the interpretation of the "possible measures" that party can take in relation to the search for the dead.

As a measure to comply with both Articles 12 and 18, a party to the conflict "may appeal to the charity" of neutral vessels to help with the rescue effort as set out in Article 21. The updated commentary on Article 21 notes that, in some situations, the assistance afforded by neutral vessels might be the best or only way of ensuring that as many wounded, sick, shipwrecked or dead persons as possible can be collected. The use of the word "may" in Article 21 implies that making such an appeal is optional. However, there may be cases, such as where a party is unable to carry out a rescue itself, where it may have to make an appeal in order for that party to comply with its obligations.

Once collected, the wounded, sick and shipwrecked must receive "adequate care" as soon as possible. This includes providing the medical care and attention required by their condition, as well as other forms of non-medical care, such as provision of food, drinking water, shelter, clothing, and sanitary and hygiene items. The parties are furthermore required to record information that can assist in the identification of the wounded, sick, shipwrecked and dead, and to forward this information to the power on which they depend. This is crucial so that families can be apprised of the fate of their loved ones. Specific obligations pertaining to the dead include respectful and honorable treatment, burial and respect for their resting place.

With regard to the position of neutral States (i.e., States not Party to the international armed conflict), the Second Convention contains a number of provisions regulating their obligations vis-a-vis the persons protected by this Convention. First, when they receive or intern such persons in their territory, they shall apply the provisions of the Convention by analogy. Secondly, when such persons are taken on board neutral warships or military aircraft, or are landed in a neutral port with the consent of the local authorities, the Convention stipulates that "where so required by international law" they shall be so guarded that they cannot again take part in operations of war. In view of the scarce and conflicting State practice and literature on this topic, the interpretation of the precise contours of the term "where so required by international law" has proven to be one of the most complex issues the updated Commentary had to deal with. Undesirable as this may be from the perspective of legal certainty, ultimately, States seem to have retained their freedom of interpretation on this point.

UN CHARTER AND ARMED CONFLICT

A. The notion of "armed attack"

i. The UN Charter system

The UN Charter was concluded in an era where the whole of the international community was in search of (a long lasting) peace. As a consequence, the prohibition on threat or use of force is set forward in very strict terms in Art. 2(4) of the Charter, which reads "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".

As strict as it is, the provision is far from being unambiguous in itself and also in relation with other related provisions of the Charter. The provisions regarding "contra-peace situations" envisaged in the Charter employ different terms. As has just been set forth, the first term we see is use of force¸ in Article 2(4). The second term is aggression in Article 39, which is utilized in relation to the powers of Security Council regarding threats to peace, breaches of the peace and acts of aggression. The last term, armed attack in Article 51 has been put as a pre-condition for the exercise of the right to self-defence of the States. However, no definition has been given to these terms and thus their relationship has been left unclear. Before going into the definition of armed attack, a clarification on how these notions are related is necessary.

Article 51 of the UN Charter, which regulates the exercise of the right to self -defence stipulates that "nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations". The undefined notion of armed attack will now be explained by comparison to the notions of "aggression" and "use of force".

ii. "Aggression" versus "armed attack"

The term aggression used in Article 39 of the UN Charter is defined in the well-known General Assembly Resolution on the Definition of Aggression. The definition given herein is composed by a general conception of the notion and a list of exemplary situations. The first Article is read as follows; "aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition."

This definition, which can be interpreted as including both direct and indirect use of force9, shows a significant resemblance to Art.2(4) of the UN Charter which prohibits the threat or use of force but it does not include "threat"; for an act to be qualified as aggression, "an actual use of armed force is required". Interestingly, the following Article of the Resolution, referring to

"relevant circumstances" that should be taken into account in defining aggression also includes certain gravity of the acts or of their consequences.

What makes defining aggression crucial for the analysis of the meaning of armed attack is the utilization of the Resolution 3314 by the International Court of Justice (ICJ) while elaborating on the notion of armed attack. Indeed, all in the **Nicaragua**, **Oil Platforms** and **Armed Activities** cases, the Court takes the Resolution as a starting point in its analysis on the definition of armed attack. Furthermore, it is also noteworthy that while the Preamble of the Resolution refers to aggression as "the most serious and dangerous form of the illegal use of force", the ICJ interprets armed attack as "the most grave form of the use of force".

Today, it is accepted by the majority of the doctrine that an armed attack necessarily constitutes aggression. It can be seen that the same view was shared by most of the states during the discussions within the Fourth Special Committee on the Question of Defining Aggression where they agreed that there is a "cascading relationship between the terms 'use of force', 'aggression' and 'armed attack'"

iii. "Use of force" versus "armed attack"

To draw the borders of the prohibition of use of force, one must primarily define "force". The general tendency in State practice, embodied in the Friendly Relations Declaration, is to limit its meaning to the military use of force.

Regarding the notion's relation with that of armed attack, it is widely accepted that the former constitutes a part of the latter. It is of note that the use of force is not only confined to the "armed force" whereas the notion of armed attack necessarily requires resort to arms. The direct and most important conclusion that can be drawn from this differentiation is that there exists a "force gap" between the two Articles and thus not every use of force can be replied by an exercise of the right to self-defence.

The distinction between the notions is made mainly due to the gravity of the act or of its effects. Brownlie, for example, explains that a use of force must attain certain gravity in order to be defined as an armed attack. Looking at formal state practice, it can also be seen that during the travaux aiming at defining aggression, numerous states were of the view that only "most serious uses of force qualified as armed attack". In any case, the most significant statement on the relationship of use of force and armed attack has been made by the ICJ, which has distinguished the "most grave forms of use of force" (i.e. those amounting to an armed attack) from "other less grave forms". This confirms the view that there indeed is a gap between the two relevant articles of the Charter. Second, it implies that there exists "a form of de minimis threshold" which is required for an act to constitute an armed attack. Thus, not every illegal use of force warrants states to resort to self-defence; the different wordings bring with them a considerable limitation to the exercise of the right to self-defence. In other words, "minor violations of the prohibition of

the use of force falling below the threshold of the notion of armed attack do not justify a corresponding minor use of force as self-defence."

It is true that the Court, with its consistent statements, have put forward the gravity element as an important factor in determining an armed attack. Thus, an armed attack under Article 51 requires "a relatively large scale, […] a sufficient gravity, and […] a substantial effect." According to the ICJ, for example, "mere frontier incidents" do not have the necessary gravity to be considered as armed attacks. However, the Court does not draw the lines of what can be an armed attack in a very concrete way; on the contrary, it can be inferred from the Oil Platforms judgment that the threshold of gravity is a flexible one, which is dependent on the specific circumstances of each case. Taking into consideration the comparison the Court made between the use of force and armed attack as the "most grave form" of it, it can be said that such an intensity threshold is not needed or at least is much lower for an act to constitute use of force.

Lastly, a recent debate must be mentioned. The prohibition embodied in Article 2(4) of the Charter includes only inter-state use of force. In other words, the only entities bound by it are the states. The traditional acceptance regarding the source of armed attack and thus the target of the exercise of self-defence was also in parallel; only states could engage in such activities. However, the post-9/11 era brought upon some discussions on possibility of non-state groups engaging in armed attacks within the meaning of Article 51 of the Charter. Acknowledgment of such a possibility would lead to the creation of a group of acts which are not covered by the prohibition of use of force but which constitute armed attacks and thus the classical hierarchical categorization of the notions will be changed.

B. The notion of "international armed conflict"

The adoption the Geneva Conventions of 1949 was a milestone in the history of the law of war; until then, the law of peace and the law of war were mutually exclusive. From the outset of a war (in legal terms), belligerent states' "normal" relations would be disrupted. The Conventions have brought about the notion of "armed conflict", a notion which is material rather than legal. With this "semantic contribution", the application of humanitarian law was no longer dependent on the will of the states which, until then, could avoid being bound by the "rules of war" by simply denying the existence of a state of war. This purpose is clearly stated in the Commentary:

One may argue almost endlessly about the legal definition of 'war'. A State can always pretend, when it commits a hostile act against another State, that it is not making war, but merely engaging in a police action, or acting in legitimate self-defence. The expression 'armed conflict' makes such arguments less easy.

Common Article 2(1) of the Conventions thus reads as follows:

In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between

two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The following paragraph states that the Conventions will also apply to the cases of occupation "even if the said occupation meets with no armed resistance". Therefore, there are three main situations to which the IHL of IAC is applicable. For the purposes of this paper, the only relevant one is that of "any other armed conflict" so the other options will just be briefly explained. The first option is declaration of war, which was a crucial element in the pre-1949 period as the laws of war and laws of peace were mutually exclusive. For the former to become into play, the war in legal terms (as opposed to in material sense) had to begin. However these declarations have today become obsolete. The second option is occupation, the beginning of which is still controversial and constitutes a debate. Be that as it may, any occupation amounts to an IAC, even without resistance, and IHL as a whole is applicable.

Turning to "any other armed conflict", it is rather straightforward that IHL applies to them. What not as clear-cut is the beginning of an armed conflict; thus, the beginning of the application of IHL. It can be said that IHL deals with the rules applicable in bello and does not thoroughly draw the borders of its scope of application. It is understandable, due to the strict distinction between jus ad bellum and jus in bello; the classification of a situation as an armed conflict is almost never detached from the political nature of the former. Even so, there are two main sources which to a certain extent clarify the notion and which have been widely accepted in the academia. The Commentaries to the Geneva Conventions are a classical starting point in clarifying the provisions and Pictet introduces the so-called "first-shot theory" regarding the beginning of the application of IHL. He explains that

Any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place. The respect due to human personality is not measured by the number of victims. Nor, incidentally, does the application of the Convention necessarily involve the intervention of cumbrous machinery. It all depends on circumstances.

According to this theory, "as soon as the first (protected) person is affected by the conflict, the first segment of territory occupied, the first attack launched" IHL starts to apply. This purely facts-based approach is also later taken by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the **Tadic** case. According to the Court, "an armed conflict exists whenever there is a resort to armed force between States". In the first glance, it can be thought that whereas the Pictet Commentary directly refers to the beginning of a conflict, the ICTY refers its general description. In any case, a conciliating interpretation of the texts together leads to the result that IHL starts to apply from the first act.

C. Comparison of the two notions

i. The nature of the act

It has been explained in the previous section that the majority view is that any violent act can trigger the application of IHL and independently of any (subjective) statements of states. There is no limit on where the act is taken; it can be in the high seas or even in the space. Equally, the appreciation on how the violent act is taken is also quite inclusive; it can be air raids, shelling and today, even launching a cyber-attack. It is crystal clear that "any kind of use of arms" activates IHL. The Pictet Commentary and the **Tadic** interpretation are both inclusive of such incidents.

Looking from the reverse angle, it is also clear that the threat of force, as long as it does not amount to a declaration of war, is not enough to commence an IAC. On the other hand, threatening to use force and taking essential steps in what can objectively end in material damage are different things. For example, laying mines, if they directly endanger even one person, is qualified as an attack in the Commentary to the Additional Protocols of 1977. The sought clarification is about the notion of attack within the meaning of Article 49 of the Additional Protocol I but it is clear that any attack that goes under that Article can a fortiori trigger the application of IHL.

Regarding armed attacks within the meaning of Article 51 of the UN Charter, that is to say an attack that warrants the exercise of right to self-defence, it is generally accepted that certain intensity is needed. In some instances, e.g. when there is artillery shelling or air strikes, it is clear that the threshold is met.

It is suggested that any act can constitute an armed attack if "they result in, or are capable of resulting in destruction of property or loss of lives". This is however, a position that takes into account the necessity and proportionality criteria that must be respected in answering the attack by resort to self-defence. That is to say, in less grave cases, as long as these criteria are respected, the answering act will be a legitimate exercise of self-defence. However, this view is connecting the notion of armed attack, which must be objectively defined in order to prevent abuses, to the respective criteria that must be observed in the use of force through self-defence. As explained in Part I, the gap left between the Articles 2(4) and 51 is on purpose, to avoid escalation of violence between states; the above-mentioned view is dangerously blurring the lines between the two. Moreover, the ICJ doesn't consider "mere frontier incidents" (unless they reach the necessary high intensity required in armed attacks) as forming armed attacks even though they are very well capable of resulting in loss of life. It rather considers them as a "less grave forms of use of force".

A more interesting debate on the nature of the triggering act is if capture of a soldier can qualify as such. The Commentary on the Geneva Convention III stipulates that

Any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces; it suffices for the armed forces of one Power to have captured adversaries falling within the scope of Article 4. Even if there has been no fighting, the fact that persons covered by the Convention are detained is sufficient for its application. The number of persons captured in such circumstances is, of course, immaterial.

This text can be interpreted in two ways. The generally accepted view is that the capture of a soldier can be the starting point of an IAC and trigger the application of (at least) the third Geneva Convention. The absence of any other hostilities or even absence of a pre-existent IAC is irrelevant; the capture is the first and the triggering hostile act of the conflict. In my opinion, it is not that clear, for two reasons. First of all, the phraseology of the text is ambiguous; it may as well be interpreted as explaining the beginning of the material application (as different from applicability – e.g. in the case of an IAC where there are no prisoners of war the third Geneva Convention is not really applying) of the third Geneva Convention during an IAC. Second, the use of the terms "capture of adversaries" can be understood as implying a pre-existing conception of an "adversary" in the moment of seizure, which itself implies a pre-existing IAC. In any case, the majority view is that the capture of a solider is sufficient for an IAC to begin.

Regarding the notion of armed attack, as will shortly be explained, certain intensity is needed. "An armed attack presupposes a use of force producing (or liable to produce) serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property."

In the clear cut armed attack cases such as artillery shelling, it is also clear that the application of IHL will be triggered; in these cases armed attack and the beginning of an IAC overlaps. However, "less grave" uses of force such as frontier incidents are not generally accepted as constituting armed attack, more due to the low intensity of the act rather than its nature. Here, the notions of armed attack and the triggering act of IHL no longer overlap as "a mere frontier incident" is accepted as being capable of initiating an IAC. It should be noted that the first act is still unlawful under jus ad bellum as it's a type of prohibited use of force. However, it does not give rise to the exercise of the right to self-defence. In other words, any forceful answer of the attacked state will still be in breach of the UN Charter. Apropos capture of a soldier as a specific triggering act, it is unlikely that it meets necessary intensity threshold for armed attacks. In this situation an act which is able to trigger the application of IHL will nevertheless not give rise to the exercise of right to self-defence.

ii. The intensity of the act

The threshold of intensity needed in an act in order for it to trigger the application of IHL is extremely low, as can be deduced from the discussion on the nature of the triggering act above. A literal reading of the commentary to Article 2 and ICTY's statement in the **Tadic** case leads to the same result. Furthermore, the text of Article 2 reads that an IAC exists "even if the state of war is not recognized by one of them"; the existence of an IAC depends on an objective assessment of the facts. However, it has been argued that in state practice isolated incidents were never taken as initiating IAC and so there indeed is an intensity threshold, but it is not the view of the majority. Thus, there is no need for an act which is intense per se or in consequences or which continues for a certain amount of time. In short, IHL "applies at the first resort to force between two state-armed forces". Returning to the example of frontier incidents, it is accepted in the doctrine as amounting to an act triggering the application of IHL.

Apropos the notion of armed attack, it has been mentioned before that there exists a threshold of intensity and the attacks that fall below this threshold are classified as use of force falling short of an armed attack. Nevertheless, this seuil is not a stable one; it is a "variable standard". It means that the necessary gravity or intensity is dependent of the specific circumstances of each case and it is not obligatory to apply them separately to each act, instead of in combination. In this regard, the decisions of the ICJ in **Nicaragua**, **Armed Activities** and **Oil Platforms** are interpreted as implying a doctrine of "accumulation of events". A concrete explanation given by Ruys to the notion is as follows:

It deals with situations where consecutive attacks take place that are linked in time, source and cause, in particular when those attacks are part of a 'continuous, overall plan of attack purposely relying on numerous small raids'. In this context, it is argued that incidents that would in themselves merely constitute 'less grave uses of force', when forming part of a chain of events, can qualitatively transform into an 'armed attack' triggering the right of self-defence.

It is true that in all the cases, even if implicitly, the Court has accepted that some acts which fall below the intensity threshold by nature can "collectively" constitute an armed attack, which would in its turn give rise to exercising self-defence. However, for the sake of peace, it is better to interpret this doctrine in a narrow manner and not be forgotten that even though the Court accepted the possibility in principle, an example in practice does not exist.

It is clear that apropos the element of intensity there is a gap between armed attack and IAC. Whereas an attack does not have to be necessarily "intense" or "grave" to be able to trigger an IAC, it must reach a certain threshold to be able to qualify as an armed attack within the meaning of Article 51 of the UN Charter. If the accumulation of events theory is accepted, there would still be discrepancy between the notions. Having a very low threshold¸ IAC would be triggered with the first act which does not (alone) constitute an armed attack. However, the armed attack would be formed at the moment of "accumulation". Thus, during the time from the beginning of

the IAC, until the formation of the armed attack, the prohibition of use of force would stay intact. (Unless an act of the answering state qualifies as an armed attack per se or cumulatively before.)

iii. The origin of the act

Traditionally, wars are carried out by the armed forces of the states. It is of no doubt that if the army of a state engages in hostile acts against another state, an IAC begins. However, this is not a prerequisite for an IAC; it is just a factual observation. Otherwise, it would practically be impossible for states which don't have armies, such as Costa Rica, to actually engage in such an activity.

Before going through other means the states may employ in IAC, it must be noted that the acts of the private persons cannot constitute an armed conflict and by private it is meant that persons or groups who are neither (de facto or de jure) organs of the state nor are under its direction or control that would lead to the attribution of their acts to the state.

First of all, other de jure organs of the state may be utilized to pursue hostile acts by the state, e.g. the police. In the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), it is set forth that a state is responsible for all the acts of its de jure organs. Furthermore, an IAC "may also materialize as a consequence of a military operation by a state but conducted by entities other than the regular armed forces, the question of "who" is involved in the operation is irrelevant." Thus, in the case where other state organs which are not integrated into the armed forces are utilized in an act which would constitute a triggering act of IHL if carried out by the regular armed forces, the consequences can still be the same as in the latter situation.

Second, normally the use of force by individual persons or groups is not sufficient to trigger an IAC. Nevertheless, under certain circumstances, some groups can be qualified as either de facto organs of the state or their acts can be attributable to the state and their acts can also amount to an IAC. In order for a group to be considered as a de facto organ of the state, it must be completely dependent to it. The ICJ has explained this concept in the Bosnian Genocide case. If this is the case, as any act of the group will be regarded as an act of the State within the meaning of Article 4 of ARSIWA, their acts will also be able to trigger an IAC. Furthermore, even if a group does not meet this high threshold of complete dependency, their acts still can be attributable to a state and thus they can initiate an IAC. The ICTY has ruled in the **Tadic** case that if a state has overall control over a group, a conflict between them and another state can be classified as an IAC between the two states. The ICJ has acknowledged in the Bosnian Genocide case that even though it adopts the effective control test in order to establish states' international responsibility, the overall control test may as well be used to qualify a conflict. Thus, if it can be established that a group is a de facto organ or under the overall control of a state, that group can be the origin of the triggering act of IHL.

Turning to who may engage in an armed attack, it is uncontroversial that a state can. Traditionally, the right to self-defence has always been exercised by one state against another. In this regard, the ICJ has held that "Article 51 of the Charter thus recognizes the existence of an inherent right to self-defence in the case of an armed attack by one state against another state."

The real debate on this subject has focused on whether an armed attack can be carried out by a non-state actor as opposed to a state rather than on which entities of the state can be used. Besides its emphasis on the fact that an armed attack can only be launched by a state against another state, the ICJ also accepts the possibility of having an indirect attack. In this regard, it seems to be of the view that only states can carry out such attacks. Especially in the Nicaragua and Armed Activities cases, the Court held that acts of non-state actors that were "sent by or on behalf of a state" may, if meeting the other criteria, amount to armed attacks. If the non-state actors are not sent by the State, for their attacks to be able to amount to an armed attack, the state must at least have a "substantial involvement therein"; this criteria is necessary, in the view of the Court, to attribute the attack to the state. Thus, an attack which was launched from the territory of a state but in which the state isn't involved or which the state was simply unable to stop will not constitute an armed attack. The main conclusion that can be reached from the statements of the Court is that self-defence can only be exercised against a state and thus for a non-state group to be the origin of an armed attack, its acts must be done on behalf of the state or must be attributable otherwise to the state. An armed attack cannot be made by a non-state group per se, without any type of involvement from a state. It is of note that the Court has not used the effective control test it had adopted in order to establish state responsibility for certain violations of non-state groups and by doing so, it has distinguished the two issues. However, the doctrine mainly accepts that Article 8 of ARSIWA which regulates responsibility for conducts directed or controlled by the state reflects the effective control test. In this case, when the threshold of this test is met, the act of non-state group will be attributable to the state and constitute an armed attacked launched by the latter.

This is the position taken by the ICJ, however, after the 9/11 attacks, the general debate and the state practice on the subject have grown towards the acceptance of the possibility that an armed attack by a non-state group alone can also justify the exercise of right to self-defence. These may be the cases for groups harboring in failed states or within states that passively tolerate them but without helping them materially. The wording of Article 51 of the UN Charter, while designating only states as targets of the attack, is silent on the issue of the origin of armed attack. There is thus space for an interpretation accepting that non-state actors can be the perpetrators of an act permitting the exercise of right to self-defence. Furthermore, in Resolutions 1368 and 1373, the Security Council has implicitly accepted the possibility to engage in self-defence against non-state actors. Lastly, even though as explained above that the majority of the ICJ has decided that an armed attack may only be engaged by a state, there was a considerable amount of judges who did not share this view. At a second stage, it is also controversial if the target of the act of self-

defence would be the group itself or the harboring state, even in the absence of any control over the group. However, this debate is beyond the topic of the present paper.

In conclusion it may be said that both for IAC to begin and for an act to constitute an armed attack, states' own organs or entities can be engaged. Regarding acts of the non-state groups, the necessary control that a state must have over the group varies from one notion to the other; whilst for an IAC to be triggered overall control is sufficient, for an act to amount to an armed attack, the required threshold is higher. In this case, some acts that may trigger the application of IHL may nevertheless not warrant the exercise of the right to self-defence and thus the prohibition of use of force may stay intact. On the other hand, if we accept that a non-state group based in another state per se can launch an armed attack within the meaning of Article 51 of the UN Charter; this act can never set off an IAC. It is a subject of a completely different debate, if then; the self-defence answer which will naturally take place on the territory of a 3rd state can trigger the application of IHL of IAC.

iv. The target of the act

For an act to trigger an IAC, it must be directed against the state. It is not obligatory that the target is the armed forces, even though normally, as explained above, they would be the ones waging the war once the conflict has begun. For example, for IHL to be triggered, the act can be directed against the civilian population or against the territory of the state. What is important is not the material target but the abstract target, i.e. the state. The triggering act may appear, since there is no level of intensity needed, as affecting only one single person. In terms of IHL, there should be no controversy if the target is a soldier, a commercial vessel or a random person. However, regarding especially capture as a triggering act, the intention of the state may prove useful; it may as well be a law enforcement act.

The controversial issue is again about the non-state armed groups based on a state's territory. Does attacking such a group necessarily trigger the application of IHL of IAC even if the host state is simply unable to stop the group or has no control over it? Or can it be considered only as a single non-international armed conflict as actually the state per se is not attacked? The majority opinion is that in these cases there are parallel conflicts; one international and one non-international. However, it has also been argued that the mere trans-border nature of the conflict does not directly initiate an IAC and that the nature of the belligerent parties (one state and one non-state group) is the decisive factor in the absence of any hostile intent against the host state.8

Regarding non-state groups over whom a state has overall control being targeted by another state, things are even less clear than the situation in which the groups per se is the origin of an act. There isn't much written in doctrine on this subject neither. First, the two mentioned situations must be distinguished; the reason why an act of a non-state group can initiate an IAC is because they are acting on behalf or under the control of a state and thus their acts are attributable to the latter. Taking into account the second view explained in the preceding

paragraph, when such a group is targeted by another state, how far can the host state itself be considered as the victim? What if the group under control is not within the territory of the controlling state? Should we again try to get some help from the element of intent as in the abovementioned case? In borderline cases, especially in ones including non-state armed groups as targets, the use of this element can prove to be useful. On the other hand, the moment the groups answers, the conflict would be classified as an international one; it seems illogical to give different classifications to the same conflict.

For the notion of armed attack, the target again must be the state itself. The attack can materialize against the "state's territory or its external manifestations abroad". So, it is not important where the target is located, it may even be within the territory of the attacking state. There has been a limited debate on the issue of differentiation between private vessels and military vessels as targets. The Definition of Aggression, a source heavily relied on by the ICJ whilst defining armed attack, does not include any non-territorial non-military targets, so a potential distinction can be appropriate. However, noting that "mining of a single military vessel" may warrant resort to the exercise of right to self-defence, the Court seems to imply that an attack against a private ship flying a state's flag (distinct from being owned by the state) can also constitute an armed attack. A possible difference on the required intensity has been left unclear.

On the issue of targeting of non-state actors based in third states, which are unable to stop them, it should first be reminded that the target of the armed attack can only be a state. In other words, if we accept that, taking into consideration jus ad bellum concerns such as avoiding the escalation of violation between states, it can be advocated that action can be taken against such groups without actually attacking the host state, i.e. without launching an armed attack. However, this is not uncontroversial, as there is definitely an attack against the territory of the state. For groups under the control of the hosting states, an interesting issue arises. As explained before, in terms of establishment of the responsibility of states, the group must either be a de facto organ of the state (ARSIWA Article 4) or must be under the effective control of it (ARSIWA Article 8). If a group is a de facto organ of the state, we may say that an attack against the former will definitely be an attack against the latter as the organs are the state. If a group is under the effective control of the state, they are not the state but their acts are attributable to it, but does this mean that any act against them is actually directed to the state? In my opinion, the object of the ARSIWA is rather to settle the rules of active attribution rather than the passive attribution. In other words, the state cannot be victimised through the group as it's the acts of the groups that are attributable but not the group per se.

In conclusion, targeting of a wide range of objects can constitute both an armed attack and trigger the application of IHL. The difference between the two groups of targets is mostly due to the intensity requirement embedded in the notion of armed attack. Regarding the targeting of non-state actors, many controversial issues arise. In very general terms, it can be said that if a group is under the overall control of a state, an act against them will trigger an IAC between the

two states as it was explained above that there is no good explanation to give two different classifications to the very same situation. If not, it is debated if a conflict between a state and a non-state actor in the territory of a third state will necessarily start an IAC. For armed attacks, depending on the level of the relationship between them and the state, an attack against the group can also constitute an attack against the state. Even in the absence of such a relationship, the territorial state may be deemed to be a victim of an armed attack. Briefly, the classical targets for both acts more or less coincide (even though the group for IAC is bigger). For the non-state armed groups, they are determined according to different sets of rules.

v. The intent of the act

The replacement of the term "war" with "armed conflict" was, as explained before, a deliberate choice of the drafters of the Geneva Conventions. This replacement sought to base the application of IHL on objective norms and rendered how the states consider/classify the situation irrelevant. Thus, the significance of animus belligerendi was ruled out. However, in some borderline cases, the element of intent may prove useful; especially for eliminating the acts occurred due to errors such as accidental entrance of the military troops of one army into a neighboring state's territory. Then, it can be said that without an "intention to harm the enemy", these mistakes will not amount to an IAC. Furthermore, in cases where, for example, a member of the armed forces engages in a hostile act individually, it would be more logical to say that an IAC is not triggered. For his/her acts to be meaningful for the beginning of IHL, they must be placed within the regular hierarchy of the army.

When the act is carried out not by the state itself but by (or through) a non-state armed group, the overall test applied by the ICTY is more clear on the fact that there is no space for animus belligerendi. According to this test "a role in organizing, coordinating or planning the military actions of the military group" is sufficient; it is not necessary for the state to "plan all the operations of the units dependent on them, choose their targets, or give specific instructions concerning the conduct of military operations". Thus, any act carried out by such a group, even the ones not foreseen or intended by the state, (in terms of IHL) will be attributable to the state.

In respect of the notion of armed attack, the "attack" itself implies a certain intention as opposed the notion of "incident". The holding of the ICJ in the Nicaragua case is also in line with this interpretation. Indeed, the Court, while analyzing if the acts in question amount to an armed attack also mentioned "possible motivations" as an element to take into account. However, as a part of the doctrine sets forth, it is not that easy to determine the intention of the aggressor party (and states will not tend to be straightforward about an intention to "attack"). They argue that for this very reason, a mens rea element should not be included in the notion of armed attack.

Regarding armed attacks carried out by non-state groups if they are accepted as being able to do it individually, the abovementioned considerations will still be valid. In the case of an armed attack attributable to a state, as explained the sub-section "Origin of the Triggering Act",

according to the ICJ, they must be sent on the behalf of the state or the state must have a substantial involvement in the act. It can be said that a state which has such a degree of involvement in the act will always also have the animus aggressionis and reversely, to meet the necessary threshold put by the Court, it is indispensable to have the said intent. Examining the same act through Article 8 of ARSIWA, thus through the effective control test, leads to the same result. In cases where a state has control over the armed group (thus is the origin of the attack), the intent that should be taken into account is that of the state and not of the armed group; it is irrelevant for what motives does the latter engage in such activities.

Briefly, it can be said that the notion of intent, at least for the simple and classical examples where states and only states are involved, does not play a crucial role in defining neither of the notions, though it can be useful in some specific cases. Mere attribution is sufficient for an act to constitute an armed attack and to trigger an IAC. Regarding the situations in which non-state actors are involved, it changes a little, especially for the notion of armed attack. The application of different attribution tests to same acts can sometimes result in an act triggering IHL without amounting to an armed attack, as the threshold of the overall test is lower. Furthermore, any act of the group under the overall control of a state is attributable to the latter, but effective control requires control for every specific act. Thus, it can be said that the second test inherently includes intent, no matter if the notion of armed attack per se requires it or not.

vi. The legality of the act

Concerning the legality of the act, the difference between the two notions stem not from their own characteristics but directly from the distinction between jus ad bellum and jus in bello. The legality of the act is irrelevant for the beginning of an IAC; "the applicability of the Geneva Conventions and Protocols does not depend on whether the use of force against another State is permitted or not." Accordingly, state's compliance/incompliance with jus ad bellum does not change the qualification of the situation as an armed conflict. The triggering act, "the act of war", just displays the application of IHL and does not refer to any jus ad bellum issues. For IHL, an armed attack is just another attack.

Armed attack is a notion of jus ad bellum and, at least within the meaning of Article 51, it is inherently unlawful. This can simply be explained by the fact that it warrants a use of force which would normally be unlawful itself. Furthermore, both in International Criminal Law and in Public International Law, self-defence is limited only against unlawful acts; it is thus impossible for an armed attack to be lawful. In other words, as long as an act is lawful (e.g. if it is itself an exercise of self-defence), it cannot be defined as an armed attack under Article 51.

The triggering act of IHL may or may not be lawful under jus ad bellum, as its scope and the scope of armed attack do not exactly coincide. In general terms, the scope of the triggering act covers more acts than what armed attack does, with the exception of independent armed attacks by non-state groups which would not amount to an IAC.

C. Non-international Armed Conflict

While it is a relatively simple matter to determine the existence of an international armed conflict, determining the existence of a non-international armed conflict presents several difficulties. In the 1949 Geneva Conventions, there is only one article referring to this type of situation. This is Article 3 common to the four Conventions, the first sentence of which is as follows:

“In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:”

The drafting of this article gave rise to lengthy debates at the Diplomatic Conference, largely on the question as to the point at which an armed entity, other than govern- mental, could be considered as a 'Party to the conflict'. Another question was what degree of intensity armed clashes had to reach before they could be termed armed conflicts. The Convention required only a very low intensity in armed clashes for the rules relating to international armed conflicts to be applied. Could this 'minimum' degree of intensity also be used mutatis mutandis for non-inter- national armed conflicts?

The Commentary gives the following reply to this question:

“Speaking generally, it must be recognized that the conflicts referred to in Article 3 are armed conflicts, with armed forces on either side engaged in hostilities.”

But, as the Commentary emphasizes, Article 3 must be implemented as widely as possible because, according to it, it calls for the observance of only a few rules which were recognized by the international community as essential long before the adoption of the 1949 Conventions. This interpretation is reinforced by Art. 1 of Protocol II of 8 June 1977 additional to the 1949 Conventions, which states that:

1. This Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.

2. This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts.

The wording of this article creates conditions for application which are not present in Article 3 common to the 1949 Conventions, i.e., responsible command and a certain degree of control of the territory by a party. Unlike Article 3 of the Conventions, it expressly excludes situations of internal disturbances and tensions. The scope of its application is therefore smaller. Protocol II, the threshold of which is higher, would not cover, for example, a situation of urban guerilla in which insurgents are neither in a position to take care of wounded and sick nor to detain prisoners in decent conditions. Neither Protocol II nor Article 3 would apply, for example, in cases of the use of armed forces to quell sporadic demonstrations or to remove strikers from their place of work. Finally, it must be remembered that failure by one party to a conflict to respect IHL does not relieve an adversary of the obligation to respect it; it must at least observe the rules relating to the protection of the human per- son (Vienna Convention on the Law of Treaties 1969, art. 60, para. 5). As it is the protection of the victims which interests us, it can be considered that there is no general condition in which the application of IHL could be suspended. Thus, a State might not subordinate, for example, the repatriation of prisoners of war which it holds to a political condition such as the recognition of a State, as in the Indo-Pakistanis conflict 1971. A further provision should be mentioned which does not directly affect the conditions for the application of Article 3 common to the Conventions or of Protocol II. This is to be found in the final paragraph of Article 3 and also applies to Protocol II: The application of the preceding provisions shall not affect the legal status of the Parties to the conflict. This rule is an implicit reminder that the essential purpose of the Conventions is to protect the victims and that efforts to ensure respect for the Conventions can never in themselves imply the attribution of a certain status to a Party to a conflict. This rule was intended to soothe the fears of the States that rebels could use the implementation of Article 3 to claim the status of subject of public international law, (i.e. having the same rights as States).

Two aspects of non-international armed conflict determining the applicability of international humanitarian Law: the organization of parties and the intensity of hostilities

In its judgment on the merits, the **Tadic** Trial Chamber interpreted the definition expounded in the Jurisdiction Decision as a ‘test’ for the existence of armed conflict and hence also for applicability of common Article 3. The definition ‘focuses on two aspects of a conflict; the intensity of the conflict and the organization of the parties to the conflict’. The Trial Chamber went on to say that in ‘an armed conflict of an internal or mixed character, these closely related criteria are used solely for the purpose, as a minimum, of distinguishing an armed conflict from banditry, unorganized and short-lived insurrections, or terrorist activities, which are not subject to international humanitarian law’.

The two aspects of non-international armed conflict stated by the Tadic Trial Chamber – the intensity of the conflict and the organization of parties to the conflict – provide grounds for the characterization of a state of armed conflict (and thus also for the application of common Article 3). The Trial Chamber in the Delalic case highlighted this interpretation of non-international armed conflict, stating that ‘in order to distinguish from cases of civil unrest or terrorist

activities, the emphasis is on the protracted extent of the armed violence and the extent of organization of the parties involved'. This approach was echoed by the **Kordic** and **Cerkez** Appeals Chamber which stated that 'the requirement of protracted fighting is significant in excluding mere cases of civil unrest or single acts of terrorism'.

In interpreting the definition of non-international armed conflict provided by the Tadic Jurisdiction Decision, the International Criminal Tribunal for Rwanda (ICTR) employed an approach in line with that of the ICTY. Applying it to the situation in Rwanda, the tribunal held that it was 'necessary to evaluate both the intensity and organization of the parties to the conflict'.

These two aspects of non-international armed conflict provide a basis for determining the existence of armed conflict and thus also the applicability of international humanitarian law. However, as noted by Idi Gaparayi, an Associate Legal Officer at the ICTY, 'determining what counts as "protracted" armed violence and as a "well-organized" armed group requires a case-specific analysis of the facts'. The sections that follow will examine the terms contained in the Tadic definition, focusing in particular on the meaning of 'organized armed group' and 'protracted armed violence'. In doing so, a framework for the analysis of facts on a case-by-case basis will be developed.

The organization of parties

The organizational requirement for the characterization of armed conflict has been highlighted on a number of occasions by the International Committee of the Red Cross (ICRC). The Seville Agreement on the Organization of the International Activities of the Components of the International Red Cross and Red Crescent Movement states that 'an armed conflict exists when the armed action is taking place between two or more parties and reflects a minimum of organization'. The importance of organization was also emphasized by the ICRC in the analysis of situations that are unclear in status.

Common Article 3 does not define the term 'party to the conflict'. In the case of an international armed conflict, the parties thereto in principle can only be States, but the situation in non-international armed conflicts is less clear, as in such cases at least one party to the conflict is not a State. The general consensus of expert opinion is that armed groups opposing a government must have a minimum degree of organization and discipline – enough to enable them to respect international humanitarian law – in order to be recognized as a party to the conflict.

Similarly, the commentary, Elements of War Crimes under the Rome Statute of the International Criminal Court , indicates the parties should be 'organized to a greater or lesser extent' in order for a situation to qualify as one of armed conflict. While the Tadic Jurisdiction Decision did not define what constitutes an 'organized armed group', indicators to this effect have been provided by subsequent case law. The Decision on Motion for Judgment of Acquittal (Miloševic Rule 98 Decision) rendered in the case of Prosecutor v. Miloševic highlights conditions indicative of the

level of organization required for an armed group to qualify as ‘organized’ under the Tadic definition.

The context of the Rule 98bis Decision concerned the trial of Slobodan Miloševic for crimes including violations of the laws or customs of war allegedly committed in Kosovo. As violations of the laws or customs of war cannot occur in the absence of armed conflict, the Trial Chamber examined the situation in Kosovo at the time the alleged violations took place to see if the requirements of the Tadic test were fulfilled.

In order for the situation to qualify as a legally cognizable armed conflict, hostilities are required to be of sufficient intensity and the parties to the conflict must be organized to a greater or lesser extent. For the **Miloševic** Trial Chamber, the latter required an evaluation of the Kosovo Liberation Army (KLA) as an organized armed group. In assessing the level of organization in the KLA, the Trial Chamber found ‘a sufficient body of evidence pointing to the KLA being an organized military force, with an official joint command structure, headquarters, designated zones of operation, and the ability to procure, transport, and distribute arms’.

The reasoning used in the Miloševic Rule 98bis Decision was cited in the Judgment of Trial Chamber II in the case of **Prosecutor v. Limaj**. In determining the existence of armed conflict during an earlier period in Kosovo, the Limaj Trial Chamber applied the Tadic test using an approach similar to that of the Miloševic Trial Chamber. The degree of organization in the KLA was assessed along with the intensity of hostilities prior to May 1998.

The Judgment of the **Limaj** Trial Chamber detailed how the KLA qualifies as ‘an organized armed group’ within the meaning of the Tadic formula. In assessing the level of organization in this armed group, considerable emphasis was placed on the role of the General Staff as the main governing body of the KLA. The functions of this body included the appointment of zone commanders, the supply of weapons, the issuance of political statements and communiqués, the distribution of KLA Regulations to units, the authorization of military action and the assignment of tasks to individuals within the organization.

According to the Trial Chamber, the organized nature of the KLA was also shown in how members of the General Staff were involved in the negotiations with representatives of the European Community and foreign missions based in Belgrade.

The level of organization within the KLA was thus also evidenced by its operational effectiveness. The ability to coordinate a unified military strategy through a chain of command was clearly important in this regard. The Trial Chamber highlighted the role of the command structure utilized by the KLA in overall functioning of the organization:

“The KLA had a General Staff, which appointed zone commanders, gave directions to the various units formed or in the process of being formed, and issued public statements on behalf of the organization. Unit commanders gave combat orders and subordinate units and soldiers

generally acted in accordance with these orders. Steps have been established to introduce disciplinary rules and military police.

The ability to recruit, train and equip new members was also cited as evidence of the level of organization within the KLA. The possession of weapons, including artillery mortars and rocket launchers, was further evidence relevant to this requirement. In the utilization of these weapons, the intensity of hostilities was emphasized by the Trial Chamber as an additional indicator of the KLA's level of organization:

"By the end of May 1998 KLA units were constantly engaged in armed clashes with substantial Serbian forces in areas from the Kosovo–Albanian border in the west, to near Prishtina/Pristina in the east, to Prizren/Prizren and the Kosovo–Macedonian border in the south and the municipality of Mitrovice/ Kosovka Mitrovica in the north. The ability of the KLA to engage in such varied operations is a further indicator of its level of organization."

Evaluating the evidence, the **Limaj** Trial Chamber concluded that 'before the end of May 1998 the KLA sufficiently possessed the characteristics of an organized armed group, able to engage in an internal armed conflict'.

Accordingly, the first requirement of the Tadic test was fulfilled. The Trial Chamber's analysis of the KLA as an 'organized armed group' reveals a number of indicators relevant to the application of the Tadic definition. It is important however to appreciate, in view of the complex nature of non-international armed conflict, that each situation has to be considered on a case specific analysis of facts. The requirement of sufficient intensity is closely related to that of organization and will now be examined in the interpretation of the term 'protracted armed violence'.

The intensity of hostilities

Similar to the organizational requirement, the threshold of 'protracted armed violence' requires the interpretation of facts on a case-specific basis. As noted in **Rutaganda** , 'the definition of an armed conflict per se is termed in the abstract, and whether or not a situation can be described as an "armed conflict", meeting the criteria of Common Article 3, is to be decided upon on a case-by-case basis'. The need to proceed to consider each situation on its merits is also highlighted by the Inter-American Commission on Human Rights in the **Tablada** case:

"The most difficult problem regarding the application of Common Article 3 is not at the upper end of the spectrum of domestic violence, but rather at the lower end. The line separating an especially violent situation of internal disturbances from the 'lowest' level Article 3 armed conflict may sometimes be blurred and, thus, not easily determined. When faced with making such a determination, what is required in the final analysis is a good faith and objective analysis of the facts in each particular case."

It is useful to consider the terms of the Tadic definition as a means of clarifying this threshold for the application of international humanitarian law. It is clear that the intensity required for the existence of armed conflict is above that of internal disturbances and tensions. It is also clear that hostilities need not reach the magnitude of 'sustained and concerned military operations'. The issue is one of clarifying the threshold of intensity that is required for the characterization of a situation as one of armed conflict. This degree of intensity hinges on the interpretation of the word 'protracted'. The level of armed violence associated with this term determines the applicability of international humanitarian law when the organizational requirement of an armed group is also met.

On the use of the term 'protracted', Sonja Boelaert- Suominen comments that the decision of the Appeals Chamber seems to indicate that this implies a time element. The case-law of the Tribunal indicates that the terms 'protracted armed violence' should be interpreted in a flexible manner and that 'protracted' does not carry the same meaning as 'sustained'. Accordingly, there is no requirement that military operations be carried out in a sustained or continuous manner.

Similarly, Bahia Thahzib-lie and Olivia Swaak-Goldman state that:

"The protracted requirement is met when the hostilities are extended over time and include events attributable to the conflict. Whether or not hostilities are 'protracted' is assessed by reference to the entire period from the initiation of hostilities to the cessation of hostilities. While an examination of the 'protracted' nature of hostilities might be fairly straightforward in a more classic non-international armed conflict, it is more problematic if several non- State parties are involved. The extent to which hostilities originating from several different non-State parties can be aggregated in considering whether hostilities are protracted will depend on the relationship between the non- State parties."

Thus to the extent that the protracted element is considered, it must be loosely interpreted. It should not be read to require that hostilities be carried out in a sustained or continuous manner. Rather, it should be judged by reference to the entire period of hostilities.

The level of armed violence required for the application of common Article 3 must be high enough to exclude isolated or sporadic acts of violence, but low enough to include situations of internal conflict where hostilities are not necessarily carried out on a continuous basis. The degree of intensity required for the existence of armed conflict was examined in the Miloševic Rule 98 Decision. The intensity requirement was assessed focusing on the length or protracted nature of the conflict and the seriousness of armed clashes, the spread of clashes over the territory, the increase in number of governmental forces sent to Kosovo and the type of weaponry used. In clarifying the threshold for the application of international humanitarian law to the situation, the Trial Chamber made two significant points in response to submissions by amici curiae. The amici curiae, Steven Kay and Timothy McCormack, submitted that the KLA did not act under an organized civil authority and that, as a consequence, the situation fell short

of the threshold of armed conflict. In responding to this claim, the Trial Chamber asserted it did not 'accept existence of a civilian authority as a requirement for the existence of an armed conflict'. In another submission, the amici curiae contended that the KLA did not exercise sufficient control over territory. In response, the Trial Chamber stated that it did not 'accept that such control of territory is a requirement for the existence of an armed conflict'.

While holding that control over territory and the existence of organized civil authority were not necessary for the characterization of a situation as one of armed conflict, the Chamber nevertheless noted these conditions did in fact exist in Kosovo during the period relevant to the indictment.

In assessing the intensity of armed violence during a different period of the conflict in Kosovo, the Limaj Trial Chamber used a similar approach to that employed by the **Miloševic** Trial Chamber.

The seriousness of armed clashes, the mobilization of troops by the government, the kind of weaponry utilized, the destruction of property, the displacement of local population and the existence of casualties were highlighted as conditions indicative of the intensity of hostilities.

In assessing the intensity of hostilities, the Trial Chamber emphasized the level of armed violence between the parties to the conflict and the irrelevance of the purpose for which the parties were fighting:

"The two forces were substantially engaged in their mutual military struggle. While the Serbian forces were far more numerous and better trained and equipped, it appears they were ill-prepared to deal effectively with small guerrilla type forces that would not engage them in prolonged fixed engagements. Serbian military intelligence may also have overestimated the strength and capability of the KLA at the time so that the Serbian forces were arraigned in greater number and with greater military resources than was warranted by the actual KLA forces. In this respect, as revealed by the evidence, many combat operations were carried out in the area of Drenica where the KLA developed earlier and was probably best organized. But, most importantly in the Chamber's view, the determination of the existence of an armed conflict is based solely on two criteria: the intensity of the conflict and organization of the parties, the purpose of the armed forces to engage in acts of violence or also achieve some further objective is, therefore, irrelevant."

This statement by the Trial Chamber indicates the irrelevance of jus ad bellum in determining the existence of armed conflict. This is an important point to note. Governments have been known to deny the applicability of international humanitarian law on the grounds of not recognizing the cause of an organized armed group. It should be emphasized in relation to such cases that the existence of armed conflict is determined on the basis of objective criteria and not the subjective judgment of either party to the conflict. As noted by the ICTR Trial Chamber in **Akayesu**:

"It should be stressed that the ascertainment of the intensity of a non-international conflict does not depend on the subjective judgment of the parties to the conflict. It should be recalled that the four Geneva Conventions, as well as the two Protocols, were adopted primarily to protect the victims, as well as potential victims, of armed conflicts. If the application of international humanitarian law depended solely on the discretionary judgment of the parties to the conflict, in most cases there would be a tendency for the conflict to be minimized by the parties thereto. Thus, on the basis of objective criteria, both Common Article 3 and Additional Protocol II will apply once it has been established there exists an internal armed conflict which fulfils their respective pre-determined criteria."

The predetermined criteria relating to common Article 3 are the level of organization possessed by parties to the conflict and the intensity of hostilities. In relation to the requirement of intensity, it is important to consider the evolution that has taken place in international humanitarian law since the drafting of the Geneva Conventions, in particular since the establishment of the international criminal tribunals for Rwanda and the former Yugoslavia, and to bear in mind that the characterization of situations should be approached on a case-by-case basis.

Some studies stipulate a numerical threshold of deaths for the recognition of a situation as one of armed conflict. The Yearbook of the Stockholm International Peace Research Institute sets a numerical threshold of 1,000 battle-related deaths, while the Uppsala Department of Peace and Conflict Research set a threshold of twenty-five battle-related deaths.

Such numerically defined thresholds would arguably be inappropriate in a legal context for a number of reasons. First, the focus of these thresholds is solely on the number of deaths and the criterion of organization on the part of non-state actors is overlooked. Second, the numbers of deaths that occur in the vast majority of armed conflicts represent only a subset of the total number of victims. Third, the stipulation of a numerical threshold would set an unwarranted restriction on the application of common Article 3 and other rules of customary international humanitarian law. The protection that might otherwise be provided by international humanitarian law would no longer apply to many situations, in particular in the early stages of hostilities or in cases of low-intensity armed conflict. As noted by Jean Pictet, 'the respect due to the human personality as such is not measured by the number of victims'.

As a condition for determining the existence of armed conflict, the intensity of hostilities is an important consideration for the application of international humanitarian law. While conditions evidencing the intensity of non-international armed conflict are often similar to those of international armed conflict, it is worth noting that the threshold for the application of international humanitarian law to the former is distinctly different from that of the latter. A state of international armed conflict can be said to exist in the absence of hostilities in cases of military occupation. A situation where two or more states are considered 'at war' also qualifies as international armed conflict in the absence of hostilities.

As a declaration of war in itself is sufficient to bring into force the Geneva Conventions, it is clear that the requirement of intensity need not be relevant to determining the status of an armed conflict initiated in this way. It is noteworthy also that the second paragraph of Article 2 stresses that the Conventions apply to all cases of occupation 'even if the said occupation meets with no armed resistance'.

Considering that the existence of hostilities is not a prerequisite for international armed conflict, it is clear that the threshold of applicability associated with such situations is distinctly different to that of non-international armed conflict. Any analogy between the two thresholds therefore needs to be carefully qualified. While there is considerable overlap in the customary international law standards applicable to international and non-international armed conflicts, it is important to recognize how such situations are characterized. The former generally manifests itself as 'a resort to armed force between States' while the latter may be characterized according to the level of organization of armed groups and the intensity of hostilities. Common Article 3 provides no indication of the degree of intensity required for a situation to qualify as 'armed conflict not of an international character'. At the time of drafting, the material field of application associated with this provision was that of civil war, i.e. an armed conflict of dimensions similar to that of a conventional international war but taking place within the borders of a sovereign state. This concept of non-international armed conflict is now of less contemporary relevance. It bears little resemblance to the current threshold of application of common Article 3.

The category of situations that qualify as 'armed conflict not of an international character' has broadened considerably since 1949. The lowering of the threshold of intensity required for the existence of armed conflict has resulted in the extension of the protection provided by international humanitarian law. The definition of non-international armed conflict as 'protracted armed violence between governmental authorities and organized armed groups' has broadened the scope of 'armed conflict not of an international character'. It also implicitly reaffirmed the exclusion of situations of internal disturbance and tensions from the remit of common Article 3.

D. Mixed Conflict

International relations have developed to the point where that which affects one State also affects the other. The fabric of alliances and sympathies within each bloc has grown to the extent that there are many States which cannot engage in a conflict without taking with them a whole series of allied or friendly States, or at least putting those States in an awkward position, to say nothing of States which may find themselves bound by the same type of mutual defence treaty with two States who suddenly enter into armed conflict with each other. Moreover, as a direct confrontation between the great powers would bring with it the danger of global war, their differences tend to find expression through conflicts between small States or within States. As the United Nations Charter (art. 2 (4)) reaffirmed the illegality of the use of force in international relations for most situations, the only type of armed intervention which remains possible is in situations not covered by the rules of the Charter, that is, those falling within the competence of

the States - internal tensions and disturbances approaching civil war and often exacerbated by foreign intervention. When such interventions take the form of direct military interference in the internal conflict, for example through the sending of troops, the conflict becomes internationalized. It is then said that there is a mixed conflict or an inter- nationalized internal conflict. Thus in Angola the conflict between UNITA and the government is also an international conflict between Angola and South Africa. In Kampuchea, the conflict between the armed forces of the government of Democratic Kampuchea and Vietnamese troops is also a conflict between the forces of Democratic Kampuchea and the forces of the government of the Peoples' Republic of Kampuchea (Phnom Penh).

LAW OF NAVAL WARFARE

Sources of Naval Warfare

The great dividing line in the historical development of the law of naval warfare must be drawn at the outbreak of the first World War in 1914, for what is generally referred to as the "traditional law" is substantially the law as it appeared at this date. In the main, the traditional law of naval warfare is customary in character, developing out of eighteenth and-particularly- nineteenth century practices. The various attempts to codify this customary law have never enjoyed the same degree of success that has attended similar efforts with respect to the codification of land warfare.

There is no convention dealing with the regulation of naval hostilities that compares in scope and importance to the Regulations attached to Hague Convention IV (1907), Respecting the Laws and Customs of War on Land. The Hague Conventions of 1899 and 1907 which dealt specifically with the conduct of naval warfare are few in number and, with the exception of XIII (1907) concerning the Rights and Duties of Neutral States in Maritime War, of relatively minor significance.

Historically, the most important, and certainly the most controversial, disputes arising in the course of naval hostilities related to the extent and character of the right of belligerents to interfere on the high seas with private neutral trade. In the Declaration of London of i9o9 the attempt was made to produce a generally acceptable codification of nineteenth century practices in this area of the law. However, the Declaration was never ratified by any of the signatory states; and despite the occasional claims of belligerents and neutral states during the First World War that the Declaration of London set forth the valid law regulating belligerent behavior at sea, it was not binding upon the naval belligerents in either World War.

In the period of over four decades that has elapsed since the outbreak of the First World War there has been only one international instrument concluded for the regulation of naval hostilities that has received general adherence, and that instrument is the London Protocol of 1936 requiring submarines to conform in their actions against merchant vessels to the rules of

international law to which surface vessels are subject. To the extent, then, that the traditional law has been changed, such change has come principally through the practices of two World Wars.

Binding force of the Law of Naval Warfare

As a general rule, the binding force of conventional rules of war is limited to the contracting parties, and then only to the extent specified by the terms of the convention in question and by the conditions accompanying ratification or adherence. On the other hand, the customary rules of the law of war are binding upon all states and under all circumstances. The statement is frequently made that reprisals form one clear exception to the binding force of customary rules. However; this manner of formulation may easily prove misleading. The act of taking reprisals does not represent a restriction to the binding force of customary law. On the contrary, this law remains fully binding, and the act of taking reprisals is itself a clear indication of the continued binding force of the customary law the violation of which forms the condition for the act of reprisal. Reprisals do not represent at least not in theory - an abandonment of the customary law (or the conventional law for that matter), but rather the enforcement of that law; at the very least, reprisals represent an act of self help permitted against a previous violation of law.

Apart from reprisals, the principle of military necessity has generally been considered as the most important qualification to the binding force of both the customary and conventional law of war. Indeed, the extent to which this principle may be held to restrict the operation of the rules of war has provided one of the most disputed issues among writers.

The core of the controversy has centered about the doctrine that interprets military necessity as serving to justify departure from any of the established rules of war when the observance of these rules either would endanger the success of a military operation or would threaten the survival (self-preservation) of a military unit. In either circumstance, the principle of military necessity is considered to be operative and to free belligerents from behaving in accordance with otherwise valid law."

As against this interpretation of military necessity it has been argued, principally by English and American writers, that military necessity more precisely, that the circumstances held to constitute a condition of military necessity can justify a departure from behavior normally demanded by the law of war only when conventional or customary rules expressly provide for the exceptional operation of military necessity.

According to this latter interpretation-which is believed to be correct military necessity must be interpreted "to denote those exceptional circumstances of practical necessity contemplated by express reservations to be found in several Articles of The Hague Regulations and other Conventions in regard to acts otherwise prohibited. The general principle is that conventional and customary rules of warfare are always binding upon belligerents and cannot be disregarded even in case of military necessity."

Hence, the principle of military necessity cannot be considered as superior to, and thereby restricting the operation of, all other rules of warfare, whether customary or conventional. On the contrary, it is the principle of military necessity that may be restricted by the positive law of war, and occasionally is so restricted. Not everything necessary to the purpose of war is allowed by the law of war.

It is this latter, and more restrictive, interpretation of military necessity that has recently received clear judicial endorsement. In the war crimes trials following the Second World War the chief preoccupation of tribunals called upon to interpret the principle of military necessity was to determine when circumstances of military necessity could be considered as serving to justify departures from conduct normally prescribed by the rules of warfare.

Although the judgments of tribunals were by no means identical on a number of points, there nevertheless was a remarkable uniformity of judicial opinion, which-taken as a whole-clearly appears to support the narrow interpretation of military necessity. The following is a brief summary of these judgments.

(1) Military necessity may serve as a defense plea against charges of committing acts normally forbidden by the law of war only when the rule in question can be interpreted as permitting such exceptional departure in circumstances constituting a condition of military necessity. Thus in the **Hostages Trial** the tribunal stated that the prohibitions contained in the Hague Regulations "are superior to military necessities of the most urgent nature except where the Regulations themselves specifically provide the contrary. In the case of conventional law the rule in question must provide expressly for military necessity. In particular, where the prohibition contained in a rule is absolute in character, military necessity cannot be used as a defense. Thus circumstances of military necessity have not been considered as justifying the killing of prisoners of war.

(2) In the case of rules allowing for the exceptional operation of military necessity, departure from normally prescribed behavior is justified for reasons of self-preservation or for insuring the success of a military operation. In addition, there must be an element of urgency involved that allowed-or seemed to allow-no alternative course of action. However, it does not appear that it is essential to establish that the circumstances constituting a condition of military necessity were objectively present in a given situation. It is sufficient only to establish that the individual putting forth the plea of military necessity as a defense honestly believed at the time that such circumstances were present.

Area of Naval Warfare

The area of naval warfare is that part of the seas in which the parties to an international armed conflict at sea are entitled to take belligerent measures. "Belligerent measures" are not restricted to the use of armed force against military objectives, they also comprise so-called prize measures, like visit, search, diversion, capture and seizure of vessels and/or cargoes. These measures may, of course, be taken in those sea areas where the belligerent states enjoy

sovereignty, i.e. in their internal waters, in their territorial seas and, where applicable, in their archipelagic waters. Moreover, there is no prohibition from conducting naval warfare in the high seas. Despite allegations to the contrary, neither the peaceful uses clauses of the UN Law of the Sea Convention nor international state practice have contributed to the emergence of a rule of international law restricting the parties to an international armed conflict at sea to their respective internal waters and territorial sea areas. In view of the special legal status of the area and in view of the rights neutral states continue to enjoy in the high seas, belligerents are, however, obliged to pay due regard to these aspects and to refrain from interference if that is feasible and reasonable. The same considerations apply if belligerent measures are taken in the Exclusive Economic Zone or on the continental shelf of neutral countries. Here, again, there is no prohibition of belligerent measures but an obligation to pay due regard to the legitimate rights neutral coastal states enjoy in these sea areas.

Certainly, the parties to an international armed conflict at sea are prohibited from taking belligerent measures within neutral waters or using them as a sanctuary. Neutral waters consist of the internal waters, territorial sea and, where applicable, the archipelagic waters of neutral states. Neutral states may, if they consider this essential for their security or for the safety of navigation, close their neutral waters to belligerent warships and auxiliary vessels. Other than in times of peace this closure may comprise the neutral state's territorial sea as a whole and may last for the duration of the entire international armed conflict. The only restriction the neutral state has to observe vis-a-vis the parties to the conflict is the principle of impartiality. If, however, neutral waters are part of an international strait or of an archipelagic sea lane, the neutral state is not allowed to prohibit belligerent warships and auxiliary vessels from transit through these waters.

Legitimate Methods and Means of Naval Warfare Affecting Neutral Navigation

According to the law of naval warfare and the law of maritime neutrality, belligerent warships are entitled not only to harm the enemy in a cost-efficient way but also to exercise all measures of control to verify that the shipping of third states is not involved in activities contributing to the enemy's war fighting effort. Since there exists a duty of neutral merchant vessels to refrain from such activities, the aggrieved belligerent is entitled to take all necessary enforcement actions in order to prevent a violation of the law of maritime neutrality.

Prize measures

Neutral merchant vessels are subject to visit and search by belligerent warships (and military aircraft) everywhere beyond neutral waters if there are reasonable grounds for suspecting that they are subject to capture. They are subject to capture if either they might be considered legitimate military objectives or if they:

- are carrying contraband;

- are on a voyage especially undertaken with a view to the transport of individual passengers who are embodied in the armed forces of the enemy;
- are operating directly under enemy control, orders, charter, employment or direction;
- present irregular or fraudulent documents, lack necessary documents, or destroy, deface or conceal documents;
- are violating regulations established by a belligerent within the immediate area of naval operations; or
- are breaching or attempting to breach a blockade.

On the one hand, visit and search do not presuppose clear evidence. On the other hand, indiscriminate and arbitrary measures of control that cannot be based on “reasonable grounds of suspicion” are illegal. But even if there exist sufficient grounds, it is not always necessary to visit and search a merchant vessel. In many instances it will suffice if it is, with its consent, diverted from its declared destination. This alternative to visit and search has to be distinguished from diversion ordered for the purpose of visit and search, which does not require the consent of the vessel's master. This kind of diversion is appropriate and legitimate if visit and search at sea is impossible or unsafe. The law of maritime neutrality, designed as a compromise between the interests of the belligerents and those of non-participating states, thus accepts that neutral merchant vessels may suffer considerable losses due to the fact that their voyage is delayed by these measures of control.

If it is determined as a result of visit and search or by other means that they are legitimate military objectives or engaged in one of the activities mentioned above, neutral merchant vessels may be captured. Capture is exercised by sending a prize crew on board the vessel that will take control over the vessel.

However, the legality of capture has to be established by the judgment of the competent prize court.

A considerable problem exists as to the legality of capture if capture is justified on the ground of carriage of contraband. Not only the practice of the belligerents of the two World Wars but also of, inter alia, Egypt, India and Pakistan, has shown that the parties of an international armed conflict tend to extend their contraband lists, especially if the conflict lasts for a longer period of time.

Moreover, the traditional categories of absolute and relative contraband, both distinguished from so-called "free goods", did not contribute to a clarification of the legal situation but rather to perturbation, both on the side of the belligerents and on the side of the neutrals. Today there is widespread agreement that only two categories of goods exist: contraband and free goods. Contraband are goods which are ultimately destined for territory under the control of the enemy

and which may be susceptible for use in armed conflict. Moreover, the belligerent must have published a contraband list beforehand. All goods not on the belligerent's contraband list are free goods, which mean that they may not be captured and their carriage does not justify capture. It needs to be emphasized that goods with a neutral destination coming from a belligerent port do not constitute contraband. This holds true even if the revenues of these exports will enable the belligerent concerned to purchase weapons or other war material abroad. This implies in particular that oil exports not destined for a belligerent do not constitute legitimate contraband even if contained in a contraband list.

In exceptional circumstances even the destruction of captured neutral merchant vessels is legal. This presupposes that military circumstances preclude taking or sending the vessel for adjudication as an enemy prize and that the following criteria are met beforehand:

- the safety of passengers and crew is provided for. For this purpose, the ship's
- boats are not regarded as a place of safety unless the safety of the passengers and crew is assured in the prevailing sea and weather conditions by the proximity of land or the presence of another vessel which is in a position to take them on board;
- documents and papers relating to the prize are safeguarded; and
- if feasible, personal effects of the passengers and crew are saved.

In addition, the San Remo Manual provides that:

“Every effort should be made to avoid destruction of a captured neutral vessel. Therefore, such destruction shall not be ordered without there being entire satisfaction that the captured vessel can neither be sent into a belligerent port, nor diverted, nor properly released. A vessel may not be destroyed under this paragraph for carrying contraband unless the contraband, reckoned either by value, weight, volume or freight, forms more than half the cargo. Destruction shall be subject to adjudication.”

Finally, it is necessary to stress that the master of the merchant vessel as well as the neutral flag state are, in principle, obliged to tolerate the exercise of prize measures by a belligerent even if there are doubts as to their legality. It will be shown that only in some instances is there a possibility of protecting neutral merchant vessels against these measures. If this does not apply, the affected state or the affected private owner will have to rely on judicial remedies, i.e. either on diplomatic protection or on the judgment of the competent belligerent prize court.

Legitimate methods and means under the maritime “ius in bello” and the law of maritime neutrality

Not only belligerent prize measures have a negative or even harmful effect on neutral shipping, so also do those methods and means of naval warfare that characterized the armed conflicts at

sea of the 20th century: naval mines, blockades, “exclusion zones” and attacks on neutral merchant vessels. Of course, submarine warfare had the most severe impact on neutral navigation during the two World Wars. Still, we will not have to specially concentrate upon submarine warfare in the present context. Today it is generally accepted that the law of naval warfare and of maritime neutrality equally apply to surface warships and submarines. Moreover, in modern armed conflicts at sea, submarines will only in rare cases be employed against merchant shipping. The submarine has become a true means of naval warfare and can no longer be considered a means of commercial warfare.

Enforcement of the Law of Naval Warfare

There are a number of means available to belligerents for inducing compliance with the rules governing war's conduct. In the event of unlawful behavior on the part of an enemy remedial action may take the form of direct protest and demand for compensation as well as for the punishment of individual offenders. Assuming, however, that the. unlawful behavior in question has either been directly instigated by order of the enemy government, or at least performed with its sufferance, other measures will generally prove necessary. The injured belligerent may direct an appeal to neutral states, requesting the latter to intervene for the purpose of bringing pressure to bear upon the delinquent party. And although neutral states have no duty to protest against the commission of illegitimate acts of warfare it has been frequently asserted that they have a right to do so. Finally, the injured belligerent may resort to repressive measures-sanctions-in reaction to unlawful behavior on the part of an enemy, measures which take the form of reprisals or of punishing captured offenders as war criminals.

A. Reprisals

As between belligerents reprisals are acts, otherwise unlawful, which are exceptionally permitted to one belligerent as a reaction against illegal acts of warfare committed by an enemy. It is generally acknowledged that reprisals should not be resorted to merely for revenge but only as a last resort in order to compel an enemy to desist from unlawful behavior. For this reason the injured belligerent should attempt, whenever possible, to obtain cessation of the illegal acts (and appropriate redress) through means other than reprisals. It is always preferable that if measures of reprisal are finally resorted to the order to employ them should emanate from the highest authority. However, in circumstances of urgent necessity it is conceded that subordinate military commanders may, on their own initiative, order appropriate reprisals. In all cases, reprisals must be terminated once they have achieved their objective, which is to induce a belligerent to desist from unlawful conduct and to comply with the rules regulating the conduct of war.

According to customary law measures of reprisal may be directed generally against the persons and property of an enemy. There need be no connection between the individuals performing the unlawful acts which give rise to the right of reprisal and the individuals made the objects of retaliatory measures. In a word, the essential principle characterizing measures of reprisal is that

of collective responsibility. However, as between the parties to the 1949 Geneva Conventions, the individuals (and their property) who may be made the objects of reprisals have been substantially restricted.

For these Conventions prohibit the taking of reprisals against any of the several categories of individuals afforded the protection of the Conventions.

But apart from the prohibitions contained in the 1949 Geneva Conventions the only remaining restriction 8 laid upon belligerents is that forbidding retaliatory measures which are out of all proportion to the unlawful behavior forming the basis of the reprisals.

B. Punishment of War Criminals

War crimes may be defined as acts which violate the rules regulating the conduct of war and which result in the liability to punishment of the perpetrators. According to customary international law belligerents have the obligation to punish their own nationals found violating the law of war and the right-in principle-to punish captured enemy individuals who have committed similar acts." Prior to World War II, however, some doubt had existed as to whether or not a belligerent was entitled to exercise jurisdiction over individuals accused of war crimes when the acts" in question were not performed either on the territory of the belligerent or against its nationals. But in the light of recent practice it now appears clear that the right of a belligerent to exercise such jurisdiction is limited neither to offenses having a particular geographical location nor to offenses committed against the nationals of the belligerent claiming jurisdiction.

In addition, there is no rule of customary law preventing a belligerent from trying and punishing war criminals during the period following the termination of active hostilities but prior to the conclusion of a peace treaty, though the past practice of states has not been to continue proceedings against individuals accused of war crimes once peace has been re-established.

It is an interesting fact that among the war crimes trials held during and since the second World War only a relatively small number concerned violations of rules regulating the actual conduct of hostilities. In part, this may be explained by a reluctance to try members of the armed forces of the defeated states for the violation of rules whose status is no longer a matter of certainty. In part, the dearth of trials concerned with infractions of the rules regulating the actual conduct of hostilities may be attributed to the conviction that where both sides in a conflict openly departed from the established law, the requirements of justice forbade the prosecution of only those who happened to be on the defeated side.

There is little question, however, but that the commission of certain acts during the course of hostilities at sea must continue to be regarded as resulting-in the absence of special reasons to the contrary-in the individual (criminal) responsibility of the perpetrators. The unnecessary use of force particularly as against the merchant vessels of an enemy, the denial of quarter at sea, the firing upon survivors of sunken ships, the failure to search out and make provision for the

survivors of sunken vessels when military interests so permit, the deliberate attack upon hospital vessels or other vessels granted special immunity, and the misuse of the Red Cross emblem constitute a summary of only the more important acts the com-mission of which may result in a liability to punishment upon capture by an enemy.

Where individuals have been charged with the commission of war crimes the principal difficulty has been that of determining what recognition ought to be given the defense plea that the acts in question were performed either by order of the belligerent government or on the command of a superior."

Prior to World War II the attitude of states-and the opinions of writers on the law of war-had varied with respect to the treatment to be accorded the plea of superior orders, though a relatively strong case may be made on behalf of the assertion that illegitimate acts of warfare performed by direct order of the state were not considered to result in the individual responsibility of those performing such acts.

A decided change from earlier opinion and practice occurred both during and after the 1939 war. While that conflict was still in progress several of the belligerents amended their military manuals to provide that a violation of the law of war is not deprived of its character of a war crime, and does not confer upon the actor immunity from punishment, simply for the reason that it was performed in response to the order of a belligerent government or a superior. In the period following the termination of hostilities Allied courts and tribunals charged with the task of trying individuals accused of war crimes have uniformly endorsed this principle.

At the same time, it has been the consensus of judicial opinion that in order to establish responsibility the person must know, or have reason to know, that the act he is ordered to perform is unlawful under international law. Thus if the rule that allegedly has been violated is itself controversial or if-though of unquestioned validity-the rule has been departed from under the conviction that such departure forms a legitimate measure of reprisal, either circumstance may prove sufficient to relieve the actor of responsibility. Furthermore, it would appear that if an individual though knowing that the act he has been ordered to perform is unlawful nevertheless has acted under duress this circumstance may be taken into consideration either by way of defense or in mitigation of punishment.

What has been termed the "inverse case" of superior orders concerns the scope of the responsibility commanding officers must bear for illegitimate acts of warfare performed by subordinates." There is no question but that military commanders are liable for the unlawful acts they have ordered or authorized subordinates to perform. Equally well established is the responsibility of military commanders for the illegal acts of subordinates which the former had knowledge of but failed to take adequate measures to control. By the failure to suppress unlawful acts of subordinates as are known to military commanders, the presumption of acquiescence in these acts must arise. It is clear, therefore, that the responsibility of commanders can result solely

from inaction, though here it is inaction based upon knowledge that unlawful acts of subordinates have been committed. Finally, it would appear that the responsibility military commanders must bear for the acts of subordinates implies a further duty to take reasonable measures to insure that the latter will refrain from unlawful behavior, and, should unlawful behavior nevertheless occur, to discover and control the misconduct of subordinates. Where the failure to take precautionary or preventive measures is palpable and gross military commanders have been held liable for the unlawful behavior of subordinates even though without actual knowledge of such behavior.

The Principle of Distinction and the Concept of the Military Objective

If a law of armed conflict purporting to regulate the conduct of military operations is to exist, an essential element of this law, no matter how inchoate, is the principle of distinction, also referred to as the principle of identification. That law is premised upon a requirement to distinguish between objects or persons that may be attacked and also that may not be attacked. The increasing percentage of civilian casualties relative to total casualties in contemporary conflicts has led some writers to suggest that the principle of distinction has become blurred, but this could not be viewed as a positive development. The principle of distinction is a fundamental aspect of the law of naval warfare, although it has not been explicitly addressed in any treaty on the subject.

The major contemporary treaty on law of armed conflict is the 1977 Additional Protocol I to the 1949 Geneva Conventions relating to the Protection of Victims of International Armed Conflicts, ratified by Canada on November 20, 1990.6 As a matter of convenience, of Additional Protocol I is not applicable to attacks directed against objects on, under, or over the seas, Article 48 of that document may be used as a statement of the principle of distinction:

“In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.”

It is necessary, however, to go further and explore the meaning of the term "military objective." "Military objective" is defined in Additional Protocol I and the relevance of that definition to naval warfare will be discussed later in this article. It suffices to note here that military objectives are not confined to warships and to naval auxiliary vessels operating in support of a nation's armed forces; depending on the circumstances, they may include privately owned vessels manned by civilian crews and flying the flags of states that are not involved in the conflict.

Conceptually, one may explain the meaning of "military objective" in the law of naval warfare by a variety of means: a general definition of military objective; a list of objects constituting military objectives; a general definition and a list or; the converse of the above indicating objects exempt from attack.

No treaty contains a general definition of military objective for the law of naval warfare. As will be seen later, some treaties contain lists from which one might derive categories of vessels that are exempt from attack. Unfortunately, some of these lists are obsolete or unclear.

Some writers have proposed a zonal approach whereby, once appropriate measures have been taken to warn all concerned that presence in an area is dangerous, and to give ships and aircraft in the area time to leave it, a belligerent may presume anything in the area without permission to be there is a legitimate military objective. This approach facilitates the making of targeting decisions but it is certainly not a part of existing law, although state practice in recent conflicts indicates that some customary law standards for exclusion zones may be emerging.

Enemy Vessels and Aircraft that May be Attacked at All Times

All of the manuals reviewed indicated that attacks may be directed against enemy warships, naval or military auxiliary vessels, and military aircraft at any time anywhere outside neutral territorial seas. These attacks may be exercised without warning and without regard to the safety of the enemy crew. It was suggested during the Falklands conflict that the action of the United Kingdom in sinking the Argentine Cruiser General Belgrano outside of proclaimed exclusion zones was unfair. There is no international legal requirement to confine attacks against warships, auxiliary vessels, or military aircraft to particular zones once an armed conflict occurs, except for the general obligation not to fight in neutral waters. None of the manuals consulted have attempted to define "naval or military auxiliary vessel." A British author has suggested that a naval auxiliary is a vessel engaged at the relevant time in direct support of enemy warships, whether or not it is formally incorporated in the belligerent fleet and whether or not it is in company with enemy warships.

The Merchant Ship as Target

The central issue concerning targeting in the law of naval warfare is, when may a merchant ship be a legitimate military objective?

A rough definition of merchant vessel is any cargo carrying vessel, publicly or privately owned, and flying the flag of a belligerent or neutral state. As indicated above, under the pre-1914 law merchant ships, enemy or neutral, could only be attacked on sight when they took a direct part in hostilities or when they were being convoyed by enemy warships, as they were then deemed to be resisting visit and search. In all other cases they had to be ordered to submit to visit and search and then refuse to comply with the order before they could be attacked, even if they were armed for defensive purposes.

The pre-914 law and its reaffirmation in the 1936 London Submarine Protocol notwithstanding, neutral and belligerent merchant ships unconvoyed by enemy warships or aircraft were attacked on sight by submarines, aircraft, and on occasion, surface warships in both World Wars. Further, unconvoyed neutral and belligerent merchant ships were attacked by aircraft and surface

warships in the Iran-Iraq war. The only case in which individuals were charged with war crimes, including the attacking of merchant ships without warning, is the trial of Doenitz and Raeder before the International Military Tribunal at Nuremberg. As said above, they were both acquitted of the charges insofar as belligerent merchant vessels were concerned, convicted insofar as neutral merchant vessels were concerned, but awarded no sentence on the charge because of similar Allied practices.

Target Identification, Ruses, and Perfidy

Target Identification - One of the major problems in modern naval warfare conducted with current technology is target identification. Simply put, there is an imbalance between the technology for seeing and the technology for killing. Naval commanders have weapons available to them which they can use to attack targets beyond visual range (BVR) or even over the horizon (OTH), where it is difficult or impossible to confirm that the target is a legitimate military objective. They have an interest in ensuring that the object attacked is a legitimate military objective and also that it is not one of their own side's ships or aircraft (the Blue on Blue problem) or a ship or aircraft otherwise exempt from attack. Blue on Blue attacks are in fact quite common in modern conflicts; aircraft, in particular, are frequently shot down by their own side. These incidents occur because on scene commanders are concerned about the protection of their own units and believe that waiting until they have positive visual identification of potential targets will place their units at too great a risk; they must make targeting decisions on an assessment of probabilities.

The commanding officer of the USS Vincennes ordered that Iran Air Flight 655 be shot down in the Persian Gulf on July 3, 1988, because he believed, erroneously but on the basis of a less than reckless assessment of the facts provided to him, that the aircraft was an Iranian F-14 which would attack his ship before it came within range for accurate visual identification.

The current law concerning ruses of war and perfidy in a naval setting is fairly straightforward but, in the light of the current state of weapons technology, one might question whether certain aspects of it, in particular the false flag rule, are not anachronistic and harmful to the underlying principles of the law of armed conflict.

Ruses - Ruses of war are permitted. They are acts that are intended to mislead an adversary and induce him to act recklessly, but they infringe no rule of international law applicable to armed conflict and are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. Examples of ruses are the use of camouflage, deceptions, utilization of enemy codes, passwords, and countersigns. The fog of war has not been completely dissipated by modern technology; it is still possible to deceive the enemy concerning the identity and location of naval units even in the era of radar and reconnaissance satellites.

Under the customary international law of naval warfare, it is permissible for a belligerent warship to fly false colors and disguise its outward appearance in other ways in order to deceive

the enemy into believing the vessel is of neutral nationality or is other than a warship. However, it is unlawful for a warship to go into action without first showing its true colors; use of neutral flags, insignia, or uniforms during an actual armed engagement at sea is forbidden.

Merchant vessels are also permitted to practice this deception but they thereby run the risk of capture, damage, or even destruction. Belligerent military aircraft are not permitted to wear false markings in order to deceive the enemy.

Perfidy - Although ruses of war are permitted, perfidy is prohibited. Perfidy is defined in Article 37 (1) of Additional Protocol I as follows:

"Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy."

Article 38 goes on to state:

"(1) It is prohibited to make improper use of the distinctive emblem of the red cross, red crescent or red lion and sun or of other emblems, signs or signals provided for by the Conventions or by this Protocol. It is also prohibited to misuse deliberately in an armed conflict other internationally recognized protective emblems, signs or signals, including the flag of truce, and the protective emblem of cultural property.

(2) It is prohibited to make use of distinctive emblem of the United Nations, except as authorized by that Organization."

Article 39 (2), however, indicates the Protocol does not alter the traditional rules of international law concerning the use of flags in the conduct of armed conflict at sea.

It is unlikely that targeting decisions in a high technology naval conflict would be made at ranges where the color of a flag flown by a ship would be a relevant consideration. One might, however, question the current desirability of a rule that encourages the disguising of warships to simulate ships which might not be legitimate objects of attack. It is one thing to say that warships need not be required to take positive measures to indicate their location and status as warships; it is another to suggest that "feigning noncombatant status" still is a desirable practice.

The identification issue has been addressed by the ICRC and other organizations in an effort to ensure that medical transports and other ships and aircraft entitled to protection under the Geneva Conventions and the Additional Protocols are properly identified before they are subjected to the risk of attack.

Methods and Means of Naval Warfare in Non-International Armed Conflicts

The law of naval warfare is part of the larger body of law applicable to international armed conflicts. Accordingly, it applies to an armed conflict between two or more States, including

conflicts involving State-sponsored forces.) Whether the law of naval warfare also applies to situations of non- international armed conflicts is a contentious issue. Therefore, the distinction between international and non- international armed conflicts is important when it comes to the applicability of the law of naval warfare to a particular armed conflict.

Unfortunately, the distinction between international and non-international armed conflicts is less clear than it seems at first glance. On the one hand, the "facts on the ground" may make it difficult to draw the line of demarcation between the two. Additionally, international scholars have taken quite different positions. For some, the distinctive criterion is the identity of the parties to the conflict, with the issue being whether or not those parties qualify as States under public international law. For others, it is not the identity of the parties alone, but also the geography of an armed conflict; they are prepared to apply the law applicable to international armed conflict to any case in which armed conflict "crosses the borders of the state," even if one of the parties is a non-State actor. Still others believe that the distinction has become irrelevant, because, they maintain, the formerly separate bodies of law have merged into a single body of law applying equally to both international and non-international armed conflict.

In armed conflicts the law of naval warfare undoubtedly applies, at least insofar as measures taken by the State party to the conflict are concerned. The non-State party to the conflict may also apply methods and means of naval warfare against its State enemy. However, the non-State actor may not interfere with neutral shipping unless the neutral State has-either explicitly or implicitly-recognized it as a belligerent.

A non-international armed conflict exists whenever there is "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."

Region of Operations

A. Internal Waters and Territorial Sea

As non-international armed conflicts occur within a State, the parties to the conflict are not prohibited from conducting hostilities in that State's internal waters and territorial sea, as those are defined by the law of the sea. As long as the parties to the conflict do not interfere with the navigation of other States, they may apply methods and means of naval warfare against their adversary in those sea areas.

At the same time, however, other States continue to enjoy the right of innocent passage. There is no indication in either treaty law or State practice that the right of innocent passage is automatically suspended at the commencement of a non-international armed conflict. Rather, the general rules continue to apply. The coastal State, under Article 25(3) of the 1982 United Nations Convention on the Law of the Sea (LOS Convention), may in certain circumstances temporarily suspend innocent passage in specified parts of its territorial sea. To be effective, the suspension must be "duly published."

The reference to "weapons exercises" in Article 25(3) as a basis for suspending the right of innocent passage is not the exclusive circumstance in which suspension may occur. The article goes on to indicate that suspension may occur when "essential for the protection of its [the coastal State's] security." In determining whether such suspension is essential, the coastal State enjoys a wide margin of discretion.

The existence of a non- international armed conflict certainly constitutes a threat to the coastal State's security; hence, the authorities of the coastal State are entitled to suspend the right of innocent passage in order to prevent foreign shipping from navigating in close vicinity to the conflict area. In view of a lack of conclusive State practice, it is unclear whether innocent passage may be suspended in the entire territorial sea. While suspension in a State's entire territorial sea would appear to be inconsistent with Article 25(3)'s "in specified areas," the circumstances of a given non-international armed conflict may be such that the government considers it necessary to close the entire territorial sea to foreign navigation. If, however, the armed hostilities are limited to a certain region, it would be difficult for the government to justify a suspension of the right of innocent passage in coastal sea areas remote from the area of operations.

The non-State party to a non- international armed conflict is not entitled to suspend or otherwise interfere with the right of innocent passage. This clearly follows from the wording of Article 25(3). If the non-State party nevertheless takes measures affecting foreign shipping, the authorities of the coastal State under Article 24(2) must "give appropriate publicity to any danger to navigation, of which it has knowledge, within its territorial sea." The government is not obligated to actively take measures with a view to protecting foreign navigation against interference by the non-State party to the conflict.

B. International Straits and Archipelagic Sea Lanes

Neither the government nor, a fortiori, the non-State party to a non- international armed conflict is entitled to interfere with the rights of transit passage and of archipelagic sea lanes passage within international straits and archipelagic waters.

Even during an international armed conflict the belligerents are obliged to preserve those passage rights. There is no indication in State practice that the existence of a non- international armed conflict would entitle the government to adopt laws and regulations relating to passage that are in excess of that permissible under the law of the sea. In particular, there may be no suspension of transit passage even if the exercise of navigation or overflight were dangerous to the transiting vessel or aircraft.

As is the case with dangers to navigation within the territorial sea, the authorities of the States bordering an international strait and the archipelagic State are obliged to give "appropriate publicity to any danger to navigation or overflight." And, again, the government is not obliged to

take active measures against the non-State party to the conflict in order to protect international navigation and aviation.

C. Sea Areas beyond the Territorial Sea

The government of the State concerned is entitled to exercise maritime interdiction/ interception operations within its contiguous zone if the conditions of Article 334 of the LOS Convention are met. Hence, the "special naval surveillance zone" established and enforced by Sri Lankan government forces in 1984 and the measures taken against foreign vessels that were engaged in smuggling weapons and supplies to the Tamil Tigers were "justified under ordinary customs and policing powers available within 24 nautical miles of Sri Lanka's baselines."

State practice seems to provide sufficient evidence that there is no rule of customary international law prohibiting the parties to a non- international armed conflict from engaging in hostilities against each other in high seas areas. As in an international armed conflict, there is, however, a positive obligation to pay due regard for the rights enjoyed by other States Moreover, the parties are prohibited from damaging submarine cables and pipelines that do not exclusively serve either party to the conflict. Hostile actions taken within the exclusive economic zone or on the continental shelf of another State during a non-international conflict are more questionable.

CASE LAWS

In the **Von Ruchteshell trial**, a former commander of German surface raiders was found guilty of continuing to fire at merchant ships after they had indicated their surrender, and of sinking enemy merchant vessels without making any provision for the safety of survivors. This case also raised the issue of whether or not it was legitimate for a surface raider to attack a merchant ship without warning and, by implication; it held that no war crime was committed by such attacks when the merchant ship was incorporated into the enemy war effort by being armed or by having wireless communications.

In the **Peleus trial** which forms the basis for Gwyn Griffin's novel, Operational Necessity. The Peleus was a Greek ship torpedoed in mid-Atlantic in March, 1944, by a German submarine. After the ship sank, all but three survivors were killed by machine gun fire or hand grenades. The captain of the submarine and four crew members were tried by a British military court in Hamburg in 1945. The report of the case contains the following comment concerning the defence of operational necessity:

“The Commander of the U-boat did not plead that he had acted on superior orders. His defence was that he thought that the floating rafts were a danger to him, first, because they would show an aero plane the exact spot of the sinking, and secondly, because rafts at that time of the war could be provided with modern signaling communications. The position of U-boats was very precarious, particularly in that part of the Atlantic where the incident occurred. Eck, therefore, thought his measure justified. It was clear to him that, as a result of his shooting at the rafts, the

survivors would die. The Judge Advocate ruled that the question whether or not any belligerent is entitled to kill an unarmed person for the purpose of saving his own life did not arise in the present case. It may be, he said, that circumstances would arise in which such a killing might be justified. On the facts which had emerged in the present case, however, the Judge Advocate asked the Court whether or not it thought that the shooting with a machine gun at substantial pieces of wreckage and rafts would be an effective way of destroying every trace of the sinking. A submarine commander who was really and primarily concerned with saving his crew and his boat would have removed himself and his boat at the highest possible speed at the earliest possible moment for the greatest possible distance.

The court found all of the accused guilty. The Captain and two crew members were executed. One crew member was sentenced to life imprisonment and the last received fifteen years imprisonment.

In **Moehle Trial**, Lieutenant Commander Moehle, an officer formerly commanding a U-boat flotilla at Kiel, was tried and convicted for ordering the commanding officers of U-boats to destroy ships and their crews.

In **Amerada Hess v. Argentina Republic**, the owners of the Liberian tanker Hercules sought damages from Argentina for a bombing attack on the Hercules during the Falklands conflict which occurred outside the exclusion zones proclaimed by Argentina and the United Kingdom. The United States Court of Appeal (Second Circuit), which seems to have relied primarily on peace time law of the sea treaties although it did conduct a cursory review of older law of naval warfare treaties, held that neutral ships had a right of free passage on the high seas, saying:

“In short, it is beyond controversy that attacking a neutral ship in international waters, without proper cause for suspicion or investigation violates international law. Indeed, the relative paucity of cases litigating this customary rule of international law underscores the longstanding nature of this aspect of freedom of the high seas. Where the attacker has refused to compensate the neutral, such action is analogous to piracy, one of the earliest recognized violations of international law.”

MODULE-V

MARITIME SECURITY IN INDIA AND INDIAN OCEAN REGION

TURBULENCE OF THE INDIAN OCEAN[25]

GEOGRAPHICAL IMPORTANCE

As the third largest ocean in the world, the Indian Ocean covers an area of 74.9 million km^2 and is surrounded by Asia, Oceania, Africa and Antarctica. It is separated from the Pacific Ocean in the southeast by the longitude line from southeast corner of Tasmania to the Antarctic continent. In the southwest, the longitude line across Cape Agulhas of South Africa forms a boundary between the Indian Ocean and the Atlantic Ocean. The Indian Ocean embraces the Antarctica in the south and the closed land in the north. The boundary line between the Pacific Ocean and the Indian Ocean lies along the northern tip of Malacca Strait, west coast of Sumatra, south coast of Java, and the Arafura Sea, south coast of New Guinea (Irian), then the east coast of Australia, the east longitude of 146°51' to the south of Bass Strait and Tasmania and the longitude of the Antarctic continent. There are totally 38 countries and regions (excluding British Indian Ocean Territory) along the coast of the Indian Ocean, with about three billion people. Five South Asian countries surrounding the Indian Ocean mainly include India, Pakistan, Bangladesh, Sri Lanka, Maldives, among which India, Pakistan, Bangladesh are coastal countries while Sri Lanka and Maldives are island countries. On one hand, as the largest neighboring country of South Asia, China shares a boundary of thousands of kilometers with India, Pakistan, Nepal, Bhutan and Afghanistan. On the other hand, the South Asia is also a region with most land neighbors in China's neighboring regions. Southeast Asian countries along the coast of the Indian Ocean consist of Thailand, Malaysia, Singapore, Myanmar Indonesia and Timor-Leste. There are fifteen African countries and regions along the coast of the Indian Ocean including South Africa, Mozambique, Tanzania, Kenya, Somalia, Djibouti, Eritrea, Sudan, Egypt, Mauritius, Comoros, Seychelles, Madagascar, Reunion (France), and Mayotte (France). Besides, there are eleven countries and regions of West Asia and Middle East along the coast of the Indian Ocean, including Saudi Arabia, Yemen, Oman, the United Arab Emirates, Qatar, Bahrain, Kuwait, Iran, Iraq, Jordan and Israel. Australia of the Oceania is also along the coast of the Indian Ocean.

As for geographical position of the India Ocean, it stretches from the Strait of Hormuz of Arabian Sea in the west to Malacca Strait in the east. The seas and gulfs belonging to the Ocean comprise the Red Sea, Arabian Sea, Gulf of Aden, the Persian Gulf, the Gulf of Oman, Bengal Bay, Andaman Sea, the Arafura Sea, Timor Sea, the Gulf of Carpentaria and Great Australian Bay. Arabian Sea and Bengal Bay are gates to Asia; the Red Sea and Persian Gulf are paths towards the Middle East; Gulf of Oman is an important link between Arabian Sea and Persian Gulf; Gulf of Aden is a vital passage to the Red Sea. The Malacca Strait at the exit of Singapore Strait, Gulf of Aden at the mouth of the Red Sea and the Strait of Hormuz at the entrance of the Persian Gulf are three strategic passages to the Indian Ocean. These geographical factors are still

[25] C. Zhu, India's Ocean, Research Series on the Chinese Dream and China's Development Path, DOI 10.1007/978-981-10-5726-7_1

of highly strategic importance although the advances in weapons and military technology have changed ways of war and world's setup since the sixteenth century.

The Gulf of Aden is a protruding part of Asia where is a narrow transportation thoroughfare with the southeast corner of Arab, which is a place frequented by pirates. In the Indian Ocean, writes Alan Villiers, "the profession of piracy is as old as seafaring itself. The first man who ever straddled a drifting log probably knocked the second man from another log. So piracy began. It has been going on ever since". The Malacca Strait and the Gulf of Aden, the Persian Gulf, the Makran coast, the Gulf of Kutch—the whole Arabian Sea in fact—has been crawling with pirates since time immemorial. Piracy is a major non-conventional security threat for countries worldwide. Especially the pirates spreading across the Gulf of Aden, pose a huge threat to the securities of offshore energy and trade channels.

Nobody can deny the importance of geographical position for a country to increase or decentralize sea power as well as to the thalassocracy. According to Alfred Thayer Mahan, there are main factors influencing sea power of a country comprise: location, form constitution including related natural productivity and climate; territorial scope; population; national characteristics; government characteristics including national institutions. If a country does not rely on land transportation to protect itself, or extend outward through land routes, but simply aims at sea, then the country possesses superior geographical location, compared to ones surrounded by mainland countries.4 As for geographical structure and features of the Indian Ocean, Kavalam Madhava Panikkar writes in his book of India and the Indian Ocean: An Essay on the Influence of Sea Power on Indian History, he describes from the perspective of geographical structure, one of the Indian Ocean's features is that land surrounds the ocean in three directions. The southern Asia forms a ridge, African continent a wall in the west, Myanmar, Malaya and unbroken islands together a shield in the east. Compared with other oceans, the Arctic ocean and Antarctic Ocean surrounding the poles have no connection with land where humans live. And the Pacific Ocean and Atlantic Ocean are like two flat avenues with no protuberant lands or lands with large area stretching into the oceans. Besides, based on distribution of islands and archipelagos in or near to continental coasts and the vast oceans, Kavalam Madhava Panikkar points out another important feature of the Indian Ocean different from the Pacific Ocean and the Atlantic Ocean: the Indian Ocean washes whole east African coast down to Somalia, south banks of Arabia, Iran and Baluchistan, as well as west banks of Indian subcontinent, Myanmar, Malay Peninsula and Sumatra. The Ocean is protected by the Mandab Strait at the west entrance and Malacca Strait at the east entrance. Both straits are prone to be controlled. The Red Sea with the Mandab Strait as an entrance is an inland sea which is easy to be controlled by lands of both sides. Malacca Strait faces vast Pacific Ocean, but its narrow lands on both sides make import and export easy to be manipulated.

On the Indian Ocean's western shores, we have the merging and volatile democracies of East Africa, as well as anarchic Somalia; almost four thousand miles away on its eastern shores the evolving, post-fundamentalist face of Indonesia, the most populous Muslim country in the world.

No imagine epitomizes the spirit of our borderless world, with its civilizational competition on one hand and intense, inarticulate yearning for unity on the other, as much as an Indian Ocean Map.

Geopolitics in the Indian Ocean Region

Resources are always a logical starting point of geopolitics. It is believed that oil is a kind of strategic material for a country's economic development and energy security, as well as a trade item with strategic significance. Of eight important oil and gas reserves in the world, three reserves including Persian Gulf and its coast, coastal areas and continental shelf of Indonesia as well as northwest continental shelf of Australia, are distributed in the Indian Ocean, accounting for over 70% of the world's total reserves. Especially the Persian Gulf in the northwest bank of the Indian Ocean, is the world's largest oil producer and supplier. It has been proved that oil reserve there comprise over 50% of the world's total reserve and its annual output accounts for 1/3 of the world's total output, which wins the title "Treasury of Oil". Produced oil is transported outward through Strait of Hormuz. Countries around Persian Gulf possess nearly 60% of the world's crude oil storage that has been explored. Besides, there is the largest export volume of petroleum in the Middle East, which accounts for 45% of the world's overall export volume, with 75% of produced oil being used for export. It can be said that almost all countries worldwide depend on in varying degrees the adequate oil resource of this region, especially the petroleum of the Middle East, making it to be a vital region for global economy and international politics. There is a figurative metaphor: a camel in the area of the Indian Ocean is referred to petroleum in Persian Gulf; on its back is most fuel supply of the world. The camel is so strong that it can bear greater burden in the next few decades as long as it would not be ruined in politics. South Africa, a place seen as "Watchdog", safeguards Cape of Good Hope for oil carriers of the Middle East and watches the gateway towards the Indian Ocean. And Zambia which is compared to be a hen, produces rare copper that likens the hen's eggs.

Apart from energy reserves, it is estimated that 65% of global strategic raw materials reserves spread in the Indian Ocean, among which the explored raw materials are uranium, gold, diamonds, tin, coal, iron ore, tungsten, manganese, copper, zinc and others. In addition, abundant reserves of precious metals are distributed in the Ocean, with manganese reserve accounting for 85% of that of the world, vanadium reserve 60%, chromium reserve 86%, uranium reserve over 50%. Iron reserve there ranks first in the world, with Indian iron reserve accounting for 25% of the world. Abundant storage of strategic mineral resources exists in African region around the west coast of southern Indian Ocean, enhancing the status of the Indian Ocean in global geopolitical system. 96% of known chromium minerals in the world spread in South Africa and Zimbabwe; asbestos in South Africa accounts for 1/10 of the world, gold 1/2, manganese minerals 1/3, uranium minerals 1/5, diamonds 1/3. It can be said that minerals resources such as copper, manganese, antimony, vanadium, play a dominant role for such African countries as South Africa and Zambia, which likens the supporting role of petroleum for Persian Gulf. It can be thus seen that resource distribution around the Indian Ocean is obviously uneven: petroleum

in the Middle East can be important as a strong camel while others are seen as small sparrows; South African Federation in Africa is significant as a strapping camel; and in Indian subcontinent, large population is like a camel while resources are like sparrows.

Except for resources' influence on geopolitics, shipping lines and strategic thoroughfares in the Indian Ocean also play a prominent role for geopolitics, which is a unique feature of the Indian ocean different from the Atlantic Ocean and Pacific Ocean. The Indian Ocean is one of the busiest maritime trading channels in the world, with 1/9 of global seaports and 1/5 of the world's goods throughput. Forty percent of seaborne crude oil passes through the Strait of Hormuz at one end of the ocean, and 50% of the world's merchant fleet capacity is hosted at the Strait of Malacca, at the other end, making the Indian Ocean the globe's busiest and most important interstate. Actually, "petroleum route" in the Ocean is a "strategic life line" that lots of developed and developing countries depend on. Currently, three major petroleum transportation lines are: Persian Gulf-Cape of Good Hope-Western Europe, North America; Persian Gulf-Malacca Strait (or Lombok, Makassar Strait)- Japan; Persian Gulf-Suez Canal-Mediterranean Sea-Western Europe, North America. Petroleum volume transported via the Indian Ocean comprises over 50% of the global petroleum transportation volume on the oceans. What people are most familiar with is the cognition about the importance of the Malacca Strait and Strait of Hormuz. There are sayings going like this, "Whatever is lord of Malacca has his hands on the throat of Venice", "Another proverb had it that if the world were an egg, Hormuz was its yolk". Besides, it is well-known that the Suez Canal artificially dug between the middle period of the nineteenth century and the middle period of the twentieth century, connects the Red Sea to Mediterranean Sea, developing the shortest shipping line between the Indian Ocean and the Atlantic Ocean. And Malacca Strait as a natural passageway, is a link between the Indian Ocean and Pacific Ocean, forming a maritime shortcut for the Middle East and the Far East. However, their vulnerabilities caused by passageways' narrowness become a major security issue globally.

Great Powers' Control Over the Indian Ocean in History

Maritime transportation is the most important factor in politics and military strategies. From a social and political perspective, the attraction of oceans is extensive sea routes like a broad boulevard or vast land where you can go forward in any direction. In this vast land, the routes that you have ever passed may be restricted or controlled by some conditions, forcing you to choose some of routes as trade routes. Sea power has had a prominent role in controlling transportation in history and the situation will continue as long as there is navy. The reason is that, as for long-distance transportation in large quantities, water transportation is much more convenient than land transportation, with larger freight volume. Therefore, oceans become the most important commercial transportation medium.

Before the thirteenth century, it was India that mainly controlled the Indian Ocean. The period that the Indians dominate the Ocean is a period featured with completely free trade and sail. There were no pirates or no interference in trade. Sea routes were open to all ships of all

countries. Arabians sailed on the seas freely and transported their goods to the remote South Asia of China. And China's ships have sailed on the Indian Ocean since the fourth century. Thus there was no monopoly or prohibition of navigation. Later, Europeans came. On July 8th, 1497, Vasco da Gama with four sailing ships started from Portugal, and landed at Kozhikode in May 1498.17 When Portuguese arrived here in 1498, the Indian Ocean was actually a maritime vacuum zone. While new invaders did not confine themselves to some region, but extended toward two maritime spaces in the east and west based on their correct judgment. In western waters, they occupied Mozambique and Girwa, the most important Muslim colonies along the African coasts. Later, they again captured Socotra and Hormuz Island where they could control the Red Sea and Persian Gulf. In the west coast of the Ocean, they occupied Cochin, Goa, Daman and Diu, thus gaining the control over Malabar and Gujarat. In the eastern waters, Ceylon around the coast of Coromandel, Masulipatam, Negapatam and Malacca at the another side of the bay of Bengal were also seized by them. It can be said that Portuguese had established their hegemony in the Indian Ocean since Mir Hossein with Egyptian fleets left the Ocean in 1509.19 In history, after Portuguese ruled the Indian Ocean for over one hundred years, they were driven away by Dutchmen. Later Dutch were replaced by English, came also with its share of blood. Then there was the supplanting of the English by the American in the high seas of Asia, which came via the bloodshed of World War II.

History of sea power is a statement about the competition and hostility between nations as well as the frequent peak violence existing in wars. In 1890, the United States adopted the Naval Act of 1890, and only spent ten years strengthening naval strength, jumping from the twelfth place to the third in the world, after France and the UK. Furthermore, The US became the strongest sea power nation after the World War I and completely controlled the Pacific Ocean after the World War II, making the Pacific Ocean an American lake. Nowadays, the US still wants to defend its hegemony based on sea power theory.

As for India, it gained the command of the Indian Ocean before the thirteenth century. Afterwards, however, the Ocean was successively controlled by Portuguese, Dutchmen, Britishers and Frenchmen. And between the early nineteenth century and the World War I, the Indian Ocean became a British lake. After India gained the independence in 1947, it became ambitious to a great power like Britain and wanted to play a major role in the world. India's strategic target was not only impacted by Mahan's idea, "Might is Right", but also influenced by strategic thoughts of K.M. Pannikar (founder of Indian maritime strategy), like "the one who controls the Indian Ocean can rule India", "the India's security is greatly tied to the Indian Ocean". Especially after the nuclear tests in 1998, India's dream to be a great power suppressed in heart for a long time was triggered again.

The Indian Ocean in the 21st Century

Usually seen negligible, the Indian Ocean is regarded as a marginal area far from global power and conflicts. European colonists once believed that the Indian Ocean and its people here should

be very colonized and exploited, and would be still attached to other areas in the foreseeable future. Hence, the Indian Ocean region, with a long history and culture as well as nearly 1/4 of the global population and nations, does not gain due attention in politics and international power fields. And the research about it is not paid enough attention by academic circle led by Occidental world.

"The one who gets sea power can control the world. And one who controls oceans can command the world", "The world's destiny will be determined in the Indian Ocean in the 21st century". Mahan's sea power theory supported by Roosevelt provided theoretical basis for American naval development and maritime military expansion. When US Defense Secretary Panetta attended Shangri-La Dialogue in Singapore on June 2nd, 2012, he said that before 2020, the US navy would change the current deployment situation with respectively 50% of fleets arranged in the Pacific Ocean and the Atlantic Ocean, into a pattern with 60% of fleets in the Pacific Ocean and 40% of fleets in the Atlantic Ocean. This high-profile adjustment of strategic focus seems a transfer of the US's focus from the Atlantic Ocean to the Pacific Ocean. Actually, it is trying to look for a foothold between the Indian Ocean and the Pacific Ocean, which is a regression after buffered sea power strategy.

Sea power strategy once helped the US to be a hegemon and proved the proposition of "the one who gets sea power can control the world", which greatly encouraged Indian politicians to pursue their dream to be a power. At the beginning of the twentyfirst century, with the rise of Indian economy, India's dream became clear. The bridge to realize its dream is to make the Indian Ocean become "India's Ocean". Vajpayee, Indian former Prime Minister, once pointed out that, "national security lies in the area from Arabian Sea in the west to Malacca Strait in the east"; after Manmohan Singh Administration took office in 2004, they continued the naval strategy of the former government and stated, "our strategy covers open ocean of the Indian Ocean"; vice-premier Lal Krishna Advani also declared that the twentyfirst century would be "Indian Century". It could be seen that India did not conceal its ambition to be a power. That's why India has kept its high military equipment investment in recent years, with military investment slightly higher than growth rate of GDP. In particular, India keeps huge investment in naval construction, hoping to become strong by building a powerful navy.

Entering the 21st century, the Indian Ocean is increasingly playing an important role in global geopolitics and its strategic status enhances, leading to strategic competitions between major countries such as the US, Japan and Russia in this region. The main causes are shown as follows: Firstly, the traditional setup that both sides of the Atlantic Ocean dominate global economy starts to change due to eastward movement of global economic centers, and nations around both sides of the Atlantic Ocean trapped in financial crisis, have been busy to overcome hardships. Therefore, global economic engine began to move to the Pacific Ocean and the Atlantic Ocean. The situation where the Indian Ocean region depends on nations around the Atlantic Ocean starts to shift, and afterwards the importance of the Indian Ocean is going to be rediscovered and reevaluated. Secondly, petroleum resource and sea passageways, the two core "selling points" in

the Indian Ocean region, become increasingly important owing to global energy shortage and eastward movement of global economic centers. The two points turn into hot topics often discussed by all major media and academic circles. Thus, the Indian Ocean has been a place that emerging powers and old empires compete for and tends to be a new field for old empires to suppress the rise of emerging China and India. Thirdly, the rise of emerging and medium powers in the Ocean is an internal factor for this region to enhance its significance. India, with nuclear weapons, oceangoing navy, the world's largest democratic state, Bangalore and Bollywood as its major five signs, possesses enormous growth potential and will rise to be a world power in the future. This prospect helps India to be an object major powers try to draw over to their side. In addition, medium powers in this region such as Australia, South Africa, Egypt, Iran, Indonesia, Thailand and others, also enhance odds to increase the attention of global geopolitics in this region. Last but not least, "success" can attract global attention, and "failure" can also be or even more impressive. In the Indian Ocean, there are not only India, the emerging power, and Australia, the medium power, but also major "failed states" and "unstable factors" around the world. Somalia ranks first for these years in global failed nations and the West Asia and North Africa regions have been a global tinderbox since the Cold War. Religious and racial conflicts become one "main theme" of this Ocean. Rise of globalization, especially worldwide spread of terrorism threat, make this region a focus of powers outside the region.

It is worth mentioning that China has increased its attention to the India Ocean in recent years. One of the reasons is that the Ocean is a key region for China's Twenty-first Century Maritime Silk Road Initiative. Actually, China has traded with Southern India since the first century B.C. In the seventh century, Chinese merchants overseas became some of the bravest navigators in the Indian Ocean; in the ninth century, Chinese could build long-range sailing vessels more skillful than those of Arab or Tamil; in the thirteenth century, people started to realize their maritime superiority in Bay of Bengal. During the first fifty years of the fifteenth century, Zheng He, the leader of naval expeditions of Ming Dynasty, together with seven huge naval expedition teams, visited major ports around the west and east maritime space of the Indian Ocean, asking nations there to pay tributes to and be subjected to the Empire of Ming Dynasty. However, in 1433, when China possessed all necessary items–skillful vessels, gunpowder and compass, which could be used to gain the control over seas in the Indian Ocean, it suddenly left this Ocean due to some unknown reasons.

In conclusion, since the new century, seaways security in the Indian Ocean have become increasingly prominent because of rampant piracy around the waters of Gulf of Aden and Malacca as well as intensity of situation around the Strait of Hormuz caused by Iran's nuclear crisis. Based on the increase strategic importance of the Indian Ocean and the continuous threat to sea routes, the world's major countries have gradually shift their strategic focus to the Indian Ocean on after another. As for China, it possesses indisputable economic and security interests in this ocean, with 80% of national imported crude oil and 50% of maritime trade carried along the Indian Ocean routes.

Emerging Turbulence of the Indian Ocean

Entering the 21st Century, especially in the second decade, when the trend towards multi-polarity is expected to be irresistible and the old order has been gradually broken but a new order hasn't yet been established, the world is entering into a stage of strategic turbulence. Or rather, the world is entering an anxious era of strategic competition, an era requiring strategic rationality and prudent thinking, and an ever changing era that needs to be studiously adapted to and carefully coped with. An outstanding feature of a strategic competition era is that, all countries have to face the uncertainty of external environment and the crisis awareness of psychological environment. External manifestation of strategic competition is turmoil or even conflict, its internal manifestation is mutual suspicion, so as to respond through arms race or making credible threats, while suspicion and threats are closely connected with safety and challenge.

Will the 21st century develop into a Pacific Century, an Indian Ocean Century or an Indo-Pacific Century? The prosperity of the Pacific Ocean is shaped by the economic growth miracle of Japan in 1970s, the economic growth miracle of the Four Asian Tigers (South Korea, China Taiwan, Hong Kong and Singapore) in 1970s–1990s and the mass rise of emerging economies since 1990s. At present, the group rise of emerging industrialized countries including China, Russia, India, Brazil and South Africa has presented an irreversible trend, the economic growth rate of emerging economies, especially BRICS, is far higher than the world average, emerging economies have taken up over one fourth of world economy, and the economic proportion of BRICS has risen to one fifth. All these factors have undoubtedly promoted the continuous prosperity of the Pacific region. However, economic prosperity doesn't mean a stable security situation, and also prosperity cannot cover the Pacific turbulence, including the Korean Peninsula crisis, Huangyan Island dispute in South China Sea, unrest caused by constant defiance of Japan in Diaoyu Islands on East China Sea. In fact, the turbulence outline in the Indian Ocean has become increasingly clear, and the continuously dynamic competition pattern and security dilemma can not be ignored. Just as Robert Kaplan says, the Indian Ocean, the world's third largest water area, has been in the competition center of the 21st century.

The Indian Ocean serves as a strategic passage of seaway transportation, and is extremely rich in natural resources, including energy and mineral resources. The combination of geopolitics and resources politics decides the core status of the Indian Ocean and adjacent waters in future resource fight and competition among great powers. In addition, as a flank of the Middle East and World Oil Center, South Asia in the Indian Ocean region plays a decisive role in global strategies of great powers. The South Asian Sub-Continent is a hub connecting Europe, Middle East, East Asia and Australia. The U.S. Marine Corps "Vision and Strategy" statement, unveiled in June 2008, covering the years to 2025, also concludes in so many words that the Indian Ocean and its adjacent waters will be a central theater of conflict and competition. Along with its continued dominance in the Pacific, the U.S. clearly seeks to be the preeminent South Asian Power. Japan hasn't clearly put forward an Indian Ocean strategy though, it has been maintaining closely relationships with India, Australia, South Africa, Iran and other main countries, and

endeavoring to enhancing its influence in the region in terms of politics, economy, foreign affairs, security and other aspects. Needless to say, India has always regarded the Indian Ocean as its backyard. India's strategists have divided the Indian Ocean into three concentric rings: Complete or Absolute Control area ensuring safety of water area with 300 sea miles offshore, mainly including territorial waters, exclusive economic zones and coastal islands; Moderate Control area keeping communication monitoring over security of channel with 300–600 sea miles offshore; a Soft Control area projecting and deterring area beyond 700 sea miles offshore. In contrast to China, whose maritime access is constrained, India enjoys free access to the open seas. Placed at the very heart of the Indian Ocean, India is in the happy geographic situation of sitting on top of the sea lines of communication in the ocean and with easy access to all the choke points that control entry into it. Meanwhile, the Indian Ocean is an important energy corridor for China. Particularly, China is one of the countries highly dependent on foreign energy, the oil import volume of which exceeded the output as early as from 2006, showing foreign dependence degree on oil above 50%. In 2010, China had a total oil import volume of over 100 million tons, and the top five countries of origin included Saudi Arabia, Iran, Oman and Iraq in the Middle East and Sudan in Africa. To safeguard its economic interests and energy security in the Indian Ocean, China must firstly attach importance to the Indian Ocean and strengthen the cooperation with coastal countries, especially South Asia Countries.

The competition between great powers such as China, the United States, Japan and India in the Indian Ocean will constantly weaken the strategic pattern already fragile here, and further enhance turbulence and uncertainty of Indian Ocean security situation. The turbulence in the Indian Ocean has dominant and recessive manifestation forms. Dominant turbulence is mainly caused by regional problems and manifested as economic interest competition, non-traditional security, national extremism, etc., while recessive turbulence is mainly generated from strategic competition and mutual suspicion. In the Indian Ocean, presently, there is no area so intensively gathering interest concerns of the great powers such as the United States, Japan, India, Australia and China, and no other ocean is more need of strategic stability than this one.

Turbulence Brought by Regional Problems

On one hand, situation remains tense and turbulent in the Indian Ocean thanks to the regional problem of struggling for benefits. Firstly, turbulence caused by the surging energy demand. The scramble for resource utilization is always the logical starting point of geopolitics. In today's world, as a strategic material, oil is not only related to nation's economic development and energy security, but also can be regarded as a kind of trade item of strategic significance. Among eight oil and gas reserves, three are distributed in the Indian Ocean region, respectively in the Persian Gulf and its coast, Indonesia coast and continental shelf and Australia North West Shelf, accounting for over 70% of the world's gross reserves. Indian Ocean tanker between the Persian Gulf and South and East Asia are becoming clogged, as hundreds of millions of Indians and Chinese join the global middle class, necessitating vast consumption of oil. The world's energy needs will rise by 50 percent by 2030, an almost half of that consumption will come from India

and China. India, soon to become the world's fourth largest energy consumer after the United States, China, and Japan—is dependent on oil for more than 90 percent of its energy needs, and 90 percent of that oil will soon come from the Persian Gulf by way of the Arabian Sea. Indeed, before 2025, India will overtake Japan as the world's third largest net importer of oil after the United States and China. With the continuously rising energy demand and various predictions and publicity, potential benefits in the Indian Ocean have been magnified virtually, and the competitive situation in this region has been aggravated. Secondly, competition caused by occupation, exploitation and utilization of marine resources. As estimated, the Indian Ocean region owns 65% of global strategic raw material reserves, and is extremely rich in precious metal, having 85% of global manganese reserves, 60% of global vanadium reserves, 86% of global chromium reserves, over 50% of global uranium reserves, and the world's largest iron reserves. In recent years, due to its available resources and acquisition of new marine resource development and utilization technology, the value of ocean has been constantly elevated, and the fight for occupation, development and utilization of marine resources, even the sovereignty ownership of islands, has become increasingly fierce.

On the other hand, turmoil brought by non-traditional security in the Indian Ocean never entirely drained away. In addition to conventional security problems, the Indian Ocean region has always been a region with relatively intensive non-conventional threats such as pirate and terrorism. First of all, the world's main "failed states" gather here, which contributes to the instability of the Indian Ocean region. Of ten countries with the lowest global peace index in 2012, five were distributed in the Indian Ocean, being respectively Somalia, Sudan, Iraq, Israel and Pakistan. Secondly, the pirate problem has been one of the most widely concerned non-conventional security problems in the Indian Ocean region in recent years. For instance, in 2011, 439 pirate armed robbery cases occurred, of which 160 occurred along the Indian Ocean, accounting for 36%.35 Among 7 areas where pirate armed robbery cases take place frequently (Somalia sea area, the Red Sea, Malaysia, Indonesia, Gulf of Aden, Gulf of Guinea and South China Sea), 5 are located in the Indian Ocean region. Again, the Indian Ocean region is the cradle of terrorism. In 2012, there were four breeding places of global terrorism: (1) Pakistan and Afghanistan; (2) Arabian Peninsula; (3) Somalia Peninsula; Maghreb, all located in the Indian Ocean region. Influenced by ideology and religious factors, the Middle East has had an unstable political situation and been always shrouded in the haze of conflicts and turbulence and active terrorism in recent years. Especially after the "9/11", the strategic region has inevitably become a main battlefield for anti-terrorist force and terrorism. It is predictable that ocean terrorism is and will be one of the main security concerns of the Indian Ocean region, as evidenced by Somali pirates from the end of 2008 as well as pirate incidents and terrorist attacks previously occurred in the Red Sea waters, Mandab Strait, India coast and Malacca Strait.

Meanwhile, turbulence incurred from National Extremism in the Indian Ocean Region can't be ignored. In recent years, the overall economic growth rate of the Indian Ocean region is higher than the world average level, affected by the US financial crisis and European debt crisis a few

years ago, its economic growth has presented an obvious downward trend, and plus with the relatively low social and economic development level in the region, the enhancement of the government's ability to establish an effective social order has been restricted, which may even lead to a social anarchy, and thus provide an advantageous space for the growth of national extremism and terrorism. Besides gathering many economically underdeveloped or very underdeveloped areas, the Indian Ocean region has an extremely low trade volume. In addition, many countries in the Indian Ocean region are the place where the impoverished concentrate and serious unemployment problems exist. Experience shows that extremism often exists in poverty and unemployment populations, as they are more likely to be mobilized and even bewitched by extremists and prone to violence. To solve this problem, the fundamental is to promote economic growth, to improve the income level, to reinforce education efforts, etc.

Turbulence Triggered by Strategic Competition

Judging from the present situation, the world's multi-polarization trend has become irresistible. A multi-polar world is inevitably full of competition, as every polar country will strain every nerve to maintain its position in the international system. Generally, to win the competition, a great power generally will enhance its strengths on the one hand, and tries everything possible to prevent or impair the development of its opponent. The strategic competition performed in the Indian Ocean is partly derived from the scramble among great powers for resources and authority influence in the region, and partly from the so-called security threat arising from responding to external environment uncertainty and psychological environment crisis, but beyond question, the results will lead the security environment in the Indian Ocean even tenser, the security dilemma may get deepened, strategic risks may gather, and the security situation may not be optimistic.

Firstly, tension and turbulence caused by US Asia-Pacific rebalance strategy. After 2010, the US former President Obama and the State Secretary Hillary declared on several occasions in high profile to transfer the strategic focus of America to the Asia-Pacific area, and some corresponding actions have been taken, including frequently attending various multilateral meetings in Asia, deploying Marine Corps to Darwin in Northern Australia, establishing closer military relations with Australia, Singapore, the Philippines, India and other countries, etc. Behind such words-to-action transfer of strategic focus, the China factor is undoubtedly a crucial consideration. Although it remains controversial whether the rebalancing strategy of the United States aims to counterbalance China, China is no doubt placed in a focal position as its most important strategic rival. Just as commander of the U.S. Pacific Command Samuel J. Locklear says, the rise of China is a major threat to American warships and service members in the Pacific region, and US army's absolute control over Pacific waters and airspace is coming to an end.

The Asia-Pacific Rebalancing Strategy of the United States includes not only reconfiguration of its strategic resources on a global scale, but also rebalancing of the unbalanced pattern caused as the US ignored the Asia-Pacific area for a long time after its adjustment of strategic resource center from the Middle East to the Asia-Pacific area. In addition to transferring some strategic

resources from the Middle East to the Asia-Pacific area, the Rebalancing Strategy also includes strengthening the contact with Asian countries in political and security fields, and establishing closer relations with countries in this area through economic dominance. US officials stressed on various occasions its attention to the Pacific and Indian Oceans, and plus with a variety of movements, it was because such discourses and actions that the tense atmosphere in this area has been intensified, and the turmoil been aggravated. In fact, after the United States withdrew from the Middle East, the security issue of the Middle East will surely bring disaster to the Indian Ocean region. The strategy transformation of the United States "braking" in the Middle East but "stepping on the gas" in Asia to implement the Rebalancing Strategy has not only planted a seed of turbulence in the Middle East, but also aggravated the arms race in the Indian-Pacific area to a certain extent, created strategic threat, intensified strategic competition among great powers in the Indian-Pacific area, led to potential imbalance of security pattern, imbalance of regional cooperation and relationship between major countries, increased the tension and conflicts in the Asia-Pacific area, and become the biggest hidden danger to regional security. It should be noticed that many countries in the Middle East couldn't establish an effective regime, even show some signs to become failed states, which results in the sharp rise of religious extremism. Failed states are bound to be training places of religious extremism or even terrorism. Both China and India are faced with challenges in protecting their interests in the Middle East. A direct impact is the eastward extension and expansion of Middle East religious extremism or even terrorism, which will directly influence the safety of Indian Ocean coastal countries and even Western Pacific.

Secondly, turbulence caused by the crash of extended great power strategies. There is reciprocal causation between a turbulent world and the extension of great power strategies. The strategy extension of great powers, especially China, US and India, will inevitably crash and lead to bilateral and multilateral instability, may intensify the politicized tendency of economic trade and investment disputes, and may aggravate the turbulence of the region.

As the world's only superpower, the United States attaches great importance to the Indian Ocean, but economic interests is not its major concern, after all the United States has few trades in this region, and its oil dependence on the Middle East presents a downtrend. The United States setting foot in the Indian Ocean is mainly for its strategic layout on a global scale, aiming to maintain its military presence in the region, expand its strategic interest space and safeguard the interests of its allies, and always keep a US-oriented world order. To achieve the goal, the United States firstly needs to ensure its dominance in the Asia-Pacific area and make sure to dominate affairs of the Indian-Pacific area in the future. This area extends from Indian Peninsula to the west coast of America, it stretches over the Pacific and the Indian Ocean, and both oceans have become more closely linked due to transportation and strategy factors. Since 2010, Obama and his senior officials of the State Department and the Defense Department have repeatedly mentioned the concept of "Indo-Pacific", indicating the United States' intention to strengthen the cooperation with Indian navy, and want to mould Indian navy into a custodian of India-Pacific

marine channels (including South China Sea, Strait of Malacca and the Pacific in a greater scope); to strengthen the coordination of policy stance between the United States and India as to East Asia marine security affairs; and to build the northwest coast of Australia a power projection point from American Indo-Pacific link to west Pacific and east Indian Ocean.

The importance of the Indian Ocean to India lies in not only India stretching into the Indian Ocean for 1600 km, but also the geopolitical significance of three peripheral gulfs. In particular, the Gulf of Aden is where pirates frequently haunt, the Persian Gulf and the Bay of Bengal serve as two flanks of the entire Indian Peninsula, all being crucial yet vulnerable. Thus, the significance of sea power to India becomes self-evident. Realizing that its future depends on the ocean, India has always treated the Indian Ocean as India's Ocean or its controlled strategic area and put forward that "the entire Indian Ocean basin—from the Persian Gulf in the north to the Antarctica in the south, from the Cape of Good Hope and east coast Africa in the west to Malacca, Malaysia and Indonesia islands in the east—is strategic periphery of India." This forms sharp contrast to the strategic concern of the United States. In the defense strategy document Sustaining U.S. Global Leadership: Priorities for 21st Century Defense released in January 2012, the United States re-emphasized the importance of the Indian Ocean: "U.S. economic and security interests are inextricably linked to developments in the arc extending from the Western Pacific and East Asia into the Indian Ocean region and South Asia, creating a mix of evolving challenges and opportunities. If we say the main objective of India's Look East Policy at the first stage is to strengthen the trade relations with relatively economically developed Southeast Area and to realize the economic interest goal of mutual benefit and shared profits, its main objective at the second stage would be to walk out of South Asia and the Indian Ocean, to carry out pragmatic cooperation with Asia-Pacific countries in terms of politics and security through the Balance Diplomacy strategy, so as to constantly expand its strategic interest space and enhance India's influence in the Asia-Pacific area. Certainly, India hasn't forgotten to tentatively depend on entering the South China Sea to respond to China' marching west to the Indian Ocean.

Not being an Indian Ocean country, China pays so much attention to the Indian Ocean is mainly due to highly dependence on energy and trade in this region. As is known to all, the facts that China is the world's second largest economy, the largest goods trading power, the largest foreign exchange reserve power and the second largest energy consumer, has a foreign trade dependence degree of over 50%, highly dependent on imported oil, etc., have boosted the dependence of China's economy on global resources and trades. Especially, China's strategic channels for oil importing and foreign trade are mainly districted in the Indian Ocean region, which determines the close relationship between China and the Indian Ocean. From this, how do China and India co-exist in the Indian Ocean in the future?

Whether due to the US' Pivot Strategy, India's Act East Policy, China's Go West Strategy or Australia's intention to promote its regional influence based on its unique geopolitical advantages, the strategic interest space has been extending continuously and crossing to a certain extent, and triggered strategic competition of great powers in the Indo-Pacific area. If any great

power has ambiguous strategic extension intention or builds threats only for the purpose of anti-threat, it may give rise to geopolitical conflicts and cause structural confrontation.

Thirdly, turbulence triggered by strategic deterrence of Great Powers. The emergence of turbulence has added a lot of uncertainties and risks to the changing world, after better recognizing the importance of self-reliance, the world and great powers have successively taken various actions and measures to improve their strategic deterrence. In this way, even if such deterrence fails and leads to conflicts and wars, great powers would have the ability to defeat the rivals with their military superiorities, and this is the implication of credibility threats in the game theory.

In practices of modern international relations, there are two ways to judge whether a country constitutes threat: unscrambling the strategic intent of a country by soft means, and judging whether the strategic capability of a country constitutes threat by hard means. As intent is quite uncertain and often unable to be definitely measured as capacity, the most reliable way to judge a country's strategic intent is actually investigating its strategic capability, of which the constitution of strategic capability is one of the most core indicators. The improvement of strategic capability and the competition for sea power have intensified the arms race among all countries, which is also a major cause of instability and conflicts.

It should be pointed out that, the strategic competition seems tranquil in the Indian Ocean though, it actually exists everywhere. Even behind economic trade and investment cooperation there is strategic competition, and as a result, economic relations are increasingly affected by political relations. However, if we examine carefully, it is not difficult to find the obvious phenomenon that, many tensions in the Asia-Pacific area and the Indian Ocean are artificially manufactured. Artificial manufacturing of tension is to some extent a kind of tactic for great powers to conduct strategic competition. "Tension" naturally brings further competition. Competition is a double-edged sword, being able to enhance the strength and trigger conflicts as well. Anyhow, it is neither the will nor strategy of all countries to make conflicts, and other western countries including the United States have no intention to create conflicts, as it does not conform to their respective interests.

In Southeast Asia off the coast of the Indian Ocean, China is the largest trade partner of Indonesia, Thailand, Malaysia, Myanmar and ASEAN countries. In South Asia, China is the largest trade partner of India and Pakistan, and also the biggest trade partner of Australia in the Oceania. In the future, China will have increased economic influence on the Indian Ocean region. The rise of economic strength will not necessarily bring about threats. Therefore, all countries need to firstly make clear which are realistic threats, which are potential and which are man-made threats, otherwise emotional factors will mislead the judgment, so as to interfere the direction and strength of force construction and utilization.

Fourthly, turbulence caused by mutual suspicion and erroneous strategy judgment among Great Powers. In the presence of cognition deviation due to the lack of sufficient understanding and communication between the countries, the pursuit of strategic interests has led to collision of strategic targets, and plus with the speculation of public opinions, mutual threat and fundamental strategic competition have been constantly upgraded. Whether it being an intra-domain country in the Indian Ocean region such as India and Australia, or an extraterritorial country such as the United States, Japan and China, mutual suspicion and mistrust always exist, which have led to the coexistence of economic cooperation and political suspicion. As to India which owns particularly favorable natural conditions in the Indian Ocean, the geographical advantages and the dream of building a great power have driven it to seek exclusive leadership in the Indian Ocean, as clearly pointed out in the strategic guiding document Indian Maritime Doctrine released in 2004 and the Freedom to Use the Seas: India's Maritime Military Strategy released in 2007. India worries that the Indian Ocean may become an arena for great powers to scramble for power in the future, the unique geopolitical advantages and abundant mineral resources of the Indian Ocean may incur the intervention of extraterritorial countries in the Indian Ocean, so as to pose a threat to India's national security. Based on such strategic judgments, India wishes to realize its great power dream by relying on a powerful navy dream. The rise of China is surely a focus attracting global attention and igniting various public opinions. Especially under the influence of the China Threat Theory, some Indo-Pacific countries worry that China's rising economic power will be accompanied with stronger sovereignty and territorial claims, and such mentality has further boosted mutual suspicion and mistrust and intensified the differences among various countries. In fact, emerging economies, mainly China and India, have gradually realized the important role of strengthening cooperation in promoting global balance of power, but the following problem still exists: insufficient actions have been taken to strengthen the cooperation, revealing the lack of initiative. China's contact with Indian Ocean coastal countries are speculated as the pursuit of certain control over the Indian Ocean. With sharp increase of both trade volume and investment amount, India and China have broad economic cooperation prospects; however, affected by the China Threat Theory, India's strategy towards China appears ambivalent and preventive. The strategy paranoia caused by mutual suspicion will lead to misjudgment of strategy, thus inevitably affect the stability and development of bilateral and multilateral relations, and ultimately affect the economic cooperation, causing political factors a stumbling block for economic cooperation. One solution to alleviate such awkward problem is to find a way to build the foundations of renewed trust.

Maritime Security: An Indian Perspective

The maritime security has assumed a new dimension in the post-9/11 era with the rapid rise in international terrorism. Sea routes are being increasingly used by the terrorist to escape high vigilance on land and penetrate countries like India with long and often not so well-protected coastlines.

The Mumbai attacks of 26/11/2008 brought home the point as to how vulnerable India is to terrorism emanating from the sea. Ten terrorists undertook an audacious journey through sea from Karachi in Pakistan to Mumbai with full backing of Pakistan‘s ISI. The whole of India was badly shaken by the sheer tenacity of the attacks on the heart of the economic capital of India. Merchant ships of different countries including India have also been increasingly facing pirate attacks over the last few years.

It would be a big headache for India and the world if there was to be collusion between the terrorist organizations and the Pirates from Somalia and other African countries. India has probably not been able to strengthen its naval capabilities in sync with ever rising threats and challenges to her security and safety. Many of the projects aimed at indigenously building shipping and weapon systems are not bearing fruit due to a variety of reasons.

Several terrorist organizations in and around the Indian Ocean are known to possess merchant fleets of various types. The former Liberation Tigers of Tamil Eelam (LTTE), for example, had an entire flotilla engaged in dubious maritime trade. Most of these are registered under flag of convenience (FOC) countries known as "pan-ho-lib," i.e. Panama, Honduras and Liberia (, and are difficult to track as they routinely change names and registry. Since the checks and balances introduced by these registries are undeniably inadequate, there is no guarantee as to the type of crew or the type of cargo that these ships carry. Such ships are considered the safest bet for carrying out terrorist-related activities.

The Mumbai attacks exposed the weakness of our coastal security apparatus. The fact that the terrorists could sail through such a long distance unchallenged by either the Coast-Guard or the Indian Navy, points to the gravity of the task of protecting such a long coastline which also houses many of India‘s prime defense installations. The attacks highlighted gaps in coastal surveillance, stressing India‘s inability to effectively monitor her long coastline—a condition that is common to many littoral states in both the developing and the developed world. Although Indian security agencies had prior information of a possible terrorist landing near Mumbai by sea, whatever measures were taken proved insufficient to monitor maritime traffic in and around Mumbai. This failure would seem to reflect the coast guard's shortage of equipment for coastal surveillance: fewer than 100 boats for more than 5,000 miles of shoreline and minimal aviation assets.

Are we well-prepared to deal with the challenges in sync with the ever rising security threats facing the country from various quarters?

India has primarily depended on Russia or former Soviet Republic for the supply of weapon systems and technology specially for its navy. The Russian Submarines have been involved in a number of accidents in the past including the infamous sinking and destruction of her nuclear submarine Kurskin August 2000.

India has during last two years faced a number of major and minor accidents involving the Russian-supplied submarines and its own shipbuilding facilities. Most serious of these was the destruction of India‘s frontline submarine INS Sindhurakshak on 14 August 2013. Eighteen crew members on board - three officers and 15 sailors - were killed when blasts ripped through the torpedo compartment of the INS Sindhurakshak while the submarine was berthed in Mumbai harbor.

Apart from this, 8 other minor accidents took place involving the naval ships and shipping facilities, in which 2 other navy personnel lost their lives and many others were injured. India‘s operational capabilities suffered a big jolt as a result of these accidents.

India being such a vast country with such a long coastline needs a credible maritime strategy to deal with the ever-rising challenges to her national security and defense. Though naval expansion in the form of new ships and weapon systems of various kinds does require a lot of spending through budgetary allocations, a strong government committed to the progress of the country can make arrangements by removing bureaucratic hurdles and by collaborating with countries that have similar goals and aims in the Indian Ocean region. India also needs to define its foreign policy goals regarding the Indian Ocean region and work towards bridging the trust deficit that has plagued the countries in this region impeding all round progress. Such a policy has the potential to ameliorate the lives of millions of people living in poverty.

India’s Maritime Security Concerns and the Indian Ocean Region[26]

India is a maritime state with a long coastline of more than 7500 km and 274 islands that sits astride the Bay of Bengal and the Arabian Sea, at the head of the Indian Ocean. The Indian sub-continent juts out nearly 1000 km into the northern expanse of the Indian Ocean like a wedge and splits this region into two distinct sub-regions.

As KM Panikkar had once said, “It is the geographical position of India that changes the character of the Indian Ocean”. India’s relation with the Indian Ocean is, therefore, a symbiotic one and history is witness to the fact that whenever India has neglected this huge body of water, it has lost its sovereignty, as was seen during the period of colonisation by the European powers. The Indian Ocean has a long history of carrying India’s foreign trade with recorded evidence stretching back to the 9th century BCE. Maritime trade still constitutes the backbone of India’s economy despite geographical shifts in the pattern of India’s trade. Considering that most of these commodities will have to come by sea, maritime security assumes an important dimension in India’s calculus for national development.

The success of recent government initiatives like the Prime Minister’s vision of Security and Growth for All in the Region (SAGAR) and the renewed emphasis on development of maritime

[26] Gopal Suri, India’s Maritime Security Concerns and the Indian Ocean Region, Indian Foreign Affairs Journal Vol. 11, No. 3, July–September 2016, 238-252

infrastructure has to be underpinned by a guarantee of maritime security in our immediate neighbourhood. This essay will examine India's maritime interests in the Indian Ocean Region (IOR) and understand the security concerns thereof. A glance at the existing maritime security frameworks in the IOR will then enable a better understanding of the responsibilities of maritime security of this region.

India's Maritime Geography

The Indian Ocean

The Indian Ocean is bounded by the Asian land mass in its northern reaches while the African continent serves to separate it from the Atlantic in the west. In the east, the Indonesian archipelago and Australia restrict its access to the Pacific while the cold continent of Antarctica provides the southern base. The sea borne shipping passages of the Indian Ocean are connected to the Pacific through narrow waterways in its southern and eastern reaches while the rather difficult passage around the southern tip of Africa connects it with the Atlantic. The Mediterranean and the continental hinterland of Europe are similarly connected to the Indian Ocean through the narrow passages of the Red Sea.

India in the Indian Ocean

India has an enviable geographical location as it sits at the head of the Indian Ocean, half way between these passages, allowing it to control these approaches and thence its trade. It is this quirk of tectonic evolution coupled with the meteorological phenomena of the monsoon and the trade winds that has given India a unique position in the history of economics and trade of the Indian Ocean. The history of the Indian Ocean is replete with stories of Indian and Arabian seafaring merchants trading to and from India with their ships borne on these winds. This geographical centrality of India also made it the base for expansion of the European colonial power to the Far East from the 16^{th} and 17^{th} centuries. The establishment of the Portuguese commercial empire in the Indian Ocean was facilitated by their base at Goa, which provided the springboard for the subsequent conquest of Malacca. This laid the template for the subsequent British rule over the Indian Ocean from Aden to India and thence to South East Asia.

Areas of Maritime Interest

The Indian Navy's Maritime Security Strategy document is arguably the only such official document, which deals with the security of the maritime realm. It clearly enunciates India's areas of maritime interest and categorises them as primary and secondary areas. The primary areas of maritime interest stretch from India's coast all the way to the east coast of Africa including the Arabian Sea, the Bay of Bengal and the Andaman Sea. It also includes the Persian Gulf and the various choke points leading into the northern IOR. The secondary areas of maritime interest are further west and east of the primary areas and encompass the South and East China Seas as also the southern IOR and Antarctica.

India's Maritime Interests

An understanding of the national maritime interests is important before identifying concerns of maritime security. A broad definition of maritime interests would encompass all those key areas of national endeavour in the maritime realm which are essential for the country's survival and growth. Preservation of these interests is essential to national security and any threat to these areas of national endeavour needs to be closely analysed for formulating both, military and national strategies.

Maritime Territory

India has a huge coastline of about 7517 km and more than 1200 islands. Many of these islands are quite distant with the farthest of the A&N islands about 1600 km from the nearest mainland. India's territorial sea has an expanse of 193,834 sqkm while the Exclusive Economic Zone (EEZ) covers 2.02 million sqkm. The living and non-living resources in this zone, which measure about two-third of the landmass of the country, are exclusive to India, as also the trade and transport facilities that navigate through this area. This expanse is also home to 51 percent of India's proven oil reserves and 66 percent of natural gas reserves. Protection and preservation of this natural resource not only implies ensuring its territorial integrity but also keeping it safe from predatory inimical entities.

Sea Lines of Communication (SLOCs)

The importance of the Sea Lines can be gauged from the fact that the oceans supported about four fifths of the total world merchandise trade in 2014. Over the last decade, India's seaborne trade has grown at twice the global growth rate of 3.3 percent, maritime container trade at 6.5 percent (higher than the world average of 5.4 percent over the past ten years) while cargo traffic at Indian ports has doubled to 1 billion tonnes per annum over the last decade (FY 2005–2015) and is expected to reach 1.7 billion tonnes per annum by 2022. This amounts to a total of 95 percent of India's trade volume wherein lies the importance of the SLOCs and the International Shipping Lanes of the Indian Ocean in India's maritime security calculus.

Maritime Economy

The Indian economy is hugely dependent on energy imports to the extent of 81 percent of the total domestic oil consumption in 2015-16. These imports are transported by sea while offshore oil gas production account accounts for 80 percent of all domestic gas production. Nearly 95 percent of India's international trade by volume and over 70 percent by value is carried over the seas. India is also the world's fourth largest producer of fish, most of which comes from the sea. This maritime economy is supported by an extensive network of 13 major and about 200 minor ports all along the coast. The Sagarmala project has provided a renewed thrust to port-led development and infrastructure for quick and efficient transportation of goods to and from ports.

Nurturing this nascent maritime economy will require concerted national efforts whilst ensuring that impediments and potential threats are kept at bay.

Maritime Investments

India has invested in a variety of sectors like infrastructure, industry, energy, and services in a number of counties in the immediate maritime neighbourhood and beyond. India operates two research stations in Antarctica for conducting research in a wide variety of disciplines, most prominent of those being global climate change. India has made significant strides towards harnessing deep sea resources with the International Seabed Authority according it pioneer status and an allocation of 75000 sqkm of seabed in the Central Indian Ocean. ONGC Videsh Ltd has invested in oil exploration in Vietnam's EEZ in two blocks allotted by the Vietnamese Government. China has protested against this activity deeming it to be illegal in the disputed waters of the South China Sea. While India still seems to be taking baby steps in this sector of the economy, it is important that this area of national endeavour be suitably encouraged whilst protecting it from being jeopardised by inimical interests.

Indian Diaspora

From time immemorial, India has had trade and cultural links with a number of countries in the IOR. The Gulf and Middle East region alone has in excess of 8 million NRIs employed in various sectors of these countries. Remittances from this Diaspora exceeded $ 100 billion in 2014. The unstable conditions in some of these countries have also prompted evacuation of our citizens during past crises as was witnessed recently in Yemen in April 2015 and from Lebanon in July 2006. Considering that many of these countries are coastal states, the safety and security of the Indian Diaspora residing there assumes importance in the maritime security framework.

India's Historic Cultural and Trade Links in the IOR

India's location in the Indian Ocean has placed it at the nerve centre of trade and cultural cross-pollination in this region throughout history. Historical evidence exists of Indian linkages with Cambodia, Indonesia, Malaysia and Mauritius with manifestations of Indian culture clearly seen in their temples and legends. Nurturing of these linkages is important for preservation of India's interests in the region as these can directly impinge on the policies of these countries in particular and thereby the region at large. The Ministry of Culture launched Project Mausam in June 2014 to re-connect and re-establish communications between countries of the Indian Ocean world. It is intended to examine key processes and phenomena that link different parts of the Indian Ocean littoral as well as those that connect the coastal centres to their hinterlands. Focused efforts to further projects such as this and others like the Kerala government's 'Spice Route' will strengthen India's maritime interests in the IOR.

India's Maritime Security Concerns

India's maritime security concerns stem from the threats, largely in the primary area of interest of the Indian Ocean, which have a direct bearing on India's maritime interests. While most of these threats also have a bearing on the other stake holders in the region, the impact on India will be greater considering India is 'already assuming her responsibilities in securing the Indian Ocean region'. Threats, from inimical and potential adversaries to national interests in times of hostilities and war are not being considered here since they would fall under the realm of war fighting. Hence, this part will restrict itself to threats to maritime interests in times of peace as also those, which affect the larger region in India's neighbourhood.

Control of Choke Points

Access to the Indian Ocean is geographically controlled by a number of choke points leading to and from the Arabian Sea and the Bay of Bengal, and from the Southern Indian Ocean, which are critical for safeguarding the Indian maritime interests. India is equidistant from most of these choke points allowing it to play a prominent role in the security of this huge maritime space. The Iran-Iraq war of the 1980s demonstrated the risks to Indian energy imports through the Straits of Hormuz. The Straits of Bab-el-Mandeb and the Gulf of Aden are similarly critical for security of energy flows. Incidents like the attack on the French tanker Limburg when an al-Qaeda boat rammed the ship off Yemen in October 2002 can severely disrupt the Indian energy supply lines, which will directly affect the economy and have cascading effects on the shipping business. The Malacca Strait brings to mind the disruptive control the Dutch had exercised over the Indian Ocean trade in the 17th and 18th centuries. It is, therefore, very important that these areas remain free from the control of inimical interests and the free flow of seaborne traffic remains the norm. India has always been an equal if not vital partner to the world's efforts in contributing towards the maintenance of freedom of navigation over these vital seaways. However, many of these regions are prone to bouts of instability, as has been witnessed in the recent past, which can then have a debilitating effect on regional as also global trade.

Threats to SLOCs

The SLOCs in the IOR have been susceptible to disruption by a variety of traditional and non-traditional threats over the years. However, India's increasing dependence on the seas for its trade may necessitate intervention to protect these SLOCs from such threats. The cooperation of other states in the region as also from those outside the region is required to ensure the security of these SLOCs in this huge ocean space. India has been a pioneer in such efforts with the Indian Navy leading the way from 2002 when Indian ships escorted US flagged carriers through the Malacca Strait following the attack on USS Cole in Aden. The ongoing operation in the Gulf of Aden for the past decade where the Indian Navy has escorted ships of all nationalities epitomises these efforts.

Regional Instability

The Indian Ocean littoral, regrettably, has been witness to large areas of political instability in the recent past. The current situation in Yemen is one such instability. The rebels of the Free Aceh Movement in Indonesia have often targeted vessels carrying natural resource commodities such as oil, tin and aluminium, off the coast of Sumatra. Instability in Somalia for the past two decades gave birth to the world's biggest piracy threat. The Iran-Iraq war of the 1980s was another occasion when vital oil trade was severely affected and required a concerted effort from a number of countries to limit the damage. India has an intrinsic stake in the stability of the northern IOR and its immediate neighbourhood since instability in these regions has a cascading effect on India itself. The past has seen political disturbance in littoral states like Sri Lanka and Myanmar spilling over to India through the sea route. Indian maritime security forces then had to conduct dedicated operations to combat this menace, like the Indian intervention in the Maldives in 1988 to foil a coup d'état.

Piracy

Somalia based piracy has caused universal worry to the international fraternity since the late 1990s and it is only collective action by the international community that has led to a reduction in piracy attacks. India has not only escorted numerous merchant ships of all countries but concerted efforts of its maritime security forces has ensured that this piracy, which had spread its wings as far east as the Lakshadweep and Maldives islands, has been controlled and the erstwhile High Risk Area was moved further west of India in October 2015. However, political instability in Somalia coupled with any reduction in counter piracy efforts can cause its resurgence. While Somalia based piracy has shown a downward trend, statistics have shown an increase in piracy, largely robberies carried out at anchorages, off the coast of Bangladesh, Malaysia, and Indonesia. Though anti-piracy action by the international community may not be warranted, actions by the littoral nations are necessary. The recent decision by the governments of Indonesia, Malaysia and Philippines for joint patrolling is a step in the right direction, which will deter these pirates and assuage the fears of the international maritime community. India's commitment to anti-piracy efforts in the IOR has been underlined by efforts like the Indian Ocean Naval Symposium, which was started by the Indian Navy in 2008, and has found traction with all the Indian Ocean states in generating mechanisms and procedures for combating these threats.

Trafficking

The Indian Ocean Region is regrettably home to the world's most notorious areas of drug production, the Golden Crescent and the Golden Triangle. The trans-national networks established by the drug smugglers also serve as conduits for other destabilising activities like gunrunning and human trafficking. Myanmar has suffered from these twin troubles in large measures as also other countries of the littoral. These networks tend to use the sea route because of its vastness with its inherent opacity to surveillance. The interdictions of the Indian Coast

Guard in the past few years reveal a rising trend of this nefarious activity.19 Political disturbance and oppression further add to this already hazardous mix with the ensuing cascading effects manifesting themselves in India's internal security, forcing India to intervene on occasion.

Maritime Terrorism

The Indian Ocean has had relatively few incidents of maritime terrorism but the potential exists. The al-Qaeda attack on the French tanker, the Limburg, off Yemen, in October 2002, was one such. India's huge coastline of more than 7500 km, a thriving maritime commercial community along its coast with nearly 200,000 fishing boats and a fishermen population of 4 million make the job of monitoring maritime activity an unenviable task. The ability of adversarial interests to exploit this vast maritime activity for launching attacks on land is therefore quite high, as was witnessed in the 26/11 terrorist acts at Mumbai, which were abetted by an inimical state. The attempted hijacking of a Pakistan Navy frigate Zulfiqar, in Sep 2014, by the al-Qaeda in the Indian Subcontinent (AQIS) for possibly carrying out attacks against US Navy ships added a new dimension to this threat. The ramifications of such incidents on the Indian state have already been witnessed and the potential for further damage exists, especially in the present frayed geo-political conditions of the sub-continent. India has put in place a comprehensive monitoring and reaction mechanism to deal with such threats, which has prevented any more events like the one at Mumbai in 2008. However, concerns remain as was witnessed last year when a boat carrying explosives was intercepted by the Coast Guard.

Extra Regional Military Presence

The Indian Ocean has always been witness to the military presence of outside powers right from the advent of the Portuguese in the 15th century till the present day. While the colonial incursions were rooted in commercial interests, the current extra-regional military presence is intended to further strategic interests of various nations. The ongoing international naval effort while critical to curbing the menace of piracy has also benefited nations in terms of operational intelligence gained and an expanded military maritime footprint. Deployments of submarines, like the Dutch and the Chinese to the region, serve no purpose other than to gain operational expertise and raise tensions in this area. The expanding Chinese Navy and its acquisition of a base at Djibouti, access facilities in Malaysia, and the 'surreptitious' base at Gwadar, albeit for justifiable logistic reasons, further exacerbate this situation. The Maritime Silk Road announced by the Chinese President in 2013 is also viewed by many as a 'disguise for China's military ambitions'. The opacity of Chinese policy and less than comfortable assurances on contentious issues coupled with the existing disputes with India has further widened an already existing trust deficit, further provoking security concerns.

Illegal Unreported and Unregulated (IUU) Fishing

IUU fishing is a major problem for marine communities around the world and governments of coastal states are severely challenged in enforcing international and national maritime laws to

control this activity. A World Wildlife Fund report on illegal fishing has found that 87 percent of the fish stocks surveyed in the Western and Eastern Indian Ocean were experiencing high levels of IUU fishing. This is a major cause for concern, especially when viewed in the light of what the Somali President stated, in an op-ed, '...the encroachment of IUU fishing vessels sparked a wave of piracy in Somalia that cost the global maritime shipping industry billions of dollars in lost revenue'. Many ASEAN countries have also faced this problem, especially from Chinese fishing vessels. The Indian Ocean has also seen such activity in the recent past with an NGO, Sea Shepherd, reporting a fleet of IUU fishing vessels, south of the Andamans, in March 2016. Indian maritime zones have not witnessed many incidents of IUU fishing though there have been unconfirmed reports of fishing trawlers, mainly from Bangladesh and Taiwan, illegally entering India's territorial waters in the Bay of Bengal. The focus on coastal security after the Mumbai attacks, has been a major deterrent to IUU fishing on account of the intensified patrolling by maritime security agencies. However, the high seas as also coastal zones of smaller neighbouring nations remain extremely vulnerable to this threat. India has provided naval assets for conducting patrolling of the EEZ of smaller nations like Seychelles and Mauritius in recent times, which has helped augment their maritime security capabilities.

Most of the threats outlined above are transnational in nature and require the cooperation of a number of regional as also extra-regional stakeholders in collaborating and developing mechanisms to combat their proliferation. However, the Indian Ocean does not have overarching security architecture. A look at the existing security architecture of the region will enable the reader to better understand the responsibilities that India will need to shoulder as a regional leader in the IOR.

Regional Security Architecture in the IOR

India has always espoused a cooperative approach and participation of all states in promoting maritime security in the IOR as enunciated by PM Narendra Modi in his vision of SAGAR – Security And Growth for All in the Region. The IOR has a number of arrangements in this sphere, which are either restricted to countries or sub-regions. A glance at some of these arrangements will provide an indicative overview of their capabilities as also their shortfalls.

Indian Ocean Rim Association (IORA)

The IORA was launched in 1997 for promoting intra-regional economic cooperation and development. However, the Charter of the IORA is a lessthan-treaty level document and is, therefore, not legally binding on the signatories. The IORA now has six priority areas to promote the sustained growth and balanced development of the region out of which maritime safety and security is the first priority. It has also emphasised that maritime security and safety, and disaster management should be aligned with, and complement a possible IONS (Indian Ocean Naval Symposium) initiatives in these areas. However, it neither has a working group to deliberate on these issues nor an institutional link with IONS.

Indian Ocean Naval Symposium (IONS)

The Indian Ocean Naval Symposium (IONS) is a voluntary initiative formed in 2008 that seeks to increase maritime co-operation among navies of the littoral states of the Indian Ocean Region. The IONS also aims to establish a variety of multinational maritime cooperative mechanisms designed to mitigate maritime security concerns among members. However, this is a purely naval initiative and is therefore hampered by an absence of governmental obligation to adhere to the Charter of the IONS.

Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP)

The ReCAAP is a regional government-to-government agreement, brought into force in September 2006 to promote and enhance cooperation against piracy and armed robbery in Asia. It is a multilateral agreement comprising 20 countries from Asia, Europe, USA, and Australia. The ReCAAP Information Sharing Centre (ISC) facilitates the dissemination of piracy-related information but does not have a mandate to initiate direct action nor is it incumbent on the signatories to take action for enhancing maritime security.

ASEAN Regional Forum (ARF)

The objectives of the ASEAN Regional Forum are to foster dialogue and consultation on political and security issues of common interest and make efforts towards confidence-building and preventive diplomacy in the Asia-Pacific region. There has been a reasonable degree of success in these two main objectives though the same degree of success has not been seen in the efforts of ASEAN with China, since China has largely abjured from multilateral resolution of disputes.

The IOR consequently does not have a pan-regional maritime security structure wherein all the major stakeholders are involved. The diversity of the region and the geographical expanse also precludes development of an all-encompassing security architecture. Hence, there is a case for regional leaders to take the mantle in addressing common security imperatives of the region to infuse the required impetus towards generating a regional security construct.

Mitigating India's Maritime Security Concerns

India's increasing economic might and rising regional status necessitate assumption of 'our responsibility to shape its (IOR) future' in the words of PM Narendra Modi. India has also emphasised the responsibility of regional states in maintaining peace, stability and prosperity in the Indian Ocean. However, the inherent weaknesses of the regional states and the nature of the threats require a concerted effort from India to mitigate these threats. The cooperative approach adopted by India on issues of regional development underpinned by a guarantee of security will serve to not only address India's own national concerns but also the littoral at large.

Regional Maritime Security Framework

An overarching security framework for the entire IOR may not be an implementable proposition considering the current geopolitical scenario and the development levels of the littoral states. Existing organisations like the IORA and IONS have elements of maritime security included in their charter. India can work towards cajoling participating governments into strengthening the IORA and creating inherent linkages with IONS to ensure effective implementation of actions for strengthening maritime security. While the IORA is not a treaty, member states should undertake agreed measures and initiate actions as decided at common fora. Simultaneously, initiatives like the Trilateral Maritime Security Cooperation have to be given a sustained impetus and also widened to include other stakeholders for dealing effectively with challenges emerging from the maritime sphere.

Fostering Close Ties with Nations at Choke Points

Control of shipping and trade at the choke points by inimical interests is unlikely in today's' world considering the stakes involved and the geopolitical linkages between states. However, disruption of trade, as witnessed during the Iran-Iraq war, can have debilitating effects. It is therefore, important to build strategic relationships with littoral nations in such regions to ensure unhindered and unimpeded flow of Indian trade and shipping for continued economic progress. Such relations will also provide tactically significant information about potential adversarial interests transiting these areas, especially in moments of crises. For a start, India needs to enhance its relations with Indonesia in the maritime sphere even as Indonesia seeks to be a key player with its Global Maritime Fulcrum initiative.

Maritime Exchanges

In the absence of regional or sub-regional security architecture, bilateral and multi-lateral exchanges like the MILAN series of exercises, in all spheres of the maritime security domain, between concerned agencies of the various littoral nations of the IOR, can be mooted by India. These should be institutionalised in terms of regularity of conduct as also connectivity between agencies to ensure a high degree of coordination for achievement of concrete results. Such exchanges and regular contact between these agencies will aid in curbing of illegal activities like trafficking, gun running, smuggling, etc.

Information Exchange

Mechanisms and protocols for exchange of tactically important information and intelligence need to be put in place for interdiction and prosecution of vessels and persons engaged in illegal activities. Exchange of such intelligence will permit coordinated tracking of such activity across maritime zones and territorial waters, thereby ensuring effective prosecution. India already has agreements with a number of countries for exchange of white shipping information. Such exchanges have to be not only maintained but also increased with countries across the region.

Common Operational Grid

Effective management of the maritime domain, especially across a complex region like the IOR, requires a common operational grid amongst the littoral nations. International maritime practices and existent procedures already provide a huge database of marine information regarding vessels and facilities through systems like the Automatic Information System (AIS) and the Global Maritime Distress and Safety System (GMDSS). In addition, various states have national systems to provide critical information concerning maritime security. While the sensitivity of states to part with such information is understandable, filtered information concerning the littoral can be provided to the other states, which will enable development of a fused and comprehensive operational picture. Establishment of a common operational grid, which fuses information from systems like the AIS, and filtered information from national maritime security networks will enable better coordination between the various national maritime security agencies and greatly enhance their operational efficiency.

Coordinated Patrols

The Indian Navy carries out coordinated patrols with Thailand and Indonesia on a bilateral basis. The ICG also has MoUs with a number of countries for cooperation on maritime issues, which include joint exercises. However, due to the small size and limited capacities of many of the littoral countries, effective patrolling of the contingent EEZs is not always possible. Pooling of assets between the various states and a multi-lateral approach could alleviate the problems and improve monitoring of these zones.

Anti-Piracy

The ongoing multi-national effort in the Gulf of Aden and off the coast of Somalia has nearly eradicated piracy in this area. The littoral navies of the region have neither the wherewithal nor the capability to maintain such sustained operations to combat this menace. The current geopolitical realities and the relations between the various states also preclude such a coordinated effort. It is therefore important that the international anti-piracy effort is continued till a more favourable climate is established in Somalia. India, meanwhile, needs to take the lead in the establishment of a sub-regional mechanism for the north-eastern IOR with the participation of Bangladesh and Myanmar to curb piracy, which has seen an upward trend in recent years. This mechanism will require participation and involvement of a host of actors from each nation including the coast guards and the police for effective monitoring and control.

India thus has an onerous responsibility being the largest nation in the IOR. This responsibility has to be also tempered with the current geopolitical realities and the aspirations of the other states. India’s historical, cultural and traditional linkages with many of these states will help accelerate development of mechanisms to bolster the maritime security for the region. However, it will require India to take the lead. This will also be in keeping with India’s desire to develop

the IOR with a collaborative and cooperative approach from all the regional stakeholders as epitomised by the Prime Minister's vision of SAGAR.

Sino-India Cooperation Dilemma

Currently, the security dilemma caused by regional conflicts and strategic competition challenges India the most. Although India has shown absolute confidence in marine power, both the turbulence triggered by regional issues and caused by strategic competition among great powers in the Indian Ocean have caught India in the security dilemma of the Indian Ocean. In this regard, India not only endeavors to strengthen its construction of naval forces, but also constantly enhances the military cooperation at sea with the United States, Japan and other extraterritorial great powers. The ultimate goal of India's ocean strategy is to strive for more exclusive power in the Indian Ocean, India would not willingly to be always controlled by the United States in the Indian Ocean.

At present, the Sino-India security dilemma is extending to the ocean, and the rising China is considered as a growing threat and challenge to India. The expectations of Chindia and Dragon-Elephant Dance do have excellent prospects, but China's rapid rise has made India feel anxious. Notwithstanding China has very little influence in the Indian Ocean, China Marching west to the Indian Ocean has made India to worry that, China's naval force may be as strong as to stretch into the India Ocean and to contest with India for the influence of South Asia as well as Indian Ocean. With such entanglement and contradiction, India wishes to weaken the United States' power over the Indian Ocean by virtue of China on the one hand, but is not willing to see a shift situation due to its leverage. This is one of the reasons why India shows a relatively positive towards the economic cooperation with China but presents to be passive in strategic cooperation. Undoubtedly, with extreme worry about or mistaken cognition of China's intention in entering the Indian Ocean, even if no obstacle will be set, India will not show positivity, and may instead of strengthening the military and security cooperation with the great powers such as the United States, Japan, Australia, etc., which will further intensity the "problem" of Indian Ocean between China and India.

For the time being, China is more and more frequently seen in the backyard of India-Indian Ocean and its surrounding area, being India's primary strategic concern. Obviously, in the eyes of India, China marching west has constitutes India's biggest threat and challenge. Some Indian scholars consider that, the strategic interests of China and India have extended beyond territorial issues and water resources problems, Chinese navy's footprint has extended continuously in the Indo-Indian area, being a main source of potential conflicts and future security dilemma. India has an urgent need to build a "ring of diamond" in response to China's "string of pearls", and to go together with other countries to contend against China's geo-strategy in the Indian Ocean. Even though the interest intersection between China and India has become gradually clear, and their challenges and threats have become increasingly convergent, India still shows a sensitive and cautious attitude or reaction to China entering the Indian Ocean. In this context, unless

carefully managed, as Indian and Chinese navy increasing far ocean actions, Sino-India competition in the sea may get intensified.

As a matter of fact, both China and India wish to change the currently unreasonable international order, and both of them have realized that, an indispensable prerequisite to pursue the great power status is powerful strength, which requires seeking a peace and safe development environment and implementing mutually beneficial and win-win development strategies. To enhance the strength, it is a more advanced and pragmatic concept to pay attention to capacity building rather than threat building. Capacity cultivation and improvement require not only steady economic growth, but also a stable surrounding environment. Accompanied with such pursuit of great power status there is the construction of strategic mutual trust, which, established on the basis of strength, is bound to become a new logical starting point of both countries' diplomatic policies. After all, threats may be short-lived and presented in various different forms, if a grand strategy or military deployment is restricted to any pre-established threat, it will turn out unable to keep pace with the changing situation. On the contrary, a capacity-oriented strategy will be more flexible, which can deal with randomly developed accidental threats by changing or utilizing national policy tools to size up the situation.

Nevertheless, the "China Threat Theory" is still intensifying the prevention and distrust of India and other neighboring countries towards China, the western academic circle even treats the rise of China as a threat and challenge. No matter how China emphasizes on peaceful development, it is unable to alter the western world's thinking set about the "China Threat Theory". China's establishment of mutual beneficial cooperation relationship with Indian Ocean coastal countries is considered the implementation of the so-called "String of Pearls" strategy to restrain the rise of India. Being allergic and lack of antibody against the "China Threat Theory", India's view of China is somewhat one-sided or more or less malposed. In addition to unsmooth communication and exchange, historical and cultural differences and other factors, the biased and irrational reporting and commentary of media and public opinions have also generated negative impact on mutual trust between the two countries, posing various difficulties to Sino-India cooperation.

Actually, Strategic competition will inevitably cause turbulence, which will increase the likelihood of conflicts to a certain extent, and conflicts will in turn trigger large-scale turbulence and greatly intensify the arms race. Under the current circumstance that global economic growth generally slows down and the political security situation becomes even tenser due to regional problems and strategic competition, it seems alarmism to predict inevitable conflicts in the Indian Ocean. However, it has become urgent responsibility of Asian countries to avoid the strategic competition from rising to strategic confrontation, make every endeavor to prevent conflicts, to prevent the waste of historical opportunities and the obstruction of Asia's prosperity trend, and to realize mutual tolerance and peaceful coexistence.

Firstly, strategic competition aiming to win strategic interests and influence often gives rise to the coexistence of economic cooperation and strategic tensions. Generally, a competitor will treat

its rival as a partner only under special circumstances, and even if there is a possibility to boost strategic cooperation, such cooperation will be restrained in a certain field, rather than all aspects. In general, a strategic competitor will treat its rival as an enemy, and such cooperation will inevitably trigger vicious competition or even conflict, and with continuously updated cognition of threat, the strategic mutual trust between countries will become even fragile, which will certainly become a product of strategic confrontation between great powers and regional security dilemma, or even lead to the emergence of structural turbulence, and it is the tense atmosphere that is exactly becoming the biggest hidden peril to regional security.

Secondly, tension is actually manufactured to make the opponent to admit or accept its strength or position. How to eliminate tension and reduce geopolitical risks? To eliminate tension, the tense mentality should be firstly eliminated. Rather than building treats on the excuse of feeling nervous or perceiving threats and generating convincing countervailing power and believable deterrent effect through arms face, it is better to strengthen the exchange and communication with all other countries and to eliminate fictitious threats artificially made based on the lack of confidence and mutual trust. Just as virtual economy being able to bring down real economy, virtual politics can also defeat the body of politics.

Thirdly, from the practical point of view, the best way to respond to the sense of uncertainty and the sense of crisis is trying to make oneself stronger. A sea power should firstly be an economic power. The mismatch of self-cognition with the strength of a country may ultimately lead to a pyrrhic victory. Economic strengthen derives from the win-win cooperation mechanism and an environment for peace and stability of the region. No one can deny the important role played by trade and economic relationship in power allocation.

Fourthly, the current broad geopolitical environment is more suitable for cooperation between great powers in the Indian Ocean, especially China, the United States and India, rather than negative competition and power competition based on mutual threat. If these great powers could maintain the safety of the Pacific and Indian oceans through naval cooperation, share interests through cooperation, resolve threats and avoid conflicts, it is possible to establish mutually beneficial and win-win relationship between great powers and a peaceful and stable regional pattern. From this perspective, strategic idea based on capability promotion, mutual benefit, win-win and risk sharing rather than that based on threat or deterrence should become a common recognition and goal. Only in this way can we seek ocean calmness and world peace.

Fifthly, in fact, China has become an economic big power, but it is true that China is not satisfied with this. Its goal is to become an economic giant and to realize great rejuvenation of the Chinese nation, not as worried by the outside world as that China is bound to challenge the hegemony and to scramble for corresponding power and influence. Unwilling to be accepted by western countries of course, but it is not a goal deliberately pursued by China. At present, with the irresistible multi-polarity trend, it conforms to fundamental interests of all countries to temporarily detain disputes, run in with each other in strategic competition, compromise and

adapt to each other without touching the core interests of other countries, grasp the limits of strategic competition, strive to seek a dynamic mechanism controlling, alleviating and eliminating tensions and turbulence and advance in twists and turns.

Sixthly, the strategic opportunity period with rising Asia calls for all countries to form resultant forces, and the developing situation calls for Sino-India cooperation in the Indian Ocean. For any country, to build a developing external environment, the first thing is to treat great powers as the key and the surrounding as the primary. Therefore, Sino-India cooperation is of strategic significance. Based on the history of Sino-India relations as well as the Five Principles of Peaceful Coexistence, there are many efficient ways of co-operations between two countries such as the construction of Bangladesh-China-India-Burma economic corridor. China and India should make joint efforts to renew their ideas, to deepen the cognition of each other, to walk out of the Indian Ocean cooperation dilemma, and to seize the opportunity for mutual development.

MODULE-VI

MARITIME CYBERSECURITY

CYBERSECURITY AT SEA[27]

INTRODUCTION

On 31 March 2017, Vice Admiral Clive Johnstone, Commander of NATO Allied Maritime Command (MARCOM), mentioned cybersecurity more than five times in his 20-minute speech at the Hellenic Armed Forces Officers' Mess on the 'Contemporary Maritime Security Threats in the Mediterranean and the Role of MARCOM in Addressing Them'. A few months before, it was Sir Admiral ret. George Zambellas, the former First Sea Lord of the Royal Navy, that highlighted the importance of cybersecurity on the maritime domain during a similar event on 'TheSecurity Challenges in Eastern Mediterranean and the Edge of Technology'. Jeremy Corbyn, the leader of the Labour party, during the 2017 election campaign, also clearly stated, on several occasions, that the priority for his government security-wise, if elected, would be to counter the two predominant threats to the UK's national security: cybersecurity and terrorism. No one can blame him since this prioritisation was confirmed during the cyber-attack at the National Health Service (NHS) and the terrorist attacks in London and Manchester, all taking place within the first quarter of 2017.

Undoubtedly, cyberspace is a global domain. It passes, dynamically, physical, organisational, geographical and time boundaries. Using commonly used infrastructures (such as the world wide web), its impacts and effects are fast and far reaching. As a threat, it may be considered as asymmetric or hybrid, since it is cheap, anonymous, anarchic, endless, like space, and overwhelmingly intangible. It may be targeted by criminals, terrorists, individuals or groups as well as state actors. These actors' motivation include financial gain, military or political advantage or even solely drawing attention to a specific situation. Actors engaged in cyber-attacks use multiple methods to achieve their goals. These may include phishing, distributed denial of service attacks (DDoS), drive by attacks, SQL injection, watering hole, spearphishing, advanced persistent threat (APT), logistic bombs and other sophisticated methods (Singer and Friedman 2014). The target groups vary from home users to small medium-sized enterprises (SMEs), market primes and even governmental structures. If you add in this equation the unexpected nature of such acts, as the cyberattacks at the NHS and the entire IT structure of the Ukrainian government in May and June 20171 aptly highlighted, an unfamiliar, high risk and impact, novel form of threat emerges. The importance of cybersecurity in the maritime domain is prominent since it engages all maritime related activities. As regards, port operations and infrastructure, cranes, logistic software and port services are Information and Communications Technology (ICT) and Operational Technology (OT) connected assets, connecting to ships, headquarters, shipping and trading companies, transport operators and pilot associations. Ships are connected through navigation aid systems and safety communication systems to their navigation and engineering systems, as well as command and control, and logistic services.

[27] P. Kapalidis, Cybersecurity at Sea; L. Otto (ed.), Global Challenges in Maritime Security, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-34630-0_8

The future in shipping suggests an autonomous shipping era which makes the aforementioned connected activities even more challenging. Finally, maritime traffic control centres heavily depend on the aforementioned ICT equipment in order to remain connected and monitor safety at sea with ships, port authorities, national shipping authorities, pilot agencies and other maritime organisations.

Several actors have identified the importance of cybersecurity in order to achieve normal conduct of operations whilst maintaining safety and security at sea. The European Union (EU), in its Maritime Security Strategy (EU 2014) and its related Action Plan, states that managing cyber threats is integral to achieving maritime security. NATO identifies cyberspace as an independent domain of operations along with air, sea, land and space, and to this end organised, amongst other initiatives its first conference on maritime cybersecurity at the NATO Maritime Interdiction Operations Training Centre (NMIOTC) in Crete, in October 2016. The International Maritime Organisation (IMO) was urged by the initiatives undertaken by the Baltic and International Maritime Council (BIMCO) and Lloyd's Register to issue its first 'Interim Guidelines in Maritime Cyber Risk Management' in 2016 (IMO 2016). Furthermore, the number of states that engage with the issue is rapidly increasing, with the United States of America (US) and the United Kingdom (UK) being the pioneering ones, issuing reports and strategies on maritime cybersecurity aware-ness, risk management and mitigation, and contingency planning.

The chapter's main aim is to raise situational awareness within the maritime community as regards existing and potential threats, vulnerabilities and risks on the cyber domain, focusing primarily on those related with the industry's most valuable asset; the ship. Drawing on these findings it will further suggest risk mitigation and contingency planning, in order to minimise the efficiency of such attacks.

In this context the main objectives are the following:

(a) Provide best practice and cybersecurity threat information to transnational shipping;

(b) Activate practitioners and academics to develop means and methods for tack-ling cyber threats, including developing an appropriate framework for information sharing, coordination and training;

(c) Encourage law enforcement and international partners to develop a cooperative construct for defeating cybercrime in the maritime domain; and

(d) Lay the framework for the application of cyber resilience together with situational awareness, business continuity plan and risk management.

To this end, the part will initially define the framework for analysis, by briefly examining existing definitions regarding cybersecurity, a rather crucial stage, since the entire analysis of the chapter will be based on these definitions. It will further identify the components of the maritime

industry. Moving onwards, the securitisation of cyberspace will be analysed, looking at specific threat actors that may target the maritime industry and digging deeper in specific case studies for a more apt analysis. Having set the framework for analysis, examples of cyberattacks at the maritime domain, along with the vulnerabilities and disruptions of the defined mari-time industry will be presented. Drawing on these findings, the chapter will assess the risk stemming from cyber-insecurity in the maritime industry and, to this end, will reach the final part of the analysis by outlining the main principles as regards cyber resilience together with situational awareness, business continuity plan and risk mitigation.

Herein, a three step analysis will be adopted in order to serve the aim and fulfil the aforementioned objectives. These are:

(a) Awareness of cyber issues in the maritime domain among key stakeholders;

(b) Assessment of what needs to be done and who needs to act; and

(c) Development and implementation of risk and threat mitigation to ensure a mari-time cyber secure environment.

In order to define the referent object for analysis in this case a holistic approach will be adopted. This comprehensive approach is assessed as the most appropriate for the goals of this chapter, since it provides a wide inception of the term maritime industry and allows relevant stakeholders to isolate and focus on the relevant, to their interests, specifics. Hence, the maritime industry is what stakeholders make of it.

Defining the Framework for Analysis

What Is Cybersecurity?

In an effort to set the framework of analysis, it is mandatory to present briefly what cybersecurity entails for the maritime sector. Prior to that though, it is important to clarify the concept in its broader context, so that the reader will be able to under-stand this new, insidious threat that is generated from the digital world. As anticipated, there are numerous definitions introduced by different stakeholders, most of which are tailored to a specific sector's needs or are representative of the author's background i.e. academic, government etc. What is common practice though is that for industrial control systems (ICS), including those used broadly in the maritime sector, security encompasses the protection of both their hardware and software components. This combination of physical and information security is often defined as converged security. Even though cybersecurity is not the same as information security, it often replaces the latter within the 'converged security' approach. Concisely, cybersecurity includes the protection of information handled in the cyber realm but is not limited to that, while information security focuses on protecting data, not restricted in the digital environment (NISTIR 2013).

Furthermore, when trying to identify the enablers towards cybersecurity and resilience, academics and practitioners focus on three pillars, namely people, processes and technology. What is problematic in this approach, when we try to apply it in the industrial sector, is that physical infrastructure is omitted. This does not, by any means, suggest that analysts are wrong in their approach. It solely aims to intro-duce a fourth pillar that is relevant in specific sectors and industries, maritime being one of them. Moving on, and in line with the scope of this chapter, it is much more applicable to look at how relevant maritime industry guidelines define cybersecurity. Hence, the UK Department for Transport (DfT) Code of Practice: Cybersecurity for Ships document, prepared by Institute of Engineering and Technology (IET) (2017) states that cybersecurity can be defined as:

> *the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's asset.*

The core conceptualisation, drawn from the aforementioned definition is that cyber-security requires a holistic approach. Achieving effective security in cyberspace requires initially for targeted policies to be adopted, which will later be interpreted into actions, that will utilise existing cutting-edge technologies to protect the organisation's cyber environment.

Drawing for that definition, the same document suggests that a ship's cyberspace is composed of:

> *interconnected networks of both IT, OT and cyber-physical systems utilising electronic, computer-based and wireless systems, including the information, services, social and business functions that exist only in cyberspace*.

What the Maritime Industry Consists Of?

In order to frame the unit of analysis, that is the maritime industry, which will be used as the basis for the chapter's analysis, a comprehensive approach is adopted. That means that the maritime industry, as set in the methodology section above, will be defined as a holistic entity, composed of several subcomponents, each of which faces specific cyber challenges. Following the aforementioned theoretical approach, the broad definition of the maritime industry incorporates all directly and indirectly related, to the industry, personnel, activities, procedures and infrastructure. These subcomponents are:

— Ports, as physical space;

— Port operations and personnel;

— Ships;

— Offshore infrastructure;

— Operational and Information Technology Systems; — Insurance agencies and vendors;

— Booking agents; and

— Related banking-economic transactions.

This categorisation suggests that the maritime industry does not only consists of core material assets but includes the peoples engaged and the activities and procedures related with the industry. Hence, these components of the maritime industry could be categorised as follows:

— Mobile assets (Ships, auxiliary platforms);

— Infrastructure (Port infrastructure, offshore energy infrastructure, safety and security controls, navigation aids, communication systems (onshore, offshore, satellite), underwater cables and pipelines); and

— Financial activities (Insurance agencies and vendors, booking/charter agencies, banking-economic transactions) (Fig. 1).

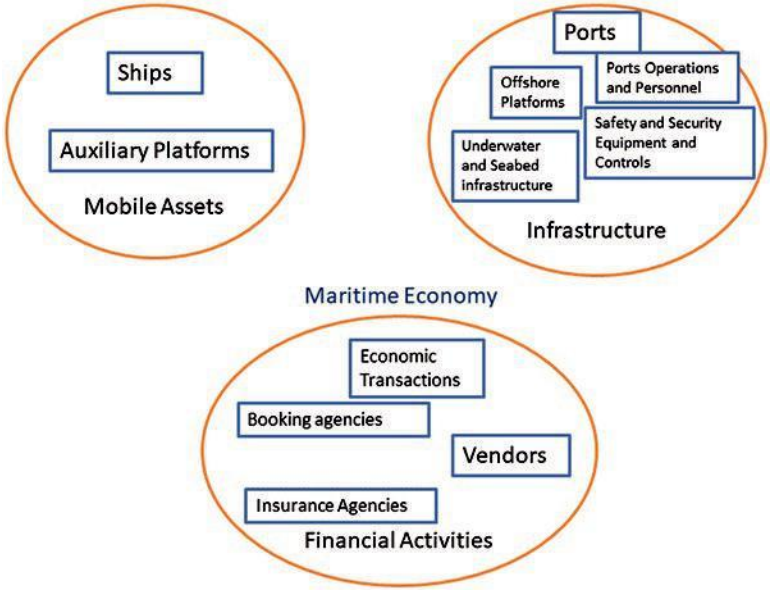


Fig. 1: The Components of the Maritime Industry

On a ship, the computer-based systems will comprise a range of information technology (IT) and OT components. The subcomponents within the ship's environment that need to be protected from the risks of a cyber incident are not only limited to the ship IT and OT systems per se, but include a much wider spectrum, encompassing people (both crew and passengers where relevant), cargo, cargo transport units and ship's stores. For that reason, all ship crew, both senior officers and junior crew members, along with all ashore staff, as stated in Elements 7 and 13 of the Tanker Management Self-Assessment 3, should receive cybersecurity training, at least at an awareness level. Hence, what should be primarily understood is that cybersecurity is everyone's

responsibility. That is of fundamental value, since cyber attacks can impact the whole spectrum of a maritime company's operations, including its entire fleet, worldwide.

Securitising the Cyberspace

The international community started engaging with security issues in the maritime domain after the 9/11 attacks and al-Qaeda's declarations that its next target was the maritime industry. This gave birth to the introduction of the International Ship and Port Facility Security Code (ISPS Code). Later, in response to the emerging piracy threat in the Gulf of Aden, industry-related associations introduced the Best Management Practice 5, that gave specific guidelines for tackling the problem, which will be further analysed in another chapter in this book. This pattern of action from the maritime international community is indicative of the way of thinking regarding security issues. This reactive approach is certainly not the best, but it offers effective measures, as practice has indicated. It can be argued that the issue of IMO's Interim Guidelines in Maritime Cyber Risk Management is the first proactive act by the prominent international maritime organisation. These were adopted in 2017 and consequently the organisation issued the Resolution MSC.428 (98) later the same year. This specific document suggests that as of January 1st, 2021 all stakeholders engaged in the industry should demonstrate cyber capability. Although not mandatory, these advisory guidelines highlight that the international maritime community has identified that cyber threats are real and could target the industry. Thus, securing the maritime cyber environment should become a priority for maritime professionals.

In that context, there is another issue that needs to be clarified at the early stages of this part. There is a lot of debate globally, not limited to the maritime sector discourse, that when it comes to cybersecurity, geography is not relevant. The part argues that cyber threats are regionally related for two main reasons, one being on the potential of an attack to be conducted when transiting over a specific part of the world and the other, in the event of such an attack occurring, is related to response mechanisms available.

Hence, it is vital to build regional situational awareness as regards cyber threats, since we should be able to identify how regional and global actors make use of the cyber domain to their end. Shipping companies operating ships in unstable regions should pre-emptively analyse the local actors' offensive cyber capabilities based on their motivation and thresholds to employ these offenses. ISIS could be a useful case study in this case. Even though they have not launched, as far as we are in a position to know, any cyberattacks, it is broadly accepted that they are rather capable in IT, practising 'hybrid warfare' tactics, through their widespread presence over the world wide web. It may be argued that, even if they do have the capabilities, they do not have the physical access to the Mediterranean or the Gulf in order to coordinate a cyber-physical attack against a high value target at sea. That is certainly not the case. Make no mistake, ISIS' expansion in Libya, apart from any other strategic objectives it might serve, offers unobstructed access to the Mediterranean along with notable proximity to Europe through the Italian coastline.

Although regional threat assessment does not a priori provide mitigation over such an attack, in the event of it occurring, the victim should have already developed a threat mitigation strategy which should incorporate relevant local internal and external partners, that can provide support, may that be either IT or even physical. Following on from the aforementioned example, in the Mediterranean, maritime professionals should know who to address, may that be the Computer Emergency Response Team of the European Union (CERT-EU), similar national CERT's, and contracted service providers. The EU's directive on security of network and infor-mation systems (NIS Directive), put into force in May 2018, dictates that EU states should, among other actions, develop and indicate the National Competent Authority for Cybersecurity, whilst setting up a national CERT. This initiative creates a road-map that shipping companies should adopt as part of their emergency response cybersecurity plan.[28] Maritime operators should also be aware of physical 'safe havens' that they could use in case a cyber attack occurs to a ship which jeopardises its safety of navigation, communication or seaworthiness in general. These 'safe havens' could literarily be commercial ports in the proximity of the ship's position, which the ship could reach in short time and remain secure until the effects of the attack are eliminated.

Is the Maritime Industry a High-Value Cyber Target?

What is becoming apparent is that in the maritime transportation sector, cyber threats are becoming more frequent and sophisticated as individual hackers, well-funded organised criminal networks, nation states, and others target shipping companies, their vessels and their shore-side facilities. The fact that maritime companies are constantly adopting new technologies, systems and platforms, in an effort to offer greater levels of capability and efficiency, is introducing new risks to their activities. The systems at risk are not only emails and office applications used widely in administrative IT-enabled office environments, but almost all modern OT systems as well: those that affect the very seaworthiness of vessels, that support safety of navigation and propulsion, and that protect human life and the environment in general. Before presenting the current and potential threats to the defined components of the maritime industry it is considered necessary to confront the argument that cyber threat actors are not actually targeting the maritime industry per se. There are several voices arguing that academics and practitioners attempt to find answers to a fictional problem, that will not affect the industry in the foresee-able future. That is certainly not the case. The threat is real, it is out there, and it has already affected the industry in numerous occasions, as illustrated in Table 1 and analysed in Annex A. As argued, "it is not a matter of if but when you will be attacked".

[28] Although common sense, research conducted by Chatham House, a UK-based think tank, has indicated that such response plans are not in place in most of the world's shipping companies in 2018.

Date	Victim
2010–2011	Greek Shipping Company
Aug 2011	Iranian Shipping Line (IRISL)
2011–2013	Port of Antwerp
2012	Australian Customs & Border
	Protection Service agency
2012–2014	Danish Port Authority
Apr 2016	South Korea
June 2017	AP Moller Maersk
June 2017	Ships in Novorossiysk
Nov 2017	Clarksons
July 2018	Cosco US
Sept 2018	Ports of Barcelona & San Diego

Table 1 Notable Maritime Related Cyber Incidents (statistics until November 2018)

The other key realisation based on Table 1 is that the frequency of reported cyber incidents has increased considerably from 2017 onwards. Previously, there were about one or two main cases reported annually, but lately we can see that this has changed. Whether this will develop into a trend or not it still remains to be seen but make no mistake, global trends are indicating that cybersecurity is about to become the number one risk for all industries in the years to come.

Case Studies and Lessons Learned

Out of the eleven notable case studies presented in Table 1 it is worth looking at three of them from a critical perspective, to try to extract lessons learned and suggest mitigation measures that could have minimised the outcome of the cyber breach.[29] Another case study is presented that examines a cyber incident in a Maritime Off-shore Drilling Unit (MODU), aiming to illustrate that all aspects of the maritime industry are vulnerable to such breaches.

Clarksons

Clarksons is one of the world's largest shipbrokers. In November 2017 the company became a victim of a cyber breach, when, as stated in an official press release by the company "unauthorised access [was] gained via a single and isolated user account". In response, an

[29] These four case studies where part of an Industrial e-paper that was published by Knect365, where the writer was asked to comment and advise. Further details can be found on Knect365 (2018).

immediate investigation was launched, and the company was able to recover and meet the year's expected financial targets, despite a short-term sharp stock drop.

> *As commented in the Knect365 report: "This incident highlights in the most apt way that the issue of cybersecurity in the maritime industry should not be solely considered for ships and ports. It affects directly the entire maritime economy, consisting of ships, ports, ship-ping companies, insurers, brokers, vendors, classes and others. It illustrates the importance for the development of 'cyber culture' or the most important pillar of cyber resilience, the human factor. If it was an unintended act it brings forward the necessity for effective cyber-security training to all maritime professionals. If it was an intended act the companies should redraft their access and administration rights, adopting a 'need-to-know'-principle, limiting them only to necessary personnel, all of which should be closely monitored" (Knect365 2018, p. 10).*

A.P.Moller Maersk

In June 2017, another major maritime company, A.P. Moller-Maersk, suffered a major business disruption cyber event. The company's terminal in Ukraine was affected by an allegedly state-drive attack, that introduced the notPetya malware. The malware spread very quickly across a large number of the company's port terminals globally, affecting as many as 76, including major ones such as Rotterdam, Los Angeles, Mumbai and Auckland. What is notable in this case is the way the company communicated the crisis in the media. In an interview with KNect365, Commissioner William P. Doyle of the US Federal Maritime Commission com-mended "Maersk for making the decision to waive demurrage and detention fees arguably accrued by customers during the period when a system outage caused by the Petya cyberattack impacted its ability to release cargo". According to the company's CEO, they suffered a $250–300 million loss due to the disrupted business operations in July and August.

> *As commented in the Knect365 report:*
>
> *This specific hack highlights two things. First, it shows the importance of the third pillar of cyber resilience: the procedures. Secondly, it stresses the significance of effective testing of all adopted cybersecurity policies and measures within each specific industry. The specific malware affected a known vulnerability, that could have been identified if efficient pen-testing was conducted by a 3rd party IT firm. Finally, on a positive side, it should be accredited to Maersk that they chose to go public; a fact that stresses the importance of information sharing (Knect365 2018, pp. 10–11).*

Port ofAntwerp

The Port of Antwerp case is different than the other two, since this was a targeted and well-orchestrated attack that was resurfaced in spring 2018. From 2011 to 2013 the digital container tracking system which controlled the movement and location of containers in the port was

breached, in order to facilitate the smuggling of illicit goods, primarily drugs, by North American organised criminal groups. Hackers, paid by these networks, were able, using initially social engineering methods to gain access to the port's system and when later discovered were resourceful enough to find alternative ways to regain access and continue their malicious acts. In 2018, the Port of Antwerp was again in the news for the same issue, highlighting that organised crime networks will continue to exploit the vulnerabilities of port environments for financial gain (WSJ 2018). As commented in the Knect365 report:

> *This case illustrates how cyberspace may be used as a facilitator for traditional organised crime. It was clear that no sufficient cybersecurity measures were in place. It also stresses the necessity for developing resilient mechanisms to such attacks by adopting a backup container control and monitoring system. Finally, it highlights the intertwinement between cyber and physical systems (Knect365 2018, p. 11).*

Maritime Off-Shore Drilling Unit

The final case is an apt example of why people are 'the weak link', when it comes to cybersecurity, not only in the maritime, but in an industry as a whole. A MODU was affected by malware, constituting it inoperable for a few weeks. The malware was introduced to the rig's systems by portable storage devices, namely USB and hard disk drives, that included downloaded adult content and illegal entertainment media. The malware affected the signals to the dynamic positioning thrusters, causing the MODU to drift away from its initial drilling position. Due to safety implications the managing company was forced to halt operations until the issue was finally resolved. As commented in the Knect365 report, this is:

> *Another example of a non-existent 'cyber culture'. The incident highlights the disastrous effects that such an attack on an offshore critical infrastructure, or a ship, could have on the environment. A case that affected both the human factor and the infrastructure and illus-trated the necessity for effective cyber training for maritime professionals, once again (Knect365 2018, p. 11).*

Fostering the Maritime Industry

Vulnerabilities and Disruptions

What these notable case studies indicate, along with those briefly presented in Annex A, is that the shipping industry has been targeted, so far, primarily for financial gain. Specifically, from a threat actor perspective, current practice has indicated that organised criminal groups is the predominant actor targeting the shipping industry. There are several reasons for that. Primarily, the industry's financial transactions are conducted mainly online, between people that often do not know each other. The scale of these transactions is so big and spread out that makes it easy for organised criminals to conduct fraud and direct payments to their preferable accounts.

Also, shipping companies face cybersecurity risks from crew (including officers), staff, current and former employees, contractors, and vendors. Having said that and although a trend regarding financial gain is apparent, this does not mean we should exclude the likelihood of other types of actors targeting the industry, aiming to achieve different outcomes such as corporate espionage, terrorism, piracy and hacktivism. What the aforementioned case studies indicate as well, is that, in several cases, companies and assets suffering consequences from malicious digital content were not targeted per se. Take the Maersk incident for example; the Danish company was, what can be described as collateral damage to a presumably, state-sponsored attack against a sovereign state. Hence, the maritime sector should develop a security and response strategy that should be in a position to address both targeted attacks and untargeted breaches. Another key question that needs answering at the very early stages on analysis is Why is the maritime industry any different from any other industry when it comes to cybersecurity? The differentiator for the maritime domain is the wide range of technical systems, infrastructure and human resources in use. With increased reliance on third party systems and personnel, as analysed above, all the different subcomponents of the maritime industry are intertwined, aiming to support the industry's most valuable asset. The very fact that ships are increasingly using systems that rely on digitalisation, integration, and automation, introduces new threats and vulnerabilities to the ship's environment.

Case Study

A Ponemon Institute survey of US oil and gas professionals responsible for securing or overseeing cyber risk in the OT environment found 59% believe there is greater cyber risk there than in enterprise IT.

"Critical network segments in production sites used to be isolated but are now connected to networks, making operational technology more vulnera-ble," said Petter Myrvang, Head of Information Risk Management, DNV GL – Oil & Gas. "It is one reason why we conduct ethical hacking for custom-ers in the sector. For further details see.

https://www.cybersecurity-review.com/study-reveals-cybersecurity-readiness-gaps-in-us-oil-and-gas-industry/

On the more technical side, without deviating from the scope of the chapter, systems, either IT or OT, that are vulnerable to cyber incidents can be broadly categorised as follows:

— Systems that are connected to the internet or other external networks. On board ships, these may be the Electronic Chart Display and Information System (ECDIS), Global Positioning System (GPS) receivers, fleet management systems and in newly built ships integrated bridge control and/or engine control consoles along with crew entertainment equipment. Connectivity is

required for either software and patch management updates or system monitoring and performance optimisation.

— Systems that are not connected to the internet but have a software element that affects/controls/monitors their operation such as loading and stability, alarm and monitoring or power management systems.

As technology continues to develop, trying to achieve operations optimisation, IT and OT onboard ships[30] are being networked together, while becoming more frequently connected to the internet or have a software component related to them, that was not in place in the past. Thus, reliance on third party systems and personnel require a holistic approach beyond purely the maritime, especially with respect to contingency and business continuity plans.

Identifying the Risk

In an effort to identify the risk, it is mandatory to counter existing fears of over-reacting and over-investing in cyber risk mitigation due to the novelty of the challenge. Ongoing discussions on how to access cyber risk are dazzled at the initial stage, where most stakeholders struggle to come up with measurable outcomes in case of a cyber breach. A first step towards untying the node is to sort what are the possible consequences of a cyber breach. What are the specific areas of any maritime transportation organisation that could be affected? Taking into consideration everything that has been presented in this chapter it could be argued that the following systems, services and fields are at jeopardy in the event of a cyber incident:

• Loss of corporate data,

• Financial loss,

• IT and OT (where applicable) systems' confidentiality, integrity and availability, and

• Safety of Life and Navigation at Sea, resulting even in environmental disruption.

What should be understood is that if the management of cyber risk is not regarded as a priority, then reactive measures needed to be applied when a cyber breach occurs will not be able to, sufficiently, minimise the consequences. A proactive approach needs to be adopted, where resilience and risk mitigation should be the predominant concepts.

[30] 8 In general, ship systems are distinguished in two categories, the IT and OT. The first category includes IT System Management, Surveillance within the ship, Maintenance monitoring, crew and passenger entertainment and any other system that offers support to a ships' operation cycle. OT systems are the core systems that control the ship's daily operations and include power generation and distribution, propulsion, navigation and steering, ship-to-ship and ship-to-shore, along with emergency and distress communications and so forth. These are the systems that are first on the priority list regarding cybersecurity for ships. For further details see http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

Risk Assessment and Management, Risk Mitigation and Business Continuity Plan

Finally, before concluding this brief introduction to the threats posed to the shipping industry by the increasing use of digital systems and services, and building on what has been analysed in the previous sections, it is crucial to understand the process that needs to be adopted in order to protect a company's and a ship's vital systems. A process which is focused on analysing the threats to an organisation's ecosystem with a risk-based approach. Risk assessment and management are the predominant principles for a manager to focus on, since these will provide him or her with a constructed framework in order to achieve and maintain effective cybersecurity within the organisation. Besides, as previously noted, the IMO, through its cyber risk management guidelines, has suggested that cyber policies and measures should be adopted as of January 2021.

These guidelines suggest that one approach is to comprehensively assess and compare an organisation's current, and desired, cyber risk management postures (IMO 2016). This comparison will probably reveal gaps that should be addressed to achieve risk management objectives through a prioritised cyber risk management plan. This is a risk-based approach designed to encourage organisations to target investments in resources in the most effective manner. It maps directly to the US National Institute of Standards and Technology (NIST) Cybersecurity framework, focusing on five main steps: Identify, Protect, Detect, Response and Recover. This framework is used by several industries as the basis or reference for their respective models. The NIST CSF was used as the basis for the model introduced by BIMCO and other maritime stakeholders, currently in its third version (BIMCO 2018), which is focused purely on the maritime industry, namely ships. What is important to understand is that this model follows a risk-based approach, where three of its six steps deal with risk mitigation, impact minimisation, contingency planning and recovery. This very fact confirms the main realisation of this chapter that it is not a matter of if we will be affected but when and, with that in mind, we should be prepared to deal with the aftermath of such an incident. Hence, cybersecurity awareness, or better put, cybersecurity approach should be comprehensive and holistic.

According to BIMCO, a cyber risk management approach should initially identify the specific threats more relevant to the organisation, both external and internal, posed by misuse of installed networks and lack of awareness. Secondly, it has to identify the vulnerabilities of all assets within an organisation. Those conducting the assessment should record all connected onboard systems, understand the consequences of breaching the security of these systems and identify the limitations of existing protective measures. Thirdly, following a risk management analysis, they should determine the possibility of these systems being targeted by external and internal actors. The next step would be to develop risk mitigation policies and specific measures that will reduce the likelihood of these vulnerabilities and also reduce the potential impact that an attack may have on a specific vulnerability of these systems. This leads to the next step which is the development of contingency plans to tackle all effects of potential attacks to the safety and security of the ship. Finally, in the event of such an attack occurring, having applied the already

developed contingency plan, the relevant staff should aim to recover normal operations as soon as possible and assess the effectiveness of the aforementioned plans in order to further amend and update them (BIMCO 2018).

Conclusion

The increasing dependency of the maritime sector to software-based technologies, combined with the key role of the maritime transportation system in global trade and critical national infrastructure mean there is a key imperative to take action to protect global shipping and maritime trade routes. It should also be widely understood that it is impossible to achieve a 100% cyber-secure environment. Practice so far has indicated that there is no absolute solution against all cyber threats; no system can be rendered 100% secure. Taking into consideration the existing cyber landscape with a variety of threat actors and the indispensable weaponry available for their goals, no maritime stakeholder can claim that his organisation is not a potential target. The case studies presented in this chapter aptly support this claim.

Even though the industry is gradually starting to come to grips with this new insidious threat, there is still a lot of ground to be made. The first step towards that goal, though, is to help senior management understand what the cyber realm entails for their organisation. Confronting with cyber risks requires a top-down approach. Once this is achieved there are specific steps to be taken, following in all cases a risk-based, people- infrastructure-and-processes approach.

In a nutshell, this new 'cyberised' risk environment represents a chronic state of affairs that is best addressed over time, resourced thoughtfully and managed collaboratively. Fortunately, managing risk is not unusual for today's modern mariners. In fact, managing risk is an activity for which they are well suited for.

Date	Victim	
2010–2011	Greek Shipping Company	For two years a Greek shipping company suffered several successful piracy attacks in the Golf of Aden, since local pirates hired hackers to gain access to the company's HQ and identify the most vulnerable ships along with route timetables. Hackers were able to gain access to the company's IT systems via wi-fi equipment that was installed at the company's offices.
Aug 2011	Iranian Shipping Line (IRISL)	The servers were hacked resulting in damage to data relating to rates, loading, delivery and location. Consequently, the location of many cargo containers remained unidentified and an undisclosed amount of financial losses were incurred as a result.
2011-2013	Port of Antwerp	The port had been a victim of an APT attack since 2011 commissioned by a drug cartel. The attack targeted terminal systems which were subsequently compromised by hackers and used to release containers without port authorities

		becoming aware. Illicit drugs and contraband worth approximately US$ 365 million, firearms and approximately US$ 1.5 million were seized when authorities finally became aware.
2012	Australian Customs & Border Protection Service agency	Cargo systems controlled by customs and border protection were hacked in order to determine which shipping containers were suspected by authorities.
2012-2014	Danish Port Authority	An email virus spread through the port network that was likely initiated through an infected pdf document. The virus spread and successfully reached other Danish government institutions.
Apr 2016	South Korea	280 ships were forced to return to port due to problems on their navigation systems. The issue was largely blamed on North Korea however this remains unconfirmed.
June 2017	AP Moller Maersk	NotPetya also known as ExPetr ransomware led to outages on A.P. Moller Maersk computer systems impacting both oil and gas production and port operations. Following the incident, Maersk claimed to have changed its IT systems to prevent similar incidents from occurring in the future. The incident resulted in an estimated US$ 300 million of losses.
June 2017	Ships in Novorossiysk	At least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32 km inland of their actual position. It is now believed to have been as a result of a GNSS spoofing attack.
Nov 2017	Clarksons	Perpetrators gained unauthorised access to computer systems, accessing confidential information and threatening to release information unless ransom payment is made. Company share prices decreased by 2.71%.
July 2018	Cosco US	Cosco's Shipping Lines suffered from a cyber breach that affected email and network telephone initially in the US, but not ships. This expanded to their Americas facilities hence the company decided to shut down the connections with other regions for further investigation. The company was able to recover within a week. It is believed to have been a malware (ransomware) incident.
Sept 2018	Ports of Barcelona and San Diego	Within a week both ports suffered from a cyber-related business disruption event. Even though both organisations did not disclose a lot of information, they both claimed that this was not a major disruption and it affected mainly IT systems at shore. It is assumed that it was the same malicious content that affected both ports.

Table 2 Case study analysis (commentary is informed by the Risk Focus Cybersecurity prepared by Thomas Miller and the UK P&I Club)

General Vulnerabilities in the Maritime Domain

Ships and ports are inherently vulnerable for a number of reasons. The reasons can be binned into the familiar categories: people, processes, and technologies. From a personnel perspective, ships and ports have crews and staff that are changed frequently and a periodically. Crew training and familiarization is often lacking with regard to cybersecurity. From a process perspective, maintenance for IS and IT systems (afloat and ashore) is often contracted out to third parties, thus expanding the attack surface.

Trend Toward Cyber Insecurity

The maritime industry (e.g., ships and ports) has trended toward more vulnerabilities as IT and OT proliferate. Ships and ports have moved to digital controls. There is efficiency in integrating IT and OT but that alone increases the attack surface for ship and port operation. Furthermore, humans play a large role in operating and using ships and ports as both passengers and employees. The result is a greater opportunity for malicious actors to compromise systems and networks (and humans) used in the maritime industry. An elaboration on these points is provided next.

Age and Obsolescence

A complicating factor for maritime cybersecurity is the age of the maritime fleet. Ships by their nature are designed to last for decades and the network and computing technology initially installed is likely to become obsolete quickly. Remediation of this situation is complicated due to the fact that such IT systems are supplied from numerous suppliers and vendors of varying ability to sustain their products over the lifetime of the ship/port. A fleet of ships in a company or country is likely to have a variety of ship types and models that are designed to operate in different environments. Any particular ship may have a unique underlying network and computer system that can easily become outdated and vulnerable. These vulnerabilities stem from

- Poor initial design;
- The need to create connections to other systems as part of a need for maintenance, awareness, and logistical support;
- Poor cybersecurity practices of operators (e.g., default passwords, in-appropriate use of removable media, poor configuration).

Systems of interest in the maritime domain can be grouped as follows:

- Afloat.
- Ashore.

• The interfaces connecting afloat and ashore (e.g., those that enable the moni-toring of ship performance and logistic data [fuel level, voyage progress]). These are illustrated in Figure 2.

The types and nature of offensive cyber operations on these systems in the maritime domain fall into the traditional categories of compromise of cybersecurity (e.g., CIA). The malicious intents include piracy, theft, fraud, and sabotage. Select examples are grouped as follows:

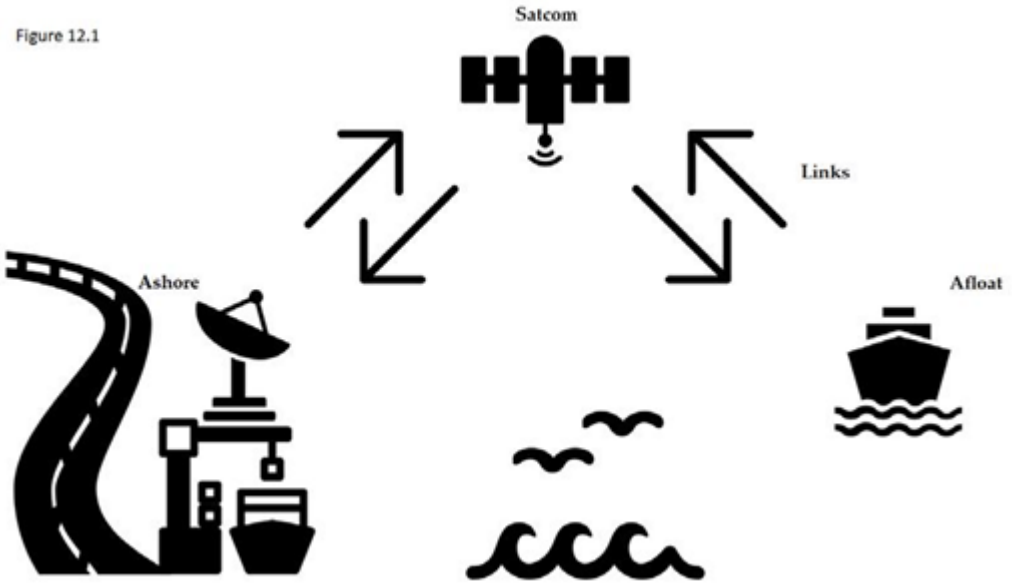


Figure 2:The maritime domain attack surface includes facilities and systems afloat and ashore

• Confidentiality: Stealing data on the cargo, crew, visitors, and passengers of a ship.

• Integrity: The manipulation of crew or passenger/visitors lists, cargo manifests or loading lists, and/or devices to capture accident details. Data manipulation may be to hide other crimes at ports like the fraudulent transport of illegal cargo.

• Availability: Blocking the operation of ship and/or ship owning company's ability to function; that is, denying a maritime organization or company access to its business systems, such as the NotPetya attack, which impacted Maersk's ability to operate. In fact, any deletion of data related to cargo and passengers could delay normal operation. There are many mays to overloading company's information systems and deny its use (e.g., DDOS).

The source of vulnerabilities in the maritime domain and on ships matches the vulnerabilities in industrial control systems and power plants. This is due in part to the fact that they share similar equipment, controllers, and software. This is explained in a DHS report and highlights from that report are as follows:

• Reliance on commercial-off-the-shelf products translates into the heavy use of widely available operating systems like Windows, Unix, and Linux. Each has known exploits.

• Personal wireless devices and other bring-your-own computing devices (BYOD) literally bring vulnerabilities afloat.

• Afloat (and port) control systems connect to vulnerable company enterprise systems that are internet-facing.

• Interdependencies exist. From *"Consequences to Seaport Operations from Malicious Cyber Activity, DHS, 2016"* : "an attack on a container terminal management system could disrupt intermodal container services involving maritime, rail and truck transportation."

• The complexity and need for coordination leads to insecurity. From *"Consequences to Seaport Operations from Malicious Cyber Activity, DHS, 2016"* : "Disconnects between the professionals who administer IT network security and the operators and technicians responsible for control system devices have led to challenges in effectively coordinating network security between these two key groups."

• Continued use of legacy systems. Older legacy systems "tend to have inadequate password policies and security administration, no data protection mechanisms and protocols that are prone to snooping, interruption and interception. [Such] insecure legacy systems have long service lives and will remain vulnerable until security issues are mitigated".

• Offshore reliance and supply chain vulnerabilities for the United States: "Many software, hardware and control system manufacturers are under foreign ownership or develop systems in countries whose interests do not always align with those of the U.S.". Technical support and maintenance is often outsourced to a third party.

• Online attack manuals: "Many ICS manuals and training videos are publicly available and many hacker tools can now be downloaded from the internet and applied with limited system knowledge". Therefore, expertise on hacking ships and ports is easily acquired and developed.

• Remote access allows another point of entry for compromise. From *"Consequences to Seaport Operations from Malicious Cyber Activity, DHS, 2016"*: "systems can be accessed by external users via networks, devices and software components either directly (i.e., wired access) or remotely (i.e., wireless) for scheduled or corrective maintenance purposes." The risk of unauthorized users gaining access is demonstratable and significant.

Figure 3 lists many of the systems that are vital to shop operations and may be computerized and thus may be vulnerable to cyberattack.

Specific Maritime Components and Their Vulnerabilities

Software underlies many of the systems (shown in Figure 3) associated with maritime systems and is critical to a number of fundamental systems and functions, including but not limited to vessel navigation, propulsion systems, cargo handling, container tracking systems at ports and onboard ships, shipyard inventories, and other shipyard automated processes. Table 2 lists the vulnerable systems as identified by the International Maritime Organization and its published guidelines. The key systems enumerated are ones infused with IT; they are essentially digital systems and thus add to the cyberattack surface. Categories of these components are enumerated in Table 2.

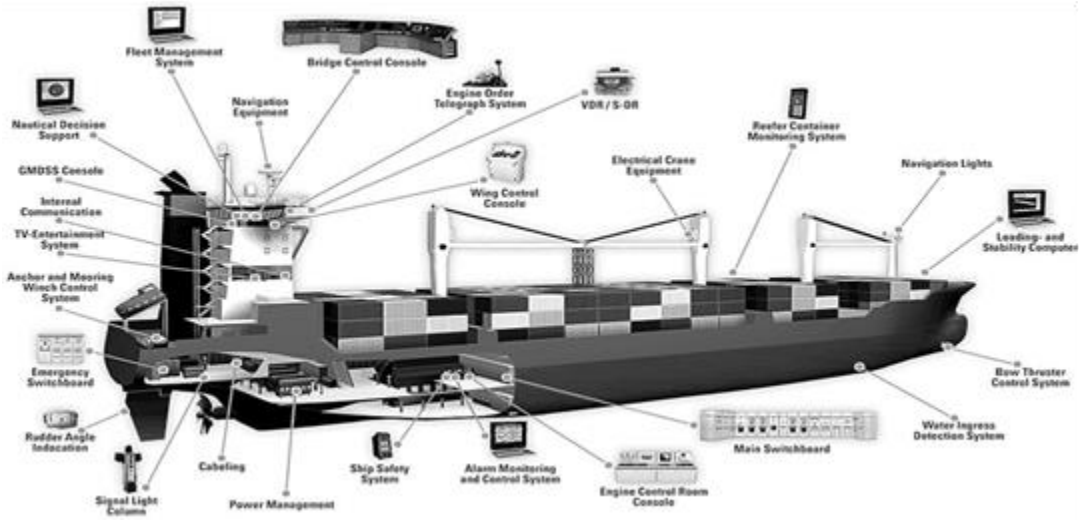


Figure 3: ICS on ships. (Source: https://rosap.ntl.bts.gov/view/dot/10057.)

Voyage Data Recorders Are Vital and Vulnerable

VDRs are the black box of ships and record status information from a ship's voyage, including but not limited to bridge audio, speed, position, and radar images. One is shown in Figure 4. The data on a VDR can be used to investigate a mishap or accident. VDRs have been described as personal computers with varying degrees of cybersecurity. Some are Linux-based and some run Windows-XP, a highly vulnerable operating system. Some have USB ports. Some of speculated that VDRs may be targeted for compromise by ship operators to alter an incident investigation; if ship operators are concerned that it might yields incriminating evidence it could be targeted.

The cybersecurity firm IOActive examined one such device and found that the integrity of the data on these devices (e.g., voice and radar data) could be completely compromised via a number attack approaches, including but not limited to exploit of (1) weak encryption, (2) buffer overflows, (3) overprivileged remote users (with root privileges), and (4) authentication flaws.

Bridge and Navigation System Vulnerabilities

Maritime navigation and communication systems have vulnerabilities, especially those essential aids used to track afloat vessels, which include

SATCOM;

GPS;

AIS;

ECDIS.

System	Description	Subsystems	Vulnerability
Cargo management systems	Systems used for the management and control of cargo, including hazardous cargo, that may interface with systems ashore. Examples include internet connected shipment- tracking tools.	Cargo control room (CCR) and its equipment, loading Computers Remote cargo and container sensing systems level indication system, valve remote control system Ballast water systems, water ingress alarm system.	Internet connections and connections to shore are vulnerable attack vectors.
Bridge Systems	Bridge systems include network navigation systems that interface to shoreside networks for update and provision of services. Such systems often have removable media, such as thumb drives, for patching and updates. Key bridge systems include ECDIS, GNSS, AIS, VDR, and radar/ ARPA.	Integrated navigation system, positioning systems (GPS, etc.) Electronic Chart Display Information System (EC-DIS), dynamic positioning (DP) systems, systems that interface with electronic navigation systems and propulsion/maneuvering systems Automatic Identification System (AIS), Global Mari- time Distress and Safety System (GMDSS) Radar equipment, voyage data recorders (VDRs) Other monitoring and data collection systems	Removable media represents an entry point and attack vector
Propulsion and machinery management and power control systems	The monitor-and-control of the onboard machinery propulsion and steering of these	Engine governor, power management, integrated control system, alarm system, emergency response system	Remote monitoring systems are a potential attack vector as well as

	systems make them vulnerable to cyberattacks.		connections to other systems, such as navigation and communications
Physical access control	Systems that ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarms, and electronic personnel-on-board systems	Surveillance systems such as CCTV network, bridge navigational watch alarm system (BNWAS), shipboard security alarm systems (SSAS), and electronic personnel-on-board systems	
Passenger servicing and management systems	Systems used for property management, boarding, and access control.	Electronic health records, financial related systems Ship passenger/visitor/seafarer boarding access systems Infrastructure support systems (e.g., DNS), user authentication/authorization systems	Collected data is an attractive target; mobile devices that interface/compose such systems are potential entry points for attackers
Passenger-facing public networks	These are fixed or wireless networks connected to the internet, installed on board for the benefit of passengers, for example guest entertainment systems.	Passenger Wi-Fi or LAN internet access, guest entertainment systems, passenger Wi-Fi or LAN internet access; for example, where onboard personnel can connect their own devices	Massive vulnerability if not isolated from any other ship system.
Administrative and crew welfare systems:	Onboard computer networks used for administration of the ship or the welfare of the crew.	Crew Wi-Fi or LAN internet access; for example, where onboard personnel can connect their own devices	Internet access and email provided by these systems is an attack vector.
Communication systems	Includes satellite and/or other wireless communication	Integrated communication systems, satellite communication equipment VoIP equipment Wireless networks (WLANs) Public address and general alarm systems Systems used for reporting mandatory information to public authorities	SATCOM represents an attack vector

Infrastructure needed for cybersecurity		Security gateways Routers Switches Firewalls Virtual private networks) (VPNs) Intrusion prevention systems Security event logging systems	

All of the above provide vital situational awareness to a bridge (see Figure 5), but the complexity and connectivity creates vulnerabilities.

GPS Vulnerabilities

The GPS and the precision, navigation, and timing function it provides is essential to both the commercial and military maritime sector. It has been the impetus to replace paper charts with electronic charts (i.e., e-charts). However, GPS signals are weak and quite susceptible to jamming, spoofing, and meaconing, as well as space weather (e.g., solar flares) and even laser attacks. Table 3 is taken from Grant, who lists the various uses of this capability afloat and ashore.

Figure 4: VDR on a ship in a protective capsule. (http://www.marine-marchande.net, https://commons.wikimedia.org/w/index.php?curid=925946.)

Figure 5: Integrated bridge system. (Image credit: https://commons.wikimedia.org/w/index.php?curid=56504885.)

Figure 6 is from the U.S. Geological Service and is exemplary of the integration of the GPS function both afloat and ashore as well as other positional sensors that aid navigation.

Afloat	Positioning, ECDIS, AIS, Gyro, RADAR, digital selective calling, VDR, dynamic positioning, surveying
Ashore	Aid to navigation (AtoN), DGPS corrections, AIS, AtoN posi-tion monitoring, synchronized lights

Table 3: GPS Dependence in the Maritime Domain

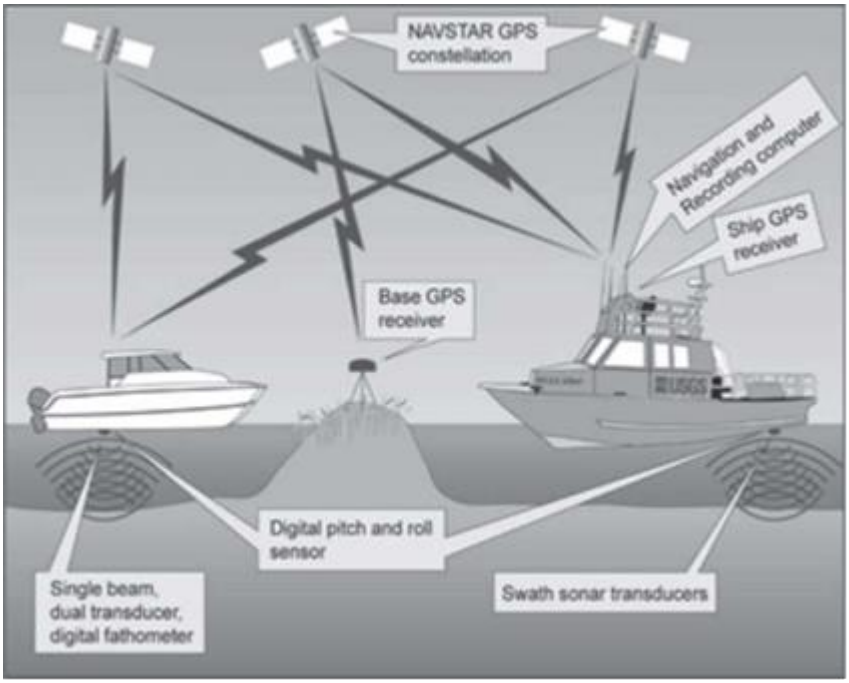


Figure 6: GPS afloat and ashore. (Image credit: https://pubs.usgs.gov/ds/675/html/images/sands_aquisitionLG.jpg.)

GPS Jamming

GPS jamming is when the GPS signal is blocked. GPS jamming attacks are not un-common and not difficult or expensive to carry out. At the nation-state level, there have been a number of incidents on the Korean peninsula. In 2015, small portable jammers were used to jam ports/waterways that impacted 250 ships. Jammers are cheap and can be purchased for hundreds of dollars if not much less. As a result, jamming of a port or waterway can be accomplished by an actor using small portable jammers.

GPS Spoofing

GPS spoofing occurs when a true GPS signal is replaced by a fake one, which can result in the malicious redirection of a ship to a location not intended by the ship drivers. A spoofed GPS signal may not be noticed until its impact (e.g., redirected off course) is felt. A well-reported demonstration of the ability to spoof a vessel was carried out by researchers at the University of Texas in 2013. The university research team developed their own custom-made GPS device used it to spoof a GPS signal intended for a 213-foot yacht. The team was successful and demonstrated the difficulty in differentiating a spoofed signal from a true one.

Impacts of Attacks on GPS

A GPS attack can result in alarms going off on the bridge, false GPS positions, and incorrect data presented on ECDIS and AIS. Ultimately, the ship operators will have compromised situational awareness due to the attack.

Why Are Attacks on GPS Possible?

The GPS used by civilians is vulnerable because it does not use encryption or authentication, two important cybersecurity controls. The exploitability of these vulnerabilities was demonstrated by the researchers at the University of Texas who took advantage of those missing controls.

AIS

AIS is required for commercial vessels of a certain size and other ships operating in certain ports. Hundreds of thousands of vessels worldwide are required to use AIS. Lighthouses and buoys also use these radio transmitters. Essentially, AIS assists operators afloat and ashore to have situational awareness of the environment and thus adds to the safe navigation of congested waterways and ports. An AIS device broadcasts the following information: identity, ship type, position, course, speed, navigational status, and other safety-related data. To an extent, it is an alternative to radar. Ships that intentionally turn off or avoid AIS are known as dark vessels and include the spectrum of operators that seek stealth, including drug smugglers and nation-state military crafts. Figure 7 shows an AIS device.

Figure 7 Device displaying AIS data. (Source: https://commons.wikimedia.org/w/index.php?curid=1725839.)

How Does AIS Work?

AIS is complex and relies on GPS signals, as shown in the illustration in Figure 8. A concise description of how it operates is as follows: “AIS transceivers automatically broadcast information, such as their position, speed, and navigational status, at regular intervals via a [very

high frequency] VHF transmitter built into the transceiver. The information originates from the ship's navigational sensors, typically its global navigation satellite system (GNSS) receiver and gyrocompass. Other information, such as the vessel name and VHF call sign, is programmed when installing the equipment and is also transmitted regularly."

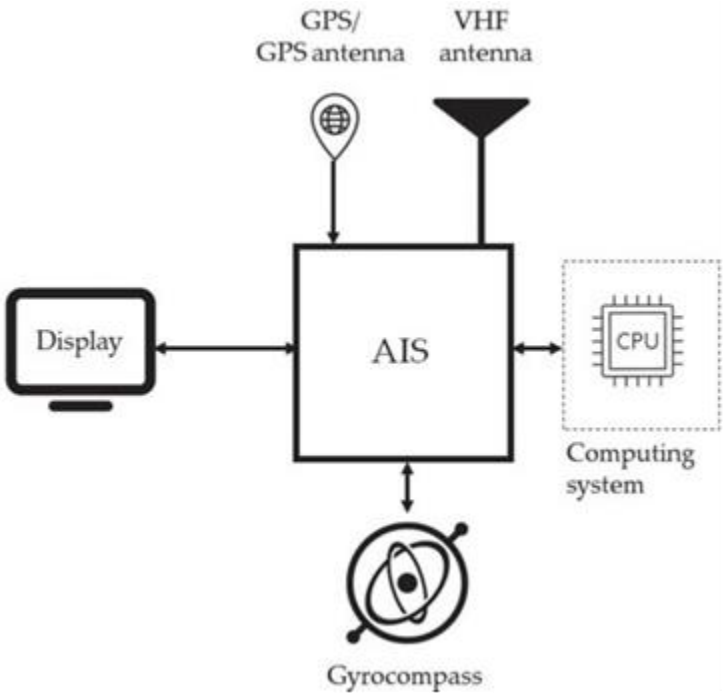


Figure 8 Sketch of AIS interfaces

How is AIS Hacked?

AIS does not employ encryption or authentication and is thus vulnerable. Cybersecurity firm Trend Micro demonstrated this in 2013 and documented it in a report that listed the following steps in their demonstration:

- They purchased an AIS device and deployed it near a maritime port;
- They intercept and modified captured signals and retransmitted them to create a false picture of the environment.

Such an attack could create phantom vessels or phantom barriers causing navigation errors and/or chaos in a busy port. Famously, Trend Micro's false tracks caused one web-based situational awareness tool to spell out the term "PWND".

It is important to note the following. AIS data is rich and available. Research efforts exist (at the Naval Postgraduate School and elsewhere) demonstrating how to use this data to predict ship trajectories. AIS provides historical data that can be analyzed to develop models to estimate time spent in certain ports; for ex-ample, Russian ports.

What Is ECDIS and How Is It Vulnerable?

ECDIS provides the electronic displays used on bridges of most commercial ships (see Figure 9). It can be called a navigation information system that connects with GPS, the gyro, radar, and other situational awareness systems. According to the cybersecurity firm Pen Test Partners, "it is possible to reconfigure a ship's EC-DIS software in order to misidentify the location of its GPS receiver". ECIDS systems are known to have outdated operating systems. From a research arcile: "Consider that some ECDIS devices still run Windows XP, and to a lesser degree Windows NT, released in 1993." Some speculate that operators fixated on ECDIS displays could be driven into obstacles in plain sight.

Figure 9: ECDIS (Image credit: https://upload.wikimedia.org/wikipedia/commons/c/cf/Navigation_system_on_a_merchant_ship_2.jpg.)

Satcom Is a Vital Capability for the Maritime Industry

A number of satcom systems are utilized on ships and some are listed as follows:

• Inmarsat-C is used for ship to shore communication and compliance with GMDSS. It can provide basic services like email and enables GMDSS, which facilitates ship-to-shore distress alerts can be sent.

• Very small aperture terminal systems (VSAsT) can exchange voice, video, and data on C-band and Ku-band channels.

• Broadband global area network (BGAN) provides Internet access and voice services;

• Fleet Broadband (FB) exchanges data and voice and can support ECDIS and other nav systems.

• SwiftBroadband is an IP-based system that exchanges voice and data.

• Classic aero service exchanges voice, data, and fax.

Satcom Terminals Have Exploitable Vulnerabilities

Table 4, taken from the report by cybersecurity firm IOActive, identified classes of vulnerabilities that may exist based on the firmware in key satcom terminals. They are

- Hardcoded credentials;
- Undocumented protocols;
- Insecure protocols;
- Weak/poor password reset procedures;
- Backdoors.

These vulnerabilities allow remote, unauthenticated attackers to compromise the affected products. In certain cases no user interaction is required to exploit the vulnerability; just sending a simple SMS or specially crafted message from one ship to another ship would be successful for some of the SATCOM systems.

Vendor	*Product*	*Vulnerabilities* H/C Credentials	Undocumented Protocols	Insecure Protocols	Backdoors	Weak Password Reset
Harris	RF-7800-VU024, RF-7800-DU024	Yes	Yes	Yes	Yes	
Hughes	9201/9202/9450/9502	Yes	Yes	Yes	Yes	
Hughes	Thuraya IP	Yes	Yes	Yes	Yes	
Cobham	Explorer			Yes		Yes
Cobham	SAILOR 900 VSAT	Yes		Yes		Yes
Cobham	AVIATOR 700 (E/D)	Yes		Yes	Yes	Yes
Cobham	SAILOR 6000 Series (Inmarsat C)	Yes		Yes		
Cobham	SAILOR FB 150/250/550			Yes		Yes
JRC	JUE-250/500 FB	Yes	Yes	Yes	Yes	
Iridium	Iridium Pilot/OpenPort	Yes	Yes			

Table 4 IOActive's Vulnerability Study of Afloat Satcom

Effective maritime cybersecurity regulation – the case for a cyber code[31]

Background

Over the last decade, the world maritime industry has amplified its reliance on cyber-enabled technology (IMO, 2017a). This technology has been used to increase both the safety and productivity of maritime activities, including the remote monitoring of vessels. However, this technology has simultaneously opened up the maritime industry to new risks from cyberspace in its efforts to safeguard vessels and cargoes. These risks range from unintentional human errors to ensuring software and data integrity to planned state-level attacks. This situation is exacerbated by integrated information technology and the intensification in communication between ships and land-based entities, which opens up many more methods in which a ship at sea could be exposed to a threat from the cyber-realm.

Within the maritime sector, the adoption of cyber-enabled technology has occurred incrementally over time, so the industry has been relatively slow to implement effective risk mitigation and appreciate the extent to which ships and ports need to be kept up-to-date in dealing with cyberspace. The International Maritime Organization (IMO), the specialized United Nations (UN) body charged with facilitating cooperation to achieve the practicable standards of maritime security and regulate shipping, has also been late and somewhat inactive in considering regulation when it comes to a number of cybersecurity standards.

While full digitalization of ships and related systems is a global risk-management issue, it is of high significance to the Indo-Pacific region, which incorporates the third largest of the world's oceans and acts as the gateway to many of the major shipping lanes, straits and canals, including the Suez Canal. At the same time, the Indo-Pacific region experienced the rise of a number of non-traditional security threats including piracy between 2008 and 2013 (IMO, 2017b). This spike was attributed to an increase in the financial value of cargoes transiting the area, being led by strong demands for imports of crude oil to both India and China, and the export of petroleum products (UNCTAD, 2017). So while maritime security does remain a high priority in a variety of ways, the expanded nature of security threats no longer entails only physical attacks by pirates and other criminal groups on the water itself. Security decisions must also deal with the digitization in the maritime industry that involves attacks on cyber-enabled ships by cybercriminals and a growing myriad of hostile state and non-state actors.

A cumulative body of literature has documented how maritime systems are vulnerable to an ever-growing range of cyber threats that can cause considerable damage (BIMCO, 2017; IET, 2016; TRANSAS, 2016). Malicious attacks on maritime systems have come about through many points of vulnerability due to not taking necessary steps for cyber security mitigation and preparedness, including poor access control to communications systems and manipulation of

[31] Rory Hopcraft & Keith M. Martin (2018) Effective maritime cybersecurity regulation – the case for a cyber code, Journal of the Indian Ocean Region, 14:3, 354-366, DOI: 10.1080/19480881.2018.1519056

employees (social engineering). The consequences of these types of issues have been varied, including extortion, the loss or compromise of business sensitive information and the opportunistic criminal disruption of chart navigation systems. Yet with both ports and vessels moving towards systems of automation and connectivity, the security of a modern-day vessels will need to ensure significant security improvements to address ongoing issues like ransomware attacks and cyber-sabotage. Such security concerns need to be assessed within the reality of globally accessible navigation systems and the fact that the operation of modern technology-dependent vessels are configured in ways that can invite these types of cyber-incidents.

In short, multiple systems may be connected together. It is therefore imperative that the maritime industry, through the IMO, creates actionable, robust and resilient cyberse-curity regulations that reflect this technological revolution. New regulations and guide-lines are vital to progress towards a less vulnerable infrastructure as well as allowing the maritime industry space to improve efficiency and decrease costs, without heedlessly comprising the safety and security of the seafarer. At the very least, navigation and associated digital communication will continue to indispensably buttress the maritime sector, improving the technology that supports activities such as international shipping, cruising, leisure boating and marine scientific exploration

This part will outline some of the central challenges in the development of robust maritime cybersecurity regulations. It will argue that there is a need to embed an appropriate risk management regime via capacity-building and the advance and championing of global cyber-security standards. We will also address how a collaborative approach by the maritime industry can help to bring about a sense of renewed urgency to ensure more formal process in establishing a self-reinforcing Cyber Code with respect to maritime cyber-security.

The maritime cybersecurity challenge

Discussing and implementing a broad-based cybersecurity strategy is a demanding task in any fast-moving, multi-cultural and multi-lingual environment. There are several core issues that make cybersecurity issues for the maritime industry especially complicated.

First is the linkage between on-board and terrestrial systems. The IMO is a ‘competent international organization’ according to the United Nations Convention on the Law of the Sea (UNCLOS) (UN, 1982), meaning they are charged with the adoption of international shipping rules and standards in matters concerning maritime safety and efficiency (IMO, 2014a). UNCLOS is explicitly targeted at the world’s oceans and seas, which places obligations on and gives responsibilities to coastal and non-coastal states. However, much of the infrastructure that enable communication is land-based, outside of the IMO’s direct jurisdiction. This land-sea infrastructure interdependence is only set to strengthen over the coming decade, either through the building of remotely monitored or fully autonomous unmanned ships without human intervention on-board.

Second, there are many different classes of vessel, all of which operate in dissimilar environments. These vessels tend to have different computer systems built into them. These systems will vary greatly depending on their class, use, and working environment. And each vessel class, as defined by the Classification Societies, has specific requirements for on-board systems. Notably, vessels are frequently designed with an operational life expectancy of over 25 years (IMO, 2005, p. 57) and a vessel may be re-purposed several times during its lifetime. So it is not uncommon for vessels to contain shipboard computer networks and systems that are badly out-dated and that are predisposed to cyber-attacks.

A third complexity is that many ships habitually carry specialist equipment which was not designed with cybersecurity in mind. Some of the aging operational technology found on vessels have been demonstrated to be inherently unreliable and insecure, such as the maritime navigational aids GPS and ECDIS. This is despite being mandated by the IMO and designed in accordance with international standards. To complicate matters, there are many different equipment providers, meaning each vendor can implement security protections in their own particular way, making the harmonizing of equipment requirements with existing cybersecurity standards adopted by other sectors problematic. Moreover, some systems need to be publicly accessible, for example, if they are required for identifying and locating a vessel in distress and that is threatened by serious and/or imminent danger.

Finally, a wide range of third-party service providers are employed by maritime operators in order to maintain and update a vessel's operational systems. Contractor visits occur when a vessel is in port, which limits the time for conducting the necessary work required to take appropriate action to protect key assets. It is perfectly possible that a ship's crew have little understanding of how on-board systems interact with each other. This might comprise of back-up and restore systems that are necessary for shipping operations or services if impaired. Frequently changing crew patterns also increase the chance that installed systems are operated by individuals who are unfamiliar with them, increasing the risk of user error and poor real-time management of security breaches and incidents. These risk operation problems will be exacerbated when the vessel is at high sea and the only immediate support available is via limited and low-speed bandwidth connections (ESC Global Security, 2015).

A community based approach to regulation building

Given both the increasing sophistication of global cyber-attacks and the enhanced digitization in shipping, the issue of maritime cybersecurity regulation requires urgent attention. One part of this process involves the establishment of appropriate conventions and workable principles. As such, it is vital that the process of establishing robust and resilient maritime cybersecurity regulations is done through international collaboration, and in a manner that respects both regional needs and mutual economic dependencies. These regulations must also address interdependencies and relationships between systems at a data or information level.

The impact of a threat to security to act as a catalyst to the creation and implementation of a regulatory security architecture is not a new concept within the maritime space. Glück (2015) suggests that threats like piracy have acted as a vehicle for the accelerated production of transnational collectives to improve maritime security relations and subsequently have led to the creation of security communities. Based on an assessment of the risk, these communities share knowledge and develop a common understanding of problems and opportunities through socialization. These convergent communities can then support shared practices and habits that aim to promote positive-sum and profitable elements, such as reducing logistics costs and 'frictionless' ship-ping that removes the need for a customs border (while still suppressing undesirable, often counter-productive or illegal, activity).

Both the EU and UN are examples of international security communities that have come to share common norms of behavior and acted to and institutionalize new platforms for mutual engagement, based on, for instance, law-bound standards of police and government conduct. So too is NATO, for instance, whose Operation Ocean Shield in 2009 was mandated – in full accordance with the relevant UN Security Council Resolutions – to con-tribute to international efforts to counter maritime piracy and to support efforts like joint surveillance with regional governments (NATO, 2016). Such capacity building missions included the building of training centers as well as developing relationships between the defence and commercial sector. Overall, collaborating through supranational organizations does allow for drafting of shared strategy documents that, over time, can support specific mandates to strengthen international and regional security initiatives.

Furthermore, security concerns on land can act as a precondition for a more systematic approach incorporating wider maritime security issues. International support can be given to help coastal states think about how to best support safe and secure shipping and set up their navies and coastguards that are tailored to specific maritime needs.

While not a stand-alone solution to the maritime security threats, the IMO can act as a platform for the international maritime community to monitor compliance and mitigate cyber risks. All IMO regulatory discussions are conducted through its membership which has a vast range of expertise and proficiencies. The Djibouti Code of Conduct is one example of how the IMO, through collaborative work has helped in the fight against piracy in the Indian Ocean. It was signed in 2009 and then later revised in 2017. Involving more than 20 states, alongside with regional stakeholders, the Code provides an example of how the IMO used its expertise and power to initiate the establishment of multi-agency, multidisciplinary maritime security partnerships. This institutional framework, where possible, coordinates military and civilian resources to avoid duplication and strengthens trans-regional coordination such as facilitating the operational coordination of regional navies.

Cyber-security however, cannot be approached through a limited regional oceanic network of like-minded actors. Due to the unique nature and scope of maritime systems and digital

infrastructure, the impacts and detrimental flow-on effects of an attack are not limited to just one region or domain. The far-reaching impacts of the cyber-attack on A.P. Moller-Maersk in 2017, highlights the importance of international collaborative approaches to addressing cybersecurity threats. This attack started on an office terminal in Ukraine, spread through the company's global network, and eventually impacted international port terminals including those in India.

Nonetheless, regional stakeholders are still important to regulatory discussions, as they are more acutely aware of the immediate geopolitical, environmental, resource and related issues for a particular region. The Indian Ocean is one of the major conduits for Middle Eastern oil transport, and therefore its shipping lanes are predominantly used by tankers, which carry their own specific risks. Also, as was seen by the worldwide implications of a 2017 ransomware attack – WannaCry through the Windows XP operating system – there are some states who lack the capability to easily implement updated technical mitigation processes (AFP, 2017). Problematically, this lack of capacity will inhibit their ability to co-ordinate with non-government stakeholders and met stringent regulatory compliance.

So maritime cybersecurity is an inter-dependent global challenge, tackled by a comprehensive strategic framework of international collaboration, feedback, coordination and communication in order to achieve common or complementary risk analysis. The creation of a stronger shared understanding of both the risks and impacts of a cyber-attack will allow the formation of a cross-sectoral security community, focused on cybersecurity and associated threats to operation-critical, technology platforms such as navigation systems. It is through standardization and certification that all relevant regional and international stakeholders will be able to better assist with incident management as well as acting to ensure the development of adaptable regulation, which is then monitored and evaluated by all within the sector.

The role of codes in the IMO

The IMO uses a mixture of conventions and codes to enforce regulation and best practices to ensure safe and efficient shipping. The IMO's main legal basis is given by the Safety of Life at Sea Convention (SOLAS) (IMO, 2014c), which is legally binding to any vessel within certain parameters. By appending regulations to SOLAS, the IMO can adapt and modernize its requirements as technology develops. Any amendments to these conventions continue to be legally binding under Article 26 of the Vienna Convention on the Law of Treaties (1969) (UN, 1980).

Codes within the IMO are normally viewed as guidelines unless they are mandated under a precise convention. Codes create standalone guidance and regulation that is specific to one certain aspect of the maritime industry. For example, the International Code for Ships Operating in Polar Waters (Polar Code), which outlines regulation that applies only to vessels operating in polar waters, has mandatory sections that are enforce-able under both SOLAS and maritime pollution conventions.

By using Codes, the IMO can highlight long-term and specific risks that are unique to a process or environment that the code pertains too. It creates an unambiguous reference to how the overarching conventions still apply, regardless of the uniqueness of a process or environment. The Polar Code outlines the requirements on safety equipment, such as life jackets and ice axes, that are distinctive to the operational environment and that are required to ensure continued compliance with SOLAS. In other words, as well as reiterating requirements, Codes allow additional requirements, above and beyond the basic requirements of compliance to be added to the overarching convention. The Polar Code outlines stringent hull specifications that vessels wishing to be classified as 'Icebreakers' require. Such a classification applies to ships constructed of steel and intended for independent navigation in ice-infested polar waters. This then allows the IMO to restrict the scope of aspects of compliance, to specific practices and process when required.

The use of Codes also allows for the harmonization of the different and discrete rules that regulate shipping. Again, taking the Polar Code, it creates a consistent regulatory framework that incorporates parts of both IMO frameworks and those of the Arctic Council. This allows other administrations' requirements, local authority law and expertise all to be incorporated into wider IMO regulations and standards. Such a uniform approach ensures there is no unfair advantage given to ships under certain administrations.

Additionally, this harmonization occurs between the various councils that form the IMO. It allows each council to use their technical expertise to develop holistic regulations through a better decision-making process. Through the use of working groups, each council will con-sider regulation and guidance that ensure the reduction of the risks present in relevant specific environments, such as in known regions of high piracy. These recommendations are then collated under the IMO parent committee, normally the Maritime Safety Commit-tee, to develop a single code that includes all the recommendations.

Codes allow a wide and varied IMO membership (via its member states, various think tanks, shipping associations and Non-Governmental Organizations) to share their expertise and experiences to the decision-making process. This collaboration is aided by Ship-ping Associations who work on behalf of smaller bodies that do not have their own seats within IMO discussions. This means that the smaller parties, that are the practitioners within the maritime community, can have a sense of ownership among all actors as their interests feed into an equally-beneficial governance process. This allows the decision-making process to consider not only the broader industry risks, but also the more nuanced risks that only a specific section of the industry might face. Codes thus facilitate information sharing, promote engagement within the maritime community, encourage greater awareness among public stakeholders, and ensure a better co-ordinated decision making process to support relevant cross-sector maritime regulation.

The case for a cyber code

There is no one regulation or standard for maritime systems and cyber security. And as discussed earlier, maritime cybersecurity poses a unique set challenges for regulators to consider. The establishment of a Cyber Code is needed to speed up the development of cyber security standards and support effective and holistic maritime cyber risk management.

Overcoming system complexities

Vessel and port systems are complex and differ vessel to vessel, therefore it is vital that the IMO draw together all the relevant security assurance regulations. This ensures that operators are aware that even when cyber is not explicitly mentioned, it might still be relevant to a specific regulation.

A Code would allow the harmonization of these numerous regulations into one succinct benchmark document, which is easier to monitor and enforce. In general terms, cybersecurity management encompasses a wide variety of regulations already in place, including navigational aids, operating systems and ballast water systems. A standalone Cyber Code would allow the IMO to draw attention to these systems, which are universal across vessels, and ensure the operators and crew are fully aware of existing vulnerabilities and the wider consequences of a cyber-incident.

A Code would also facilitate harmonization between a number of existing best practice cybersecurity standards that are relevant to, but not explicitly targeted at, the maritime sector, like the internationally-adopted US National Institute of Standards and Technology (NIST) framework (NIST, 2018), which aims to standardize practices to ensure uniform protection of cyber assets. As these existing standards already have international acceptance, compliance should meet less resistance from the IMO membership. Moreover, a single Cyber Code document makes it easier to update regulations, since the IMO would be able to more readily review and modernize regulations as new technology or processes are introduced. Such a process was evident by the 2018 ‘e-waste’ amendments to the Maritime Pollution Convention, which has acted to ensure the correct disposal of maritime electrical equipment (IMO, 2018b).

Enabling enforcement

The creation of a Cyber Code would increase the ability to enforce cybersecurity regulation from within the maritime industry itself. The Code would highlight the authority of authorized members to carry out inspections to ensure the continued compliance with these regulations. A vessel in breach of these regulations could be detained.

Enforcement authorities within the maritime industry, such as Flag Administrations and Classification Societies, would be party to discussions about establishment of a Cyber Code. This would provide the necessary leverage to develop a cohesive enforcement structure. The

Code would serve to create a framework for states to use entering regulations into national law and in ensuring the consistency of these across the international community and relevant third party stakeholders.

In 2017, the IMO amended two of their general security management codes to explicitly include cybersecurity. The International Ship and Port Facility Security Code (ISPS) and International Security Management Code (ISM) detail how port and ship operators should conduct risk management processes. Making cybersecurity an integral part of these processes should ensure that operators are at least conscious of cyber-risks.

Hopefully, the above developments could initiate a more holistic approach to maritime cybersecurity regulation. The knowledge gained from these new cyber-risk assessments may enable the IMO to develop a broader set of cybersecurity regulations. Readily attainable is, for example, the harmonizing of some equipment requirements with existing cybersecurity standards adopted by other sectors.

The inclusion of cyber risk management into both the ISM and ISPS security assessments will allow administrations to have the enforcement capabilities required to ensure compliance, and thus increase the security of maritime cyberspace. As part of a Cyber Code these requirements are not left as standalone assessments, but would form part of a wider assessment and mitigation process that includes compliance with other standards and regulations, thus ensuring that all systems have a basic level of security. There also seems to be a lack of urgency to get the house in order. It is also worth noting that the cyber-specific amendments to the ISM and ISPS do not come into force until January 1 2021 and they only represent starting point to move towards a more holistic approach to maritime cybersecurity regulation.

Overcoming sovereign resistance

A Cyber Code would, like the IMO's other Codes, have mandatory and voluntary components. The mandatory section would include regulation that ensures the continued safety and productivity of modern shipping. It would do this by drawing together the expertise and combining this input with other existing regulations and standards. This would ensure that the relevant parts of these other regulations are applicable to cyber risk and are brought to the attention of stakeholders.

Many of the IMO regulations do not specify cyber-security principles but are broad enough to be considered within them. This is similar to other sectors, for example by the application of a modern understanding of cyber-security to traditional definitions of broadcasting in the United Nations Convention of the Law of the Sea (UNCLOS) by the Tallinn Manual 2.0 (NATO, 2017). In providing advice regarding the international law of cyber operations,

> *… .understanding the points about which application and interpretation are subject to disparate views allows States to focus their efforts where clarification of the law is*

needed and in their national interest. Such clarification will help deter other States from exploiting these grey zones in the law of cyberspace.

Given a major obstacle is that maritime surveillance is strongly linked with national sovereignty, the voluntary section of the Code would allow the IMO to build in recommendations that states could enact into national law. This combination of mandatory and voluntary elements would allow minimum standards to be set by the mandatory section, with additional security supplemented through the voluntary section. This voluntary section permits states to implement additional security in ways that they see fit, but which might be seen as too prescriptive in other legal jurisdictions. By including these regulation as voluntary, with no obligation to implement, states with reservations can still agree to the Code, allowing it to enter into force.

As discussed previously, maritime cyberspace is closely connected to terrestrial infrastructure, which falls under the individual sovereignty of states. Within IMO discussions, issues that are seen to infringe on state sovereignty, like submarine cabling, are often met with resistance and outright rejection of the suggested regulation. Therefore, creating a Cyber Code which is goal-based, a concept the IMO has utilized since the early 2000s, could help overcome some of this resistance. This is because goal-based standards do not specify a means of achieving compliance, but rather set flexible goals permitting alternative ways to achieve compliance. This would allow sovereign states the freedom to implement practices that fit in with their national guidance, as long as the overall goal is met, and are included in operational security assessments, to be assessed by the Flag Administration This would involve controlling checking all the security navigation documentation and having direct control on the compliance of foreign-registered vessels calling at domestic ports.

The establishment process of a cyber code

The IMO has currently made little progress in the creation of cybersecurity regulation, as there has been only ad hoc attention paid to it within major policy discussions. In 2014, the IMO opened a cybersecurity discussion at a supranational level, by engaging not only with its member states but also the broad spectrum of consultative Non-Governmental Organizations within its membership regarding cybersecurity regulations and policies (IMO, 2014b). Yet the resulting cybersecurity guidelines, which act as a precursor for regulation, addressed only a broad set of non-maritime specific cyber risks.

Before a specific set of cybersecurity regulations, or dedicated Cyber Code, can be formed more work is required to understand the cybersecurity risks faced by the maritime industry. From previous experience, the IMO has a timeline for the establishment of a Code. But is still a way to go before the sustainable creation of a Cyber Code occurs. Significantly, it is often a specific newsworthy event, or disaster, which acts as a catalyst for discussion and change within the IMO. It is through these discussions that the experience and expertise present within the IMO's membership help create a Code.

One such event was the sinking of the Titanic in 1912. The tragic loss of life was a catalyst for the international maritime community to create a holistic set of regulations to ensure the safety of life of both seafarers and passengers at sea. The discussion led to the International Convention for the Safety of Life at Sea (SOLAS), which has become one of the single most significant conventions within the IMO relating to life saving appliances and arrangements. The Deepwater Horizon explosion in 2010 – the largest marine oil spill in history – also led to the instigation of numerous amendments to IMO regulations relating to oil spills because existing regulations had applied to tankers and not drilling platforms.

Yet it would seem unlikely that an incident on the scale of the Titanic or Deepwater Horizon is likely to arise from cyber threats to the maritime industry. The significant attack on A.P. Moller-Maersk's land-based systems in 2017 did not involve loss of life and operations were restored within one week, although they suffered a $300 million loss in the relevant financial quarter. Therefore, a better example for the establishment of a Cyber code would be the sinking of the Polar passenger ship 'The Explorer' in 2007. The sinking did not result in a catastrophic loss of life, however, the reaction of the maritime com-munity, through the IMO, was the creation of the Polar Code. Again, this addressed the unique challenge of strengthening existing conventions in a way where compliance was only required by those who operated within that specific environment.

The process of a code creation

The blueprint for the establishment of a Code provided by the Polar Code does suggest a three-phase process. Firstly, a threat or danger is formulated. Following this is a 'negotiation' phase, which allows the IMO membership to come to a consensus regarding the threats, the impacts and the subsequent management of that threat. The final stage is the ratification of the Code, which embodies the agreement by IMO committees to the regulations built from its members' comments and opinions.

For cybersecurity, the formulation of the risk came in 2014, when the IMO engaged with their membership to raise awareness of common cyber vulnerabilities on board existing ships. This put cybersecurity on the Maritime Safety Committee's agenda, which can be seen as the first step towards establishment of a Cyber Code. This has occurred without an obvious referent object or disaster that has commonly been the catalyst for regulatory discussions.

The second phase, the negotiation stage, started with the production of the IMOs Interim Guidelines on Maritime Cyber Risk Management (IMO, 2016). Like the Circulars which acted as the pre-curser to the Polar Code, it only contains recommendations, with no binding and uniform acceptance. However, these allow all parties to be able to influence the decision-making process ahead of ratification of regulation into a formal Code. Yet more work is required to appreciate the growing cybersecurity risks faced by the maritime industry before negotiations can continue.

As mentioned, in 2017, the IMO had highlighted the relevance of both the ISM Code (IMO, 2018a) and the ISPS Code (IMO, 2012) within this negotiation phase. By including cyber risk assessments as an integral part of the security certificate of compliance for both port facilities and vessels, all operators are made aware of the risks that their systems and processes represent, and are required to communicate this back to the IMO.

This process goes beyond a general understanding of the systems and possible threats and must indirectly include mitigation measures contained in security plans. The IMO does not suggest specific and definitive methods for mitigating cyber risk, but rather suggests that organizations become more aware of the inherent vulnerabilities that their systems and practices have, and design their own appropriate mitigation practices. This process ensures that there is collaboration with all parties and practices that are in some way invested with day-to-day maritime cyber-security, leading to a better-informed negotiation phase.

For the third and final stage of the ratification of a Cyber Code to occur, there must be a baseline agreement on the basic structure and content at a legal and technical level. This basis for this would not need to be created from scratch, but rather, by utilizing Article 30 of the Vienna Convention on the Law of Treaties (UN, 1980). So it would be formed from other previous, legally binding conventions. This subsequent governance basis would be supplemented by the additional outputs and decisions identified in the negotiation phase and then eventually ratified by the IMO Assembly. It should be noted that before any convention does come into force – that is, before it becomes binding upon governments which have ratified it – it has to be accepted formally by individual governments.

Overall, the bulk of the cyber-specific regulations that would be included in a Cyber Code are directly formed from the initial information gained through ISM and ISPS assessments. It can be argued that the voluntary incorporation of these assessments will form a much better stimulant for development of a Code rather than being reactive and knee-jerk. Instead, such an assessment process will allow the industry to utilize the strength of its collective participants to develop comprehensive regulation based from best practice and not be reliant on intentions based from past experiences.

There is no inevitability that a Cyber Code will be created from this process. However, as this research note has outlined, it would be the logical and productive step. Currently, there does seem a trend from the maritime industry not to want a Cyber Code, but this may come from the lack of appropriate risk management regime across shipping organizations. With an increased clarity about applicable risk boundaries and the threats to systems or services posed by digitization and integration, the industry might tap into new opportunities to drive an international standard. This standard, in the form of a Cyber Code, would then act to ensure a uniform and parallel approach is adopted while increasing the cost and consequences of non-compliance.

Conclusion

The maritime industry is undoubtedly behind other transportation sectors, such as aerospace, in cybersecurity terms. The co-operative establishment of a holistic Cyber Code by the maritime community would allow the development of robust maritime cybersecurity regulations. These would equip the sector with the capability and adaptability to address whatever future cyber security challenges arise.

References:

Amirell SE (2016) Global maritime security studies: the rise of a geopolitical are of policy and research. Secur J 29(2):276–289

Attri VN (2018) IORA, the blue economy and ocean governance. In: maritime governance and South Asia. Security and Sustainable Development in the Indian Ocean, Trade,

Barron L (2018) Pentagon official says U.S. Can 'take down' man-made islands like those in the South China Sea. http://time.com/5298185/pentagon-kenneth-mckenzie-warning-south-chinasea-islands/.

Brewster D (2017) Silk roads and strings of pearls: the strategic geography of China's new pathways in the Indian Ocean. Geopolitics 22(2):269–291

Bueger C (2015) What is maritime security? Mar Policy 53:159–164

Bueger C, Edmunds T (2017) Beyond sea blindness: a new agenda for maritime security studies. Int Aff 93(6):1293–1311

Buzan B (1983) People, states and fear: the national security problem in international relations. University of North Carolina Press, Chapel Hill

Buzan B, Wæver O, de Wilde J (1998) Security: a new framework for analysis. Lynne Rienner Publishers, Boulder

China Power (2017) How much trade transits the South China Sea? https://chinapower.csis.org/much-trade-transits-south-china-sea/.

Dabas M (2017) Here is all you should know about 'string of pearls', China's policy to encircle India. https://www.indiatimes.com/news/india/here-is-all-you-should-know-about-string-ofpearls-china-s-policy-to-encircle-india-324315.html.

Germond B (2015) The maritime dimension of European security. Palgrave Macmillan, London

Granieri RI (2015) What is geopolitics and why does it matter? Orbis 2015(Fall):491–504

Khurana GS (2008) China's 'string of pearls' in the Indian Ocean and its security implications. Strateg Anal 32(1):1–39

Mudrić M (2015) Maritime security: editorial note. Croat Int Relat Rev XXII(75):5–7

Qi X (2006) Maritime geostrategy and the development of the Chinese navy in the early twenty-fist century. Naval War Coll Rev 59(4):47–63

Rahman C (2009) Concepts of maritime security: a strategic perspective on alternative visions for good order and security at sea, with policy implications for New Zealand. Discussion paper no.07/09. Centre for Strategic Studies/Victoria University of Wellington, New Zealand/Wellington

Rogers J (2010) To rule the waves: why a maritime geostrategy is needed to sustain European Union. Security Policy Brief, Egmont, the Royal Institute for International Relations, Brussels

Roy N (2017) Fantasy or fiction? Marching of the dragon in the South China Sea. Asian Aff 48(2):257–270

Stone M (2009) Security according to Buzan: a comprehensive security analysis. Security discussion papers series 1, Spring 09. France, GEEST

Van Rooyen F (2011) Africa and the geopolitics of the Indian Ocean. Occasional paper no. 78. South African Institute of International Affairs, Johannesburg

APT. (2017, May 14). Manhunt for hackers behind global cyberattack. Seychelles News Agency [online]. Retrieved from http://www.seychellesnewsagency.com/articles/7262/Manhunt+for + hackers +behind+global+cyberattack

Bai, J. (2015). The IMO polar code: Emerging rules of Arctic shipping governance. The International Journal of Marine and Coastal Law, 30(4), 674–699. doi:10.1163/15718085-12341376

Basarn, I. (2015). IMO-polar code: History, content, and shortcomings. Arctic Summer College 2015 Contributions [online]. Retrieved from

https://arcticsummercollege.org/sites/default/files/ASC% 20Paper_Basaran_Ilker.pdf

BIMCO. (2017). The guidelines on cyber security onboard ships [online]. Retrieved from http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

Bueger, C. (2015). What is maritime security? Marine Policy, 53, 159–164. doi:10.1016/j.marpol.2014. 12.005

ESC Global Security. (2015). Maritime cyber security white paper – safeguarding data through increased awareness [online]. Retrieved from

http://www.escgs.com/files/WP_ESC_Safeguarding%20data%20through%20increased%20awareness.PDF

Glück, Z. (2015). Piracy and the production of security space. Environment and Planning D: Society and Space, 33(4), 642–659. doi:10.1068%2Fd14245p

Hoppe, H. (2005). Goal-based standards – a new approach to the international regulation of ship con-struction. WMU Journal of Maritime Affairs, 4(2), 169–180. [online]. doi:10.1007/BF03195072

Institute of Engineering and Technology. (2016). Code of practice – cyber security for ports and port systems [online]. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/ system/uploads/attachment_data/file/546160/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

International Maritime Organisation. (2005). Report of the maritime safety committee on its eightieth session. MSC 80/24 [online]. Retrieved from https://docs.imo.org/Shared/Download.aspx?did= 31865

International Maritime Organisation. (2012). ISPS code - guide to maritime security and the ISPS code. London: IMO Publishing.

International Maritime Organisation. (2014a). Implications of the United Nations convention on the law of the sea for the International Maritime Organization. LEG/MISC.8 [online]. Retrieved from http:// www.imo.org/en/OurWork/Legal/Documents/LEG%20MISC%208.pdf

International Maritime Organisation. (2014b). Measures toward enhancing maritime cyber security. MSC 94/4/1 [online]. Retrieved from https://docs.imo.org/Search.aspx?keywords=MSC%2094% 2F4%2F1

International Maritime Organisation. (2014c). SOLAS - safety of life at sea. London: IMO Publishing.

International Maritime Organisation. (2016). Interim guidelines on maritime cyber risk management.

MSC.1/Circ.1526 [online]. Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_ Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf

International Maritime Organisation. (2017a). Guidelines on maritime cyber risk management. MSC-FAL/Circ.3 [online]. Retrieved from

http://www.imo.org/en/OurWork/Security/Guide_to_