M.A. (Security and Defence Laws)

ROLE OF INTERNATIONAL AND REGIONAL ORGANISATIONS IN CYBER SECURITY: AN ASSESSMENT

By
Name of Candidate
Roll Number/ID Number
Year: 2 Semester: IV

DISSERTATION

DD -MM- YYYY

NALSAR UNIVERSITY OF LAW
HYDERABAD

CERTIFICATE

This is to certify that **Name of Candidate,** Roll Number **MSDL xx_yy** has submitted her dissertation titled **"Role of International and Regional Organisations in Cyber Security: An Assessment"** in partial fulfilment of the requirement for the award of Master Degree in Security and Defence Laws to the NALSAR University of Laws, Hyderabad under my guidance and supervision. It is affirmed that the dissertation submitted by him is original, bonafide and genuine research done by him.

DATE: Day, Month, Year

Place : Hyderabad

Prof.(Dr.) V.Balakista Reddy

M.Phil.,Ph.D. (JNU),

Director, Centre for Aerospace and Defence Laws (CADL),

Registrar, NALSAR University of Law, Hyderabad

DECLARATION

I declare that the present Dissertation titled **"Role of International and Regional Organisations in Cyber Security: An Assessment"** has been prepared and submitted by me to the NALSAR University of Law, Hyderabad in partial fulfilment of the requirement for the award of Master Degree in Security and Defence Laws under the guidance and supervision of Prof. (Dr.) V. Balakista Reddy, Registrar is an original, bonafide and legitimate work of the undersigned, and has been pursued purely for an academic interest. This dissertation shall not be used for any political purposes or connotations or as a testimony against any person or communities or regime. The views and idea expressed in this Dissertation are exclusively of the research and do not represent any person, organization, or community.

Signature of the candidate

Name of the Candidate

Roll Number/ID Number

DATE: Day, Month, Year

Place : Hyderabad

ACKNOWLEDGEMENT

I am highly indebted to **Prof. (Dr.) V. Balakista Reddy** for his guidance and constant supervision as well as for providing necessary information regarding the project & also for his support in completing the project. I would like to express my gratitude towards **Ms Ruchi Jain** for her kind co-operation and encouragement which helped me in completion of this project. I would like to express my special gratitude and thanks to NALSAR University for giving me such a cultivated opportunity. My thanks and an appreciation also goes to my colleagues in developing the project and people who have willingly helped me.

TABLE OF CONTENTS

Table of Statutes and Policies

- African Union Convention on Cyber Security and Personal Data Protection
- Budapest Convention
- Chicago Summit in 2012
- Convention on Cybercrime, 2001
- Conventional Armed Forces in Europe (CFE) Treaty
- Covenant of the League of Nations
- Cybersecurity Tech Accord
- Deauville Declaration 2011
- Electronic Communications Act, 2000
- Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. §§ 7001-7003
- GCSC Six Critical Norms
- Informational Technology Act, 2000
- International Telecommunications Union (ITU) (2008) Global Cybersecurity Agenda, High level Experts Group, Global Strategic Report, ITU.
- International Telecommunications Union (ITU) (2008a) Q.22/1 Report on Best Practices for a National Approach to Cyber Security: A Management Framework for Organizing National Cybersecurity Efforts (2008), ITU-D Secretariat, January 2008.
- International Telecommunications Union (ITU) (2011) National Cybersecurity Strategy Guide, ITU, September 2011.
- Law to adapt the formal requirements of private law to modern legal transactions (Federal Law Gazette I 2001 p. 1542)
- Paris Call for Trust & Security in Cyberspace
- Siemens Charter of Trust
- Southern African Development Community Model Laws on Cybercrime
- UN Charter
- UNGGE Consensus Report of 2015
- Washington Treaty

Table of Abbreviations

- Advanced Persistent Threat - APT
- Affirmation of Commitments - AoC
- African Union - AU
- Anti-Counterfeiting Trade Agreement - ACTA
- Association of Chief Police Officers - ACPO
- Association of South East Asian Nations - ASEAN
- Central Intelligence Agency - CIA
- Central Propaganda Department - CPD
- Centre for the Protection of National Infrastructure - CPNI
- China Crime Information Centre - CICC
- Cloud Security Alliance - CSA
- Communications-Electronics Security Group - CESG
- computer emergency response teams - CERTs
- Computer Maintenance Corporation - CMC
- Computer Security Incident Response Teams - CSIRT
- Confidence Building Measures - CBMs
- Conventional Armed Forces in Europe - CFE
- Cooperative Association for Internet Data Analysis - CAIDA
- Cooperative Cyber Defence Centre of Excellence - CCDCOE
- Council of Europe - CoE
- country code top-level domain - ccTLD
- Critical Information Infrastructure Protection - CIIP
- Critical Infrastructure Protection - CIP
- Cyber Defence Management Board - CDMB
- Cyber Readiness Index - CRI
- Cyber Threat Intelligence Integration Center - CTIIC
- Department of Defence - DoD
- Department of Electronics and Information Technology - DeITY
- Department of Justice - DoJ

- Department of State - DoS
- Domain Name System - DNS
- Education Research Network - ERNET
- European law enforcement agency - EUROPOL
- European Network and Information Security Agency - ENISA
- European Telecommunications Standards Institute - ETSI
- European Union - EU
- Federal Bureau of Investigation - FBI
- Financial Services Sector Coordinating Council - FSSCC
- Forum and information sharing for CERTs - FIRST
- Global Cybersecurity Agenda - GCA
- Global Institute for Security and Research - GICSR
- Government Advisory Council - GAC
- Government Communications Headquarters(UK) - GCHQ
- Indian Department of Electronics - DoE
- Information and Communications Technology - ICT
- Information Security Research Association - ISRA
- Information Sharing and Analysis Centers - ISAOs
- Internal intrusion detection systems - IDS
- International Multilateral Partnership Against Cyber Threats - IMPACT
- International Organisations - IOs
- International Relations - IR
- International Telecommunication Union - ITU
- Internet Engineering Task Force - IETF
- Internet Governance Forum - IGF
- Internet Protocol version - IPv
- Internet Service Providers - ISPs
- memorandum of understanding - MoU
- Ministry of Electronics and Information Technology - MeitY
- Ministry of Industry and Information Technology - MIIT

- Mission Mode Projects - MMPs
- National Critical Information Infrastructure Protection Center - NCIIPC
- National Cyber Security Coordination Centre - NCCC
- National Cyber Security Programme - NCSP
- National e-Governance Plan - NeGP
- National Informatics Centre Network - NICNET
- National Security Advisory Board - NSAB
- National Security Agency - NSA
- National Security Strategies - NSS
- National Technical Research Organisation - NTRO
- National White Collar Crime Center - NW3C
- NATO Communications and Information Agency - NCI
- NATO Computer Incident Response Capability - NCIRC
- NATO Consultation, Control and Command Board - NC3
- NATO Military Authorities - NMA
- Network and Information Security - NIS
- Non-Align Movement - NAM
- North American Electric Reliability Corporation - NERC
- North Atlantic Treaty Organisation - NATO
- Organisation for Economic Cooperation and Development - OECD
- Organisation of American States - OAS
- Organization for Security and Co-operation in Europe - OSCE
- Organization of the Islamic Conference - OIC
- Personal Digital Assistants - PDAs
- public security intelligence - PSI
- Serious Organised Crime Agency - SOCA
- Shanghai Cooperation Organisation - SCO
- South Asian Association for Regional Cooperation - SAARC
- Strategic Defence and Security Reviews - SDSR
- top-level domains - TLDs

- Unique Identification Authority of India - UIDAI
- United Kingdom - UK
- United Nations Development Programme - UNDP
- United Nations Office of Drugs and Crime - UNODC
- United States Dollor - USD
- United States of America - USA
- United States Security Treaty - ANZUS
- Working Party on Information Security and Privacy - WPISP
- World Wide Web Consortium - W3C

CHAPTER-1

1.1. Introduction

Fred Allen, an American Comedian once said, "*It is probably not love that makes the world go around, but rather those mutually supportive alliances through which partners recognize their dependence on each other for the achievement of shared and private goals*". This quote can be quite relevant in the context of Security threats, specially to the emerging ones like cyber security, environment security, health security, food security etc. Information and Communications Technology (ICT) presents one of the most critical modern challenges to global security[1]. There is a urgent need for the state cooperation to mitigate the threats associated with the ICT like cybercrime, cyber attacks on critical infrastructure, application of power and force in and through cyberspace and so on.

The global community had recognised the salience of cyberspace and cybersecurity in day-to-day life. Cyberspace has become a game changer in International Relations (IR) and new digital technologies, ways of communicating have a considerable impact on security and strategic stability. In a report published in 2020, by Steve Morgan, editor-in-chief of Cybercrime Magazine, it was predicted that there would be damages totalling $6 trillion USD in 2021, which amounts to 3rd largest economy after United States of America (USA) and China. This shows how much of the world economy is involved in the cyberspace and the need for more robust security. The rate of cybercrime is increasing every year and it is also estimated that there would be increase in 15 per cent in next 5 years[2].

This shows the gravity of the issue concerned to security in cyberspace. With the pandemic, there has been restrictions on movements and other fundamental rights. These restrictions have increased the dependence on ICT and also vulnerability in the cyberspace. With Cyberspace being cross border in nature, various issues arise when there are any damages or incidents. For example, in case of cyber crimes, the jurisdiction plays an important role, like where the perpetrator resides, where the damage occurs, where the servers are and son on. The same goes for other cyber related crimes.

---

[1] International Institutions and Global Governance Program, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms", Council on Foreign Relations, February 23, 2018; available at: https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms; Last accessed: June, 2021.

[2] Steve Morgan, "Cybercrime to cost the world $10.5 Trillion annually by 2025", Cybercrime Magazine, November 13, 2020; Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ ; Last accessed: June, 2021.

These being one face of the cyber-crimes where the individuals are victims or some corporation are victims and the accused being the non-state parties, the other side of the cyber crimes are related to the state parties and the accused or the initiator is the state or state-sponsored. Then the paradigm of the legal applications changes. The Humanitarian Law or the Law of War governs such situations. This second type is sometimes considered as cyber warfare and the laws relating to the armed conflict is applicable[3].

To overcome such incidents and issues, many domestic laws[4] are implemented in lines of the International Laws and many agreements[5] are entered into as well. Various alliances were formed to fight the cyberthreats and also to maintain cybersecurity. In addition to the legislations, conventions, agreements, accords there are various Institutions and Organisations which are active in promoting cybersecurity and protecting from cyberthreats. Owing to the requirement and need of cybersecurity, this paper analyses the role of International and regional Institutions in maintaining cybersecurity.

1.2. Research Objective

The objective of this paper is Three-fold: firstly, the research aims to analyse the theory of Institutionalism and evolution of Institutions; Secondly, it aims to analyse cyber security setting globally and regionally; Thirdly, the research aims to signify the importance of Organisations, both governmental and non-governmental; International, Regional, and domestic and also propose suggestions to enhance cybersecurity co-operation among them.

1.3. Research Gap

While most of the literature is on concept of cyber security, threat perception, cyber crimes, there is very little literature on the role played by various players in the cybersecurity setting. It is the players in cybersecurity architecture that shaped the current setting. International and regional organisations play key role as they come second to the sovereign nations while

---

[3] However, for the purpose of the present paper, the cyber warfare is not separated from the concept of cybercrime and where and when cybercrime is used, it includes all the crimes including the cyber warfare, cyber terrorism etc, which some scholars consider it as a separate part of the study.

[4] Informational Technology Act, 2000 in India; Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. §§ 7001-7003 in USA; Electronic Communications Act, 2000 in UK; Law to adapt the formal requirements of private law to modern legal transactions (Federal Law Gazette I 2001 p. 1542) in Germany and so on. Country-wise list available at: https://unctad.org/page/cybercrime-legislation-worldwide.

[5] African Union Convention on Cyber Security and Personal Data Protection; Southern African Development Community Model Laws on Cybercrime; Paris Call for Trust & Security in Cyberspace; UNGGE Consensus Report of 2015; Cybersecurity Tech Accord; Siemens Charter of Trust; GCSC Six Critical Norms; Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecurity etc.

enabling the cybersecurity. Hence this paper tries to fill that gap in the literature which highlights these players of Institutions.

1.4. Hypothesis

It is hypothesised that the International and regional organisations play important role in enabling and enhancing cybersecurity.

1.5. Research Questions

The principle research questions are - 1. What is the current cybersecurity setting globally and regionally?; 2. What is the need of Organisations in maintaining peace and security?; 3. What is role played by the Organisations in enhancing and enabling cybersecurity?

To address these questions, the research will analyse the following critical Issues:

1. How did the evolution of International and regional organisations take place?
2. What is cybersecurity?
3. What is the need of cyber security?
4. What are the various International Organisations working in the domain cybersecurity?
5. How do the International Organisations play key role in enhancing and enabling cybersecurity?
6. What is the status of regional organisations in America, Europe and South Asia in cybersecurity architecture?
7. What are the laws covering such organisations and what are the principles binding the states in co-operation among them?

1.6. Research Methodology

The research is predominantly desk-based. The researcher employed empirical research and vastly depended on the descriptive analytical method to answer the above questions. This research is aimed at analytically examining the existing situation, challenges and determine the possible reforms and strategies to overcome the issues.

As stated earlier, the research is predominantly library-based and where practicable , data is drawn from the publications and presentations by the experts and policy experts and

strategists. The researcher mostly relied on government reports, speeches by eminent personalities, journal articles, online sources, monographs, scholarly writings, conference materials and text books, reports and publications in attempting the research questions.

1.7. Value of Research

With the evolution of technology, the risk to protect it has also increased. As the cyberspace is dual-use in nature, and has strategic standing, it is important to protect the same. The interdependent of states has increased with the increase in cross-border threats and crimes. This interdependence and co-operation is assisted by the Organisations, both International and Regional. Therefore it is important to note the relevance and importance of the same.

1.8. Research Plan

The researcher will achieve the objective by analysing the literature through the following chapters -

1. Introduction

This chapter introduces the topic and also highlight the aim, scope and purpose of research.

2. Concept of Alliance and evolution of International Organisations

This chapter analyses the alliance formation and theory of evolution of International organisations.

3. History and Purpose of Regional Organisations

It deals with the history, purpose and importance of regional organisations.

4. Concept of Security

This chapter analysis the concept of security and shifting paradigm of security.

5. Introduction to Cyberspace, cybercrime and cybersecurity

This chapter highlights the classification of cybercrime, nature and meaning of cybercrime and also explains cybersecurity.

6. International Institutions relating to Cybersecurity: An Overview

This chapter gives the overview of various International institutions working in the domain of cybersecurity.

7. Global Cybersecurity ecosystem

This chapter analyses the existing cybersecurity ecosystem and highlights ICANN and IGF.

8. Multilateral Organisations and cybersecurity

This part analyses and highlights various organisations like G8, UN, ITU, NATO, OECD, CoE and their importance and functions in maintaining cybersecurity.

9. Cyber security setting in European Union

This chapter analyses the cyber security setting in EU.

10. Cyber Security setting in United Kingdom

This Chapter analyses the existing cybersecurity ecosystem in UK.

11. Cyber Security setting in China

This Chapter analyses the existing cybersecurity ecosystem in China

12. Cyber Security setting in India

This part analyses the national strategy, incident response and various organisations in India.

13. Conclusion

This chapter contains the conclusion and the drawbacks in the existing system.

CHAPTER - 2: CONCEPT OF ALLIANCE AND EVOLUTION OF INTERNATIONAL ORGANISATIONS

"*Alliances and international organizations should be understood as opportunities for leadership and a means to expand our influence, not as constraints on our power*".

Chuck Hagel, Former United States secretary of defence

Concept of Alliance

Introduction:

Alliances are one of the most significant occurrence in the security studies. These alliances showcase the need and importance of foreign relations in International politics. Alliances also show the relations between states. These alliances signifies the nature or requirement of these collaborations. Some alliances like NATO are purely formed for security purposes. While some alliances like SAARC is formed for economic and social purposes. As rightly said by eminent American political scientist George Modelski, "alliance is one of a dozen or so key terms of International Relations"[6]. Over the years many alliances were formed and many were broken for a variety of reasons. However, these alliances have formed a major part in the foreign policy and International Relations.

Kenneth Waltz classified the means available for states to achieve their ends in two categories. One Internal efforts and other is external efforts including the moves to strengthen and enlarge one's own alliance or to weaken and strengthen an opposing one. From his observation it can be deducted that Alliances are primary tools for enhancing ones security in face of Internal and external threats. This is specially true for smaller states with limited resources. These states have to rely on alliances. Thus the formation and use of alliances is a frequent response to the dangers of aggression and the opportunities for aggrandizement present in the international system[7].

Definition of Alliance:

The conclusions that one draws about the causes and effects of alliances depend very much on what one counts as an alliance. Unfortunately, the process of developing theories of alliances has been complicated by the use of widely varying definitions.

---

[6] John S. Duffield and Others, "Alliances", Security Studies: An Introduction, Routledge, 2008.

[7] Ibid

A number of influential definitions of alliances have been overly broad. For example, **Walt**, in his seminal study of the origins of alliances, defined alliance as 'a formal or informal relationship of security cooperation between two or more sovereign states'.[8] An almost identical definition was used by **Michael Barnett** and **Jack Levy** in their path-breaking work on the domestic sources of alliances[9]. More recently, **Patricia Weitsman** has described alliances as 'bilateral or multilateral agreements to provide some element of security to the signatories'[10].

Such broad definitions are reflected in quantitative coding schemes. In their efforts to be comprehensive, the most complete alliance databases have grouped together defensive alliances, offensive alliances, non-aggression pacts, neutrality pacts and consultation agreements. Further complicating matters is the fact that a high percentage of these so-called 'alliances' – more than half (364 of 648) in the case of the ATOP dataset – consist of two or more types.

There are at least two potential problems with such broad definitions of alliances. First, they may be so expansive as to encompass just about any imaginable security arrangement between states. Of particular concern is the fact that they blur the important distinction between alliances, on the one hand, and collective security arrangements, on the other, which involve fundamentally different orientations. Alliances are primarily, if not exclusively, outwardly oriented, intended to enhance the security of their members vis-à-vis external parties. In sharp contrast, collective security arrangements and related phenomena such as arms control agreements are designed to enhance the security of their participants vis-à-vis each other.

The other problem is the failure to distinguish between various forms of security cooperation. The above definitions would seem to embrace all manner of security cooperation, no matter how innocuous. Thus they include alliances that might be limited to supportive diplomacy or economic aid with security objectives. What has traditionally distinguished alliances from

---

[8] Walt, Stephen M. (1985), 'Alliance formation and the balance of world power', International Security, 9(4): 1–43

[9] Barnett, Michael and Jack Levy (1991), 'Domestic sources of alliances and alignments', International Organization, 45(3): 369–395

[10] Weitsman, P.A. (2004). Dangerous Alliances: Proponents of Peace, Weapons of War (Stanford, CA: Stanford University Press).

many other security arrangements between states, however, is the emphasis that they place on military forms of assistance, especially the use of force.

Such considerations suggest the need for a subset of alliance definitions that take these important distinctions into account. Four decades ago, **Robert Osgood** defined alliance as 'a formal agreement that pledges states to co-operate in using their military resources against a specific state or states and usually obligates one or more of the signatories to use force, or to consider (unilaterally or in consultation with allies) the use of force in specified circumstances'[11]. Similarly, **Glenn Snyder**, in his magnum opus Alliance Politics, wrote that 'Alliances are formal associations of states for the use (or nonuse) of military force, in specified circumstances, against states outside their own membership'. He went on to emphasize that '[t]heir primary function is to pool military strength against a common enemy, not to protect alliance members from each other'[12]. Even **Walt** later amended his conception of alliances, noting that 'the defining feature of any alliance is a commitment for mutual military support against some external actor(s) in some specified set of circumstances'[13].

These definitions clearly exclude a number of agreements that have sometimes been treated as alliances. In particular, they would seem to militate against the inclusion of pledges by states to refrain from engaging in aggression against one another, promises to remain neutral in the event of a military conflict with a third party, and commitments to consult in the event of a crisis that threatens to lead to war. Nevertheless, hundreds of security arrangements meet the more stringent criteria contained in them.

Theories of alliance formation:

The first place to look is at explanations of alliance formation. Such an approach may at first seem counter-intuitive. But, arguably, as long as the factors that caused the alliance to form in the first place remain in place, then the alliance will endure. Should those conditions change, however, the alliance may lose the glue that held it together and fall apart.

In principle, states can freely join alliances. In practice, however, they do not enter into such arrangements lightly, since alliance membership has costs as well as potential benefits.

---

[11] Osgood, R.E. (1968), Alliances and American Foreign Policy (Baltimore, MD: The Johns Hopkins University Press).

[12] Snyder, Glenn H. (1997), Alliance Politics (Ithaca, NY: Cornell University Press).

[13] Walt, Stephen M. (1997), 'Why alliances endure or collapse', Survival, 39(1): 156–179

Among those costs may be the loss of autonomy and the creation of dependence. Thus, we need to ask, under what circumstances are states willing to assume and bear these costs? For the purposes of this chapter, the most relevant theories of alliance formation fall into two categories: those that emphasize international determinants and those that focus on domestic factors.

International Determinants: Capabilities Aggregation Models:

The most prominent international explanations of alliance formation are associated with the realist school of International Relations. Also known as capabilities aggregation models, they emphasize how states form alliances in order to combine their military capabilities and thereby improve their security positions. But when precisely will states do so?

The most parsimonious explanation is balance-of-power theory[14]. It posits that states form alliances to balance the power of other states, especially when they are unable to balance power through their individual efforts or when the costs of such internal balancing exceed those of alliance membership. From this perspective, unbalanced power alone represents a threat to the survival of less powerful states. Therefore, two or more relatively weak states, when confronted with a much more powerful state, will ally.

Clearly, balance-of-power theory can also serve as a theory of alliance persistence and disintegration. In this case, shifts in the international distribution of power may threaten the existence of established alliances. For example, the previously predominant state may decline, to the point where an alliance of other states is no longer required to balance its power. Indeed, with the passage of time, an alliance member may become the most powerful state, prompting its erstwhile allies to cut their ties and perhaps even to form counterbalancing alliances against it.

An important refinement of balance-of-power theory is balance-of-threat theory. Sometimes, alliances appear to be unbalanced in terms of power. For example, during much of the Cold War, the alliances centred on the USA were more powerful, as measured on a number of indices of capability, than those revolving around the Soviet Union. Walt addressed such apparent anomalies by arguing that states form alliances in response to common threats, not just power. Although aggregate power is an important component of threat, it is not the only

[14] Walt, Stephen M. (1985), 'Alliance formation and the balance of world power', International Security, 9(4): 1–43

one. How threatening a particular state appears to be is also a function of its geographical proximity, its offensive capabilities and the aggressiveness of its intentions. Thus the Soviet Union, by virtue of its relative proximity, its massive ground forces and its hostile ideology, seemed to pose much more of a threat to its strong but less powerful neighbours, such as France, West Germany, Japan and Britain, who chose to ally instead with the USA[15].

By the same token, balance-of-threat theory should also illuminate the question of alliance durability and collapse. A decline in the magnitude of the threat posed by an adversary will cause an alliance to weaken or dissolve. This may happen, moreover, even in the absence of any shift in overall power, if, for example, an adversary significantly mutes its offensive military capabilities or seems to moderate its intentions.

Some scholars have noted that states may also use alliances to manage, constrain and control their partners[16]. Obviously, this function is contingent upon the existence of some external balancing purpose; otherwise, we could not speak of the arrangement as an alliance. However, assuming that the condition of a more powerful or threatening third party is met, this function can nevertheless be an important, albeit secondary, one. Although this perspective may not be especially helpful for explaining alliance formation, it may shed additional light on the dynamics of alliance disintegration. In this case, if the ally that the alliance is intended, at least in part, to contain becomes too threatening or too powerful to manage successfully, then the alliance will not long survive.

Domestic Determinants:

Balance-of-power theory may be excessively crude as an explanation of alliance formation, persistence and collapse. In contrast, balance-of-threat theory represents a more nuanced approach, but this refinement comes at the cost of other analytical problems. After all, is it always so obvious which state will be regarded as a threat by others? In particular, when will a state be regarded as harbouring aggressive intentions? Threat perception may depend as much, if not more, on the internal characteristics of states, a subject to which we now turn.

Fortunately, scholars have been equally productive at identifying possible domestic determinants of alliance formation. One set of explanations focuses on similarities and

---

[15] Ibid

[16] Weitsman, P.A. (2004). Dangerous Alliances: Proponents of Peace, Weapons of War (Stanford, CA: Stanford University Press)

differences in the culture, ideologies and political institutions of states. The general argument is that, other things being equal, states will tend to ally with states whose political orientations are similar to their own (e.g. Walt 1987). Thus conservative monarchies will prefer alliances with other monarchies, dictatorships with dictatorships, liberal democracies with liberal democracies, and so on.

Scholars have advanced several interrelated reasons for this tendency. Similar value systems may generate common interests and common interpretations of what constitutes a threat. In the case of states sharing a formal ideology, such as Marxism-Leninism, they may even be operating under an explicit injunction to join forces in the face of a hostile international environment. Not least important, forming an alliance with like-minded states may enhance the domestic legitimacy of a weak regime by suggesting that it is part of a broader, popular movement[17].

Such arguments also suggest possible causes of alliance disintegration. Most obviously, a sudden regime change in one partner or another as the result of a revolution, coup or other internal upheaval will immediately loosen the bonds of affinity that held the alliance together. Even more gradual changes in political outlook can have the same effect over a longer period. And in some cases, tensions may arise even among states with a common ideology, since it may dictate that national interests must be subordinated to a single authoritative leadership.

In view of such considerations, scholars have suggested that alliances among liberal democratic states are likely to be especially strong and resilient[18]. One reason is the relative stability of public preferences and the greater continuity of national leadership. Although different administrations may come and go, the democratic process ensures that leadership transitions occur smoothly and abrupt policy shifts are unlikely. In addition, the international commitments associated with alliances become more deeply embedded in domestic law and institutions. That tendency, combined with a more general respect for legal commitments, enhances the ability of leaders in liberal democracies to tie the hands of their successors.

Alliance institutionalization and socialization:

---

[17] Ibid

[18] Gaubatz, K.T. (1996), 'Democratic states and commitment in international relations', International Organization, 50(1): 109–150.

Thus far, the discussion has been limited to explanations of alliance formation that may also shed light on the question of alliance duration. Despite their differences, these theories have in common the idea that when the conditions that promoted the creation of an alliance are no longer present, we should expect the alliance to dissolve. There is, however, another set of factors and processes that can promote alliance persistence even in the face of significant changes in those formative conditions.

Institutionalization:

One of these is alliance institutionalization. Some alliances are endowed with important institutional characteristics from the outset, and some may become increasingly institutionalized over time, with important implications for their staying power. Two particular dimensions of alliance institutionalization stand out.

First, alliances may include or develop intergovernmental organizations to facilitate cooperation among their members. These organizations often include a formal bureaucracy with a staff, budget and physical location. Although presumably of use to the alliance members, such bureaucracies are also actors in their own right with some degree of autonomy and an inherent interest in perpetuating themselves[19]. As Robert McCalla[20] has noted, such actors may engage in various types of behaviour to ensure the organization's survival. For example, they may actively resist change; they may affirm the necessity of the organization; and they may try to manage change by promoting modifications in the alliance's roles and missions that will maintain member state support while not threatening the organization's core functions.

Second, alliances may contain or acquire institutional capabilities that can be used for tasks beyond those for which they were originally designed[21]. Thus even when an alliance's original raison d'être fades, member states may find that they can readily employ such institutional assets to address new threats and security concerns. This tendency will be especially pronounced when states are risk averse or the costs of maintaining pre-existing capabilities are clearly less than those of creating new ones from scratch.

---

[19] Bennett, D.S. (1996), 'Testing alternative models of alliance duration, 1816–1984', American Journal of Political Science, 41(3): 846–878.

[20] McCalla, R.B. (1996), 'NATO's persistence after the cold war', International Organization, 50(3): 445–475

[21] Wallander, Celeste A. (2000), 'Institutional assets and adaptability: NATO after the cold war', International Organization, 54(4): 705–735.

The overall implication of such reasoning is that alliances characterized by high levels of institutionalization will last longer on average. Of course, some scholars may reply that the level of institutionalization of an alliance is itself a function of other determinants of alliance formation and persistence. For example, states facing particularly acute threats may choose to create especially capable alliance organizations, or liberal democracies may find it easier to establish and abide by the additional constraints associated with alliance institutions. Once established, however, such alliance institutions may assume a life of their own and exert an independent impact on subsequent member behaviour. Their consequences cannot simply be reduced to the influence of other factors.

In fact, there has been considerable variation in the initial level of institutionalization of alliances. Of the agreements establishing the 263 defensive alliances in the ATOP dataset, 70 have contained a named organization with regularly scheduled meetings or a stand-alone organization with a permanent bureaucracy; 28 agreements provided for an integrated military command among the allies; and 63 have called for official contact among national militaries during peacetime or committed the members to conducting a common defence policy.

Moreover, the initial degree of alliance institutionalization has tended to increase over time, suggesting a possible explanation for the greater longevity of more recently formed alliances. Although some 150 (57 per cent) of the 263 defensive alliances were established following the Second World War, 36 (88 per cent) of the 41 with a permanent bureaucracy date from the post-war era, as do 21 (75 per cent) of those providing for an integrated military command and 49 (78 per cent) of those calling for close military contacts. Nevertheless, such indices of institutionalization leave much to be desired, since they do not directly measure organizational autonomy or the fungibility of institutional assets. Moreover, the existing data do not yet capture changes in the level of institutionalization that may occur after the alliance is established.

Socialization:

Another process that can promote alliance longevity is the socialization of member states, or more precisely, of their political elites and possibly their general publics. Alliance-related social interactions can lead to the development of more similar worldviews and even a common identity. Thus, as Walt has noted, an alliance may persist because its members come to see themselves as integral parts of a larger political community.

Scholars have lamented that the processes of socialization in international relations are undertheorized and poorly understood[22]. Nevertheless, it is possible to identify a number of mechanisms through which alliances might promote the socialization of their members, both directly and indirectly. For example, institutionalized alliances may facilitate substantial contact among elites through regular meetings. Within formal organizational structures, both civilian and military personnel seconded from member governments will often work side-by-side with their counterparts from other countries. In addition, similar to the organizational arguments presented above, international civil servants may actively seek to cultivate a sense of community among elites and attentive publics through their pronouncements and lobbying activities.

Socialization need not be limited to highly institutionalized alliances, however. The existence of even a weakly institutionalized alliance between two states may reinforce or lead to other connections between the members that facilitate socialization. Because allied states have less to fear from one another than from third parties, other things being equal, they may be more likely to engage in trade and to be receptive to the exchange of capital, technology, information, ideas and people. And as the eminent political scientist Karl Deutsch[23] argued some five decades ago, it is through such mundane material and ideational flows that political communities may be forged.

Conclusion:

From the above discussion, it is evident that the recent trends in alliance formation leads to Institutions. It can also be interpreted that the Institutions are a form of alliance made by the states for the peaceful existence and co-operation among them for various reasons, especially the security concerns and to avoid threats.

---

[22] Checkel, J.T. (2005), 'International institutions and socialization in Europe: introduction and frame- work', International Organization, 59(4): 801–826.

[23] Deutsch, Karl W. (1957), Political Community in the North Atlantic Area (Princeton, NJ: Princeton University Press).

CHAPTER-3: HISTORY AND PURPOSE OF REGIONAL ORGANISATIONS

Introduction:

Regional cooperation is not a new phenomenon; this type of cooperation had existed since the formation of the great civilizations of the world and before the advent of international organizations. Rivers Commissions such as The Commissions of the Danube and Rhine Rivers are examples[24]. The emergence of the first international organization in the field of peace and security after the First World War not only did not cause any hindrance to the survival of regional organizations, but established a sort of the symbiosis between them (Article 21 of the Covenant of the League of Nations). Although the regional organizations were not mentioned in draft Charter of the United Nations, the governments of Latin America and the Arabic countries pressure in San Francisco conference caused the Chapter VIII of the Charter to be devoted to regional agreements[25].

Regional organizations are formed to serve the following purposes: to promote human rights and democracy, to provide security and safeguard territorial integrity of member countries, and to secure economic alliances through trade and economic cooperation for rapid development. In addition, some regional organizations are established for more general reasons, such as to preserve cultural heritage (e.g., the Arab League and Organisation of Islamic Co-operation) or to address environmental issues (e.g., the Arctic Council is organized around environmental protection of the Arctic region)[26].

Although in general parlance "regions" are considered to be contiguous geographical areas, international regional organizations are formed both with geographical contiguous and noncontiguous areas. Regional organizations based on economic, cultural, and environmental factors often conform to regional contiguity, but many of the regional organizations based on security factors have member countries that do not share borders with other member countries; that is, they are geographically noncontiguous. In addition, some regional groups

---

[24] Mahdi Haddadi, "Regional Organisations and International Peace and Security in Middle East", International Journal of Academic Research in Business and Social Sciences, March 2015, Vol. 5, No. 3; Available at: https://hrmars.com/papers_submitted/1518/Regional_Organizations_and_International_Peace_and_Security_in_the_Middle_East.pdf

[25] Ibid

[26] Karl Heinz Gaudry Sada and others, Regional Organizations, "The SAGE Encyclopedia of War: Social Science Perspectives", SAGE Publications, Inc.; 2017; available at: http://dx.doi.org/10.4135/9781483359878.n551

based on geography may exclude nations for various reasons[27]. For instance, the League of Arab States rests on geographical factors but excludes Israel, Turkey, and Iran because they are not Arab. In contrast, the Organization of the Islamic Conference (OIC) is based mainly on identity rather than geography. This entry discusses regional organizations within the framework of categorizations based on purpose, explaining the conditions that facilitated their emergence and providing examples of relevant organizations, and then examines new challenges facing regional organizations, especially in the current era of a single superpower.

Purposes

Human Rights and Democracy

The misery and devastation that World War II brought led to collective thinking and mobilization of countries against such reoccurrence and to promote democracy and human rights. Furthermore, the division of countries along ideological lines, such as the capitalist bloc and socialist bloc, and the rising Cold War between the United States and the Soviet Union further galvanized countries to come together for collective security or to align themselves with groups led by the United States or the Soviet Union. Those countries that wanted to remain equidistant from both the Soviet Union and the United States, mainly countries from the global South, created the Non-Align Movement (NAM)[28].

The first two decades or so after World War II saw the emergence of the Arab League in 1945; the Pacific Community in 1947; the Organisation of American States (OAS) in 1948; the Council of Europe in 1949; the North Atlantic Treaty Organization (NATO) in 1949; the European Union (EU) in 1951; the Australia, New Zealand, United States Security Treaty (ANZUS) in 1951; the Nordic Council in 1952; the Western European Union in 1954; the Organization of African Unity (now African Union) in 1963; and the Association of South East Asian Nations (ASEAN) in 1967.

Security

Although regional organizations based on security can be categorized in various types based on their number, funds, or military power, an important factor is the categorization based on the functions the organizations perform. On the basis of the functions, the security-based

[27] Ibid

[28] Ibid

regional organizations can be grouped into four subtypes, based on alliance, collective security, security regimes, and security communities.

The regional organizations based on alliance often aim at defense and attack using military power against a common threat—external or internal. The opponent, or enemy state or organization, is often excluded from this type of regional organization. Suitable examples of this type of regional organizations are NATO and ASEAN.

Collective security–based organizations work toward preventing and containing wars or acts of internal aggression among its members. Examples of such organizations are United Nations– based organizations as well as the African Union, OAS, and the Organization for Security and Co-operation in Europe (OSCE).

The security regime–type organizations mainly aim to regulate the use of force and acceptable types of weapons and to create transparency to overcome conflicts and build confidence among their members. Suitable examples of this type of organization are the Conventional Armed Forces in Europe (CFE) Treaty and OSCE[29].

Lastly, the security community–type regional organizations aim at persuading their members to settle conflicts without military engagement. To do so, these regional organizations encourage interactions and establish confidence-building measures among their members. The EU is a suitable example of this type of organization.

The emergence of a significant number of economic-based regional organizations since the mid-1980s can also be seen as a security response: By promoting collective economic interests, states aim to ward off wars and strife among their members[30].

Economic Cooperation and Development

While during and after World War II, security, human rights, and democracy were of primary importance in creating regional organizations, by the end of the 20th century and with the end of the Cold War, regional grouping for trade and economic cooperation became a prime concern. This gave birth to the Economic Cooperation Organization in 1985, the South Asian Association for Regional Co-operation in 1985, the Asia Pacific Economic Cooperation in 1989, the Central European Initiative in 1989, the Arab Maghreb Union in 1989, the Central

[29] Ibid

[30] Ibid

American Integrations System in 1991, the South African Development Community in 1992, the North American Free Trade Agreement in 1994, the Common Market for Eastern and Southern Africa in 1994, the ASEAN Regional Forum in 1994, the ASEAN Plus Three in 1997, the Central African Economic and Monetary Community in 1998, the Community of Sahel- Saharan States in 1998, and the East African Community in 1999.

Even further new subgroups formed within the larger regional groups for economic cooperation. This new regionalism, led by economic aspirations in the post–Cold War period, became quite prominent and is very much reflected in the formation of ASEAN Plus Three, the Central European Initiative, and the Central African Economic and Monetary Community.

The two decades of relative peace at the international level after World War II and changing international politics from war to development galvanized many states to group together into regional organizations and work collectively toward development. Prior to the mid-1980s, before the neoliberal economic policy focusing on free market and economic development was dominant, several regional organizations had already emerged for economic cooperation and development. Some of these were the Council of Arab Economic Unity, which emerged in 1964; the Andean Community of Nations, or Andean Pact (1969); the Pacific Islands Forum (1971); the Caribbean Community (1973); the Mano River Union (1973); the Economic Community of West African States (1975); the Latin American Integration Association (1980); and the Gulf Cooperation Council (1981).

Conclusion:

Regional organizations are increasingly facing and adapting to new challenges, such as environmental issues, climate change, terrorism, violence by nonstate actors, energy security, prevention of proliferation of weapons of mass destructions, crime, and drug trafficking. Although regional organizations work as democratic decision-making bodies to resolve territorial and larger security and economic issues, there remain many issues—internal democracy, coercion within states, hegemonic relations with other organizations, inability to expand or contract as needed, and shifting of conflict from stronger regional organizations to weaker nonmember nations—that need to be resolved. Weaker nations have often become victims of conflict between powerful organizations and nations—examples of such victim nations include Vietnam and Afghanistan.

CHAPTER-4: CONCEPT OF SECURITY

Introduction:

Security is an inherently contested concept, encompassing a wide variety of scenarios, and is commonly used in reference to a range of personal and societal activities and situations.

Security can be distinguished between day-to-day security at the individual level (nutritional, economic, safety), security for favorable conditions (the rule of law and due process, societal development, political freedom), and security against adverse conditions or threats (war and violence, crime, climate change).

The term security is used in three broad segments. The first is the general, everyday use of the term. In this instance, security refers to the desire for safety or protection. Second is the usage of the word for political purposes; relating to political processes, structures, and actions utilized to ensure a given political unit or entity is secure. The term "security" is frequently used as a political tool to assign priority to a given issue or perceived threat within the broader political realm.

Third, and finally, "security" can be employed as an analytical concept to identify, define, conceptualize, explain, or forecast societal developments such as security policy, institutions, and governance structures[31].

Politically speaking, the usage of the term "security" increased drastically in the second half of the twentieth century. Following the allied victory that ended World War II, the United States government's military and intelligence institutions underwent a major restructuring.

A Shifting International Security Landscape

After the Soviet Union collapsed, the international landscape changed fundamentally. The previously bipolar world order was restructured under as a unipolar order. The United States, being the sole remaining superpower, was ideally positioned as the global hegemon.

A new international security framework was required when the Cold War ended. The previously bipolar international system became replaced by a unipolar global order dominated by the United States. Globally, the odds of a major war between two great powers were increasingly low. From the 1990s through the first decade of the twenty-first century, major

[31] Joshua Ball, What is Security? Everything, Global Security Review, 2019; available at: https://globalsecurityreview.com/what-is-security-everything/

conflicts were asymmetrical. The United States and its allies, with or without a mandate from the UN Security Council, employed the use of force multiple times arguing that they were doing so on behalf of the international community.

Some actions, such as the first Gulf War and the U.S.-led invasion of Afghanistan in 2001, enjoyed broad support from the international community. The only time (to date) that Article 5 of the NATO charter has been enacted was following the September 11, 2001, terrorist attacks. These operations were authorized by the United Nations Security Council, which has the responsibility of acting on behalf of all UN member states in matters of global security. The threat of significant conflict between two sovereign states substantially dissipated, for a time.

Security is Everything[32]

With a return to great power competition, national security priorities are shifting. States, rather than non-state actors like terrorist groups or insurgencies, are the primary security threat. The idea that security encompasses more than military and defense issues alone has returned, particularly in light of threats posed by rising nationalism and hostile foreign information operations. The security paradigm of the twenty-first century has expanded to nearly every facet of human life.

Rising nationalism is driving ontological and societal insecurity. This trend is fueled, in part, by economic inequality and stagnation, coupled with an influx of migrants and refugees fleeing violent conflicts, humanitarian disasters, and economic hardship. Unless Western societies implement substantial reforms for integrating immigrants and refugees, existing social divisions will widen, damaging the legitimacy of democratic institutions and polluting national identities with xenophobic sentiments.

There is also growing concern over gang violence, radicalization, transnational crime, privacy threats, and human rights violations worldwide. These issues all impact individual or personal security, and the widespread use of social media and other mass-communications technologies only serve to heighten the emphasis individuals and societies place on individual security.

[32] Ibid

Issues like climate change and pollution are also increasingly regarded through a security lens. These issues jeopardize human security, meaning they pose a threat to both individuals and humanity as a species.

Finally, cyberspace presents a whole host of new security threats. Cyber attacks not only compromise personal data and steal information, they can cause physical destruction, as well. Critical infrastructure like communications, power plants, water treatment centers, and oil refineries are all vulnerable to a debilitating cyber attack. Such an attack could disrupt operations, inflict sabotage, and even destroy the target facility. Cyber operations can be used by state and non-state actors to complement or augment kinetic operations to achieve a political goal. This is exemplified by Russia's invasion of Eastern Ukraine.

In the twenty-first century, the concept of security is all-encompassing. The geopolitical element of great-power competition is further exacerbated by a transnational cyberspace, rapidly developing and increasingly accessible technologies, alongside a global economic system which has created complex inter-dependencies between states. In this new order, the traditional security debate between those who see it as a military and defense matter, and those who subscribe to the broader perspective that everything is security.

CHAPTER-5: INTRODUCTION TO CYBERSPACE, CYBERCRIME AND CYBERSECURITY

Internet is among the most important inventions of the 21st century which have affected our life. Today internet have crosses every barrier and have changed the way we use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, greet your friend on his birthday/ anniversary, etc. You name it, and we have an app in place for that. It has facilitated our life by making it comfortable. Gone are the days when we have to stand in a long queue for paying our telephone and electricity bills. Now we can pay it at a click of a button from our home or office. The technology have reached to an extent that we don"t even require a computer for using internet. Now we have internet enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7[33].

Not only internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost effective. It was not long back, while making an ISD or even a STD call, the eyes were stricken on the pulse meter. The calls were very costly. ISD and STD were used to pass on urgent messages only and the rest of the routine communication was done using letters since it was a relatively very cheap. Now internet have made it possible to not only talk but use video conference using popular applications like skype, gtalk etc. at a very low price to a level where a one hour video chat using internet is cheaper that the cost of sending a one page document from Delhi to Bangalore using speed-post or courier service. Not only this, internet has changed the use of the typical devices that were used by us. Television can be used not only for watching popular tv shows and movies but can be used for calling/ video chatting with friend using internet. Mobile phone is not only used for making a call but viewing a latest movie. We can remain connected to everyone, no matter what our location is. Working parents from office can keep eye on their children at home and help them in their homework. A businessman can keep eye on his staff, office, shop, etc with a click of a button. It has facilitated our life in more than one way. Have you ever wondered from where this internet came? Let us discuss the brief history of internet and learn how this internet was invented and how it evolved to an extent that now we cannot think of our lives without it.

Introduction to Cybercrime:

[33] Jeetendra Pande, Introduction to Cyber Security, Uttarakhand Open University, 2017; Available at: https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

The internet was born around 1960‟s where its access was limited to few scientist, researchers and the defence only. Internet user base have evolved expontinanlty. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980‟s the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widespread beacouse internet was only comfined to defence setups, large international companies and research communities. In 1996, when internet was launched for the public, it immeditly became populer among the masses and they slowly became dependent on it to an extent that it have changed their lifestyle[34]. The GUIs were written so well that the user don‟t have to bother how the internet was functioning. They have to simply make few click over the hyber links or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or wether the data can accessed by another person who is conneted to the internet or wether the data packet sent over the internet can be snoofed and tempered. The focus of the computer crime shifted from marely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are incresing at a rapid pase. Every second around 25 computer became victim to cyber attack and around 800 million individuals are effected by it till 2013[35]. CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around $160 million are lost per year due to cyber crime. This figure is very conservative as most of the cases are never reported.

Accoring to the 2013-14 report of the standing committee on Information Technology to the 15th Lok Sabha by ministry of communication and information technology, India is a third largest number do Intrernet users throughout the world with an estimated 100 million internet users as on June, 2011 and the numbers are growing rapidly. There are around 22 million broadband connections in India till date operated by around 134 major Internet Service Providers(ISPs).

Meaning of Cybercrime:

The term cyber crime is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand

[34] Ibid

[35] Ibid, page 15

alone or a part of a network are used as a tool or/and target of criminal acitivity. It is often commited by the people of destructive and criminal mindset either for revenge, greed or adventure[36].

Classification of Cyber Crimes[37]

The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

Insider Attack: An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparitively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and wealness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when a employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vernability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.

External Attack: When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information.An expreicend network/security administrator keeps regual eye on the log generated by the firewalls as extertnal attacks can be traced out by carefully analysinig these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company

---

[36] Ibid, page-16

[37] Ibid

wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

Unstructured attacks: These attacks are generally performed by amatures who don‟t have any predefined motives to perform the cyber attack. Usually these amatures try to test a tool readily available over the internet on the network of a random company.

Structure Attack: These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems(IDSs). Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

What is Cyber Security?

Today an individual can receive and send any information may be video, or an email or only through the click of a button but did s/he ever ponder how safe this information transmitted to another individual strongly with no spillage of data? The proper response lies in cybersecurity. Today more than 61% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cybersecurity has become a most recent issue[38]. The extent of cybersecurity does not merely restrict to verifying the data in IT industry yet also to different fields like cyberspace and so forth. Improving cybersecurity and ensuring that necessary data systems are vital to each country's security and financial prosperity.

Creating the Internet safer (and safeguarding Internet clients) has become to be essential to the improvement of new management just as a legislative strategy. The encounter against cybercrime needs an extensive and more secure practice[39]. The particular estimates alone cannot keep any crime; it is essential that law authorization offices are allowable to investigation and indict cybercrime efficiently. Nowadays numerous countries and

---

[38] Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.

[39] Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

administrations are compelling strict rules on cyber safeties to keep the loss of some vital data. Each should be equipped on this cybersecurity and save themselves from these increasing cybercrimes.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure[40]. It alludes to a lot of exercises and measures, both specialized and non-specialized, expected to ensure the bioelectrical condition and the information it contains and transports from all possible threats. This research aims to gather all the information and overview related to cyber-crime and provide the historical facts and perform reports on the analyzed data of different attacks reported everywhere in the last five years.

Trends of Cyber Security[41]

Cyber Security assumes a critical role in the area of data technology. Safeguarding the data have become the greatest difficulty in the current day. The cybersecurity the main thing that raids a chord is cybercrimes which are increasing tremendously step by step[42]. Different administrations and organizations are taking many measures to keep these cybercrimes. Additional the different measures cybersecurity is as yet an enormous worry to numerous. Some main trends that are changing cybersecurity give as follows:

Web servers and Mobile Networks

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications[43]. Web servers are mainly the pre-eminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an

---

[40] Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.

[41] Rohit, KALAKUNTLA and others, Cyber Security, HOLISTICA Vol 10, Issue 2, 2019, PP. 115-128;

[42] Samuel, K. O., & Osman, W. R. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.

[43] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-

additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

Encryption

It is the method toward encoding messages so programmers cannot scrutinize it. In encryption, the message is encoded by encryption, changing it into a stirred-up figure content. It commonly completes with the use of an "encryption key," that demonstrates how the message is to encode. Encryption at the earliest reference point level secures information protection and its respectability[44]. Additional use of encryption obtains more problems in cybersecurity. Encryption is used to ensure the information in travel, for instance, the information being exchanged using systems (for example the Internet, online business), mobile phones, wireless radios and so on.

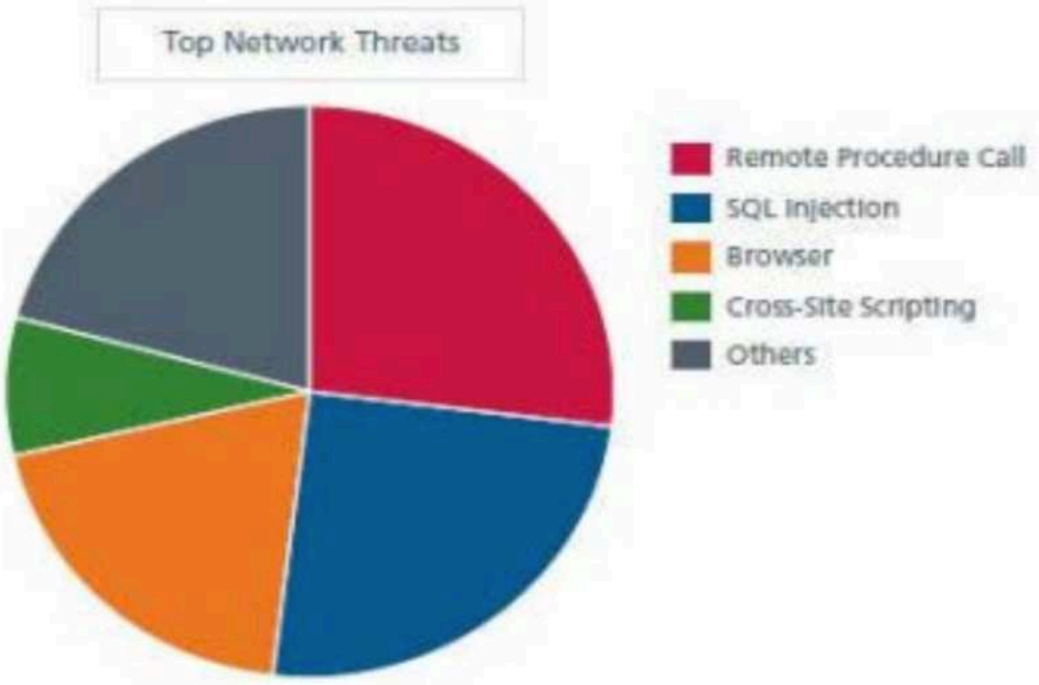
ADP's and targeted attacks

Advanced Persistent Threat (APT) is a whole of the dimension of cybercrime ware. For quite a long time network security capacities. For example, IPS or web filtering have had a key influence in distinguishing such focused-on assaults[45]. As attackers become bolder and utilize increasingly dubious methods, network security must incorporate with other security benefits to identify assaults. Thus, one must recover our security procedures to counteract more dangers coming later on. Subsequently the above is a portion of the patterns changing the essence of cybersecurity on the planet. The top network threats are showing in figure 1.

[44] Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).

[45] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-

Figure 1. Threats for Cyber Security



CHAPTER-6: INTERNATIONAL INSTITUTIONS RELATING TO CYBER SECURITY: AN OVERVIEW

Institutional "ecosystem": a baseline[46]

Building a "baseline" for cyber security institutions in international relations is particularly daunting given the trajectory of evolution for the cyber domain.

To begin with, cyberspace was constructed by the private sector – albeit with the support and direction of the dominant power in world politics, the United States. The state system formally defined in cyberspace is a relatively recent development; the entire cyber domain is managed by non-state entities, an important aspect of scale and scope in international relations.

Second, the usual mechanisms for tracking activities in the physical world – statistics, standards, measurements, etc. – are not automatically conducive to "virtual' traces or counterparts.

Third, the very nature of the "virtual" contradicts that which is physical. Threats in the "virtual" domain are often identified after the fact, rather than tracked "in process." In the cyber domain, there is not only no early warning system; there are as yet few early signals of a cyber-threat, if any.

The broad institutional domain presented in Table 1 provides a baseline view of the cyber security "institutional ecosystem" is a complex assortment of national, international, and private organizations. Parallel to the organic fashion in which cyberspace itself developed, these organizations often have unclear mandates or possess overlapping spheres of influence. Our purpose here is only to highlight these major entities and, to the extent possible, to signal their relationships and interconnections, compiling something of a census of institutions. A secondary, but also important, objective is to explore data quality and the extent to which we may infer organizational performance from public metrics, creating a performance assessment of sorts.

In the research catalogue many of the major institutional players in this aspect of cyber security, the researcher do not claim to provide an exhaustive "census." The researcher used

---

[46] Nazli Choucri and others, Institutions for Cyber Security: International Responses and Data Sharing Initiatives, Working Paper CISL# 2016-10, Massachusetts Institute of Technology Cambridge, Available at: http://web.mit.edu/smadnick/www/wp/2016-10.pdf

two criteria for the selection of institutions, namely, (a) data provision of public qualitative or quantitative data in each of our areas of focus (international, intergovernmental, national, non-profit, and private sector) and (b) coordination responsibility based on formal mandates issued by recognized international or national bodies.

Table-1: International Institutional Ecosystem

Institution	**Role**	**Data Availability**	**Example variables (if applicable)**
CERTs			
AP-CERT	Asian regional coordination	High	Collation of security metrics from member CERTs in Asia
CERT/CC	Coordination of global CERTs, especially national CERTs	Moderate	Vulnerabilities catalogued, hotline calls received, advisories and alerts published, incidents handled
FIRST	Forum and information sharing for CERTs	Low	Secondary data from conferences and presented papers
National CERTs (e.g. US- CERT)	National coordination; national defense and response	High	Varies -- volume of malicious code and viruses, vulnerability alerts, botnets, incident reports
TF-CSIRT: Computer Security Incident Response Teams	European regional coordination	N/A	N/A
ISACs			

Critical Infrastructure Sector-focused ISACs	Collect, analyze and disseminate actionable threat information	Moderate	Operation Centers collect, catalogue and share threat information and vulnerabilities with members; Some industry best-practices presented, newsletters summarizing ongoing activities for members
National Council of ISACs	Collaborate and coordinate cyber and physical threats and mitigation strategies among ISACs	Low	Secondary data from conferences and testimonies
International Entities			
CCDCOE: Cooperative Cyber Defense Centre of Excellence	Enhancing NATO's cyber defense capability	Low	Secondary data from NATO member states on individual cyber security strategies and legislation
Council of Europe	International Legislation	Moderate	Legislation and ratification statistics; secondary data from conferences and presented papers
EU: European Union	Sponsors working parties, action plans, guidelines	N/A	N/A
ENISA: European Network and Information Security Agency	Awareness-raising, cooperation between the public and private sectors, advising the EU on cyber security issues, data collection	Low	Awareness-raising stats, spam surveys, regional surveys, country reports. Qualitative data assessing the EU cyber security sphere
G8: Subgroup on High- Tech Crime	Sponsored 24/7 INTERPOL hotline, varioujs policy guidelines	N/A	N/A

IMPACT	Global threat response center, data analysis, real- time early warning system	N/A	N/A
INTERPOL	Manages 24/7 hotline, trains law enforcement agencies, participates in investigation	N/A	N/A
ITU	Sponsors IMPACT. Global Cybersecurity Index. Organises conferences, releases guidelines and toolkits, facilitates information exchange and cooperation	Moderate	Internet Usage and penetration statistics; publishes cyber wellness profiles of countries and a global cybersecurity Index to promote information exchange. Publishes secondary data from conferences and presented papers.
NATO	Responding to military attacks on NATO member states	N/A	N/A: Classified
OECD	Develops policy options, organises conferences, publishes guidelines and best practices	Low	Secondary data from conferences and presented papers
UNODC: United Nations Office of Drugs and Crime	Promotion of legislation, training programs, awareness, enforcement	N/A	N/A
UNODA: United Nations Office of Drugs and Crime	Issuance of information security reports	Low	Publishes country views of information technology trends in cybersecurity

WSIS	Global summit on information security; publishes resolutions and monitors implementation through stock-taking efforts	Low	Stock-taking database and secondary data from conferences and presented papers
OAS: Organisation of American States	Supports efforts to fight cyber crime; strengthen cybersecurity capacity of member states	Low	Publishes reports and methods to respond to incidents
US national entities			
NSA: National Security Agency	Shares Director, Admiral Michael Rogrs, with US CYBERCOM; Specialises in cryptology services and research	N/A	N/A: Classified
CIA: Central Intelligence Agency	Defence of intelligence networks, information gathering	N/A	N/A: Classified
DHS	Protection of federal civil networks and critical infrastructure; information sharing and awareness; coordinating federal response and alerts	Moderate	Data released through US-CERT; National Vulnerability Database; Automated Indicator Sharing initiative through the National Cybersecurity and Communication Integration Centre (NCCIC)

DoD: Department of Defence	Defence of military networks, counterattack capability	N/A	N/A: Classified
DOJ: US Department of Justice	Federal prosecution	Moderate	Non-aggregated data: prosecuted cases, crime by industry
FBI	Federal investigation	Low	Total reported incidents, number of referrals to law enforcement agencies, Annual surveys on corporate computer crime incuding type and frequency of attacks, dollar loss, attack source
CTIIC: Cyber Threat Intelligence Integration Center	Investigating foreign cyber threats	N/A	N/A: Classified
DoS: Department of State	Promotion of an open, interoperable, secure, and reliable information and communications infrastructure	Low	Office of Coordinator for Cyber Issues publishes testimonies, speeches, and cyber policy strategy reports
FTC	Consumer protection	Low	Publishes best practices and other advisory guides
IC3	Cybercrime reporting and referral center	High	Total complaints, referred complaints, estimated dollar loss, complaints by industrial sector
NW3C: National White Collar Crime Center	Provides training and support to law enforcement agencies, helps administer the IC3 with the FBI	N/A	N/A: statistics released through IC3

FSSCC: Financial Services Sector Coordinating Council	By DHS mandate, identifies threats and promotes protection to protect financial secotr critical infrastructure assets	N/A	N/A
Secret Service	Investigation of economic cyber crimes	N/A	N/A
US-CERT	Defense of federal civil networks (.gov), information sharing and collaboration with private sector	Moderate	Incidents and events by category, vulnerability reports
DOE: Department of Energy	Assists energy sector asset owners by developing cybersecurity solutions for energy delivery systems	Moderate	Publishes models to help organizations enhance cybersecurity capabilities; issues guidance, reports, risk mitigation plans
ISAOs: Information Sharing and Analysis Centers	Information sharing organizations to facilitate public-private exchanges	N/A	N/A
Non-US national entities (frequent collaborative partner)			
GCHQ: Government Communications Headquarters(UK)	One of three of Britain's intelligence agencies responsible for information assurance and cryptology; Britain's leading authority on cyber security	N/A	N/A
National Cyberdefense Centre (Germany)	Agency for cyber security in Germany; responds to repots of cyber attacks on critical infrastructure	N/A	N/A

National Police Bureaus (e.g. Taiwan, South Korea, Japan, France)	Investigation and enforcement	Varies	Cases, arrests, prosecutions, demographics
Center for the Protection of National Infrastructure (UK)	Provide advice on physical security, personnel security and cyber security/ information assurance to critical national infrastructure entities	Moderate	Publishes reports, case studies on attacks, best practices, and research
Non-profits			
GICSR: Global Institute for Security and Research	Conducts R&D with industry leaders, public-private sector, and academia to develop policy and strategy for cyberspace	N/A	N/A
Internet Society	Non-technical branch of Internet Engineerign Task Force; provides leadership in addressing policy issues that confront the future of the Internet	N/A	N/A
Cyber Watch	Develops educational programs and cirriculum to train next generation of cyber security experts	N/A	N/A

CAIDA: Cooperative Association for Internet Data Analysis	Gathers Data that will increase situational awareness of Internet topology structure, behavior, and vulnerabilties	High	Graphs and visuals of Internet traffic patterns
NERC: North American Electric Reliability Corporation	Assures the reliability of the bulk power system in North America.	Moderate	Publishes reliability standards; coordinates with Electricity ISAC; conducts GridEx security exercise
The Honeynet Project	Investigates attacks and develops open source tools to improve Internet security	low	Publishes reports and holds annual security workshops
The SANS Institute	Develops, maintains, and makes available a collection of research documents about various aspects of information security; operates the Internet's early warning system - the Internet Storm Center.	Moderate	Publishes reports, trainings, enterprise solutions, and webcasts on threats, vulnerabilities, and tools to improve security
Center for Internet Security	Provides resources to enhance the cyber security readiness and response of public and private sector entities; fosters collaboration between communities	Low	Publishes annual reports, intelligence advisories; hosts MS-ISAC

Internet Security Alliance	Multi-sector international trade association focused on advancing the development of a sustainable system of cyber security, and increase awareness	Moderate	Publishes policy reports, books, and blogs on APTs, cyber risk, mobile security, supply chains, and insider threats; promotes information sharing programs with government and private sector
International Association of Cryptologic Research	Researches cryptology	Low	Secondary data from conferenes and workshops and presented papers
ISRA: Information Security Research Association	Security research and cyber security awareness activities	Low	Hosts forums for discussing and sharing information on vulnerabilties, forensics, malware, cryptography, informationa security management
CSA: Cloud Security Alliance	Researches and promotes awareness of best practices to ensure a secure cloud computing environment	Low	Educational opportunities an certifications; publishes research and secondary data from working groups
Cyber Threat Alliance	Share threat information to improve defenses against advanced cyber adversaries across member organizations	Moderate	Cryptowall Dashboard with detailed data on threats, IPs, URLs, SHA256s
Private Sector			

MacAfee	Industry leader in antivirus software; computer security services	Moderate	White Papers
Raytheon	Cyber security solutions division offeres wide arrange of information assurance services	N/A	N/A
Lockheed Martin	Defense contractor that supplies consulting, training and solutions for many governmental cyber security G&S and for private institutions	N/A	N/A
Kapersky Labs	World leading cybersecurity company, focused on endpoint protection	N/A	N/A
FireEye/Mandiant	Cyber security endpoint solutions and consulting leader	Low	Publishes threat intelligence reports
Ponemon Institute	Research on privacy, data Moderate protection and information security policy; strategic consulting	Moderate	Publishes research studies and white papers
Arbor Networks	DDoS and advanced threat protection services	-	Publishes threat briefings, data visualization attack map, data from ATLAS global threat monitoring system, annual security report, whitepapers,and data sheets; holds webinars and briefs

Facebook	Sponsors ThreatExchange, a platform for sending and receiving information about cyber threats for developers	Low	Educational videos and product documents;ThreatExchange platform
Microsoft	Security division provides annual reports and worldwide infection and encounter rate maps	Moderate	Publishes white papers
IBM Security	Division of IBM that offers security intelligence, integration, expertise, and R&D to protect against cyber security threats	Moderate	X-Force Exchange platform for community collaboration, information sharing on cyber threats and vulnerabilities; publishes annual threat intelligence report
Red Tiger Security	Investigates cyber attacks	N/A	N/A
International Computer Security Association	Specializes in antivirus, anti- spam, and firewall services among a wide array of other cyber security services	Moderate	Graphs of which countries sent the most spam per week
Palo Alto Networks	Network and enterprise security with specialization in firewalls	N/A	N/A
Verizon	Enterprise security solutions, products, and services	High	Publishes annual data breach investigations and compliance reports, solutions briefs, and fact sheets

CHAPTER-7: GLOBAL CYBERSECURITY ECOSYSTEM

Introduction:

According to Steve Purser of ENISA, 'International collaboration is essential. Security within national boundaries doesn't make sense. Everything is globally connected. A European approach doesn't make sense unless aligned to the approach of international partners' (SDA Report 2012). Thus the EU's construction of its cybersecurity ecosystem is embedded within, bounded by, and inexorably connected to the evolving global ecosystem of cybersecurity governance, and more broadly, Internet governance. The EU has emphasised in its Internal Security Strategy (November 2010) and the European Guidelines and Principles for Internet Resilience document (March 2011) the importance of working in partnership with global partners to address the civilian and military aspects of cybersecurity challenges. The global interconnectedness of the Internet ecosystem means that threats can emanate from any source around the world, which in turn requires solutions and policies that are borderless. The vulnerability of the Internet, and the interdependence between networks, information systems and individuals, makes it impossible for any single actor to assess and respond to cyber threats and risks. Moreover, national responses alone cannot be effective given the integration between electronic, economic and political networks across the globe, and in order to achieve this there must be a step-change in the coordination of approaches not only downwards, but also upward and outward to institutions, networks and actors, technical and political, that have a role to play in constructing security resilience within the many different aspects of cybersecurity.

This chapter will therefore provide an overview of the prominent global and regional institutions, networks and actors involved in the security of resilience in cyberspace, and an assessment of the logics that are at play within the emerging ecosystem. Moreover it will assess how 'best practice' in cybersecurity, recommended or institutionalised in one way or another (through code, practice or law) at different levels, has been adopted by other actors, as a basis for understanding EU cybersecurity policy in the proceeding chapters. Whilst the EU has clearly been active across several fora, platforms and bilateral relationships, including the UN Group of Experts tasked to construct norms for cyberspace and the Organisation for Security and Cooperation which has designed confidence building measures, this chapter will only implicitly analyse the EU's role within different institutions, as this will be done more

explicitly in relation to specific policy areas and the EU– US relationship in the chapters that follow. The ambition here is simply to provide a context, through conceptually informed assessment of what approaches (or debates) are emerging in the complex global Internet and cybersecurity landscape, in order to provide an understanding of the possible influences on the EU's emergent ecosystem of security governance in cybersecurity. The focus, for this purpose then, will be on the key actors and organisations involved in constructing a resilient governance ecosystem for cybersecurity and in particular, on what sorts of logics of resilient governance are emerging. Indeed, a primary aim of the chapter, is to uncover the extent to which there is convergence or divergence in the approaches advocated by key global players, and what this, in turn, implies for the EU in its approach and emerging strategy on Internet security.

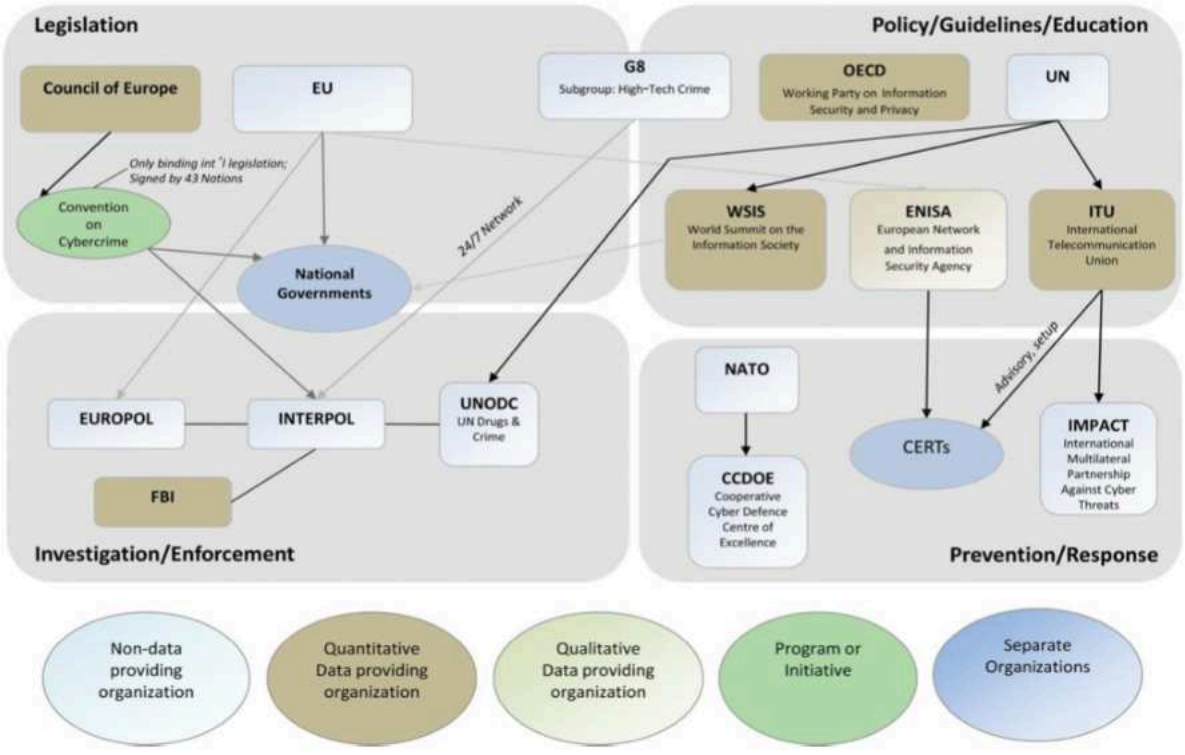


Figure 2. Key Intergovernmental Institutions

Internet governance and cybersecurity

ICANN

ICANN has responsibility for three critical Internet functions: the allocation of Internet Protocol number resources for individual computers and machines; their corresponding

Domain Name Service names; and, the allocation of top-level domains (TLDs) to registries that assign identifiers to individual users and organisations globally. These three functions and how they evolve have important implications for Internet security, and the governance approach that underpins the Internet and its security. Important here, in the context of resilient security governance, is the challenge to self-regulation, which has been the dominant approach for managing Internet names and addresses since ICANN was established in 1998 as a not-for-profit, public benefit corporation, under- pinned by California law. ICANN was founded on pre-existing technical organisations, with the purpose of exposing the Internet to public and private commerce[47]. As the Internet has grown and evolved, so too has the role of ICANN, often through processes of internal reflection and review as well as external criticism and pressure. Moreover, as the issue of domain names has become more important, in a strategic sense, national governments as well as the EU have called for and, to a certain degree, secured a more active role in the formation of ICANN policy through the Government Advisory Council (GAC)[48]. They have also exerted pressure on the US government with regard to the issue of accountability and influence – ICANN was originally contracted to the US Department of Commerce, with a very strong US influence on policy and its direction. Whilst this situation changed in 2009, under a new agreement, the Affirmation of Commitments (AoC), the issue of representation, influence and accountability are far from resolved. Furthermore, the strategic importance of domain names at national level has seen the strengthening of national registries to manage security and other issues related to their country code top-level domain (ccTLD). These trends, alongside increasing technical developments have resulted in challenges for ICANN, in particular in the security realm, which it has sought to respond to. Perhaps not surprisingly, this has also had implications for the nature of resilient security governance evolving for domain names and numbers (European Parliament 2011), and more specifically, has undermined the self-regulatory principle that has underpinned Inter- net governance since its inception given the perceived 'public good' dimension attached to cybersecurity issues.

---

[47] Klimburg, A. (2011b), 'Ruling the Domain: Self-Regulation and the Security of the Internet', Austrian Institute of International Affairs, Paper Distributed at the 11th Meeting of the ICANN Studienkreis, 28/29 April 2011.

[48] Christou, G. and Simpson, S. (2007), The New Electronic Marketplace: European Governance Strategies in a Globalising Economy, London: Edward Elgar.
Christou, G. and Simpson, S. (2011), 'The European Union, Multilateralism and the Global Governance of the Internet', Journal of European Public Policy, 18(2), 241–257.

ICANN's role in the security of domain names and numbers has manifested itself through three main issues at policy and technical level: Domain Name System Security Extensions (DNSSEC2), Internet Protocol version (IPv), and related to the privacy of data, the WHOIS information database. The issue of security for the Domain Name System (DNS) arose after security researcher, Dan Kaminsky, found a critical vulnerability in the DNS system in the summer of 2008. The DNS, basically, translates domain names that humans can remember for example, www.europa.eu, into the numbers used by computers (Internet Protocol (IP) addresses) to look up its destination within different levels of the directory service (each level managed by different entities for example, ICANN manages the first level or 'root zone'). What the Kaminsky incident exposed is the ability of any attacker to hijack the DNS process within any given level (in what is often termed as DNS cache poison- ing or spoofing). Such spoofing allows attackers to 'take over control of a session to, for example, direct users to their own deceptive websites' (ICANN, DNSSEC, Fact Sheet 2011), where the user can enter confidential passwords and account details, or potentially be subject to attack through inadvertently downloading malicious software. There are also more serious variants of such attacks, whereby they are not localised but rather globalised redirections of Internet traffic. The classic case here is the case of the rogue Chinese name server that hijacked up to 10% of the Internet, routing it through China and subverting a proportion of the world's information flow to the automated web censorship regime in China[49].

The DNSSEC solution, which was operationalised in July 2010, is intended to counter the more serious threats rather than simply the spoofing, even though both have significant implications for security. At a basic level, it works through digitally 'signing' data (it does not encrypt data) so that users can be assured of its validity. In order for this technology to work effectively, however, it must be deployed at each level of the look up process from root zone (managed by ICANN) to domain name (for example, dot eu managed by the EURID registry). In effect then, such a system rests upon the notion of 'trust anchors' to provide valid information at different levels (generic, national, sub- national and so on), and this is where problems may arise, which have implications for the resilience of the security governance provided by DNSSEC.

[49] Klimburg, A. (2011b), 'Ruling the Domain: Self-Regulation and the Security of the Internet', Austrian Institute of International Affairs, Paper Distributed at the 11th Meeting of the ICANN Studienkreis, 28/29 April 2011.

At a technical level, the threat of denial-of-service attacks would not be eradicated by DNSSEC, and might potentially make them more effective given that servers would be working with an increased workload[50]. There is also the potential of contamination of the system through the spreading of false DNS information if ccTLD registries misidentify local trust anchors[51]. Furthermore, at a policy and governance level it is reliant on a commercial logic, which treats some of the symptoms, but is corrective rather than antidotal in nature. More specifically, although it allows the management of some risk in the form of spoofing and more severe hijacking of the DNS, even this is reliant on a cost-benefit calculation, in particular with regard to the management and administration of DNSSEC. This is especially problematic for smaller ccTLD registries and registrars, but also those in less advanced countries where DNSSEC implementation is not even on the agenda[52]. The problem is not just at the micro level, however. Indeed, the way in which DNSSEC is managed and governed at a macro-level by ICANN is not conducive to constituting a shared logic of action in the short term – in particular as it is reliant on voluntary compliance and 'crisis' to incentivise action among the stakeholders involved. Whilst there is no immediate solution to this, and many more registrars have signed up to DNSSEC since its introduction moving to a mandatory – more hands-on meta-governance approach – could potentially incentivise many more stakeholders at different levels to implement DNSSEC. Indeed ICANN's generic TLD (gTLD) programme did this this at the registry level, with this purpose in mind and the hope that it would incentivise high-security authenticated zones to enforce the protocol at the second level too[53]. Whilst there have been successful joint initiatives (for example ICANN and the Internet Society) to recruit more registries and other stakeholders to the DNSSEC initiative, not all are yet convinced of its efficacy or value in constructing a resilient DNS; additional incentives need to be provided if such actors are to think beyond the commercial logic to the longer term logic of sustainable security as resilience through the implementation of DNSSEC.

Internet Governance Forum

---

[50] Ibid

[51] Scott, M. (2010), 'With Three Months to go to DNSSEC, Someone's Fudging Root Zone Records', Betanews, March 2010. Available at: http://www.betanews.com/article/with-three-months-to-go-to-DNSSES-someones-fudging-root-zone -records/1269642342 (accessed June 2013).

[52] Mohan, R. (2011), DNSSEC Baby Steps Reported at ICANN 41, CircleID Internet Infrastructure, 29 July 2011.

[53] Ibid

The Internet Governance Forum (IGF) was established in 2005 at the second phase of the WSIS process as a multilateral, multi-stakeholder, democratic and transparent institutional forum for discussing issues of Internet governance. The IGF mandate at the WSIS Summit in Tunis (2005) stipulated that it 'would have no oversight function and would not replace existing arrangements, mechanisms, institutions, or organisations, but would involve them and take advantage of their expertise. It would be constituted as a neutral, non-duplicative and non- binding process' (WSIS, Tunis Agenda for the Information Society 2005).

Importantly, the IGF was constituted as a body that would arrive at positions through deliberation rather than make decisions, where discussions were open, free and frank on any themes seen as important for the future of Internet governance, including issues relating to child protection, cybercrime and cybersecurity. Its normative strength has been in its inclusive and bottom-up nature, and in the fact that in its first five years, it has become a forum for learning through discussion of ideas that can be utilised in policy construction and development[54].

Given its institutional nature and the broad stakeholder make-up in the IGF, it is perhaps inevitable that the logics coming from the IGF on different aspects of cybersecurity will differ in emphasis and importance. However, having said this, it is clear from analysing workshop outcomes and IGF thematic reports between 2008 and 2014 (Security, Openness, Privacy) that particular security governance themes and debates are pervasive in the context of discussing potential approaches and models. Prominent among discussions have been: first, the relationship and balance to be struck between security, privacy and openness; second, what sort of governance model is suitable and effective for regulating issues related to cybersecurity in the context of the global Internet ecosystem. On the first issue, the debate has been not simply about balance but also proportionality. In this sense the discussion has been about degrees of balance not simply between security and privacy, but between individuals as individuals and individuals as part of a larger group. The broader political and legal context, of course, relates to ensuring the security of the state without eroding or transgressing individual rights and liber- ties, thus leading to a lack of trust in the Internet ecosystem in relation to identity, and specifically, the privacy of personal data.

[54] Christou, G. and Simpson, S. (2007), The New Electronic Marketplace: European Governance Strategies in a Globalising Economy, London: Edward Elgar.

CHAPTER - 8 : MULTILATERAL ORGANISATIONS AND CYBERSECURITY

Beyond the Internet governance institutions, multilateral fora have also been active in contributing to the evolution of resilient governance for cyber threats.

The G8 group of states

The G8 has addressed cybersecurity since the Okinawa Summit in July 2000 where it committed to strengthening cooperation in order to improve access to the Internet for the poorest and protect intellectual property rights. It has supported the draft Anti-Counterfeiting Trade Agreement (ACTA) and the work of the Organisation for Economic Co-operation and Development (OECD) on the economic impact of counterfeiting and piracy (French G8–G20 Presidency 2011). The G8 view on cybersecurity and Internet governance, reflected in the Okinawa Charter for the Information Society (2000), was of the private sector playing a lead role but with a responsibility on governments to create a regulatory and policy environment that is predictable, transparent and non-discriminatory. Discussions on cybersecurity regulation and governance really came to the fore though after 9/11, even though the Lyon Group (formerly Senior Experts Group on Transnational Organised Crime) was established in 1995, and expressed the need to review 'laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalised and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect to such abuses are effectively addressed' (P8 Senior Experts Group 1996, p.4). It is claimed by Hart[55] that in governance terms, the success of the Lyon group has stemmed from the participation of private interests, even though the main work was done by the law-enforcement agencies of the G8 governments. Indeed, and ironically, the initial 'heads primarily' format of the G8 gave it the flexibility to invite nongovernmental actors to discussions on security and other issues that required a multi-stakeholder approach.

One of the important subgroups created from the Lyon Group was the G8 Sub-Group on High-Tech Crime in 19977 (subsequently expanded to include non-G8 countries), which established the Ten Principles[56] in the combat against computer crime as a platform for ensuring that criminals are suitably dealt with in legal terms (as well as an Action Plan). The

[55] Hart, A. G. (2001), 'The G8 and the Governance of Cyberspace', in Fratianni, M. (ed.) New Perspectives on Global Governance: Why America Needs the G8, Aldershot: Ashgate Publishing Limited.

[56] see G8, http://www.cybercrimelaw.net/G8.html

focus in governance terms has been on how to improve the legal environment within which to address cybercrime through further international sharing of information, cooperation and coordination between those authorities and private actors involved in enforcing criminal laws. Thus, this has not implied a sole role for public actors, but rather, the recognition that there must be cooperation between government and industry and that the industrial sector must be responsible for developing technical standards (governance) within global communications networks. Moreover there is a clear steer for the industrial sector, facilitated by the necessary legal frameworks, to develop and distribute secure systems and best practice in relation to personnel security, preserving electronic evidence, and ascertaining the location and identity of criminals (Communique, Justice and Interior Ministers of the Eight, 9–10 December 1997). On issues of mutual legal assistance and extradition, the emphasis has been on enhancing cooperation and coordination, and importantly, creating an international legal environment that is flexible enough to accommodate multi-jurisdictional cases, minimise constraints, and allow the necessary collection and sharing of evidence to prosecute cybercriminals.

The more recent discourse to emanate from the G8 on cybercrime and security supports more explicitly 'the multi-stakeholder model of Internet Governance . . . with flexibility and transparency . . . in order to adapt to the fast pace of technological and business developments and uses' (Deauville Declaration 2011). It also acknowledges the key role that governments must play in this multi-stakeholder model alongside regional and international organisations, the private sector, and civil society in order to 'prevent, deter and punish the use of ICTs for terrorist and criminal purposes'.

Indeed there is an emphasis on all stakeholders, with governments, it seems, playing a key steering and facilitating role, to 'develop norms of behaviour and common approaches in cyberspace' that embed within them the proportionate balance between security and privacy/ individual rights. On intellectual property infringements and personal data specifically, the G8 positions again reflect the logic of the multi-stakeholder model, with governments creating the regulatory environment for action and implementation and the private sector at the forefront of driving initiatives. There is also, again, an emphasis on international cooperation and a 'common' approach based on consideration of national 'legal' frameworks and the right balance between individual rights and sharing personal data. Importantly and within the multi-stakeholder logic the G8 conclusions call for enhanced cooperation between all stakeholders (including users), and recognise the need for flexibility and transparency, to ensure

adaptability to 'the fast pace of technological and business developments'. This bodes well for creating sustainable security as resilience, even though in practice, it seems, there is no clear agreement on which 'model' is more effective.

The United Nations (UN)

The United Nations is seen by many as the ideal interlocutor and platform for fostering the necessary dialogue and cooperative climate on cybersecurity. However, it also sits at the centre of a major debate on which international organisation should address issues related to cyber – including that of security. Essentially, and to oversimplify a little, there are those, such as Russia and China (and certain Arab countries) that operate with a 'sovereign logic' on matters of cyber threat that would like to see a global treaty agreed through the UN. Others, such as the EU, UK and US, argue that the UN (and the ITU as a UN agency) is not suited to Internet governance or leading on global cybersecurity governance given the slow and cumbersome nature of the decision-making process, and the rapid pace of technological development.

Beyond this debate, however, the UN, in particular the UN Office on Drugs and Crime (UNODC), the ITU and UNESCO have contributed to raising awareness on issues of cybersecurity and cybercrime, and provided recommendations which it has encouraged its members to adapt in order to improve their national cybersecurity resilience. Importantly, the UN Group of Governmental Experts on Developments in the Field of Information and Cyber Telecommunications in the Context of International Security produced a report on cybersecurity in 2010 that provides recommendations on reducing cyber risk and protecting critical infrastructures nationally and internationally. Salient among those in governance terms was improved international cooperation between states, enhanced cooperation through measures to share 'best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability', improved collaboration between state actors, private actors and civil society with cooperative actions and measurements to support this, and finally, capacity building in order to facilitate the improvement of security of other states in order to improve ICT security globally (UN Report 2010, p.7). The UN report on cybersecurity (2010) also provided important guidance on how cyber warfare issues are related to existing principles of international law (how international law applies to cyberspace). Further than this, in 2013 the UN Group of Experts on Cybersecurity 'for the

first time at the UN level...was able to agree to an important set of recommendations on norms, rules, and principles of responsible behavior by states in cyberspace'[57]. Whilst this was no doubt an important step-change in terms of international consensus on a controversial issue which also included important recommendations on issues such as extending Confidence Building Measures (CBMs), building capacity globally and information sharing, it will rely on states embedding the central norms underpinning the agreement into practices, if a resilient and secure cyberspace is to truly emerge in the medium to long term. Evidence suggests that this is unlikely given the disagreements that still exist between states on key principles, which have only been exacerbated by the Snowden revelations in the debates and continuing work of the Group of Experts at UN level[58].

More broadly, the UN General Assembly produced five major Resolutions[59] on the issue of cybersecurity, with an emphasis on building trust in using ICTs in order to maintain and enhance the socio-economic benefits of ICTs for society. In resilient governance terms the resolutions steer towards a multi-stakeholder approach with strong legal frameworks to combat the threats of cybercrime and attacks on critical information infrastructures, and with a need for enhanced cooperation between states on these matters, as well as better coordination with all stakeholders.

International Telecommunications Union (ITU)

A fundamental role of the ITU, following the WSIS and the 2010 ITU Plenipotentiary Conference, was to build confidence and security in the use of ICTs. At WSIS, Heads of States and world leaders entrusted the ITU to take the lead in coordinating international efforts in the field of cybersecurity, as the sole Facilitator of Action Line C5, 'Building confidence and security in the use of ICTs'. In response, ITU Secretary General, Dr Hamadoun I. Touré, launched the Global Cybersecurity Agenda (GCA), which is a framework for multi-stakeholder international cooperation aimed at enhancing confidence and security in the information society.

---

[57] Volter, W. (2013), 'The UN Takes a Big Step Forward on Cybersecurity', Arms Control Today. Available at: https://www.armscontrol.org/act/2013_09/The-UN -Takes-a-Big-Step-Forward-on-Cybersecurity

[58] Meyer, P. (2013), 'Cyber Security Takes the Floor at UN', Canadian International Council, 12 November 2013. Available at: http://opencanada.org/features/the -think-tank/comments/cyber-security-takes-the-floor-at-the-un/

[59] International Telecommunications Union (ITU) (2011) National Cybersecurity Strategy Guide, ITU, September 2011.

The central tenets or pillars of the GCA are Legal Measures, Technical and Procedural Measures, Organisational Structures, Capacity Building and International Cooperation, with the aim to promote cybersecurity and maintain resilient and reliable information infrastructure[60]. In order to operationalise the GCA the ITU signed an agreement with the International Multilateral Partnership Against Cyber Threats (IMPACT), which supports, through its various Centres8 the GCA achieve its strategic goals including legal measures, organisational structures, developing strategies for the creation of a global framework for watch, warning and incident response, capacity building and international cooperation. Furthermore, ITU-IMPACT is underpinned by the 'partnership approach', with partners from Industry, Academia, International Organisations and Think Tanks. The ITU also signed a memorandum of understanding (MoU) with UNODC in May 2011 order to assist the ITU and UN members mitigate the risks posed by cybercrime. Activities have taken the form of joint assessment missions, conferences and training activities, with collaboration across the five pillars of the GCA. In line with the idea of public-private partnership, the ITU also signed an MoU with the Symantec Corporation, with the latter providing quarterly Internet Security Threat Reports in order to increase awareness of and readiness for cybersecurity risks among the ITU membership. Finally, under the GCA, the ITU launched the Child Online Protection initiative (November 2008), which has been established as an international collaborative network, providing guidance on safe online behaviour to relevant stakeholders.

In governance terms, the ITU has proposed a cybersecurity strategy model as a guide for member states to develop their own strategies[61], with an emphasis on multi-stakeholderism and coordinated local, national and global multi-sector action [62]. Within this context, the logics of this model are underpinned by the five pillars or platforms of activity already outlined above: Legal Measures, Technical and Procedural Measures, Organisational Structures, Capacity Building and International Cooperation. Indeed the justifications for such a model are argued to be strategic, social and economic in nature, even though in practice, there might be a conflict between each of these logics as demonstrated in the case of the implementation of DNSSEC.

---

[60] Ibid

[61] International Telecommunications Union (ITU) (2008a) Q.22/1 Report on Best Practices for a National Approach to Cyber Security: A Management Framework for Organizing National Cybersecurity Efforts (2008), ITU-D Secretariat, January 2008.

[62] International Telecommunications Union (ITU) (2008) Global Cybersecurity Agenda, High level Experts Group, Global Strategic Report, ITU.

To elaborate further, it is clear that within the ITU model, there is an emphasis on governments as facilitators, even though it also argues that national governments should lead in setting any goals for cybersecurity strategy. In other words, whilst the ITU argues that all stakeholders have a role to play in elaborating and implementing strategy (from the judiciary to civil society, vendors and the intelligence community), the model does not suggest a key role for all stakeholders in the agenda setting stage. Indeed, the ITU recommends 'that Governments focus on setting the agenda and the conditions for all stakeholders to work together' with the agreed strategy then providing a platform for cooperation at all levels[63]. In terms of monitoring the effectiveness of the strategy, in governance terms, it is reflective of a classic regulatory state approach, that of appointing an independent agency. At a basic level it advocates a multi-pronged governance approach that includes hands-on legislation and hands-off incentives for collaboration within an overarching collaborative strategy constructed by national governments[64].

Interesting within the approach is the call for minimising bureaucracy in order to maximise flexibility and adaptability in passing legislation on cybercrime and cybersecurity[65], and establishing national security frameworks procedurally and technically as well as legally, in order to facilitate the development of common standards and solutions and a culture of cybersecurity. Importantly, it highlights the role of public-private partnerships in addressing the issue of cybersecurity given the involvement and role of different actors within the cyber sector. Indeed, on the latter, it is argued that successful collaboration between the public and private sector requires three elements:

a) A Clear Value Proposition: that all stakeholders know exactly why collaboration is necessary and what the benefits are;

b) Clearly Delineated Roles and Responsibilities: that these are agreed upon according to the overall strategy and its goals and the objectives of the stakeholders;

c) Trust: that each party trust the others' motives and ability to fulfil duties (for example, on information exchange and privacy).

---

63 International Telecommunications Union (ITU) (2011) National Cybersecurity Strategy Guide, ITU, September 2011.

64 Ibid

65 Ibid

The final elements relating to capacity building and international cooperation are cross-cutting pillars, but are nevertheless important to a sustainable and effective cybersecurity strategy, and the creation of a global culture of cybersecurity premised on a set of norms of behaviour for cyberspace. Significant here is not only capacity building in terms of the professionals involved in cybersecurity activities, but also society, and indeed in terms of research and development in technologies to support robust and resilient cybersecurity strategies.

North Atlantic Treaty Organisation (NATO)

Whilst the first distributed denial-of-service attack against NATO's Public Affairs website occurred in 1999[66] and the protection of its information and communications systems was officially placed on its political agenda at the Prague Summit in 2002, it is not until the attacks on Estonia's public and private institutions in April and May 2007 that more urgency was injected into cyber defence. The war in Georgia in the summer of 2008, also further underlined the potency of cyber tools, demonstrating the potential for them to be used as a component of conventional warfare. The use of cyber tools in this way then, and the threat that they might also pose to the Euro-Atlantic community, further underlined the urgency and need for a NATO cyber defence policy for the alliance as a whole[67] in terms of both the military and civilian aspects.

Since then NATO has done much to address the issue of cyber-attacks and highlighted the issue in its new Strategic Concept adopted at the Lisbon Summit in November 2010. NATO also adopted its new cyber defence policy in June 2011 (reaffirmed at the Chicago Summit in 2012). In parallel to the policy, a cyber defence Action Plan was agreed that will serve as the tool to ensure its timely and effective implementation. The policy offers a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber threats and building the resilience of existing networks. Among other things the policy sets the principles on NATO's cyber defence cooperation with partner countries, international organisations, the private sector and academia[68]. It also aims to bring all NATO structures under centralised protection with cyber defence being integrated into NATO's defence planning process, and outlines a framework through which it can assist, and collaborate with Allies with regard to

---

[66] Tick, E. (2010), Global Cyber Security – Thinking About the Niche for NATO, The SAIS Review of International Affairs, Fall 2010 (pre-publication).

[67] www.nato.int/cps/en/natolive/topics_78170 .htm

[68] http:// www.nato.int/cps/en/natolive/news_75195.htm

intelligence, information sharing, and security interoperability based on a common set of NATO standards. The policy highlights the need for improving the security and resilience of Allies within NATO in order to strengthen in a sustainable way, the collective cyber defence policy – given that the latter can only be as strong as its weakest link. The policy further develops new political and operational mechanisms through which such a policy can be pursued, including the establishment of a NATO Computer Incident Response Capability (NCIRC) and a Threat Awareness Cell for enhancing intelligence sharing and situational awareness. In addition, at NATO's Chicago Summit in May 2012, as part of a reaffirmation of the commitment to improve NATO's cyber defence policy, there was an agreement to bring NATO military and civilian networks under centralised protection – with the NATO Communications and Information Agency established on 1 July 2012 to facilitate this centralising process and enhance NATO's operational capability.

With regard to the institutional governance of its cyber defence policy, the North Atlantic Council provides the political oversight and takes decisions in cyber defence related crisis management. Below this, at the working level, the NATO Cyber Defence Management Board (CDMB) is responsible for the coordination of cyber defence throughout NATO's Civilian and Military bodies, and at expert level, the advice on the Alliance's Cyber Defence efforts and capabilities is offered by the Defence Policy and Planning Committee. MoUs exist between CDMB and national cyber defence authorities to facilitate sharing of information, dialogue and so on, and to inform NATO Rapid Reaction Teams on how they can support Allies in case of cyber crisis. The CDMB includes political, military, technical and operational staff that operate under the auspices of the Emerging Security Challenges division, with the NATO Consultation, Control and Command Board (NC3) the main body that is consulted on cyber defence in terms of the technical and implementation aspects. Finally, the NATO Military Authorities (NMA) and NATO Communications and Information Agency (NCI) are responsible for operational requirements, acquisition, implementation and operation of NATO's cyber capabilities, with the NCI Agency through its NCIRC Technical Centre providing technical and operational cybersecurity services throughout NATO[69]. Beyond this, NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), established in Estonia in 2008, was set up to provide and develop training and education, and conduct research on legal and policy issues in the field of cyber defence. It is linked to NATO Allied Command

[69] See, www.nato.int/cps/en/ natolive/topics_78170.htm

Transformation and serves as a useful interface between NATO military bodies, academia, and the private sec- tor. Moreover, it has a large outreach capacity, including NATO nations' cooperation with the EU. Indeed, the EU's ENISA and CoE CCD have organised joint events – sharing best practice that has emerged in the field – with this serving as a learning platform for preparedness in cyber defence issues. Moreover, the CoE CCD was also responsible for producing through the Tallinn Manual Process, the 'Tallinn Manual on the International Law Applicable to Cyber Warfare', essentially setting out rules governing cyber warfare within the international legal context[70].

What then does this all mean in terms of the security logics that underpin NATO cyber defence policy? Whilst NATO faces the same general challenges on cybersecurity as many other organisations, its focus on cyber defence (and therefore primarily protection and deterrence) means that it also faces specific challenges in terms of its evolving policy, and the governance logics that underpin it. First, it faces the task of delineating more precisely what constitutes an attack, the use of force and an act of war in cyberspace. Second, there is the issue of putting into place a governance structure that allows timely and effective action against threats through a common set of standards and laws. Third, the creation of norms of behaviour to govern cyberspace, which requires the difficult task of harmonising national strategies through common understandings, and facilitating the sharing of information and threat mitigation, which member states are not always willing to do. Finally, there is the trade-off between protecting individual liberties and collective security which also exists more generally, but has particular connotations for NATO and its cyber defence policy[71].

Whilst NATO's approach to cyber defence is certainly comprehensive at first glance, suggesting a more coordinated, collaborative and inclusive policy than previously, with new supporting structures and learning through training and education at its centre to address individual and collective resilience, it also suffers from certain deficiencies. Put another way, there are certain obstacles that need to be addressed if it is to move forward successfully towards a security as resilience approach.

---

[70] Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), Pre- pared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press.

[71] Noshiravani, R. (2011), NATO and Cyber Security: Building on the Strategic Concept, 20 May 2011, Rapporteur Report, The NATO Science for Peace and Security Programme, Chatham House.

The first of these issues is that of the responsibilities of the different actors involved – in particular at member state level. NATO's emphasis is on collaboration with national governments to achieve harmonisation of standards and information sharing, but given the nature of the ownership of critical information infrastructure and cyber activity, this relies on effective public-private partnership at national levels. Although governments can no doubt develop a regulated standardised approach, it often has very different objectives to that of private industry that operates through an economic logic, and aims to deliver value to shareholders. In this sense, the private sector is often reluctant to move in the direction of the greater regulation of cyberspace – in particular given the difficulty for multinationals in navigating and indeed standardising the current complexity of regulatory legal measures that exist across different cyber-related sectors. It is not impossible, of course, to incentivise the private sector to cooperate and coordinate in effective partnership (the Dutch model here, among others, is instructive), but this does require a common lexicon and a collective logic, as well as the issue of cybersecurity being elevated beyond the responsibility of ICT departments to the boardroom in many larger ICT companies. NATO's proposal for an Industry Cyber Partnership which members agreed on at the Cardiff Summit in 2014, aims to ensure that expertise and innovation from the private sector is exploited as much as possible in order to achieve the objectives of NATO's Enhanced Cyber Defence Policy and should go some way to addressing this issue if successful.

The second issue is that of obtaining clarity on the thresholds and standards that will apply to questions relating to: use of force in the cyber domain; when a cyber-attack can be labelled an armed attack (under Article 51 of the UN Charter and Article 5 of the Washington Treaty); what sort of action is permissible in response to a cyber-attack and which body of law applies to any such responses. Two issues are pertinent in this context. First, whilst there is much debate on this topic there is a general consensus that for a cyber-attack to be considered an armed attack it must have physical consequences – with the use of force being of a direct or indirect nature. Second, is the issue of attribution of blame in cyberspace, as the difficulty in identifying an attacker can affect the ability of states and organisations to respond in terms of timing and the relevant international legal framework, as well as the nature of any response to a cyber-attack. Whilst the Tallinn Manual has gone some way to addressing the above issues; that is, it provides a mutual point of reference for definitions of military attack, the application of international law, distinctions between civilian and military targets, and methods of

establishing which parties are or were involved in specific cyberspace conflicts it still falls short, for some, on resolving certain other salient issues. The manual, for example, does not provide clear criteria by which an attack can be defined as an act of war, arguing instead that this must be assessed case by case according to the gravity and potential effects of any decision. For Bendiek[72] 'using international law to set up rules for cyber war just makes these kinds of actions seem more doable and...there is no precedent for norms that deal with conflict below the threshold of armed assault'. In addition, the exclusion of non-NATO experts from the discussion group that constructed the rules for cyber warfare has limited not only the scope but also the potential effect of such rules. Finally, for some, the Tallinn Manual has scant regard for citizens' rights given that the broad definition of a military attack does not in principle ban governments from taking military action against non-state groups or even individual alleged hackers. From this perspective, the lines between police and military operations could become even more blurred, with ethical implications side-lined in the interests of cyber defence.

A third issue is that of international cooperation and collaboration, especially with the EU given the overlapping membership of the two organisations. Indeed NATO–EU cooperation, if coordinated effectively, can certainly facilitate the emergence of security as resilience. Given the EU's ability to implement Regulations and Directives and NATO's ability to conclude international agreements, both agencies can contribute to the emergence of common standards, laws and practices that influence the direction and nature of international norms and principles for cybersecurity. Having said this, there are many impediments to effective NATO–EU cooperation in issues of cybersecurity which includes their different mandates and thus competencies, and the Cyprus–Turkey issue, placing legal limits on their ability to cooperate formally, at least (although not informally). In addition, given that both the EU and NATO have limited (geographical) memberships, any effective cooperation struck up between the two organisations would not address the needs or indeed reflect the preferences of the 'global' community of actors that operate in cyberspace and therefore seek to secure it. The implication here then, in terms of governance at least, is that any norms and principles agreed by the two organisations, in order to have global influence and relevance, would have to engage with other important stakeholders in the cybersecurity milieu, through other new or existing fora, and including the private sector and civil society.

---

[72] Bendiek, A. (2014), 'Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection', Stiftung Wissenschaft und Politik (SWP), SWP Research Paper, Berlin, March 2014.

Organisation for Economic Cooperation and Development (OECD)

The OECD in producing information on best practice with regard to critical infrastructure resilience is a useful tool for the EU and its member states in terms of developing their cybersecurity ecosystems. The OECD Working Party on Information Security and Privacy (WPISP) produces regular reports on resilience building, privacy, and the information society. Indeed, it has an established network of experts from government, business and civil society that serve to facilitate exchanges of information between stakeholders and to monitor activities in relation to cybersecurity[73]. In this sense, its governance structure is reflective of effective partnership and its steer in terms of best practice emphasises the need for a culture of cybersecurity to emerge given the wider number of threats and risks now associated with information technology developments and increased interconnectivity.

To this end the OECD has produced a set of generic guidelines (2002) intended to facilitate the movement towards a culture of cybersecurity. The approach advocated is inclusive, with the underlying rationale that 'each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks'[74]. Moreover, it emphasises, consistent with the conditions set out in Chapter 2 for effective security as resilience, the need for guidelines to be adopted and implemented at policy and operational levels, and that 'efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy'[75]. In addition, it is argued in the report that factors such as leadership, in particular from governments and extensive participation by all participants is essential for creating an environment where security planning and management, and better understanding of the need for security is achieved[76].

---

[73] European Parliament (2011), On the Proposal for a Directive of the European Parliament and of the Council on Combating Sexual Abuse, Sexual Exploita- tion of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, (COM(2010)0094 – C7-0088/2010 – 2010/0064(COD)), Draft Report, {LIBE} Committee on Civil Liberties, Justice and Home Affairs, 24 January 2011. Available at: http:// www.europarl.europa.eu/sides/getDoc.do? type=COMPARL&mode=XML&language=EN&reference =PE452.564

[74] OECD (2002), 'OECD Guidelines for the Security of Information Systems and Net- works – Towards a Culture of Security', Organisation for Economic Cooperation and Development, Paris, France.

[75] Ibid

[76] Ibid

The OECD Report argues that the principles that underpin the Guidelines are not an attempt to provide a one-size fits all approach to the security of information systems and networks, but rather, 'to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security'[77]. In other words, the principles represent a set of conditions that if implemented in policies, practices, measures and procedures, are most likely to create the type of environment whereby security as resilience, including prevention and reaction, will become embedded at all levels and amongst all active participants in cyberspace, individually and collectively. Of course it can be argued that such principles whilst broadly acceptable for most Western audiences (for example, the principle on democracy) are fiercely contested among those countries, organisations and individuals that operate under different government and security logics, as demonstrated with the Council of Europe Cyber Crime Convention. It can also be argued that some of the guidelines do not go far enough; for example, the principle on response states in connection with cybersecurity incidents that, 'Where permissible, this may involve cross-border information sharing and co-operation'. Such sharing of information across borders is a pre-requisite for security as resilience – and a norm that all participants involved in cybersecurity should adopt and operationalise in order to ensure effective reaction and response to cyber incidents. Finally then, such guidelines are voluntary in nature, and whilst providing a generic framework for the creation of a culture of cybersecurity, do not provide principles that are universally acceptable, or indeed that have been universally adopted and implemented by all participants. Indeed, the world in 2015 is even more complex than in 2002, with the OECD also active in providing more specific recommendations for policy measures by Internet service providers against botnets, underpinned in governance terms by private sector initiatives and public-private partnerships (OECD 2012).

Council of Europe

The Council of Europe's (CoE) central contribution to the governance of cybersecurity comes in the form of the Convention on Cybercrime which was agreed in 2001 and entered into force in July 2004. Also commonly referred to as the Budapest Convention, it is politically important and is the only binding agreement on cybersecurity issues, which has been drawn on for best practice within and outside Europe. At the time of writing (March 2015) 45 countries (including the US) have signed and ratified the convention, which includes 24 EU

[77] Ibid., p.14

member states[78] ; a further eight countries have signed it without ratification.[79] Having said this, it is also subject to contestation given its call for international cooperation and information sharing – including cross-national and trans-boundary cooperation between police forces. Countries such as Russia and China (as well as certain developing countries) have stated their clear opposition to ratifying the convention due to the concern that it would undermine national sovereignty, which is certainly problematic to achieving global security resilience given the number of Internet users in these countries and the fact that they are the alleged source of many cybersecurity breaches and attacks in recent years.

In governance terms, the Budapest Convention is voluntary in the sense that it is not mandatory for all states, in particular outside Europe, to sign up to it. Its purpose, however, is to establish 'a common criminal policy aimed at the protection of society against cybercrime' (Convention on Cybercrime 2001, Preamble). In order to achieve this it requires those that have signed up to the convention to adopt and implement legislation on the procedural aspects of cybercrime, such as illegal access and interception, misuse of devices, fraud, forgery, intellectual property (IP) offences, interference with data and systems and child pornography. Moreover, it provides a transnational legal and law enforcement framework that requires signatories to adopt laws concerning the investigation of cybercrime, and to cooperate, via extradition and mutual-law enforcement assistance, in the investigation of such crimes with other countries. In addition to the Budapest Convention the CoE Parliamentary Assembly has also provided recommendations on the Internet and Law, and expounded the view that whilst the nature of the Internet makes it impossible to regulate, an Internet code of ethics should be established through use of a legal instrument and the establishment of a European Internet ethics authority, in order to induce 'civic' behaviour on the Internet through the establishment of basic rights and duties of Internet users (CoE Parliamentary Assembly Recommendation 1670, 2004)[80].

Whilst the EU has clearly bought into and deferred to the CoE's Budapest Convention with regard to cybercrime, which is also reflected in the Stockholm Programme for internal security, there is much debate on its efficacy, related in particular to its lack of enforcement

---

[78] Those that had not ratified it at the time of writing (March 2015) include: Greece, Ireland, Luxembourg and Poland. Sweden ratified it in 2014.

[79] See, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185& CL=ENG.

[80] O'Neill, M. (2012), 'Cyber Crime and Cyber Security: A Late Developer in the EU's AFSJ', Draft Paper, Presented at Cybercrime and Cyber Security Workshop, University of Abertray, Dundee, 10 September 2012.

mechanism when signatories fail to meet their obligations under the terms of the treaty. Moreover, weaknesses remain in the context of the EU's 28 member states, not least because whilst the CoE 'Convention remains the only international legal instrument to date', it nevertheless, 'shows weaknesses due to the fast-moving developments in cybercrime'[81]. Such weaknesses include the lack of reference on how to deal with large-scale cyber-attacks as well as structural and cultural problems related to the functioning of national contact points in the context of cooperation in cybercrime.

More broadly, a central issue relates to the international nature of cybercrime, and the problem already alluded to above with regard to contestation. Cybercrime is a global problem requiring global cooperation if a robust security as resilience is going to emerge, and therefore the CoE Convention as a tool for combating cybercrime can only become truly effective if countries outside Europe sign up to the norms that underpin it. The Global Project on Cyber Crime has been established for just this purpose – to promote the Convention beyond Europe – and has had partial success in terms of certain countries in Asia and Latin America drawing on the convention and implementing legislative reforms based on it. Others still posit and propose an alternative view, grounded on alternative norms and principles. The Shanghai Cooperation Organisation nations (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan) for instance, have an agreement in place – the International Information Security Agreement – that emphasises a primary role for national security and the primary role of the state in controlling information technology and managing risks and threats. Moreover, it sees Western nations and their dominance of the information space as a major threat to them, their socio-political systems and cultural way of life[82]. Similar to other norms and tools invented in Europe and the EU, the convention embodies many useful principles for ensuring effective security as resilience, but agreement and implementation beyond Europe is critical if it is going to have any real impact on cybercrime given its global nature.

Organisation for Security and Cooperation in Europe (OSCE)

Discussion of a comprehensive approach to cybersecurity in the OSCE forum was driven by the Estonian Chairmanship in 2008 following attacks on its own systems in 2007. Prior to this the OSCE focused on enhancing different aspects of cybersecurity, for example. cybercrime,

---

[81] European Commission 2010, p.157 final

[82] Goldsmith, J. (2011), Cybersecurity Treaties: A Skeptical View, Future Challenges Essay, Hoover Institution, Stanford University.

cyber terrorism, and on efforts to ensure 'freedom' of assembly, expression and information on the Internet. Since then, activities have included high-level meetings and conferences on strategic cybersecurity issues and a comprehensive approach, but with no exact agreement on what role the OSCE can play. One fruitful discussion to emerge in this context is that for the development of norms on state behaviour for cyberspace, a notion which has also been discussed in other multilateral organisations. An OSCE conference in May 2011 also explored questions of how the OSCE mandate might be strengthened to enhance its international role in cybersecurity, as well as possibilities for developing internal OSCE mechanisms in cybersecurity and an elaboration of an OSCE strategic document on a comprehensive approach to cybersecurity.

However, membership of the OSCE, which brings together countries from North America to Central Asia, including member states of the EU, NATO and Commonwealth of Independent States, means that there are a diverse range of normative visions and strategic approaches to security resilience in cyberspace. Thus, whilst at the OSCE level there has been progress on agreeing an initial set of CBMs for cyberspace which suggests its broad membership is an advantage and not an obstacle to achieving consensus on certain issues, that very same advantage dissipates precisely because of its diversity, and, of course, because China is not a member of the OSCE[83].

A good example of this is the contrast between UK[84] and US (and other Western states and International Organisations [IOs]) proposed norms for cyberspace on the one hand and those of Russia and China on the other. As expected, there is convergence and overlap between the UK, US and ITU positions, in particular if we focus on the dimensions of universal access, approaches to cybercrime, international collaboration and the principle of uphold- ing fundamental freedoms. If we compare the principles advocated by the US, UK and ITU to those of the Shanghai Cooperation Organisation (SCO), then we can observe different logics at play with regard to the norms advocated for state behaviour in cyberspace[85], whilst also noting some element of convergence. Although the SCO agreement (2008) did not explicitly

---

[83] European Parliament and the Council (2011), Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA.

[84] Downing, E. (2011), 'Cyber Security – A New National Programme', Science and Environment Section, SN/SC/5832, House of Commons Library, 23 June 2011.

[85] Healey, J. (2011a), 'Comparing Norms for National Conduct in Cyberspace', 20th September 2011. Available at: http://www.acus.org

discuss norms, it emphasised ‘state control’; indeed in previous proposals from Russia there was a clear and predictable steer to the limitation of cross-border flows of information because of the impact that this might have on the culture of security. Developments since then have seen a very broad consensus emerge between Russia, China, the US and the UK on some of the general principles and norms for governing cybersecurity such as confidence- building, but such discussions have avoided the more controversial issues of content and information control[86].

In September 2011, members of the SCO (Russia, China, Tajikistan and Uzbekistan) proposed that the UN Secretary General facilitate a dialogue around their new draft proposal, the ‘International Code of Conduct for International Security’. This was drafted as a formal document of the 66th session of the UN General Assembly, with the express purpose of it being used to reach a consensus on international norms of behaviour for the Internet. This Code of Conduct[87] raises a series of basic principles, which at first glance do not seem divergent from what is being advocated by the US, the UK and the ITU[88]. For example, complying with the UN charter, international infrastructure and a commitment to ensure supply chain security are all ‘norms’ that chime with many of the principles proposed by the US and UK. Despite this, however, a deeper look at the security logics behind the proposal also raises potential points of concern for many that advocate a multi-stakeholder approach to cybersecurity and the preservation of freedom of access, expression, and information. Sceptics have argued, for instance, that the emphasis on promoting the ‘establishment of a multilateral, transparent and democratic international management of the Internet’, and the expected commitment to ‘ . . . prevent other states from using their resources, critical infrastructures, core technologies and other advantages, to undermine the right of the countries...to independent control of ICTs, or to threaten other countries’ political, economic and social security’, and ‘To cooperate in combating criminal and terrorist activities which use ICTs including networks, and curbing dissemination of information which incites terrorism, secessionism, extremism or undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment’, are underpinned by a sovereign logic of control rather than freedom and resilience.

---

86 UN Group of Government Experts Report 2010

87 See, see http://news .dot-nxt.com/2011/09/13/china-russia-security-code-of-conduct

88 Healey, J. (2011b), ‘Breakthrough or Just Broken? China and Russia’s UNGA Proposal on Cyber Norms’, 21 September 2011. Available at: http://www.acus.org

In terms of the first of these codes, promotion of the ITU to take a lead role in Internet governance, that is, a move to a traditional intergovernmental model, could lead to the Balkanisation of a spate of national Internet spaces, rather than multi-stakeholder governance; and China would also acquire greater weight and influence in terms of voting behaviour through the UN system. This also has implications then for the notion of security as resilience for all and an emergent culture of cybersecurity if other actors are side-lined in favour of a state-led, constructed and enforced approach. For the second and third of these codes, given the previous commitments by members of the SCO to limit information flows if it impacts on their own security, alongside the perceived dominance of the US in controlling the Internet, there are concerns that it would provide justification for repressive regimes to further limit free speech and access to independent external news sources, as happened during the Arab uprisings in Egypt and Libya[89]. Moreover, it might also provide an excuse to introduce draconian laws on access and dissemination of information that might threaten national security[90]. Finally, there are also further concerns about what is not visible in the Codes of Conduct, including, for example, no commitment to control patriotic hackers supported by states that are seen to be at the centre of cyber conflict, and of which Russia and China are seen as sponsors.

[89] Gjelten, T. (2010), Seeing the Internet as an 'Information Weapon', 23 September 2010, Available at: http://www.npr.org/templates/story/story.php? storyId=130052701

[90] Healey, J. (2011b), 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms', 21 September 2011. Available at: http://www.acus.org

CHAPTER - 9: CYBER SECURITY SETTING AND GOVERNANCE IN EUROPEAN UNION

The European Union (EU) approach to cybersecurity has five priority areas[91], and essentially three central strands. The first relates to protecting against and combating cybercrime. The second focuses on Network and Information Security (NIS), Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) and the third, less developed strand, on cyber defence. This chapter will focus on the former of these strands, although with the recognition that overlap does exist between them when analysing the security as resilience that underpins them within the EU institutional milieu. This is particularly important to be aware of in the context of the existing European Principles and Guidelines for Internet resilience and stability and the construction of a Cybersecurity Strategy for the European Union (EUCSS 2013). The EU institutional set up is still reflective of policy separation with DG Home leading on criminal law elements, DG Connect on network security and resilience, and cyber defence under the remit of the CSDP: the EU is, however, developing integrated working structures in order to facilitate a coherent approach to its cybersecurity strategy.

Cybercrime in the global market has become a serious issue given the growth of the Internet and its importance to our economic and social lives. According to Eurostat (2010), 80% of young Europeans connect with each other through online social networks, and online e-commerce transactions total approximately $8 trillion. This increase in the use of the Internet has been accompanied by the proliferation of cybercrime activity – varying from identity theft, to selling stolen credit cards, to child sexual abuse. Reports have suggested that there are over one million cybercrime victims per day worldwide[92] and that the global cost of consumer cybercrime alone is approximately $113 billion – and the cost to Europe $12bn (Norton Cybercrime Report 2013) – with a suggestion that cybercrime is more profitable than the illegal drugs trade. Whilst any such figures and information on cybercrime must be treated with caution given the variance in which cybercrime is defined and therefore cost reported (not to mention the agenda of those doing the reporting), it is clearly an issue that has a damaging impact on citizens, governments and businesses in Europe; and an activity that is low-risk and highly profitable for cybercriminals. In short, it is an issue that if not addressed

---

[91] 'Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace' (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7 February 2013, JOIN (2013) 1 final

[92] See, Norton Cybercrime Report 2013

through an appropriate and effective security as resilience can severely hinder the EU's plans for economic growth embodied in the Europe 2020 strategy (2010) and the Digital Agenda for Europe[93].

Cybercrime policy within the EU has been driven and underpinned by its evolving Internal Security Strategy (2010), and externally by the European Convention on Cybercrime (2001) (hereafter referred to as the Budapest Convention). The Stockholm Programme (2010) setting out the European Union's priorities for developing an area of justice, freedom and security (2010–2014), has emphasised that EU member states should, as soon as possible, 'ratify the 2001 Council of Europe Convention on Cybercrime' seeing it as the 'central legal framework of reference for fighting cybercrime at global level'. It also highlights a central role for the European law enforcement agency (EUROPOL), as a resource centre for Europe and the EU that can act as a platform for providing data and identifying offenders and offences, as well as assisting in the exchange of best practices between EU member states through communication and cooperation with national alert platforms. To this end, EC3 established on 1 January 2013, is seen as a central node in fighting cybercrime through pooling expertise and information, supporting criminal investigations, promoting EU-wide solutions, and raising awareness of cybercrime issues across the Union. Cybercrime and cybersecurity also figure high on the priority list of the next programme – the Rome Programme (2015–2019). Indeed the UK's House of Lords review of the Stockholm Programme has recognised that cybercrime and cybersecurity would require further attention during the life time of the new programme – and have in particular recommended a more strategic approach and emphasised the need for closer cooperation between the public and private sector[94].

Beyond this, the EU has developed a series of other initiatives that seek to address the issue of cybercrime across its different dimensions. This includes, for example, the Directive on combating the sexual exploitation of children online and child pornography (2011), as well as a Directive on attacks against information systems with a focus on penalising the exploitation of cybercrime tools, in particular botnets (2010). Cybercrime remains a top political priority

---

[93] European Commission (2010), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A Digital Agenda for Europe', COM (2010) 245 final/2, 26 August 2010.

[94] House of Lords, EU Committee 13th Report of Session 2013–2014, 'Strategic guidelines for the EU's next Justice and Home Affairs Programme: Steady as She Goes', HL Paper 173, House of Lords, April 2014. Available at: http:// www.parliament.uk/business/committees/committees-a-z/lords-select/eu -home-affairs-sub-committee-f-/inquiries/parliament-2010/rome-programme/

for the EU and is one of the eight priorities of the EU policy cycle for organised and serious international crime. According to the European Commission, 'it forms an integral part of efforts to develop an overarching EU strategy to strengthen cyber-security'. The EU has, clearly, recognising the global nature of the cybercrime threat, also sought to engage with international partners, with the EU–US working group in cybersecurity and cybercrime of primary importance. Among the key objectives of the partnership are to advance the Budapest Convention (2001) and to increase public-private partnerships for the purpose of sharing best practices on issues such as botnets. The latter objective of creating and enhancing public-private partnerships is also spelt out in the Stockholm Programme (2010, p.23), as is clarifying legal rules that promote cooperation in cross-border investigations into cybercrimes. Finally the EUCSS details further how the EU plans to facilitate movement to enhanced capability to combat cybercrime and improve coordination between key actors in Europe and globally.

Many of the initiatives outlined above, including the creation of EC3, have been triggered by obstacles that continue to exist for dealing with cybercrime effectively, including: 'jurisdictional boundaries, insufficient intelligence-sharing capabilities, technical difficulties in tracing the origins of cybercrime perpetrators, disparate investigative and forensic capacities, scarcity of trained staff, and inconsistent cooperation with other stakeholders responsible for cyber-security'.

Governing cybercrime in the European Union

EU approaches towards cybercrime have developed in parallel to its information society strategies such as the eEurope[95] initiative for enhancing the use and enjoying the benefits of digital technologies in a socially inclusive way. As the EU's aspirations to become an information society have progressed, so too have its efforts to protect those emerging benefits from criminal activity. In this context the eEurope initiative was followed by an eEurope Action Plan agreed in June 2000 at the Feira European Council, which emphasised the salience of addressing issues of network security and combating cybercrime. More specifically, the proposed approaches at this stage were both of a policy and a technical nature. For enhancing Internet security, whilst acknowledging that industry was primarily

[95] European Commission (1999), Communication of 8 December 1999 on a Com- mission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000 – eEurope – An Information Society for All, COM (1999) 687 Final (not published in the Official Journal).

responsible for this[96], it also argued for the evolution of a public-private relationship for nascent industry, whereby the public sector was seen as playing a catalysing, stimulating role for private initiatives. There was a clear steer towards a hands-off meta- governance approach to reinforce private sector driven action. There was also an emphasis in the Action Plan on developing better co-operation and co-ordination related to the discussion of the Budapest Convention in different international fora. In terms of a the technical layer, the increased use of smart cards was proposed, 'as an enabling technology which can increase the level of confidentiality and privacy in information society services' (for example, SIM, wire/ contactless, embedded and wearable devices with multiple functionalities – access, identification, authentication and so on). The smart card initiative was backed with 100m Euros research funding, and culminated in a smart card charter that was launched in December 2002.

The final report on eEurope (2003) noted some progress on the issue of Internet security, but also that use of the Directives launched (Electronic Signatures, 2001) remained limited. However, eEurope did provide the basis for a more comprehensive approach to network and information security by the EU. In June 2001, two parallel documents were published by the European Commission that outlined the contours of this comprehensive approach that also aimed to address crime in cyberspace. The first of these, a communication[97] entitled 'Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime', proposed a series of substantial and procedural legal provisions, as well as non-legal measures to address the criminal activities domestically and transnationally, whilst also stressing the need to preserve the balance between security and respect for the fundamental rights of individuals.

In terms of substantive law, for instance, there was an emphasis on agreeing on common definitions of cybercrime, as well as common incriminations and sanctions and introducing EU enforcement mechanisms that build on the Budapest Convention to enable it to take effective action on issues such as child pornography, racism and xenophobia online[98]. Procedurally, the central focus was on criminal law and the steer was on the improved

---

[96] Ibid, page 11

[97] European Commission (2001a), 'Creating a Safer Information Society by Improv- ing the Security of Infrastructures and Combating Computer-Related Crime', COM (2000) 890, 26 January 2001.

[98] Ibid

cooperation of law and other enforcement agencies (through mutual recognition but also enhanced mechanisms), in line with EU law, to facilitate more effective responses and requests from other countries in relation to cybercrime offences[99]. A critical security governance dimension here was cooperation at the international level, and clear rules on trans- border search and seizure. Finally, the non-legislative element focused on practical measures – or conditions – very much in line with the G8, ten point action plan which in terms of broad themes, included: creating specialised cybercrime police units at national level (with law enforcement and judiciary personnel) where they did not exist; improved cooperation between stakeholders, that is law enforcement agencies, industry, consumer representatives and data protection authorities; and encouraging appropriate industry and community-led initiatives. Within these themes, and connected to the technical and policy layer, was incorporated attention to the liberalisation of encryption tools within the remit of community law, and the development of technical expertise and training, common rules for keeping records and information (for the purpose of information sharing), cooperation between EU actors and action from industry, in particular through research and development[100].

The second, a proposal entitled, 'Communication on Network and Information Security: Proposal for a European Policy Approach',[101] focused on issues such as identity theft, cyber and infrastructure attacks and provided recommendations on how to enhance security as resilience within the technical, legal and policy layer. It was also underpinned by the security governance logic that 'market forces do not drive sufficient investment into security technology or security practice' and thus that 'policy measures can reinforce the market process and at the same time improve the functioning of the legal framework'[102]. There was a clear indication then of a move away from the meta-governance of identities to hands-off (facilitation, incentives) and hands-on methods of security governance (legal framework), in

[99] Ibid, page 16-24

[100] Ibid

[101] European Commission (2001b), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Network and Information Security: Proposal for A European Policy Approach, COM (2001) 298 Final, Brussels, 6 June 2001.

[102] Ibid, page-14

order to secure the internal market for information and communications services and 'benefit from common solutions' as well as being able 'to act effectively at global level'[103].

The central proposed tools or actions included: awareness raising and educational measures for all stakeholders; sharing best practices in security between member states; and the enhancement of cooperation between computer emergency response teams (CERTs) in Europe in order to ensure that information on potential and imminent threats is being exchanged, effectively. In addition, there was a strong steer towards 'strengthening the public/private cooperation on dependability of information infrastructures'[104] in the context of the eEurope Action Plan; investment in network and information security which was considered to be sub-optimal, and specifically, in order to facilitate this, the inclusion of security in the Commission frame- work research programmes; ensuring the interoperability of security – enhancing solutions through standardisation and certification (that is, ensuring the use of standards that can be implemented across platforms) through supporting user-friendly solutions, stimulating internationally agreed standards, and encouraging participation of stakeholders in European and international standardisation organisations and activities (European Committee for Electrotechnical Standardization (Cenelec), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C)); legal measures that sought to approximate national criminal laws related to cybercrime and security, as well as efforts to develop a common understanding of the legal implications of security in electronic communications and support for access to encryption products throughout Europe; finally, there was also an emphasis, given the borderless nature of cybercrime and security, on continuing efforts to support and con- tribute to the development of international efforts to combat cybercrime and security[105].

Building on the above the EU sought to enhance its comprehensive approach through various framework decisions and communications. The framework decision on attacks against information systems[106], in essence, provided for a more robust legal layer or environment for prosecution and aimed specifically to 'improve cooperation between judicial and other competent authorities...through approximating rules on criminal law in the member states'.

---

[103] Ibid., p.15

[104] Ibid., p.17

[105] Ibid., p.17–22

[106] See, Council Framework decision 2005/222/JHA, p.1

This framework decision provided common definitions for cyber-attacks with agreement on definitions by member states on what constituted criminal activity, which included: 'Illegal access to information systems', 'Illegal system interference' and 'Illegal data interference'. With a similar aim of moving to a common legal environment on the issue of sexual exploitation of children and child pornography a separate Council framework decision was agreed (2004/68/JHA), which included provisions to prevent the exchange of child pornography over the Internet. This framework decision, however, stipulated only minimal requirements in terms of approximation of legislation across member states, and subsequently led to problems in prosecuting offenders, within and between national borders. The security as resilience logic behind these framework decisions though was to make cooperation and coordination of efforts easier among the relevant public authorities, even if in practice there remained constraints given that there was no real culture of security that underpinned them.

Such a lack of 'culture' was highlighted in a communication from the European Commission outlining a 'Strategy for a Secure Information Society' (2006), and following the launch of 'i2010 – A European Information Society for Growth and Employment' which underlined the reliability and security of networks and information systems[107] for society and economy. More specifically, this communication aimed to 'develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment'[108]. The Commission recognised that it had to achieve convergence and coherence on the hitherto multi-pronged approach to ensuring the security of the Information Society, which consisted of the fight against cybercrime, but also specific network and information security measures and a regulatory framework for electronic communications that addressed the issues of privacy and data protection.

Indeed, despite previous efforts to address the issue of cybercrime not only at European, but also at international and national levels, several key challenges remained that would require further regulatory and policy attention. The first was the motive for cybercrime, which had switched from simple disruption to the desire to make profit. This had seen the proliferation of a number of malware vehicles for cybercriminals to achieve their aims, including spam, spyware and phishing, with an increasing reliability of compromised servers and computers

[107] European Commission (2005), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'i2010 – A European Information Society for growth and employment', COM (2005) 229 Final, Brussels, 1 June 2005.

[108] Ibid, p.3

for their distribution. Mobile telephony (mobile based network services) and 'ambient intelligence' (intelligent devices supported by computer and network technology) constituted other challenges to the integrity and security of the Internet, as platforms that opened up new opportunities for attack by cybercriminals. Significant here was that the approach advocated by the Commission indicated more explicitly a movement towards a 'holistic approach' that chimed with an open, adaptable and inclusive resilience, through hands-off (supporting partnership, coordination) and hands-on (legislation to add legal clarity and improve cooperation between law enforcement agencies) meta-governance. Moreover, it demonstrated an understanding that a multi-stakeholder approach and improved knowledge of the problems would be required if a culture of cybersecurity was going to emerge that was more likely to deal not just with the symptoms, but also the underlying causes of cybersecurity problems, at individual and institutional levels (public and private).

The Commission also indicated in this document that such an approach would complement its activity for protecting CIP, for which ENISA established in 2004 would play a key role in identifying best practice, improving awareness, and cultivating trusted partnership among all stakeholders. More specifically, ENISA was also tasked in its original mandate (2005) with supporting national CERTs, for which it established a CERT programme and Working Group on CERT Co-operation and Support. This work included the identification of broad baseline capabilities, and gap analysis in the area of operational considerations and legal and regulatory factors, and has involved more recently work on good practice in relation to the network and information security aspects of cybercrime[109].

Clearly then, even at this early stage, the EU, at least in its official documentation and discourse, recognised the conditions necessary for an effective security as resilience to emerge. The hands-on meta- governance dimension was further developed in the Commission's communication 'Towards a general policy on the fight against cybercrime' where it sought to improve cooperation and coordination at an operational and strategic level among law enforcement agencies, and at a political level among member states of the EU. In addition it promoted cooperation, legal and political, with third countries, and it put a specific emphasis, in the context of an evolving security as resilience, on continuous learning – through articulation of training needs in relation to cybercrime issues for law enforcement and

[109] ENISA (2012), 'On National and International Cyber Security Exercises: Survey, Analysis and Recommendations', ENISA, October 2012. Available at: http:// www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/ cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1.

judicial authorities, and indeed, increased linkage and commonality between the training programmes of the authorities involved in order to achieve better coordination.

Furthermore, and given the important role of the private sector in any effective security as resilience solutions, the improvement of the public- private aspect of the Commission's cybercrime policy through enhanced mechanisms of dialogue was emphasised. Examples of good practice in this sense included efforts to combat child pornography, where effective collaboration between credit card companies and law enforcement agencies assisted police in tracking down those that purchased online child pornography, as well as structures such as the Fraud Prevention Expert Group. Despite this, the challenge was to improve operational cooperation in Europe given the lack of legal obligation for private companies to share information on cybercrime with public authorities and the economic logic within which the former operated that prioritised the business model, and therefore secrecy rather than open sharing of information that might threaten reputation and profit[110].

Integral to improving cross-sectoral exchange of information, a crucial condition for security as resilience, was also the EU's rules on data privacy, retention and protection of personal data. The Directive on Data Retention (2006) is particularly salient here in achieving an information-sharing culture and integrated framework and approach, as there was a requirement within it for all member states to put legislation in place that ensured ISPs and telecommunications companies maintained records on user traffic (connections not content) for between six months and two years. Whilst this was already established practice for many telecommunications companies, this was not the case for many ISPs – and added to this was the many technical and legal differences in national provision on data retention, which made measures to combat cybercrime largely ineffective, technically and at policy level.

This Directive sought to remedy this situation, although not without controversy, as many digital rights groups have been critical of the lack of transparency with regard to the use of collected data and the potential for its misuse. The European Parliament has also argued that it fosters a surveillance society and undermines fundamental rights. Moreover, the Directive whilst transposed in the majority of member states has been the subject of legal challenge at national and European level (ECJ) – and the Commission's report on the evaluation of the Directive (2011) revealed that there were many inconsistencies in the way in which it was

[110] Ibid

implemented and which authorities were able to access the data. In addition, the European Data Protection Supervisor (EDPS) argued that the European Commission has not proved that the Directive is necessary and proportionate, which would make it illegal under the EU Charter of Fundamental Rights constituted by the Lisbon Treaty (European Frontier Foundation 2011).

There is then a real tension between ensuring access for security, and preserving the privacy of personal data, which is embedded not just in the legal, but also the political and cultural dimension of achieving a politics of resilience. The European Commission in its review of data protection rules carried out over the last few years, although rein- forcing that the core principles underpinning its approach (from the original 1995 Directive) are still valid – to protect people's fundamental rights and freedoms, including data protection, whilst ensuring a free flow of data – acknowledge that modern technology throws up new challenges with regard to ensuring the highest standards for data protection within the EU and globally. However, it has not yet diffused the tension between security and rights; indeed, the exposure of the PRISM programme by Edward Snowden in 2013 only served to exacerbate this tension – with implications across the different levels and layers of cybercrime. Even prior to the Snowden revelations there was a great degree of scepticism with regard to the balance between security and privacy for individuals, with civil society groups asking for further oversight on the impact of the Directive on citizen privacy and evidence to suggest that it cannot be designed in a less privacy-intrusive way in the future. A shadow evaluation report by European Digital Rights (April 2011, p.20) concluded that

the evaluation report of the Commission and the shadow report of European Digital Rights show that the Directive has failed on every level. It has failed to respect the fundamental rights of European citizens, it has failed to harmonise the Single Market and has proven unnecessary to fight serious crime.

The European Commission has recognised, in the past, the complexity of achieving balance through its actions, and has often taken the pragmatic view that the right to anonymity (privacy) and accountability (access) are not mutually exclusive when it comes to online crime (Interview, DG Home, November 2011). For example, such an approach was embedded in the proposal for 'A comprehensive approach on personal data protection in the European Union' which argues that there is 'a need to consider the extent to which the exercise of

certain data protection rights by an individual would jeopardise the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in a specific case' and that this might very well 'directly affect the possibilities for individuals to exercise their data protection rights in this area'.

The new proposed comprehensive 'legal' framework then, would not replace sector-specific legal instruments in the area of police and judicial cooperation in criminal matters that govern the functioning of agencies such as Europol and Eurojust. These agencies either operate under their own specific data protection regimes or, more usually, utilise data protection instruments at the Council of Europe. The task for the EU then – in particular given that the Data Retention Directive was declared invalid by a European Court of Justice decision in April 2014 ruling that it represented an infringement on the individual's right to privacy and protection of data – is to align the specific data protection rules with the more general legal data protection framework, and more broadly, to demonstrate that targeted 'harmonised limitations' to certain data protection rules are beneficial to securing the very rights and freedoms that individuals enjoy online. This is no easy task given the broad debate on privacy and security, and the many different interpretations of EU rules on data protection by stakeholders, including National Data Protection Authorities. In resilient security governance terms, there is no uniform interpretation, application, or implementation of such rules, thus making it much more difficult to ensure effective cooperation and coordination with regard to cybercrime.

The Regulation (General EU Framework for Data Protection) and Directive (on protection of personal data related to criminal and judicial activities) that were produced in 2012, sought to navigate through these issues for the purpose of achieving a more coherent and comprehensive approach to data protection. The new framework (Regulation and Directive) is a clear step change with regards to further handson meta-governance in this area. The Regulation seeks to introduce further rights for individuals concerned with disclosing personal data online and to create legal certainty for business, whilst the Directive is intended to clarify the relationship between the protection of personal data and the processing of personal data for police and criminal justice cooperation. Although the latter was previously covered by a framework decision (2008/977/JHA), it did not provide the EU with the power of enforcement, and was limited to cross-border processing activities, which caused significant practical difficulties in implementation due to the confusion over when and how

domestic data could be included, processed and used in any investigation[111]. In theory then, this new framework will facilitate the emergence of certain key conditions for an effective security as resilience to emerge in this area through enhancing trust between the transnational actors involved (police and judiciary), whilst also improving cooperation and smoother cross-border exchange of data in cybercrime investigations. Specifically, for example, both the Directive and the Regulation may be beneficial to certain CERTs and law enforcement agencies (LEAs) with regard to set- ting common ground rules that would help to legitimise their activities in relation to cybercrime investigations and incidents (ENISA, 2012b, p.52). It remains to be seen in practice, however, how far the logics and specific measures within the overall framework integrate satisfactorily the notions of privacy and security, in particular as according to certain commentators this legislation is still underpinned by 'a classical security vision, and an opposition of rights and security'[112].

[111] see Implementation Report on the Framework Decision (COM (2012)

[112] Porcedda, G. M. (2012), Data Protection and the Prevention of Cybercrime: The EU as an Area of Security? EUI Working Papers, Law 2012/25, Department of Law. Available at: http://cadmus.eui.eu/bitstream/handle/1814/23296/ LAW-2012-25.pdf?sequence=1

CHAPTER - 10: CYBER SECURITY SETTING IN UNITED KINGDOM

Cybersecurity in the UK has been driven by several logics over the last five years: first, by the perceived threat to national security and the potential of this threat to disrupt networked, digital activities in military and security terms; and second, the broader economic, political and social implications of cybersecurity threats given the increased reliance of many individuals, businesses, and critical infrastructure providers on cyber-based (ICT) systems. Such logics have been underpinned by a narrative that has evolved within the UK's Strategies for Information Assurance, National Security Strategies (NSS) and Strategic Defence and Security Reviews (SDSR), culminating in its updated Cyber Security Strategy (CSSUK 2011) which spelt out in some detail the main dimensions of the UK government's National Cyber Security Programme (NCSP).

For example, there was recognition early on of the threat by non- military means, focused in particular on state-led threats to the UK via cyber-attack or cyber espionage (NSS 2008). This initial narrative was focused on cyber defence and developing cyber offence in relation to state-sponsored cyber-attacks; and very much influenced by the 2007 cyber-attack on Estonia's public and private systems and infrastructure as well as the cyber-attacks on Georgian infrastructure in 2008 during the (conventional) Russian military offensive in the country. However, it was also clear that the cyber threat was understood in broader terms and that the effective functioning of cyberspace was essential not only in terms of the defence dimension, but also with regard to citizens, business and government being able to exploit the opportunities that cyberspace presents in the economic, social, cultural and political sphere[113].

To this end there was recognition that certain measures and new institutional structures had to be established and developed in order to ensure a more effective security as resilience in the UK. For example, the CSSUK[114] spoke of the need for 'a coherent approach to cyber security, and one in which the Government, organisations across all sectors, the public, and international partners all have a part to play'. Of course there were a number of other existing organisations that were tasked with dealing with cyber threats, most important including:

---

[113] Cyber Security Strategy of the UK: Safety, Security and Resilience in Cyberspace' (2009), Office of Cyber Security and UK Cyber Security Operations Centre, June 2009
'Digital Britain' (2009), Final Report, June 2009. Department for Culture Media and Sport and Department for Business, Innovation and Skills. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf

[114] Cyber Security Strategy of the UK: Safety, Security and Resilience in Cyberspace' (2009), Office of Cyber Security and UK Cyber Security Operations Centre, June 2009

Communications-Electronics Security Group (CESG which was part of Government Communication Headquarters (GCHQ)) which ran the Computer Emergency Response Team (GovCertUK) that acted on behalf of the public sector to provide warnings and assistance in resolving serious IT incidents and also provided the National Technical Authority for Information Assurance; The Centre for the Protection of National Infrastructure (CPNI) which played a similar role to GovCertUK but for business and UK critical infrastructure providers; and in terms of cybercrime the Home Office, Serious Organised Crime Agency (SOCA) and police (important here was the Police Central e-crime Unit established in 2008) worked together through initiatives such as the Association of Chief Police Officers (ACPO) e-crime strategy. However, it was felt that in order to achieve more effective resilience, a central cybersecurity capability was required and this was subsequently created for the first time in the UK through the establishment of: The Office of Cyber Security (set up in the Cabinet Office) for the purpose of providing greater coherence and leadership strategically across government; the Cyber Security Operations Centre in GCHQ to monitor and coordinate incident response, enable a better understanding of attacks against UK networks and users and provide better advice and information about the risks to business and the public.

Beyond this, the underlying principles outlined in the CSSUK certainly pointed to an understanding of the conditions required to create a more resilient UK cyber ecosystem. For instance, there was an emphasis on engaging with all stakeholders through partnership and retaining strong, balanced and flexible capabilities, as well as working with international partners in order to ensure a global, rule-based environment for addressing issues of cybersecurity. The new cyber structures and principles were seen as key for achieving the workstreams that were identified to drive change forward in order to achieve a better security as resilience. This included not just enhancing preparedness and protection, and improving the legal, regulatory and policy environment domestically and internationally, but also, and importantly, awareness and cultural change. Indeed, instilling the necessary changes in cyber culture and ‘embedding cyber security in wider aspects of policy formulation’ were important objectives within this workstream. In addition to this there was a recognition that skills and education needed to be enhanced to meet skills gaps, that an industrial strategy for cybersecurity had to be developed, that cybersecurity was a global issue that needed coherence beyond the UK, and that an understanding of what was required in terms of

capabilities and governance to ensure effective security as resilience, would have to be improved.

The Labour government in the UK then, constructed an initial plat- form and the principles for building an effective security as resilience, and had a practical awareness of the conditions they had to foster to achieve a mature level of resilience in the UK. Having said this, it was also the case in practice, despite certain achievements (with regard to e-crime for instance), that there were serious shortcomings for achieving such conditions within the existing structures – not least in terms of the skills, expertise, leadership and resource to establish a resilient ecosystem and indeed the culture of understanding, cooperation and coordination that was required within government, between government and other stakeholders and between the government and international partners.

Table ·.1 Data on government agencies cyber security in selected cities (Ceprei Labs 2017)

Rank	City	Vulnerabilities detected	Reported third-party vulnerabilities	Vulnerability attacks	DDoS attacks	Tampered websites	Websites infected with Trojans	Overall cybersecurity index
1	Tianjin	0.421	0.227	0.931	1	0.911	0.518	0.883
3	Guangzhou	0.72	0.226	1	0.066	0.598	0.735	0.852
4	Shanghai	0.64	0.08	1	0	0.156	0.8	0.847
5	Beijing	0.625	0.285	0.202	0.116	0.764	0.633	0.831
6	Shenzhen	0.709	0.13	0.606	0.076	0.927	0.668	0.83
7	Chengdu	0.338	0.124	0.991	0.809	0.683	0.51	0.772
18	Chongqing	0.427	0.191	0.271	0.223	0.027	0.465	0.653
25	Urumqi	0.866	0.382	1	0.62	0.471	0.84	0.495
33	Lhasa	0.661	0.143	1	1	0.005	0.701	0.246
35	Haikou	0.45	0.322	1	1	0.103	0.424	0.209

Thus a key challenge for the UK coalition government (Conservative/Liberal Democrat) that came to power in May 2010 was to build on this approach, raise the profile of cybersecurity further[115] and provide the resource and narrative that would convince all stakeholders that cybersecurity had to become a national security priority. Indeed it seems that despite the ambition and understand- ing from certain elements in government to create a more integrated approach to constructing cybersecurity resilience there was much still to do on a cultural level to persuade certain government departments beyond the Ministry of Defence (MoD) and GCHQ, as well as the private sector that the cyber threat had to be understood in broader (economic and social) terms, thus requiring the involvement of a range of stakeholders[116]. In

[115] Downing, E. (2011), 'Cyber Security – A New National Programme', Science and Environment Section, SN/SC/5832, House of Commons Library, 23 June 2011.

[116] Neville-Jones, P. and Phillips, M. (2012), 'Where Next for UK Cyber-Security?' RUSI Journal, 157(6), Dec 2012, 32–40.

addition to this lack of skills and expertise, lack of resource was highlighted as a key barrier to developing more effective responses, in particular with regard to cybercrime[117]. There was also a certain perception of the central response mechanism as fractured and incoherent, with information-sharing between public and private sector actors in need of improvement in terms of quality and quantity. The approach in the UK, certain evidence suggests, was not as comprehensive as it needed to be; with a cultural shift needed in the public and private sector in order to ensure a more effective security as resilience[118].

Accelerated prioritisation of cybersecurity was achieved through what certain scholars might describe as securitisation of cyber (in)security[119] – with carefully selected examples demonstrating the increasing degree to which e-crime had affected key government departments such as the Department for Work and Pensions (DWP), and more broadly, the theft of intellectual property such as information regarding the design and performance of the F-35 Joint Strike Fighter[120]. Such examples were used during the SDSR to convince government departments of the urgency in which cybersecurity needed to be treated, culminating in cybersecurity being elevated to a tier one risk in the UK National Security Strategy (UKNSS) of October 2010, thus making it a national security priority. To this end it categorised 'hostile attacks upon UK cyberspace by other states and large scale cybercrime' as one of the priority risks alongside military crises, major accidents and natural hazards and terrorism. These priorities also reflected the EU's Strategic Priorities for its Internal Security (The EU Internal Security Strategy 2010). Finally, new money was allocated to (only) cybersecurity in the SDSR – a sum of £650 million over a five year period. Indeed, as part of a spending review in 2013, an additional £210 million was allocated for new and existing cybersecurity projects – increasing the total budget for the programme to £860 million (to be spent by March 2016).

---

[117] Downing, E. (2011), 'Cyber Security – A New National Programme', Science and Environment Section, SN/SC/5832, House of Commons Library, 23 June 2011.

[118] Cornish, P., Livingstone, D., Clemente, D. and York, C. (2011), 'Cyber Security and the UK's Critical National Infrastructure', A Chatham House Report, Chatham House, September 2011.

[119] for example, see Dunn Cavelty, M. (2008a), Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London and New York: Routledge. for the US case

[120] Neville-Jones, P. and Phillips, M. (2012), 'Where Next for UK Cyber-Security?' RUSI Journal, 157(6), Dec 2012, 32–40.

CHAPTER - 11: CYBERSECURITY ECOSYSTEM IN CHINA

The crowning glory of Chinese cyberspace security is its internal surveillance and intelligence collection system. The Chinese terms for this activity is "public security intelligence" (PSI). China may be the most capable country in the entire world in this regard, the country is only a few decades away from having a decidedly Orwellian capability in this field. This section of the chapter uses an understanding of China's PSI capability as a proxy for its ability to defend its governmental cyber systems. The proposition is that the weaker its PSI is in cyber space, the weaker its defences in cyber space are in general.

We know that China deploys large numbers of people in a wide variety of roles to patrol cyberspace and collect intelligence through it. We know that China uses cutting edge technologies for this, including where necessary foreign technologies. We also know that China's technologically-driven, automated censorship and surveillance can be highly effective. The former blocks key words or websites, while the latter tracks key words and websites for alert to items of intelligence interest. The MPS maintains a robust and expanding R&D capability of its own, mostly through its Third Research Institute and its Intelligence Science and Technology Institute (qíngbào kē jì suǒ). As early as 1994, three of the four MPS research institutes had a heavy focus on information security[121].

We have less understanding from public domain sources of the quality of cyber defenses of these internal agencies. Can they protect their own cyber secrets? It is far from clear in the public record just where and in what manner electronic data is collected and stored by these agencies, but there is considerable evidence that the security ecosystem for this information is in a rather poorly developed state. If these agencies can't deliver high standards of cybersecurity for themselves, then it is questionable just how effective they can be in supporting information security of other government agencies across the breadth of the country.

As good and as unique as China's surveillance assets are, the government agencies cannot for now escape its cyber vulnerabilities and the generally uneven state of informatization throughout its large territory. Moreover, they cannot easily escape the historically low per capita ratio between law enforcement officials and citizens, nor citizens' contempt for Chinese

[121] Wong KC (1994) Public security reform in China in the 1990s. In: Brosseau M, Lo CK (eds) China annual review 1994. Chinese University Press, Hong Kong, pp. 5.1–5.33

police and the legal system. The wide-ranging intelligence collection brief of China's internal security agencies makes them a prime target for attack by adversary intelligence agencies. If a foreign agency can raid processed Chinese intelligence about the internal security situation in the country it need not spend so much effort collecting that information itself. Information in the internal security databases will be of interest to foreign military intelligence and operational planners as well.

To understand the current condition of the cybersecurity of China's PSI system, we have to discuss it under two quite distinct sub-sets: content security (preventing information "pollution") and system security (preventing technical intrusions of net- works and computerized systems, and protecting the data). As discussed later, there is reason to believe that the government's heavy emphasis on maintaining content security for political reasons has undermined the necessary attention and resource flow to system security. But as revealed later, China does not do either mission as well as it claims.

Content security has both a technical aspect and social aspect. Sometime around 2001, the Politburo of the CCP agreed that there would not be any purely technical solution in its efforts to censor the internet in China and that there would have to be a highly developed set of social controls as well. This meant that China would pursue technical surveillance and censorship options to the fullest extent possible while developing armies of allies in universities and business enterprises to exercise social discipline to ensure their members did not cross the line. It also meant that in between these two forms would sit battalions of internet police and citizen volunteers supported by new laws and large investigative assets. On the technical side, there are two powerful tools unique to China[122]: a small number of con- trolled international gateways (only three) and highly efficient filtering capabilities (the "Great Firewall").

However, these is an additional, larger perspective that goes well beyond censor- ship and social discipline of people who use politically sensitive or banned content. The people who conduct internal surveillance by cyber means also have responsibility to collect internally generated information of high relevance to external security interests to China in its assessment of foreign intelligence topics. This was acknowledged in U.S. congressional hearings in a U.S. specialist's view that "due to its growing internal database, technical

[122] Zeng Z, Yang K, Zhang Y and Zhou P (2013) Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management. In: 2013 Fourth International Conference on Digital Manufacturing & Automation. 684–687

sophistication and cyber capabilities, it [MPS] is having a more counterintelligence mission shared with the MSS"[123]. As Yang (2017)[124] observes, the public security police have a legislated mandate (Article Two of the People's Police Law) to "take the safeguarding of state security as the foremost duty of the police". He concludes that the public security police do "not fall strictly into either the [public] order or political police category" but "simultaneously fight common and political crimes".

The internal cyber-enabled surveillance system is not only directed at people with views that the authorities do not like or at people subscribing to internet gambling or pornography websites, but at the full spectrum of Chinese intelligence interests, especially people who have meaningful ties to targets of foreign intelligence interest. While specialized units exist for cyber intelligence collection outside China, those that conduct cyber "surveillance and monitoring" inside China must be responsive to a wide range of needs in addition to censorship.

The massively large list of intelligence collection priorities for these agencies operating domestically in cyberspace is a very long one and would look something like the list in Box 1. The importance of the list is that it is suggestive of a relative low priority for network security of public security systems given the work burdens associated with this list or tasks, adding some corroboration for reports that MPS personnel around China are seriously overworked, and under considerable political pressure on a daily basis.

To understand the normalcy of such a large intelligence collection brief, one need only reflect on the Prism program revealed by Edward Snowden and in which NSA was taking a direct feed from telephone companies of calls made in the United States into its computerized databases. Of special note is that in the United States, such action represented by the Prism program was outside the scope of the Constitution and the law, whereas in China, there would be no such obstacles to domestic surveillance of the same kind.

The agencies involved in China's comprehensive public security intelligence (PSI) ecosystem have been identified as comprising two types: intelligence units found in public security comprehensive command centres (CCC) and intelligence units established in the offices of the

---

[123] USCC (2016) China's intelligence services and espionage operations hearing before the U.S.-China economic and security review commission, 9 June 2016. https://www.uscc.gov/sites/default/files/ transcripts/ June%2009%2C%202016%20Hearing%20Transcript.pdf

[124] Yang Z (2017) China's public security intelligence: progress, challenges, and prospects. George- town J Asian Aff. https://asianstudies.georgetown.edu/sites/asianstudies/files/documents/gjaa_3. 2_yang.pdf (Spring 2017)

MPS[125]. Inside the CCC, there are two main types: the China Crime Information Centre (CICC) and the Super Intelligence System (SIS). Little else is known in the public domain about these centres.

The work horses of the CCP's cybersecurity defence system domestically are "cybersecurity bureaus" under the MPS that are spread around the country. The mission sets of these bureaus are:

1. supervision, inspection, guidance of information system security work

2. organization and implementation of security assessments of information systems

3. investigating and dealing with cyber crime

4. collations of data on major security incidents

5. prevention and management of intrusion by viruses and other malware

6. provision of information system security services and products for management

7. managing information system security training
8. other duties prescribed by laws, regulations and regulations.

These units have been in place for many years. By February 2017, under a policy foreshadowed as early as 2014, they had been augmented by the creation of cybersecurity police units (as mentioned above) in 1116 major firms throughout the country-a move unequalled by any other country and one which reflects a level of governmental insecurity and authoritarian intent seen in few others. According to the newspaper that reported this figure, such a policy "inclines netizens to practice self- censorship to avoid punishment"[126]. This uniformed force deployed in the private sector provides both technical security support as well as content security support. The latter mission is also supported by an army of "volunteers" through- out large organizations in China who conduct internet patrols since the government sees employers as responsible for ensuring their employees don't breach leadership preferences for content management.

---

[125] Huang S (2016) Research on the problems and countermeasures of public security information application. J Hubei Police Acad (2):71–75 (In Chinese)

[126] Wang H (2017) 1116 cyber-security police units have been set up nationwide. Beijing: Guangming 14 Feb 2017. http://epaper.gmw.cn/gmrb/html/2017-02/14/nw.D110000gmrb_20170214_2-04. htm (In Chinese)

Box 1: Domestic Intelligence Collection Priorities for Cyber Capable Agencies
1. Personal security of the highest level leaders (against possible physical threats, foreign espionage and internal political action—around 50 to 200 high value targets to protect)
2. Security of CCP rule from home threats
(a) Monitoring labour unrest throughout the work force (thousands of individual targets in critical sectors?)
(b) Monitoring people who have ties with Taiwanese independence activists in Taiwan and internationally (thousands of individual tar- gets?)
(c) Monitoring people who have ties with Tibetan independence activists inside China and their links to outsiders (thousands of individual targets?)
(d) Monitoring people who have ties with Xinjiang independence activists inside China and links to outsiders (thousands of individual targets?)
(e) Monitoring dissidents and potential dissidents in major mainland cities opposed to Party rule and their links with supporters and like- minded individuals outside China (thousands of individual targets?)
(f) Monitoring activists and intelligentsia inside China who might organize public ad hoc opposition events in major cities (up to several thousand targets per year?)
(g) Monitoring workers and community groups involved in ad hoc public protests throughout the country (up to several thousand people per year?)
(h) Monitoring the police for signs of disloyalty that threaten the leaders or CCP rule
(i) Monitoring the armed forces for signs of disloyalty that threaten the leaders or CCP rule
(j) Monitoring Falun Gong activities down to high school level (thou- sands of people?)
3. Foreign subversion activities directed into China from outside that are not directly connected to Chinese activists inside the country (hundreds of targets?)
4. Counter-espionage against foreign spies and their potential agents in China (all diplomats, all journalists, many business people, professionals, teachers, students—up to 20,000 people at any given time)
5. Security of China from economic crisis, economic disadvantage or economic threat
a. National economic issues
b. Trade negotiations
c. Foreign currency and derivatives positions, stock markets
d. Plans or foreign investors, both inside and outside China
e. Counter espionage.

But the lead organization for content security is the Central Propaganda Department (CPD) which organises centralized monitoring and take-down of material deemed inappropriate. The CPD blends with parts of the CAC, the Cyber Emergency Bureau and the Coordination Bureau for Cybersecurity. The Ministry of Industry and Information Technology (MIIT) also has a Cybersecurity Administration Bureau which is responsible for industry supervision in the interests of both content and technical security. It is unclear what role the Ministry of State Security (MSS) has for domestic information security (either technical or content related), but we can assume it has a direct interest in monitoring the possible leaking of state secrets in cyberspace. Since China has a propensity to make even the most anodyne information into

state secrets. MSS must be very busy in cyberspace monitoring. Numerous ministries and agencies apart from the MPS, CPD and MIIT play important roles in day-to-day cybersecurity operations. All national ministries and peer agencies have a cybersecurity unit that reports directly to a very senior official but there is little public domain information on how capable these teams are.

As reported by a U.S. specialist, the State Councillor and Minister of Public Security, Meng Jianzhu, announced in 2008 the nation-wide adoption of "public security informatization": the "process of integrating information more closely into police operations, including both domestic intelligence gathering and information management components"[127]. At around this time, the Chair of the CPLC, Zhou Yongkang, and Meng's superior, made a tour of some key MPS sites to promote greater attention to the speed of informatization in the public security sector. While there is not a direct or linear relationship between the pace of informatization in an organization and its levels of cybersecurity, the former can—in the absence of other stronger evidence—be taken as a proxy for the latter.

The assessment by a Chinese specialist that the country's PSI system is far from perfect[128] seems credible. The author identifies six challenges:

1. the informatization of the intelligence system is inadequate (no unified standard for intelligence reporting and slow updates of intelligence data)

2. inadequate data integration (SIS system covers nearly 10 billion pieces of information, some of which is "disorganized")

3. security risks in the preservation of intelligence data

4. some investigation personnel are incapable of collecting useful information

5. in some places, intelligence collection has not yet attracted enough attention

6. conflicts between the work of public security intelligence and the privacy of citizens.

---

[127] Mattis P (2012) The Analytic Challenge of Understanding Chinese Intelligence Services. In" Studies in Intelligence. 56(3):47–57. https://www.cia.gov/library/center-for-the-study- of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding% 20Chinese%20Intel.pdf

[128] Huang S (2016) Research on the problems and countermeasures of public security information application. J Hubei Police Acad (2):71–75

Another scholar reports three major short comings in their PSI work in general: “clogged intelligence sharing, limited analytical and quality control capabilities, and old ways of policing based on obsolete ideas”[129].

While these do not pertain directly to information security of the MPS systems, and they are challenges shared with other countries, these judgements add weight to the view that the deficiencies in MPS information security are likely to be substantial. Two key questions, addressed further below, are: just how large are the information security teams of the MPS offices throughout the country and how well trained are the personnel.

Chinese assessments of the cybersecurity ecosystem inside China’s national security agencies reveal high levels of dissatisfaction. In general terms, there was a com- mon view around 2013 that the government sector suffered from the low cybersecurity awareness of its top leaders and employees, particularly on issues like psychology and incentivization[130]. This study implied that China’s public sector had yet to consolidate the “institutionalization” phase of information security: where the practices became a “natural aspect of the daily activities of all employees” .

These judgments were corroborated in a 2017 commentary by an official of the Jintan Branch of Changzhou Public Security Bureau[131]. He described “security vulnerabilities in software”, lack of standardization of hardware between MPS offices, resulting potential for data leakage, unsecured nodes and terminals linking to secured systems. He also complained about a lack of cybersecurity awareness among colleagues, access by non-authorized police to MPS systems, improper use of USBs and mobile hard disks, and storage of confidential documents in unsecured computers. The findings of this study reappeared in several later articles attributed to officials of the MPS.

In a 2016 study of public security studies in China, the authors from the Yunnan Police College complained of several shortcomings in public security training and talent building in

---

[129] Yang Z (2017) China’s public security intelligence: progress, challenges, and prospects. George- town J Asian Aff. https://asianstudies.georgetown.edu/sites/asianstudies/files/documents/gjaa_3. 2_yang.pdf (Spring 2017)

[130] Zeng Z, Yang K, Zhang Y and Zhou P (2013) Increasing Employees’ Awareness and Enhanc- ing Motivation in E-Government Security Behavior Management. In: 2013 Fourth International Conference on Digital Manufacturing & Automation. 684–687

[131] Li H (2017) Discussion on public security computer network and information security. In: Net- work security technology and application magazine. 2017(8) In Chinese. http://www.xueshu. com/wlaqjsyyy/ 201708/29810655.html

cyberspace[132]. These included an over- emphasis on theory and "scant attention to practice" that contributed to a decline in student interest; the rapid pace at which knowledge acquired during studies is overtaken by new technologies, thus making student knowledge outdated; and the related difficulty teachers had in updating their knowledge. The authors lamented the dearth of talents in applied cybersecurity compared with engineering and research.

The authors cited a member of the National Informatization Expert Advisory Committee, Shen Changxiang, who suggests that the government should take a stronger lead in guiding the construction of cybersecurity discipline and accelerate the pace. There was, Shen was cited as saying, a need for innovation in approaches to talent cultivation processes; and significant reform of the pedagogical processes ("build teacher teams to promote education quality"; "improve textbooks and curricula"; and "set up a training platform to strengthen practical exercises for cyber attack and defence").

Other complaints raised include: many defects in the existing intrusion detection of public security defence units (lack of active defence capability and the system's error/leakage rate is high)[133]; and cyber monitoring in the western provinces has been relatively backward[134]. In fact, the most advanced intelligence sharing system for the MPS in China is only available in 131 cities (mostly those with a population of around one million or greater) out of several hundred cities. Many rural and semi-rural areas will also not have access to this intelligence system.

---

[132] Jia X, Wang J (2016) Discussion on the reform of public security information security personnel training mode based on the teaching of network attack and defense. Information and Computers 9:231–233

[133] Yu Y, Hu W (2013) Intrusion detection algorithm design in the public security system for network monitoring. Bull Sci Technol 29(6):185–190

[134] Zeng X (2010) Research on management of internet by police in west of China. Netw Secur Technol Appl 4:18–20

CHAPTER - 12: CYBER SECURITY SETTING IN INDIA

Introduction:

In the 1970s, the Indian Department of Electronics (DoE) started working with the United Nations Development Programme (UNDP) to formulate a strategy to bring computing to India–an action seen as crucial to the informatization of Indian society and to the boosting of local economies. In 1985, the National Center for Science and Technology was created and became responsible for the establishment of India's first Internet Service Provider (ISP), the Education Research Network (ERNET) – an Internet platform aimed primarily at academic and research institutions. ERNET introduced the extension ".in" for domain names in the country and provided Indian academic institutions with their first international connections.[135] This was one of three main initiatives that surfaced concurrently to connect society, academia, and government in India. The Indian Computer Maintenance Corporation (CMC) – originally a government-owned entity later converted to a public limited company in 1977 – initiated India's first public network, the INDONET network, which became operational in 1986. INDONET's goal was to create a networked infrastructure and culture within the country and it was the first to provide electronic mail, file transfer services, applications, and data networks to public and private sector entities.[136] Finally, the National Informatics Centre Network (NICNET) – a satellite-based network – connected the central government with the state governments and district administrators to enable bi-directional information sharing on censuses, medical services, election results, national policies, and other government services.[137]

In 1995, the Internet became widely available to the Indian public, and the central government has since continued to support Internet up-take as a catalyst for economic growth, job creation, more efficient government operations, and increased access to public services. The Internet penetration rate today, however, is still among the lowest in the Asia-Pacific region and far behind other large, developing countries like China and Brazil, with only 26 percent of the population connected to the Internet.[138] With nearly a billion people still not connected to

---

[135] Biswarup Sen, "Digital Politics and Culture in Contemporary India: The Making of an Info-Nation," (New York, NY: Routledge, 2016): 71-72.

[136] Ibid

[137] Institute for Defense Studies and Analyses, "IDSA Task Force: India's Cyber Security Challenge," (March 2012): 19.

[138] International Telecommunications Union, "Percentage of individuals using the internet," (2015).

the Internet, India is home to the world's largest offline population.[139] However, unofficial 2016 statistics suggest that India's Internet penetration rates are on the rise.[140]

The government continues to push digitization to make government services available to all Indians electronically, however, these goals remain difficult to achieve because of the size of the off-line population. For example, in 2006, the Indian government launched the National e-Governance Plan (NeGP) and initiated 31 Mission Mode Projects (MMPs) to offer citizen-centric services, including pension payment, income tax collection, banking and insurance services, and other projects. Although many of these projects were implemented across the country, NeGP did not ultimately reach its desired goals.[141] Yet, India's initiatives in these areas have continued to evolve over the last decade, and lessons learned from previous setbacks have played an important role in shaping future initiatives. One of the more successful e-governance projects is the Aadhaar biometric identification scheme – the world's largest national identification number program, led by the Unique Identification Authority of India (UIDAI).[142] This biometric tool – a 12-digit unique identification document which captures details such as demographic and other biometric data – allows for timely and efficient delivery of welfare services to Indian residents and is now utilized by over 80 percent of the population.[143] While this program may allow more citizens to access e-government services, critics have expressed concern that this large repository of information could be misused for state surveillance or breached by criminals to exploit the information.

Transforming India into a "digitally empowered society and knowledge economy" is one of the main goals of the current government. Prime Minister Nerendra Modi laid out his vision in his 2015 digital strategy, called "Digital India" – a broad economic plan to prioritize job creation through innovation enabled by a robust telecommunications-connected

---

[139] World Bank, "World Development Report 2016: Digital Dividend," Wash- ington, DC: World Bank (2016): 7-8.

[140] "India Internet Users," Internet Live Stats, July 1, 2016, http://www.inter- netlivestats.com/internet-users/india/.

[141] Ministry of Communications and Information Technology, "National e-Governance Plan," http://meity.gov.in/content/national-e-governance-plan.

[142] Unique Identification Authority of India, "UIDAI Background," https:// uidai.gov.in/about-uidai.html.

[143] Unique Identification Authority of India, "State/UT wise Aadhaar Saturation: Annexure 1," https:// uidai.gov.in/images/ news/aadhaar_saturation_15082016.pdf.

infrastructure.[144] Realizing that connectivity underpins economic growth, the plan outlines initiatives to improve telecommunication services, including accelerating broadband deployment by at least 50 percent (currently about 7 percent) and provisioning universal access to mobile connectivity – increasing in rural India by 30 percent (currently about 45 percent). If successful, this plan could have a two-fold effect: (1) attracting foreign direct investment, and (2) increasing high-tech exports, which in turn could result in an additional GDP growth of 9 percent (~$180 billion).[145] Additionally, "Digital India" encourages industry innovation in ICT solutions for the healthcare sector, knowledge management, and financial services. This plan is one of many other related programs, such as "Make in India," "Skill India," "Start-up India," and "Stand up India," launched to further en- courage younger generations and the IT industry to innovate, develop creative solutions, and promote domestic production of electronic devices – India's second largest import.[146] This is India's "digital revolution" to fully realize the economic benefits of ICT. The implementation of "Digital India" is being coordinated by the Ministry of Electronics and Information Technology (MeitY) – former Department of Electronics and Information Technology (DeI- TY), and each of its initiatives – including the establishment, expansion, and modernization of core ICT infrastructure infrastructure – identifies specific milestones and objectives to be completed by mid-2018.

These plans continue to position India as an ICT leader in the global marketplace. In 2016, the Indian ICT sector contributed $143 billion in revenue, $108 billion in exports, and employed about 3.7 million people.[147] E-commerce – India's fastest growing market – has grown by over 20 percent since 2015 (about $17 billion), as companies have adopt- ed hyper-local e-commerce, innovative mobile platforms, and online payment solutions.[148] As a result, some Indian IT services companies, such as Wipro and Infosys are emerging as global competitors

---

[144] Ministry of Electronics and Information Technology (MeitY), "Digital India: About the Programme," http:// www. digitalindia.gov.in/content/about-pro- gramme, and "Digital India: Programme Pillars," http:// www.digitalindia.gov. in/content/programme-pillars.

[145] This is based on a World Bank report that noted that a 10 percent increase in mobile and broadband penetration can deliver increases in per capital gross domestic product of 0.81 per- cent to 1.38 percent, respectively in developing countries. For statistics, see: Deloitte, "Digital India: Unleash- ing Prosperity," Deloitte (2015): 3.

[146] "Digital India: PM Modi Says India, Can Play a Big Role in Cyber Security Globally," July 2, 2015, NDTV, http:// www.ndtv.com/india-news/digital-india- pm-modi-says-india-can-play-a-big- role-in-cyber-security-globally-777319.

[147] NASSCOM, "IT-BPM Overview," http:// www.nasscom.in/indian-itbpo-industry.

[148] NASSCOM, "eCommerce Snapshot," http://www.nasscom.in/ecommerce.

in the world's marketplace, while others such as Flipkart (online shopping), Quikr (online marketplace), and Nauki.com (jobs site) are becoming major players in the fast growing domestic e-commerce space.[149]

Although India's digital strategy has the potential to generate greater digital dividends and has already been quite successful in attracting foreign direct investments in the ICT sector, the government has yet to make cyber security an equal priority – aligned with the economic initiatives. Cyber security is not a new issue for India, but the government now recognizes that it can also transform cyber challenges into opportunities to drive India's ICT security and resilience agendas. In launching "Digital India," PM Modi equated cyber risks to a "global threat of bloodless war," and asserted that "India has a big role to play [in dealing with global cyber threats]" and that his country "can provide innovative and credible solutions [...] to ensure that the entire world lives in peace."[150]

While national statistics are not readily available, India continues to rank high on both the list of countries identified as major points of origin for cyber attacks – third behind the US and China – and as a leading target for cyber crime and ransomware. Countries like India are an attractive target for hackers because they have experienced a rapid increase in ICT uptake, e-commerce activities, online banking and financial transactions, but this increased connectivity has not been accompanied by higher security awareness.[151] The High Court of India commissioned a study that showed that cyber crimes such as ransomware, identity theft, and phishing attacks cost the country over $4 billion in 2013.[152] In 2015, India's National Security Advisor, Ajit Kumar Doval, included cyber security as one of the major internal security challenges faced by the country.[153]

Despite the several cyber security-related initiatives that India has put forward, including the initial 2008 Information Technology (IT) Act, the recent establishment of a dedicated National

---

[149] Dhruva Jaishankar, "Internet Free- dom 2.1: Lesson's from Asia's De- veloping Democracies," German Marshall Fund (March 2015): 13.

[150] "Digital India: PM Modi Says India Can Play a Big Role in Cyber Security Globally," July 2, 2015, NDTV.

[151] Venkatesh Ganesh, "India lagging Lagging in cyber Cyber security Security awarenessAwareness," The Hindu BusinessLine, August 29, 2016, http://m.thehindubusinessline.com/ info-tech/india-lagging-in-cyber-security-awareness/article9046626.ece.

[152] "Cyber frauds cost India $4 billion," The Hindu, October 23, 2013, http://www.thehindu.com/business/Economy/cyber-frauds-cost-india- 4-billion/article5261594.ece.

[153] Press Trust of India, "Internal Security Will be a Big Challenge for India: Ajit Doval," NDTV, October 31, 2015, http://www.ndtv.com/india-news/ internal-security-will-be-a-big-challenge-for-india-ajit-doval-1238573.

Cyber Security Coordination Centre (NCCC), and the commitment of "Digital India" to strive for a safe and secure cyberspace,[154] India's infrastructure security and resilience, legal and regulatory measures, and broader economic reforms have not kept pace with the digital revolution envisioned by PM Modi. This is magnified by India's lack of a professional cyber security workforce and the persistent digital, educational, income, and gender divide between on- and off-line populations. In addition, India's 2013 "National Cyber Security Policy" lacked an implementation plan and most of the government's current policies are best described as "piecemeal."[155] Critics have also pointed to a number of recent cyber espionage attacks as indicative of India's lack of a resilient cyber and coordinated security response apparatus.[156] Finally, senior national security officials have drawn attention to the lack of an integrated approach between the various agencies mandated to protect India's critical information infrastructure.[157] In summary, there is still a substantial gap in terms of national-level preparedness for cyber risks.

India faces many challenges that make it difficult to determine how cyber security will be prioritized moving forward. The primary objective for India is, in fact, the preservation of law, order, and security. Past and continuing challenges, including existing and perceived threats associated with separatism, sectarianism, terrorism, and militancy, have dominated the national security agenda.[158] Improving the country's cyber security posture will require committing sufficient resources and up-leveling the importance of it to the future of India's national and economic security.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate India's current preparedness levels for cyber risks. This analysis provides an actionable blueprint for India to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment and maturity to closing the gap between its current cyber security posture and

---

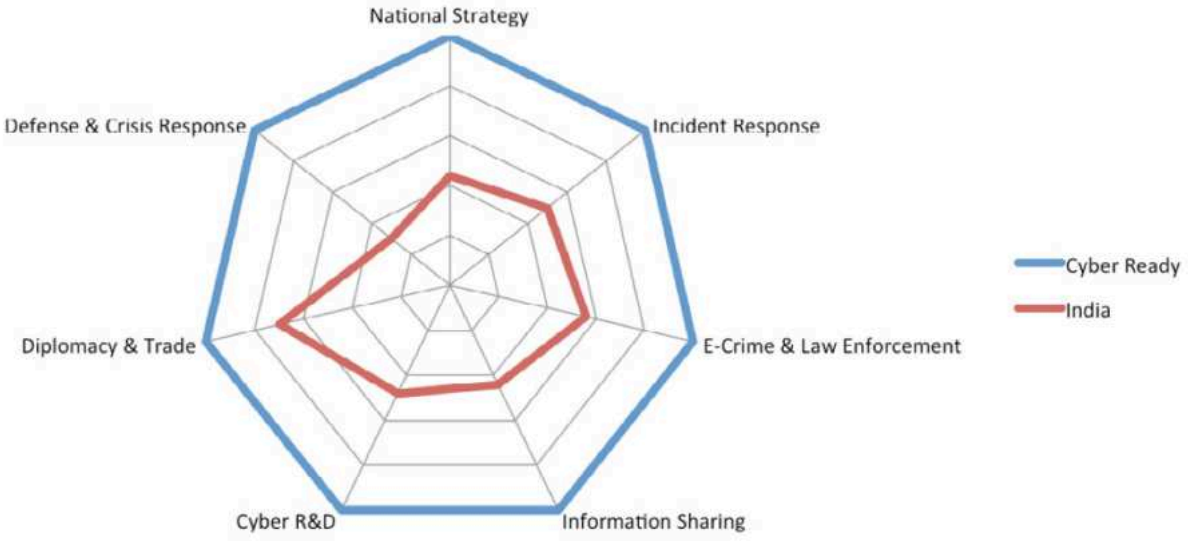
154 Department of Electronics and Information Technology, "Digital India," http://www.cmai.asia/digitalindia/pdf/Digital-India-DeITY-Details.pdf.

155 Dilip Kumar Mekala, "The government needs to be more serious about India's cyber security," Force, July 2015, http:// forceindia.net/MuchtoWorryAbout.aspx.

156 Abhishek Bhalla, "Modi government gets cracking on cyber espionage," Mail Today, June 28, 2016, http:// indiatoday. intoday.in/story/modi-govt-gets-crack- ing-cyber-espionage/1/702377.html.

157 SD Pradhan, "Cyber security: Need for an overall national cyber strategy," The Times of India, January 18, 2016, http://blogs.timesofindia. indiatimes.com/ChanakyaCode/ cyber-security-need-for-an-over- all-national-cyber-strategy/.

158 Dhruva Jaishankar, "Internet Freedom 2.1: Lesson's from Asia's Developing Democracies," German Marshall Fund (March 2015): 8.



India Cyber Readiness Assessment (2016)

the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows.

National Strategy:

In 2010, the Indian government fell victim to a series of high-profile computer intrusions at the National Security Council, the National Security Advisory Board (NSAB), and other high profile offices. The government responded to these incidents by creating an Inter-ministerial Task Force on Cyber Defence & Preparedness, chaired by the National Technical Research Organisation (NTRO) – India's technical intelligence agency.[159] [160]This was also one of the earliest multi-stakeholder initiatives on cyber defence.

The Task Force on Cyber Defence & Prepared- ness helped inform India's cyber policy and future organizations. In 2013, the Department of Electronics and Information Technology (DeITY) – which was elevated and given the status of Ministry of Electronics and

[159] Vijay Mohan, "Fresh wave of cyber attacks hits India," The Tribune, February 11, 2016, http:// www.tribuneindia. com/2010/20100212/main7.htm.

[160] Pukhraj Singh, "Thinking Offensively!", Seminar: The Monthly Symposium, October, 2016, http:// www.india-seminar. com/2013/650/650_pukhraj_sing.htm

Information Technology (MeitY) in 2016 – released the first "National Cyber Security Policy." The cyber security strategy noted that increased ICT penetration had been a catalyst for Indian economic growth and social development, increasing employment opportunities, and raising the standards of living. Moreover, the document highlighted the role of the Indian government in driving ICT adoption in public services (e.g., government-to-citizen services, citizen identification, and public distribution systems), health care (e.g., telemedicine, remote consultation, and mobile services), education (e.g., e-learning and virtual classrooms), and financial services (e.g., mobile banking and payment gateways). While the document summarized the benefits India has realized based upon increased ICT penetration, it also warned about the inherent risks associated with an unsecured cyberspace, which in turn has the capacity to "reduce state resources" and "undermine confidence" in the state and its supporting infrastructure.[161]

The document articulated a clear vision for India, stating that its goal was "to build a secure and resilient cyberspace for citizens, business- es, and government."28 Additional objectives to ensure resiliency and trust in cyberspace included: strengthening the regulatory framework for ensuring a secure cyber security ecosystem; enhancing and creating national and sectoral level 24x7 mechanisms for obtaining cyber threat information; operating a 24x7 National Critical Information Infrastructure Protection Center (NCIIPC); and creating a cyber security workforce of 500,000 individuals by 2018. The document provided 15 additional objectives and related action areas, such as creating a secure cyber security ecosystem; developing an assurance framework; encouraging open standards; promoting the protection and resilience of critical information infrastructure; and creating cyber security awareness. In many ways, the document was highly aspirational, because while it outlined clear objectives and action items, it did not offer an implementation plan or specific guidelines to achieve those goals.

The strategy called for the creation of a central national body charged with coordinating all matters related to cyber security in India. However, while a National Security Council Secretariat (NSCS) was established as the central coordinating body for cyber security and Internet governance, the Ministry of Communications and Information Technology within the

[161] Ministry of Communications and Information Technology, "National Cyber Security Policy," Department of Electronics and Information Technology (July 2, 2013): 2.

Department of Telecommunications was the body tasked with the implementation of national-level cyber security policy.[162]

In 2015, the position of the National Cyber Security Coordinator was created and staffed – taking advantage of institutional knowledge – by the former head of India's CERT at MeitY. The Coordinator is positioned within the Prime Minister's Office and is also the head of the newly established National Cyber Coordination Center (NCCC), located under MeitY. The NCCC's mission is to engage public and private sector entities, including intelligence agencies, law enforcement, ISPs, and industry to mitigate the effects of online threats, facilitate cyber threat intelligence sharing, and evaluate malicious information that may flow into the networks. The Finance Ministry has allocated US$130 million for NCCC operations, but the NCCC is still building capacity and staffing the organization and it is unclear how it will carry out its intended operational activities and mission from a technical perspective.[163]

Although the Indian government has yet to publish an updated national cyber security strategy that aligns the country's economic vision with its national security imperatives, it has outlined nine core principles for cyber security: (1) the promotion of peace and stability; (2) a multi-stakeholder approach; (3) the support of funding for the United Nations Group of Government Experts (UN GGE); (4) capacity building and research and development (R&D); (5) technical cooperation among Computer Emergency Response Teams (CERTs) and standard setting; (6) the promotion of economic growth; (7) cooperation between law enforcement officials; (8) the support of freedom online; and (9) the protection of data and privacy.[164]

Moreover, the Indian government has recognized the benefits and threats derived from the use of ICTs, and both the 2013 "National Cyber Security Policy" and the 2015 "Digital India" initiative acknowledged the importance of Internet connectivity and ICT development as key drivers of Indian economic growth. Yet, while "Digital India" seeks to increase ICT penetration and ICT applications in citizen-facing services, the national cyber security strategy squarely focuses on securing India's information infrastructure and building cyber security awareness. Thus, until the digital and cyber security strategies are aligned, India may

---

[162] Ibid, 3

[163] In July 2016, the Ministry of Communications and Information Technology was bifurcated into the Ministry of Communications and Ministry of Electronics and Information Technology (MeitY). For more information on MeitY, see: http://meity.gov.in/.

[164] Muktesh Chander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," National Technical Research Organisation, http:// www.slideshare.net/CERCatIIITD/ national-critical-information-infra-structure-protection-centre-nciipc.

not realize the economic promises and national security guarantees needed to support its digital future.

Incident Response:

The amended 2008 IT Act (section 70A) pro- posed the designation of a government organization as the "national nodal agency" for the protection of critical information infrastructures, and section 70B assigned that role to the Indian Computer Emergency Response Team (CERT-In), charging it with "securing Indian cyberspace."[165]

However, it was not until 2014 when malicious software was discovered throughout India's industrial control systems,[166] that DeITY (now the Ministry of Electronics and Information Technology, MeitY) officially announced the creation of the National Critical Information Infrastructure Protection Centre (NCIIPC) under the National Technical Research Organisation (NTRO) as the dedicated agency for critical sectors. The government defines critical information infrastructure as "those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation."[167] This includes 12 sectors that fall under NCIIPC's mandate, including: energy, transportation, banking and finance, telecommunications, manufacturing, defense, law-enforcement, e-governance, and water, among others.[168] A mandate for this type of governmental organization that includes a combination of both the public sector and private sector is notable and offers some opportunities to further information sharing activities and collaboration. NCIIPC's key responsibilities include: identifying critical sub-sectors; issuing daily and monthly cyber alters and advisories; conducing malware analysis and cyber forensics; tracking malware and botnets; promoting cyber security awareness and training; operating a 24x7 help desk.[169] In order to facilitate better incident

---

165 Geetha Nandikotkur "India Opens Cyber Coordination Centre" April 13, 2015, http://www.bankinfose- curity.asia/india-opens-cyber-co- ordination-centre-a-8100.

166 Melissa Hathaway's interview with Arvind Gupta, Deputy National Security Advisor, at the Cyber 360: A Synergia Conclave, Bangalore India, September 29, 2015.

167 The Gazette of India, "The Information Technology Act of 2008," Indian Ministry of Law and Justice, (February 5, 2009): 14, http://meity.gov.in/sites/ upload_files/dit/files/downloads/ itact2000/ it_amendment_act2008.pdf.

168 Pukhraj Singh, "In Cyberspace War- fare, India is Still Shooting in the Dark", The Quint, February 26, 2016, https://www.thequint.com/opin- ion/2016/02/25/in-cyberspace-warfare- india-is-still-shooting-in-the-dark.

169 Muktesh Chander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," National Technical Research Organisation, http:// www.slideshare.net/CERCatIIITD/ national-critical-information-infra- structure-protection-centre-nciipc.

response among critical information infrastructure providers, the NCIIPC has each organization or ministry within a designated critical sector identify a "nodal officer" or computer information security officer (CISO) to be the key point-of-contact with NCIIPC.

CERT-In was established in 2004 and today acts as the national central body for cyber incident response, incident cross-sectoral coordination, and the implementation of proactive measures to reduce cyber risks across federal and state governments, industry, and academia. CERT-In serves also as an advisory body for both the public sector and critical information infrastructure, and works to develop cyber security standards for all enterprises.[170]

The amended 2008 Act and the 2014 IT Rules assigned CERT-In a broader set of objectives, including: collecting, analyzing and disseminating information on cyber incidents; forecasting and publishing alerts of cyber security incidents; providing emergency measures for handling cyber security incidents; coordinating cyber incident response activities; issuing guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response, and reporting of incidents; and other cyber security-related functions as prescribed.[171]

Subsequently, CERT-In released a framework document allowing it to track its progress towards meeting the objective areas outlined in the 2008 amended IT Act. Each objective area was assigned associated actions and measures of success. Since the release of the framework document, CERT-In has updated its Cyber Crisis Management Plan (CCMP) to counter cyber attacks and cyber terrorism, as well as other cyber-related incidents that impact critical national assets and endanger public safety or national security. In addition, CERT-In is conducting security audits of critical infrastructure organizations; cyber security exercises at the sectoral, national, and international levels; and entering into formal agreements to collaborate with other national CERTs and sectorial CERTs. CERT-In is also utilizing media advertising to boost citizen awareness and provide additional cyber awareness training.[172]

---

[170] National Technical Research Organisation, "National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter, and Responsibilities," http://www.slideshare.net/CERCatIIITD/ national-critical-information-infrastructure-protection-centre-nciipc.

[171] Indian Computer Emergency Re- sponse Team, "Welcome to CERT- In," http://www.cert-in.org.in.

[172] The Gazette of India, "The Information Technology Act of 2008," (February 5, 2009), and "The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013," (January 16, 2014), http://meity.gov.in/sites/upload_files/ dit/files/G_S_R%2020%20(E)2.pdf.

Additionally, CERT-In established a security alert system that publishes daily "advisories" and "vulnerability notes" on potential cyber threats and vulnerabilities on their website and distributes them to interested CERT-In list- serve subscribers.[173] Moreover, CERT-In publishes an annual report that provides an overview of CERT-In activities, including a summary of its botnet tracking and training workshops and statistics regarding cyber-related incidents.[174] Finally, in response to increasing incidents of cyber fraud and underlying insecurities of digital transactions, India Finance Minister Arun Jaitley recently announced the establishment of a dedicated CERT for the financial sec- tor (CERT-Fin) to strengthen the security and resilience of the Indian financial system.[175]

The government allocated ₹85 (~$13.6 million) during the 2015-2016 financial year for three activities: CERT-In operations, the Cyber Appellate Tribunal,[176] and cyber security research and development (R&D).[177]

National Centre or Responsible Agency:

National Critical Information Infrastructure Protection Centre (NCIIPC)

National Critical Information Infrastructure Protection Centre (NCIIPC) is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014 based in New Delhi, India. It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.

It envisages to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation.

---

[173] Department of Information Technology, "RFD: Results-Framework Document for ICERT 2011-2012," (2012), http://www.cert-in.org.in/ Images/CERT-In_RFD2011-12.pdf.

[174] Indian Computer Emergency Response Team, "Welcome to CERT- In," http://www.cert-in.org.in.

[175] Indian Computer Emergency Response Team, "Annual Report," http://www.cert-in.org.in.

[176] PTI, "Cashless push: Computer Emergency Response Team to check cyber frauds," The New Indian Express, February 1, 2017, http://www.newind- ianexpress.com/business/union-bud- get-2017/2017/feb/01/cashless-push-computer-emergency-response-team- to-check-cyber-frauds-1565845.html.

[177] The Cyber Appellate Tribunal allows any person that may be aggrieved by an order by the Controller of Certify- ing Authorities, or by an adjudicating officer, to file an appeal before the Tribunal. For more information, see: Ministry of Electronics and Information Technology, "Cyber Appellate Tribunal," http:// meity.gov.in/content/cat.

Its mission is “To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders”.

Functions and Duties:

- National nodal agency for all measures to protect nation's critical information infrastructure.
- Protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats.
- Identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.
- Provide strategic leadership and coherence across Government to respond to cyber security threats against the identified critical information infrastructure.
- Coordinate, share, monitor, collect, analyze and forecast, national level threat to CII for policy guidance, expertise sharing and situational awareness for early warning or alerts. The basic responsibility for protecting CII system shall lie with the agency running that CII.
- Assisting in the development of appropriate plans, adoption of standards, sharing of best practices and refinement of procurement processes in respect of protection of Critical Information Infrastructure.
- Evolving protection strategies, policies, vulnerability assessment and auditing methodologies and plans for their dissemination and implementation for protection of Critical Information Infrastructure.
- Undertaking research and development and allied activities, providing funding (including grants-in-aid) for creating, collaborating and development of innovative future technology for developing and enabling the growth of skills, working closely with wider public sector industries, academia et al and with international partners for protection of Critical Information Infrastructure.
- Developing or organising training and awareness programs as also nurturing and development of audit and certification agencies for protection of Critical Information Infrastructure.

- Developing and executing national and international cooperation strategies for protection of Critical Information Infrastructure.
- Issuing guidelines, advisories and vulnerability or audit notes etc. relating to protection of critical information infrastructure and practices, procedures, prevention and response in consultation with the stake holders, in close coordination with Indian Computer Emergency Response Team and other organisations working in the field or related fields.
- Exchanging cyber incidents and other information relating to attacks and vulnerabilities with Indian Computer Emergency Response Team and other concerned organisations in the field.
- In the event of any threat to critical information infrastructure the National Critical Information Infrastructure Protection Centre may call for information and give directions to the critical sectors or persons serving or having a critical impact on Critical Information Infrastructure.

CHAPTER - 13: CONCLUSION

Many guidelines and debates exist at international level on how governments and organisations can create security as resilience through a variety of governance methods, forms and modes. It is also evident, however, that among the stakeholders involved, there is still much debate as to how security as resilience should be achieved, in particular in relation to the fundamental rights and security balance debate. The Snowden revelations have only served to exacerbate argument on such a balance, and provide justification to states that have used a national security first approach to enforce a security of control around their Internet space. Aside from this, there is also somewhat of a tension between the commercial logic and the security as resilience logic that at the moment is not adequately addressed in terms of the meta-governance of regulation, as well as between the sovereign logic of certain states and the open multi-stakeholder approach advocated by many leading states and international organisations.

There is a clear recognition in the international community that global norms to govern the behaviour of states and other actors are required if a global culture of security is going to emerge in cyberspace, and there are also very clear guidelines and a broad consensus on some of the key principles that should underpin any global framework. Indeed progress has been made by the UN Group of Experts on the applicability of international law; the Tallinn Manual was published, and CBMs were agreed at the OSCE. However, whilst there is certain convergence at the level of broad principles, consensus is far from apparent when analysing the logics of resilient security governance that underpin the construction of the more specific aspects of such principles, and the policy prescription that results from them across different state borders. Indeed, it is apparent that how cybersecurity is perceived between and within levels by the different international actors creates both opportunities and constraints for achieving security as resilience in a truly global sense – which is critical given the borderless nature of the cybersecurity problem.

Moreover, this points to the importance of the politics of security resilience being at the centre of the debate in the development of an effective global ecosystem. The tensions and contradictions at the centre of the different logics within the (geo)politics of cyberspace – represented within various codes of conduct, guidelines, principles and international laws and charters constructed and agreed, are what the EU must continue to engage with, draw from

and effectively connect with and shape, if its own efforts to create a comprehensive ecosystem of resilient security governance are to bear fruit. It is already evident that the EU, in constructing its current positions, is embedded within the broader global ecosystem: the chapters that follow will provide an analysis of how such existing global norms have been shaped by and helped to shape national and EU strategies within the different facets of cybersecurity.

baseline conclusions

As presented above, the institutional cyber security landscape consists of a complex array of organizations that exhibit significant diversity with regard to missions, mandates, interests, opportunities, and constraints.

Characteristic Features

On these bases, we put forth the following observations:

a) The information technology-sustainable development linkage has become an integral feature of the international community's policy priorities.

b) The current institutional landscape resembles a security patchwork that covers critical areas rather than an umbrella that spans all of the known modes and sources of cyber threat.

c) Given the multiple contexts and diverse institutional motivations, we expect that responses will be driven more by institutional imperatives and reactions to crisis than by coordinated assessment and proactive response.

d) Due to the complex global agenda at all levels of development, states may not be willing to proceed until international norms are developed, rather they will 'take matters in their own hands' and develop first order responses.

e) Cross-sector collaboration among public, private, and volunteer organizations may serve as a temporary measure to cover holes in the current defense network. However, at some point effective institutions will be necessary; they may develop in parallel with rising public awareness.

f) So far, we have not yet seen large terrorist groups engaged in intense cyber malfeasance. This pattern cannot be expected to continue. Efforts to infiltrate critical US infrastructure and the devastating attacks on Estonia and Georgia in 2007 and 2008 underline the dangers of

being lulled into a false sense of security. As the Internet becomes increasingly central to modern society, it is likely that criminals, terrorist groups, and other opponents to state authority will target this sector in the hopes of disrupting critical national functions. So far, the potential for significant threats is far greater than institutional capabilities to contain these threats. In other words, the 'demand' for security far exceeds the provision of effective "supply."

Institutional anchors for cyber security

Such features notwithstanding, based on the evidence to date, we suggest that considerable strides have been made to establish foundations for collaborative responses. In the best of all possible worlds, we would expect to see the emergence of a collaborative framework – a large umbrella network – allowing autonomous organizations to flexibly adapt to emerging threats in a coordinated manner and increases the impetus for information sharing in the realm of cyber security. While the potential for such an umbrella network has yet to be realized, we can now point to some institutional anchors that could support, or even consolidate, such a development:

a) The establishment of not-for-profit institutions designed to focus on cyber threats (CERT/CC, FIRST, private CERTs, and ISACs), however "disorganized," is a growing trend on the international landscape. In some instances, these institutions have transitioned to private-public partnerships.

b) A number of International institutions established to manage interactions among advanced states (notably supported by the OECD) reinforce rather than undermine this development.

c) International conferences designed to communicate the potential for information technology to facilitate transitions towards sustainable development (WSIS), while not centered on security issues, nonetheless have the advantage of large-scale private and public participation, thus raising the political profile of cyber issues globally.

d) The functional international organizations with core missions and competencies (notably the ITU) have adopted security as part of their missions.

e) Despite these seemingly complex and uncoordinated responses at the national level, specific agencies are more and more tasked with responding to cybercrime (notably the FBI in the US).

f) The development of binding international legislation (i.e. the Convention on Cybercrime) elevates the sense of vulnerability as well as the need to coordinate responses to a higher level of awareness than ever before.

g) In the field of military security framed more formally, we observe the salience of organizations and strategies focused on the defense of military and intelligence networks (i.e. CCDOE, CNCI).

h) Sharing between public and private institutions is increasingly hampered by liability, reputational and economic concerns, which the US is increasingly addressing by establishing or promoting private-led information sharing institutions (notably ISACs and ISAOs) to further facilitate these exchanges.

Each of these institutional responses reflects mandates, rules and responsibilities. None are accorded complete regulatory power. Indeed, there is little evidence of overarching institutional coordination or routinization. On one hand, this pattern represents a certain degree of disconnect. On the other, it can be seen as a dynamic and shifting response to dynamic set of cyber threats. In the latter context, one could argue that the increasingly dense landscape of institutional responses is an excellent indication that the international community is taking serious steps to control a cyber threat of epidemic proportions.

In this connection, it can be expected that, over time, we will see more and more forms of lateral intergovernmental cooperation with the requisite institutional cross-border institutional collaboration. The theoretical foundations for such developments are accommodated by the structure of the process of transnational activities as framed by Nye and Koehane (1977) and the extensions in transnational governance outlined by Slaughter (2004) in the context of globalization processes.

Critical missing piece

Although the current system of institutional arrangements shows signs of weakness, it is also true that the level of organization and cooperation has been steadily increasing. Missing from these international institutional developments (and thus from the above analysis) is a critical piece of institutional architecture to support a fundamental function, namely systematic consideration for data issues and matters of data provision and alignment. To some degree, the effectiveness of this effort can be quantified through the use of statistics.

While a relatively small number of organizations produce reliable data, sufficient information exists to develop a model that maps degree of vulnerability versus the effectiveness of organizational response. For instance, international data on cybercrime legislation and awareness can be correlated with arrest rates in individual countries. When combined with stocktaking databases, this method allows one to determine the rate of progress in individual nations versus cybercrime issues. Similarly, quantitative data provided by national CERTs can be used to obtain insights about their performance in their respective national contexts and constituencies. An example of these kinds of analysis, along with a Data Dashboard tool, can be found in the report (Madnick, Li, et al., 2009b).

Over time, we anticipate the possibility of pairing international and national statistics with information from the private sector. Security and monitoring companies such as Symantec, Arbor Networks, Microsoft, and McAfee provide quantitative data that address the global spread of Internet vulnerabilities. In many cases, the volume and quality of data released by these organizations far outpaces the information released by international and national organizations; however, the true value of this information lies not in an isolated analysis, but in the intersection of private data with the national and international sphere. For instance, statistics concerning the originating country of cyber attacks or the absolute volume of attacks can potentially be paired with national CERT data to determine the degree of national vulnerabilities and traffic that each CERT is capable of handling.

These metrics, and others that can potentially be derived, may provide a powerful method of simultaneously evaluating data quality and organizational performance. An important next step in our inquiry is to examine additional data providers and explore ways of pairing this data with national and international organizations to form evaluative statistical models. While doing so, it is important to remain cognizant of the institutional context that that enables or constrains the provision of information.

BIBLIOGRAPHY

- Abhishek Bhalla, "Modi government gets cracking on cyber espionage," Mail Today, June 28, 2016, http://indiatoday. intoday.in/story/modi-govt-gets-crack- ing-cyber-espionage/ 1/702377.html.
- Barnett, Michael and Jack Levy (1991), 'Domestic sources of alliances and alignments', International Organization, 45(3): 369–395
- Bendiek, A. (2014), 'Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection', Stiftung Wissenschaft und Politik (SWP), SWP Research Paper, Berlin, March 2014.
- Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-
- Bennett, D.S. (1996), 'Testing alternative models of alliance duration, 1816–1984', American Journal of Political Science, 41(3): 846–878.
- Biswarup Sen, "Digital Politics and Culture in Contemporary India: The Making of an Info-Nation," (New York, NY: Routledge, 2016): 71-72.
- Can Play a Big Role in Cyber Security Globally," July 2, 2015, NDTV, http:// www.ndtv.com/india-news/digital-india- pm-modi-says-india-can-play-a-big- role-in-cyber-security-globally-777319.
- Checkel, J.T. (2005), 'International institutions and socialization in Europe: introduction and framework', International Organization, 59(4): 801–826.
- Christou, G. and Simpson, S. (2007), The New Electronic Marketplace: European Governance Strategies in a Globalising Economy, London: Edward Elgar.
- Christou, G. and Simpson, S. (2011), 'The European Union, Multilateralism and the Global Governance of the Internet', Journal of European Public Policy, 18(2), 241–257.
- Cornish, P., Livingstone, D., Clemente, D. and York, C. (2011), 'Cyber Security and the UK's Critical National Infrastructure', A Chatham House Report, Chatham House, September 2011.
- Cyber frauds cost India $4 billion, The Hindu, October 23, 2013, http:// www.thehindu.com/business/ Economy/cyber-frauds-cost-india- 4-billion/ article5261594.ece.
- Cyber Security Strategy of the UK: Safety, Security and Resilience in Cyberspace' (2009), Office of Cyber Security and UK Cyber Security Operations Centre, June 2009

- Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7 February 2013, JOIN (2013) 1 final
- Deloitte, "Digital India: Unleashing Prosperity," Deloitte (2015): 3.
- Department of Electronics and Information Technology, "Digital India," http:// www.cmai.asia/digitalindia/ pdf/Digital-India-DeITY-Details.pdf.
- Department of Information Technology, "RFD: Results-Framework Document for ICERT 2011-2012," (2012), http://www.cert-in.org.in/ Images/CERT-In_RFD2011-12.pdf.
- Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.
- Deutsch, Karl W. (1957), Political Community in the North Atlantic Area (Princeton, NJ: Princeton University Press).
- Dhruva Jaishankar, "Internet Freedom 2.1: Lesson's from Asia's Developing Democracies," German Marshall Fund (March 2015): 13.
- Dhruva Jaishankar, "Internet Freedom 2.1: Lesson's from Asia's Developing Democracies," German Marshall Fund (March 2015): 8.
- Digital Britain (2009), Final Report, June 2009. Department for Culture Media and Sport and Department for Business, Innovation and Skills. Available at: https://www.gov.uk/ government/uploads/system/uploads/ attachment_data/file/228844/7650.pdf
- Digital India: PM Modi Says India Can Play a Big Role in Cyber Security Globally, July 2, 2015, NDTV.
- Dilip Kumar Mekala, "The government needs to be more serious about India's cyber security," Force, July 2015, http:// forceindia.net/MuchtoWorryAbout.aspx.
- Downing, E. (2011), 'Cyber Security – A New National Programme', Science and Environment Section, SN/SC/5832, House of Commons Library, 23 June 2011.

- Downing, E. (2011), 'Cyber Security – A New National Programme', Science and Environment Section, SN/SC/5832, House of Commons Library, 23 June 2011.

- Dunn Cavelty, M. (2008a), Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London and New York: Routledge.

- ENISA (2012), 'On National and International Cyber Security Exercises: Survey, Analysis and Recommendations', ENISA, October 2012. Available at: http:// www.enisa.europa.eu/ activities/Resilience-and-CIIP/cyber-crisis-cooperation/ cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1.
- European Commission (1999), Communication of 8 December 1999 on a Com- mission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000 – eEurope – An Information Society for All, COM (1999) 687 Final (not published in the Official Journal).
- European Commission (2001a), 'Creating a Safer Information Society by Improv- ing the Security of Infrastructures and Combating Computer-Related Crime', COM (2000) 890, 26 January 2001.
- European Commission (2001b), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Network and Information Security: Proposal for A European Policy Approach, COM (2001) 298 Final, Brussels, 6 June 2001.
- European Commission (2005), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'i2010 – A European Information Society for growth and employment', COM (2005) 229 Final, Brussels, 1 June 2005.
- European Commission (2010), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A Digital Agenda for Europe', COM (2010) 245 final/2, 26 August 2010.
- European Parliament (2011), On the Proposal for a Directive of the European Parliament and of the Council on Combating Sexual Abuse, Sexual Exploita- tion of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, (COM(2010)0094 – C7-0088/2010 – 2010/0064(COD)), Draft Report, {LIBE}Committee on Civil Liberties, Justice and Home Affairs, 24 January 2011. Available at: http://www.europarl.europa.eu/ sides/getDoc.do? type=COMPARL&mode=XML&language=EN&reference=PE452.564

- European Parliament and the Council (2011), Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA.
- Gaubatz, K.T. (1996), 'Democratic states and commitment in international relations', International Organization, 50(1): 109–150.
- Geetha Nandikotkur "India Opens Cyber Coordination Centre" April 13, 2015, http:// www.bankinfosecurity.asia/india-opens-cyber-co- ordination-centre-a-8100.
- Gjelten, T. (2010), Seeing the Internet as an 'Information Weapon', 23 September 2010, Available at: http://www.npr.org/templates/story/story.php? storyId=130052701
- Goldsmith, J. (2011), Cybersecurity Treaties: A Skeptical View, Future Challenges Essay, Hoover Institution, Stanford University.
- Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018
- Hart, A. G. (2001), 'The G8 and the Governance of Cyberspace', in Fratianni, M. (ed.) New Perspectives on Global Governance: Why America Needs the G8, Aldershot: Ashgate Publishing Limited.
- Healey, J. (2011a), 'Comparing Norms for National Conduct in Cyberspace', 20th September 2011. Available at: http://www.acus.org
- Healey, J. (2011b), 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms', 21 September 2011. Available at: http://www.acus.org
- Healey, J. (2011b), 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms', 21 September 2011. Available at: http://www.acus.org
- House of Lords, EU Committee 13th Report of Session 2013–2014, 'Strategic guidelines for the EU's next Justice and Home Affairs Programme: Steady as She Goes', HL Paper 173, House of Lords, April 2014. Available at: http:// www.parliament.uk/business/ committees/committees-a-z/lords-select/eu -home-affairs-sub-committee-f-/inquiries/ parliament-2010/rome-programme/
- Huang S (2016) Research on the problems and countermeasures of public security information application. J Hubei Police Acad (2):71–75

- In July 2016, the Ministry of Communications and Information Technology was bifurcated into the Ministry of Communications and Ministry of Electronics and Information Technology (MeitY). For more information on MeitY, see: http:// meity.gov.in/.
- India Internet Users, Internet Live Stats, July 1, 2016, http://www.inter- netlivestats.com/ internet-users/india/.
- Indian Computer Emergency Response Team, "Annual Report," http://www.cert-in.org.in.
- Indian Computer Emergency Response Team, "Welcome to CERT- In," http://www.cert-in.org.in.
- Indian Computer Emergency Response Team, "Welcome to CERT- In," http://www.cert-in.org.in.
- Institute for Defense Studies and Anal- yses, "IDSA Task Force: India's Cyber Security Challenge," (March 2012): 19.
- International Institutions and Global Governance Program, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms", Council on Foreign Relations, February 23, 2018; available at: https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms; Last accessed: June, 2021.
- International Telecommunications Union (ITU) (2008) Global Cybersecurity Agenda, High level Experts Group, Global Strategic Report, ITU.
- International Telecommunications Union (ITU) (2008a) Q.22/1 Report on Best Practices for a National Approach to Cyber Security: A Management Framework for Organizing National Cybersecurity Efforts (2008), ITU-D Secretariat, January 2008.
- International Telecommunications Union (ITU) (2011) National Cybersecurity Strategy Guide, ITU, September 2011.
- International Telecommunications Union, "Percentage of individu- als using the internet," (2015).
- Jeetendra Pande, Introduction to Cyber Security, Uttarakhand Open University, 2017; Available at: https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf
- Jia X, Wang J (2016) Discussion on the reform of public security information security personnel training mode based on the teaching of network attack and defense. Information and Computers 9:231–233

- John S. Duffield and Others, “Alliances”, Security Studies: An Introduction, Routledge, 2008.
- Joshua Ball, What is Security? Everything, Global Security Review, 2019; available at: https://globalsecurityreview.com/what-is-security-everything/
- Karl Heinz Gaudry Sada and others, Regional Organizations, “The SAGE Encyclopedia of War: Social Science Perspectives”, SAGE Publications, Inc.; 2017; available at: http://dx.doi.org/10.4135/9781483359878.n551
- Klimburg, A. (2011b), ‘Ruling the Domain: Self-Regulation and the Security of the Internet’, Austrian Institute of International Affairs, Paper Distributed at the 11th Meeting of the ICANN Studienkreis, 28/29 April 2011.
- Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.
- Li H (2017) Discussion on public security computer network and information security. In: Net- work security technology and application magazine. 2017(8) In Chinese. http://www.xueshu. com/wlaqjsyyy/201708/29810655.html
- Mahdi Haddadi, “Regional Organisations and International Peace and Security in Middle East”, International Journal of Academic Research in Business and Social Sciences, March 2015, Vol. 5, No. 3; Available at: https://hrmars.com/papers_submitted/1518/Regional_Organizations_and_International_Peace_and_Security_in_the_Middle_East.pdf
- Mattis P (2012) The Analytic Challenge of Understanding Chinese Intelligence Services. In” Studies in Intelligence. 56(3):47–57. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding% 20Chinese%20Intel.pdf
- McCalla, R.B. (1996), ‘NATO’s persistence after the cold war’, International Organization, 50(3): 445–475
- Melissa Hathaway’s interview with Arvind Gupta, Deputy National Security Advisor, at the Cyber 360: A Synergia Conclave, Bangalore India, September 29, 2015.
- Meyer, P. (2013), ‘Cyber Security Takes the Floor at UN’, Canadian International Council, 12 November 2013. Available at: http://opencanada.org/features/the -think-tank/comments/cyber-security-takes-the-floor-at-the-un/

- Ministry of Communications and Information Technology, "National Cyber Security Policy," Department of Electronics and Information Technology (July 2, 2013): 2.
- Ministry of Communications and Information Technology, "National e-Governance Plan," http://meity.gov. in/content/national-e-governance-plan.
- Ministry of Electronics and Information Technology (MeitY), "Digital India: About the Programme," http://www. digitalindia.gov.in/content/about-pro- gramme, and "Digital India: Programme Pillars," http://www.digitalindia.gov. in/content/programme-pillars.
- Mohan, R. (2011), DNSSEC Baby Steps Reported at ICANN 41, CircleID Internet Infrastructure, 29 July 2011.
- Muktesh Chander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," National Technical Research Organisation, http:// www.slideshare.net/ CERCatIIITD/ national-critical-information-infra- structure-protection-centre-nciipc.
- Muktesh Chander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," National Technical Research Organisation, http:// www.slideshare.net/ CERCatIIITD/ national-critical-information-infra- structure-protection-centre-nciipc.
- NASSCOM, "eCommerce Snapshot," http://www.nasscom.in/ecommerce.
- NASSCOM, "IT-BPM Overview," http:// www.nasscom.in/indian-itbpo-industry.
- National Technical Research Organisation, "National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter, and Responsibilities," http:// www.slideshare.net/CERCatIIITD/ national-critical-information-infra- structure-protection-centre-nciipc.
- Nazli Choucri et al, "Institutions for Cyber Security: International Responses and Data Sharing Initiatives, Working Paper CISL# 2016-10, August 2016, Cybersecurity Interdisciplinary Systems Laboratory (CISL), 2016
- Neville-Jones, P. and Phillips, M. (2012), 'Where Next for UK Cyber-Security?' RUSI Journal, 157(6), Dec 2012, 32–40.
- Noshiravani, R. (2011), NATO and Cyber Security: Building on the Strategic Concept, 20 May 2011, Rapporteur Report, The NATO Science for Peace and Security Programme, Chatham House.
- O'Neill, M. (2012), 'Cyber Crime and Cyber Security: A Late Developer in the EU's AFSJ', Draft Paper, Presented at Cybercrime and Cyber Security Workshop, University of Abertray, Dundee, 10 September 2012.

- OECD (2002), 'OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security', Organisation for Economic Cooperation and Development, Paris, France.
- of Performing Functions and Duties) Rules, 2013," (January 16, 2014), http://meity.gov.in/ sites/upload_files/ dit/files/G_S_R%2020%20(E)2.pdf.
- Osgood, R.E. (1968), Alliances and American Foreign Policy (Baltimore, MD: The Johns Hopkins University Press).
- Porcedda, G. M. (2012), Data Protection and the Prevention of Cybercrime: The EU as an Area of Security? EUI Working Papers, Law 2012/25, Department of Law. Available at: http://cadmus.eui.eu/bitstream/handle/1814/23296/ LAW-2012-25.pdf?sequence=1
- Press Trust of India, "Internal Security Will be a Big Challenge for India: Ajit Doval," NDTV, October 31, 2015, http://www.ndtv.com/india-news/ internal-security-will-be-a-big-chal- lenge-for-india-ajit-doval-1238573.
- PTI, "Cashless push: Computer Emergency Response Team to check cyber frauds," The New Indian Express, February 1, 2017, http://www.newind- ianexpress.com/business/ union-bud- get-2017/2017/feb/01/cashless-push- computer-emergency-response-team- to-check-cyber-frauds-1565845.html.
- Pukhraj Singh, "In Cyberspace Warfare, India is Still Shooting in the Dark", The Quint, February 26, 2016, https://www.thequint.com/opin- ion/2016/02/25/in-cyberspace-warfare- india-is-still-shooting-in-the-dark.
- Pukhraj Singh, "Thinking Offensively!", Seminar: The Monthly Symposium, October, 2016, http://www.india-seminar. com/2013/650/650_pukhraj_sing.htm .
- Rohit, KALAKUNTLA and others, Cyber Security, HOLISTICA Vol 10, Issue 2, 2019, PP. 115-128;
- Samuel, K. O., & Osman, W. R. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.
- Scott, M. (2010), 'With Three Months to go to DNSSEC, Someone's Fudging Root Zone Records', Betanews, March 2010. Available at: http://www.betanews.com/article/with-three-months-to-go-to-DNSSES-someones-fudging-root-zone-records/1269642342 (accessed June 2013).

- SD Pradhan, “Cyber security: Need for an overall national cyber strategy,” The Times of India, January 18, 2016, http://blogs.timesofindia. indiatimes.com/ChanakyaCode/ cyber-security-need-for-an-over- all-national-cyber-strategy/.
- Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).
- Snyder, Glenn H. (1997), Alliance Politics (Ithaca, NY: Cornell University Press).
- Steve Morgan, “Cybercrime to cost the world $10.5 Trillion annually by 2025”, Cybercrime Magazine, November 13, 2020; Available at: https:// cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ ; Last accessed: June, 2021.
- Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), Pre- pared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press.
- The Gazette of India, “The Informa- tion Technology Act of 2008,” Indian Ministry of Law and Justice, (February 5, 2009): 14, http://meity.gov.in/sites/ upload_files/dit/files/ downloads/ itact2000/it_amendment_act2008.pdf.
- The Gazette of India, “The Information Technology Act of 2008,” (February 5, 2009), and “The Information Technology (The Indian Computer Emergency Response Team and Manner
- Tick, E. (2010), Global Cyber Security – Thinking About the Niche for NATO, The SAIS Review of International Affairs, Fall 2010 (pre-publication).
- Unique Identification Authority of India, “State/UT wise Aadhaar Saturation: Annexure 1,” https://uidai.gov.in/images/ news/aadhaar_saturation_15082016.pdf.
- Unique Identification Authority of India, “UIDAI Background,” https:// uidai.gov.in/ about-uidai.html.
- USCC (2016) China’s intelligence services and espionage operations hearing before the U.S.-China economic and security review commission, 9 June 2016. https:// www.uscc.gov/sites/default/files/ transcripts/ June%2009%2C%202016%20Hearing%20Transcript.pdf

- Venkatesh Ganesh, “India lagging Lagging in cyber Cyber security Security awarenessAwareness,” The Hindu BusinessLine, August 29, 2016, http:// m.thehindubusinessline.com/ info-tech/india-lagging-in-cyber-secu- rity-awareness/ article9046626.ece.
- Vijay Mohan, “Fresh wave of cyber attacks hits India,” The Tribune, February 11, 2016, http://www.tribuneindia. com/2010/20100212/main7.htm.
- Volter, W. (2013), ‘The UN Takes a Big Step Forward on Cybersecurity’, Arms Control Today. Available at: https://www.armscontrol.org/act/2013_09/The-UN -Takes-a-Big-Step-Forward-on-Cybersecurity
- Wallander, Celeste A. (2000), ‘Institutional assets and adaptability: NATO after the cold war’, International Organization, 54(4): 705–735.
- Walt, Stephen M. (1985), ‘Alliance formation and the balance of world power’, International Security, 9(4): 1–43
- Walt, Stephen M. (1985), ‘Alliance formation and the balance of world power’, International Security, 9(4): 1–43
- Walt, Stephen M. (1997), ‘Why alliances endure or collapse’, Survival, 39(1): 156–179
- Wang H (2017) 1116 cyber-security police units have been set up nationwide. Beijing: Guangming 14 Feb 2017. http://epaper.gmw.cn/gmrb/html/2017-02/14/ nw.D110000gmrb_20170214_2-04. htm
- Weitsman, P.A. (2004). Dangerous Alliances: Proponents of Peace, Weapons of War (Stanford, CA: Stanford University Press)
- Weitsman, P.A. (2004). Dangerous Alliances: Proponents of Peace, Weapons of War (Stanford, CA: Stanford University Press).
- Wong KC (1994) Public security reform in China in the 1990s. In: Brosseau M, Lo CK (eds) China annual review 1994. Chinese University Press, Hong Kong, pp. 5.1–5.33
- World Bank, “World Development Report 2016: Digital Dividend,” Wash- ington, DC: World Bank (2016): 7-8.
- Yang Z (2017) China’s public security intelligence: progress, challenges, and prospects. George- town J Asian Aff. https://asianstudies.georgetown.edu/sites/asianstudies/files/ documents/gjaa_3. 2_yang.pdf (Spring 2017)
- Yu Y, Hu W (2013) Intrusion detection algorithm design in the public security system for network monitoring. Bull Sci Technol 29(6):185–190

- Zeng X (2010) Research on management of internet by police in west of China. Netw Secur Technol Appl 4:18–20
- Zeng Z, Yang K, Zhang Y and Zhou P (2013) Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management. In: 2013 Fourth International Conference on Digital Manufacturing & Automation. 684–687