INTERNATIONAL BODIES IN INFORMATION TECHNOLOGY

By Group Captain P Aanand Naidu (retd)

CHALLENGES AND SOLUTIONS

- Cyberthreats and attacks give rise to ever-growing security challenges for both the public and private sectors in all countries. Cybersecurity-related incidents can compromise the availability, integrity and confidentiality of information transiting on networks and disrupt the operations and functioning of critical infrastructures. They can also compromise the security of people and whole countries.

- In increasingly digital societies, cyber-incidents may have greater impact in the physical world on infrastructure connected to the public Internet. They can impact countries' economic and social development, compromising the integrity of critical information and communication infrastructures (including emergency services, water supplies and power grids, food distribution chains, aircraft and shipping, navigation systems, industrial processes and supply, healthcare, public transportation and government services).
- Attacks can be mounted from any part of the world, and they can transcend borders. It is often stated that cybersecurity is only as strong as its weakest link. Therefore, countries need to work together to achieve a minimum appropriate level of security capacity, so weak links can be identified and strengthened.

Organisations

- International organizations
  - IGOs
  - INGOs
- National/state Org
  - Govt/state
  - NGOs

International Org

- International organizations are the organizations established by a treaty or other instrument governed by international law and possessing its own international legal personality
- International organizations generally have States as members, but often other (non-state) entities can also apply for membership.

International Org

- International and supranational organizations: an intergovernmental organization or international governmental organisation (IGO) is an organization composed primarily of sovereign states (referred to as member states), or of other intergovernmental organizations.
- Intergovernmental organizations are called international organizations, although that term may also include international non-governmental organization such as international non-profit organizations or multinational corporations.
- IGOs are generally established by a treaty or convention that acts as a charter creating the group. Treaties are formed when lawful representatives (governments) of several states go through a ratification process, providing the IGO with an international legal personality.

International Org

- The two main types of international organizations are
  - intergovernmental organizations (IGOs)
  - International nongovernmental organizations(INGOs)

- Important Int Org in IT and Cyber Security are:
  - UNO
  - ITU
  - Interpol

Regional Organisations

- Regional organization: Regional organizations (ROs) are, in a sense, international organizations (IOs), as they incorporate international membership and encompass geopolitical entities that operationally transcend a single nation state
- Membership is characterized by boundaries and demarcations characteristic to a defined and unique geography, such as continents, or geopolitics, such as economic blocs.
- Established to foster cooperation and political and economic integration or dialogue among states or entities within a restrictive geographical or geopolitical boundary.

Regional Organisations

- Eg:
  - the African Union (AU),
  - Association of Southeast Asian Nations (ASEAN); Arab League (AL)
  - Caribbean Community (CARICOM); Council of Europe (CoE)
  - Eurasian Economic Union (EEU); European Union (EU)
  - South Asian Association for Regional Cooperation (SAARC)
  - Asian-African Legal Consultative Organization (AALCO),
  - Union for the Mediterranean (UfM)
  - Union of South American Nations (USAN)

UN Res 55/63 of 2000

Combating the criminal misuse of information technologies

- States should ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies
- Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States
- Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies
- Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies
- Prevention of Crime and the Treatment of Offenders

UN Res 55/63 of 2000..

Combating the Criminal misuse of IT

- Recalls the UN Millennium Declaration on beneficial use of IT
- Role of UN Commission on Crime and Criminal Justice
- Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations
- Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases

UN Res 55/63 of 2000..

- Cooperation between states and private Industry
- To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence
- The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse
- Protection of confidentiality, integrity and availability of data

UN Res 55/63 of 2000..

- Timely investigations of cases involving criminal misuse of IT
- The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies
- It systems design to facilitate prevention and detection of crimes , tracing criminals and collect evidence
- Invites States to take into account the above-mentioned measures in their efforts to combat the criminal misuse of information technologies

UN Res 57/239

Creating a global culture of cybersecurity

- Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks (“participants”) must approach cybersecurity.
- Cyber security is not a matter of govt and law enforcement practices but addressed through prevention and supported by society

UN Res 57/239

- A global culture of cybersecurity will require that all participants address the following nine complementary elements:
  - Awareness. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security
  - Responsibility. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment

UN Res 57/239…

- Response. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation
- Ethics. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;
- Democracy. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency

UN Res 57/239…

- Risk assessment. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected
- Security design and implementation. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks
- Security management. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations
- Reassessment. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

UN Res 58/199

Elements for protecting critical information infrastructures

- Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents
- Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them
- Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures
- Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures

UN Res 58/199….

- Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations
- Ensure that data availability policies take into account the need to protect critical information infrastructures
- Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States
- Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities

UN Res 58/199…

- Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate
- Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws
- Promote national and international research and development and encourage the application of security technologies that meet international standards.

UN Res 64/211

- Voluntary self-assessment tool for national efforts to protect critical information infrastructures
- Taking stock of cybersecurity needs and strategies
  - 1. Assess the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.
  - Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures and civil society that must be managed.
  - Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present and the current management plan; note how changes in the economic environment, national security priorities and civil society needs affect these calculations.
  - Determine the goals of the national cybersecurity and critical information infrastructure protection strategy; describe its goals, the current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives and how such a strategy fits within regional and international initiatives

UN Res 64/211

- This is a voluntary tool that may be used by Member States, in part or in its entirety, if and when they deem appropriate, in order to assist in their efforts to protect their critical information infrastructures and strengthen their cybersecurity.

Stakeholder roles and responsibilities

- Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including: • National Government ministries or agencies, noting primary points of contact and responsibilities of each; • Other government (local and regional) participants; • Non-governmental actors, including industry, civil society and academia; • Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity. Policy processes and participation

UN Res 64/211

- Identify formal and informal venues that currently exist for Government industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.
- Identify other forums or structures that may be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals. Public-private cooperation 8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for informationsharing and incident management.

UN Res 64/211

- Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure. Incident management and recover
- Identify the Government agency that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.
- Separately, identify national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing tools and procedures for the dissemination of incident-management information.

UN Res 64/211

- Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate Legal framework
- Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime
- Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues
- Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

UN Res 64/211

- Examine national participation in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network
- Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere. Developing a global culture of cybersecurity
- Summarize actions taken and plans to develop a national culture of cybersecurity referred to in General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements.

73/27 on 'Developments in the Field of Information

Open-Ended Working Group (OEWG) comprising the entire UN membership will be set up in 2019. The OEWG will report to the UNGA in 2020. Its mandate will be:-[3]

* to make the United Nations negotiation process on "security in the use of information and communications technologies more democratic, inclusive and transparent";
* to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations;
* to further develop the rules, norms and principles of responsible behaviour of States… and the ways for their implementation; and if necessary, to introduce changes to them or elaborate additional rules of behaviour;
* to continue to study the potential threats in the sphere of information security and identify possible cooperative measures to address them;
* to study how international law applies to the use of information and communications technologies by States,
* to study confidence-building and capacity building measures.

73/266 on 'Advancing Responsible State

Group of Governmental Experts (UNGGE) will be set up to study the question of norms and behaviours in cyber-space. The new group will have 25 members. Its chair will also hold informal consultations with all UN member states in between its sessions as well as with regional organisations such as African Union, the European Union, the Organisation of American States and the Organisation for Security and Cooperation in Europe and the ASEAN regional Forum. The UNGGE will produce its report by 2021. The mandate of the group is to continue to study[4]:-

* possible cooperative measures to address existing and potential threats in the sphere of information security,
* the norms, rules and principles of responsible behaviour of States,
* confidence building measures,
* capacity-building,
* how international law applies to the use of information and communications technologies by States,
* how international law applies to the use of information and communications technologies by States.

ITU

- ITU serves as a platform for
  - global dialogue, helping its Member States and membership in setting security-related international standards, helping countries define cybersecurity strategies and set up computer incident response teams (CIRTs)
  - protecting children online, building human capacity and facilitating policy dialogue.ITU assists Member States in developing and improving effective national cybersecurity frameworks or strategies.
  - At the national level, cybersecurity is a shared responsibility which requires coordinated action for prevention, preparation and response on the part of government agencies, authorities, the private sector and civil society. To ensure a safe, secure and resilient digital realm, a comprehensive national framework or strategy is necessary.
- In 2008, ITU launched the Child Online Protection (COP) Initiative, a multi-stakeholder effort which works towards creating a safe and empowering online experience for children around the world. In cooperation with diverse partners, ITU has been providing guidance and building capacities in various countries - involving policy-makers, parents, educators and children.
- ITU issues the Global Cybersecurity Index (GCI) which sheds light on the commitment of ITU Member States to cybersecurity to create a safe space for Internet users in their country.

ITU

- Effective mechanisms and institutional structures are necessary at the national level to reliably deal with cyberthreats and incidents. ITU assists Member States in establishing and enhancing National Computer Incident Response Teams (CIRTs). In response to the fast-evolving technologies and manifestation of related threats, incident response must be continuously updated and improved.
- ITU conducts regional and national cyberdrills to strengthen national and international cooperation among ITU Member States against cyberthreats and cyberattacks. To date, ITU has conducted cyberdrills involving over 100 countries.
- ITU study groups provide a neutral, global platform for ITU members to develop international standards addressing security.
- ITU-T Study Group 17 is the lead ITU group for security, mandated to 'build confidence and security in the use of ICTs'. The group develops global security architectures and frameworks supporting authentication and identity management, security aspects of communication applications, cybersecurity, the protection of personally identifiable information, and more.
- To maximize impact, ITU is working closely with partners from international organizations, the private sector, industry associations and academia, including e.g. the World Economic Forum and Interpol.

ITU Global Cybersecurity Agenda (GCA)

- The **ITU Global Cybersecurity Agenda (GCA)(2007)** is a framework for **international cooperation** aimed at enhancing confidence and security in the information society.
- The GCA is designed for cooperation and efficiency, encouraging **collaboration with and between all relevant partners** and building on existing initiatives to avoid duplicating efforts.
- The GCA has fostered initiatives, such as Child Online Protection, and together with the support of leading global players from all stakeholder groups, continues to deploy cybersecurity solutions to countries around the world.

The GCA has five strategic pillars, also known as work areas:

- Legal Measures
- Technical & Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation

Child Online Protection

- Protecting children online is a global challenge, which requires a global approach. While many efforts to improve child online protection are already under way, their reach has been more national than global.
- ITU launched the Child Online Protection (COP) Initiative in November 2008 as a multi-stakeholder effort within the Global Cybersecurity Agenda (GCA) framework.
- The initiative brings together partners from all sectors of the global community to create a safe and empowering online experience for children around the world. COP was presented to the ITU Council in 2008 and endorsed by the UN Secretary-General, Heads of State, Ministers and heads of international organizations from around the world.

Telecom

- The GCI aims at leaving no country behind regarding its cybersecurity development, using the following objectives to measure:
  - the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
  - progress in cybersecurity commitment of all countries from a global perspective;
  - progress in cybersecurity commitment from a regional perspective;
  - the cybersecurity commitment divide (i.e. the difference between countries in terms of their level of engagement in cybersecurity initiatives).

IGF

The **Internet Governance Forum (IGF)** is a multistakeholder governance group for policy dialogue on issues of Internet governance. It brings together all stakeholders in the Internet governance debate, whether they represent governments, the private sector or civil society, including the technical and academic community, on an equal basis and through an open and inclusive process. The establishment of the IGF was formally announced by the United Nations Secretary-General in July 2006. It was first convened in October–November 2006 and has held an annual meeting since then.

Interpol

- Criminal Police Organization, an inter-governmental organization. Has 194 member countries, and helps police in all of them to work together to make the world a safer place.
- Enables sharing and access data on crimes and criminals, and offers a range of technical and operational support.
- Half of humanity at risk
- Online Crime Is Real Crime
- *Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19*
- *In today's highly digitalized world, the sooner countries are aware of a threat, the sooner they can take steps to mitigate the risk and minimize the cyberthreats coming from all directions*

ICANN

- The **Internet Corporation for Assigned Names and Numbers** is an American multistakeholder group and nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation.
- ICANN performs the actual technical maintenance work of the Central Internet Address pools and DNS root zone registries pursuant to the Internet Assigned Numbers Authority (IANA) function contract. The contract regarding the IANA stewardship functions between ICANN and the National Telecommunications and Information Administration (NTIA) of the United States Department of Commerce ended on October 1, 2016, formally transitioning the functions to the global multistakeholder community.

Thank you