INTERNATIONAL COOPERATION IN FIGHT AGAINSTCYBER-CRIME

INTERNATIONAL COOPERATION IN FIGHT AGAINSTCYBER-CRIME

By

Brigadier Saurabh Tewari

Centre for Joint Warfare Studies
Kashmir House, Rajaji Marg, New Delhi-110 001
Tel. Nos: 011-23792446, 23006535, 23006538/9, **Fax:** 011-23792444
Website: http://cenjows.gov.in, **e-mail:** cenjows@cenjows.gov.in

Price in India : ₹150 /-

The views expressed in the book are of the author and not necessarily those of the Centre for Joint Warfare Studies/publishers.

Printed in India

Printed by
Xtreme Office Aids Pvt. Ltd.
*Basement Bhanot Building (Below Syndicate Bank)
Nangal Raya Commercial Complex, N.D-110046
Ph.: +91-9811707220
E-mail: xtremeofficeaids@gmail.com
Website: www.xtremeonline.in*

INTERNATIONAL COOPERATION IN FIGHT AGAINSTCYBER-CRIME

Disclaimer

The views expressed and suggestions made in this work are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with the author.

Introduction

1. The potency and overwhelming lethal effects of cyber warfare has outpaced the technological development in conventional military weapons space, changing the very character of future wars and the role of cyber warfare in them. Worldwide cyberspace is now being acknowledged as the 5th domain of warfare. There has been a major rise in the use of cyber warfare by nation states over the last decade or so. Further cyber-attacks and cyber-crimes are also on the rise. Some examples of cyber-attacks on critical infrastructure are given below:-

(a) In 2007, Estonian government servers were attacked severely crippling the e-services.[1]

(b) In 2007, Operation Orchid was carried out by the Israeli air force to destroy Syrian nuclear facilities near the border, in which Israel resorted to cyber warfare to blind the Syrian air defence system (radars) deployed along the Syrian- Israel border. Taking advantage of same, the Israeli air force fighter aircrafts bombed the nuclear facility without being detected by Syrian radars.[2,3]

(c) In 2010, the stuxnet virus destroyed a major portion of an Iranian nuclear facility. This incident was globally assessed as a joint effort of Israel and the USA.[4]

(d) In 2012, there was a major power grid failure in northern India, and reports indicate that the same could be attributable to hacking of the Supervisory Control and Data Acquisition (SCADA) system by a China-Pakistan nexus.[5]

(e) In 2013, there was an attack on the command & control system of New York dams - reported only in 2016.[6]

(f) In 2014/15, during Russian- Ukraine conflicts, Russians resorted to blanking of Ukraine military communication systems, thereby forcing them to use the cellular network, which enabled their location fixing, and thus easing their neutralization.[7,8]

(g) In Dec 2015, there was a huge power outage in Ukraine due to SCADA attack; almost 2,30,000 household went without power for hours. There was a similar attack after one year.[9]

(h) In 2015-16, the SWIFT (Society for Worldwide Interbank Financial Telecommunication) code system was targeted. A group by the name of Lazarus conducted the attack and stole millions of dollars.[10]

(j) In 2016, the deadly ransom-ware virus Wannacry played merry-hell with individuals and organisations across the globe. This was followed by another ransomware called the Petya/ NotPetya.[11]

(k) In 2017, the Wolf Creek Nuclear Operating Corporation at Kansas, US reportedly had its servers compromised.[12]

(l) In 2018, the US energy sector servers were compromised, allegedly by Russia.[13]

(m) In Aug 2018, Cosmos bank in Pune was attacked (again by Lazarus group) and almost Rs 94 Crore was stolen. The money was transferred to almost 30 countries, and it was withdrawn in about 10,000 transactions.[14]

2. In addition to above there have been major events like the famous Yahoo data breach in 2013/14,[15] the *Mafiaboy's* billion dollar hacks against Dell, Yahoo, Amazon and eBay,[16] the famous Sony pictures data breach of 2011,[17] the Citibank hack in 1995,[18] and many more.

Rise in Cyber-Crime

3. Inimical activities in the cyberspace range from cyber warfare (attacking critical National infrastructure) to cyber-attack (data breach, encryption of data, defacing of website), cyber-crime (social engineering, financial frauds, obscenity, pornography, child porn, copyright infringement, software/ music/ video piracy, etc), social crimes (inciting riots, violence, trolling, hate messaging, fake news, etc) and cyber terrorism (attacking critical National infrastructure, cyber propaganda, radicalisation, narrow casting, etc). Ibid events only go to show that cyberspace is the new domain to watch for; cyber warfare has now become the preferred tool, being non-contact, shrouded in obscurity, and low cost, but having an infinite reach. It's becoming clear that the dark side of cyberspace is now a permanent part of our daily lives, and each attack is as different from the other as chalk is from cheese. Nations across the world are grappling with the new challenges, including cyber terrorism, which is another menace becoming larger by the day. An important challenge in cyberspace is that it is frequented by state and non-state actors both, and identification is usually a problem. Attribution of the crime is another problem. While nuclear tests can be easily detected (by detection of radiations), often the perpetrators of cyber-crime can hide themselves easily and even make the investigators believe that the attack came from a third party.

4. The rapid growth of internet has fuelled the rise of cyber-crimes which are transnational by nature. They have no respect for international boundaries and may affect anyone across the globe. Territory based traditional penal codes fail to address the unique nature of cyber-crimes as criminals operate from safe havens out of the reach of Law Enforcement Agencies (LEA) of the country where the victim resides. Further, the fact that there is no central Internet regulating agency makes things worse. In the absence of legal framework, system administrators also find it difficult to keep check on cyber-crimes. Our reliance on internet for day to day functioning (to include financial transactions, government services, air/train ticket booking, taxi services, food delivery, communications, etc) is increasing with each passing day; governments all over the globe are putting more and more services online. Estonia is touted to be the global leader in e-governance and has borne the brunt of cyber-attacks in the past. In 2018 alone, the financial loss due to cyber-crimes was estimated at US$ 1.5 Trillion and is expected to rise to US$ 2 Trillion by the end of 2019, and US$ 6 Trillion by 2021. Understandably, the cyber security spending across governments and enterprises is on the rise. The business of cyber insurance is also catching up. Bajaj Allianz General Insurance was one of the first companies to venture into this business in India, in 2018.

5. A few revealing statistics pertaining to cyber-crime are given below:-[19,20,21,22,23,24,25]

(a) 3 billion Yahoo user accounts were compromised in 2016.

(b) Data of 540 million Facebook users was compromised in 2019.

(c) IT infrastructure of 31% of organisations has been attacked.

(d) In 2017, the average number of breaches suffered by a country was 24,089.

(e) The nation with the most breaches annually was India with over 33,000 instances; the US had 28,500.

(f) 24,000 infected mobile apps are blocked every day.

(g) Malware variants were up by 88% in 2017.

(h) Wannacry virus affected 400,000 machines in 150 countries in 2016, costing almost $4 billion.

(j) Ransomware attacks are growing at 350% annually.

(k) A ransomware attack happens every 13.275 seconds.

(l) Ransomware damage costs exceeded $5 billion in 2017, 1500% up from 2015, and are expected to be around $10 billion in 2019.

(m) In 2017 there was a 29% increase in industrial control system attacks.

(n) Between 2016 and 2017 there was 22.7 % increase in cyber security costs.

(o) Gartner reported that global spending on cyber security was US$ 96 billion in 2018, and is set to grow at 7% per annum.

(p) By 2025 cyber security expenditure will cross $1 trillion.

(q) Average global cost of cyber-crime increased by over 27% in 2017.

(r) By 2020, annual cyber-crime damage costs will reach $5 trillion.

(s) By 2021, cyber-crime costs are expected to reach $6 trillion annually.

(t) In 2017, more than 20% of cyber-attacks came from China, 11% from the US and 6% from Russia.

(u) Over 1 billion bots were involved in 210 million fraud attempts in Q1 2018.

(v) The ITU reports that globally, every second, 18 adults become cyber-crime victim.

6. As per a cyber-crime survey conducted by consulting firm Accenturein 2019:[26]

(a) Data is not the only target; industrial control systems are next in line. Also, while data theft is the current trend, attacking data integrity is the next frontier in cyberspace.

(b) The human layer is increasingly becoming the preferred means as a path to cyber-crimes (social engineering, phishing, vishing etc).

(c) There has been a 67% increase in cyber breach incidents in the last five years.

(d) The annual cost of cyber-crime has increased by 72% in the last five years.

7. ***The above statistics may seem frightening, and they are!*** Despite various nation states having strict cyber-crime regulations, the menace is ever increasing. This trend can be attributed to certain key factors as discussed further.

Challenges to Solving Cyber-Crimes

8. The challenges to solving cyber-crimesand booking of criminals are far too many (especially those with transnational footprints):-

(a) Firstly, the attacker and the victim may be residing in different countries.

(b) Even, if they are in the same country, the evidence may be in another country.

(c) For extradition laws to apply, the activity must be seen as a crime in both the nations.

(d) Sometimes, innocent (compromised) machines may be used for cyber-crime without the knowledge of the owner.

(e) Permissions for transnational crimes for evidence collection may take time, during which the cyber evidence may get wiped/ tampered.

(f) The definition for crime may be differing in two countries involved, e.g. the degree of nudity or sexually explicit scenes which are allowed in mainstream cinema may differ- what is considered porn in one country may not be in another.

(g) The dark-web and other such technologies provide obscurity to perpetrators of crime.

(h) At times, attackers, victims and evidence may spread across multiple countries.

(j) Techniques like the IP spoofing, etc often mislead the investigation agencies.

(k) Cloud based services provide another level of virtual environment.

(l) Poor public awareness on cyber hygiene makes it easier for cyber criminals to make hay.

(m) Mapping of cyber-crime to traditional laws (when no specific cyber law applies) can be big challenge.

9. **<u>Increasing Cyber-Crime Landscape</u>.** The available landscape for cyber-crime is increasing by the day. Reasons for the same are as given below:-

(a) The reducing costs of fixed broadband and mobile data connectivity have brought down affordability to lowest strata of society. This has increased dependency of people on internet based services. As per an estimate, in 2018, the number of internet users was more than 50% of world's population; this will grow to 75% by 2022 and 90% by 2030.[27]

(b) Increased automation in businesses, corporate, services and government sector alike.

(c) Increased ICT (Information and Communication Technologies) in industrial control systems and automation of infrastructure/services in critical sectors like telecom, banking, stock trading, railway traffic control, air traffic control, irrigation and waterways, road traffic system, healthcare, etc.

(d) Proliferation of new concepts like the Internet of Things (IoT). As per an estimate there will be 200 billion IoT devices connected to the internet by 2020, including half a billion wearable devices like smart-watches, cameras, fitness monitors, etc.[28]

(e) There are 110 billion lines of new software codes being produced every year, each with its own vulnerabilities.[29]

(f) The global digital content is set to grow from 4 billion terabytes in 2018 to 96 billion terabytes in 2020.[30]

10. The methods for committing cyber-crimes are also evolving with time. Some of the common methods employed are:-

(a) Hacking

(b) Virus dissemination

(c) Logic bombs

(d) Denial-of-Service attack

(e) Phishing

(f) Email bombing and spamming

(g) Web jacking

(h) Cyber stalking

(j) Data diddling

(k) Identity Theft and Credit Card Fraud

(l) Salami slicing attack

(m) Software Piracy

11. The list is endless, and is the very reason for requirement of a very specific and custom-made cyber-crime law at national and international levels. To makes matters worse, new methods of committing cyber-crimes are popping every day. As technology is progressing, the cyber landscape is changing, making lives easy for society; however, this also opens up new avenues of conducting cyber-crimes. Concepts like cloud based services, data centres, virtual assistants, AI based applications/ services, intelligent drones, driverless cars, robotics based industrial automation, etc are new concepts for exploitation of internet and cyberspace for the good of people and societies, businesses. However, parallel, new and innovative crime methodologies are being devised by criminals and hackers. The existing global conventions fail to address this new landscape of the cyber-crime world.

12. Probably the ***involvement of state actors*** themselves in collection of cyber intelligence through clandestine means towards larger strategic aims is a deterrent/ dilemma of these very states to support strong and fool-proof cyber legislation. The absence of mutual trust that emanates from such strategic interests of Nation States is probably a big road block for strengthening of International initiatives like the Budapest Convention on Cyber-Crime -2001 or adoption of the Tallin Manual (discussed later).

Global Cyber Index

13. As per the GCI (Global Cyber Security Index) report published by the ITU in 2018, only 58% of countries have published National Cyber Strategy.[31] That still leaves almost 42% the world's nation without a cyber

security strategy! Further, 9% of the Nations do not even have a cyber law in place,[32] 21% do not attend any International forums pertaining to cyber-crime and/or cyber security and 51% of Nations do not have any public-private partnership model for strengthening of cyber security measures.[33]

14. There is thus a need to strengthen cyber related legislation across the globe, and more so the international cooperation in terms of forensic examination, evidence seizure/ collection & extradition of cyber criminals.

Need for International Regulation to Tackle Cyber-crime

15. It is no state secret that there is a consistent rise in cyber-crimes across the globe. No country has remained untouched by this menace. Cyber security strengthening is a regular and continuous process for all business activities and they are struggling to keep pace with advancements in hacking expertise. Even government infrastructure is severely affected. Cyber-crime is affecting our daily lives also very badly. The dangers are growing faster than we can prepare ourselves for. Billions of dollars are being lost to cyber-crimes whether against individuals, business houses, financial institutions or the government. Even cyber-terrorism is raising its head in various parts of the world. As technology is advancing, critical infrastructures are more dependent on ICT, thus providing good opportunities to terrorists to cripple a nation's will by impacting its public service infrastructure like water supply, electricity, telecom, railways, air traffic, financial system, etc through cyber means.

16. Despite various nation states having strict cyber-crime regulations, the menace is ever increasing. This trend can be attributed to certain key factors as discussed below:-

(a) There is a never ending technology superiority race between the cyber security guys and the perpetrators of cyber-crime. As technology is improving by leaps and bounds new and novel ways of conducting cyber-attack are being invented, and cyber security team of any organisation is always playing catch-up. Further, the management has to strike a balance between severities of attacks versus financial spending on beefing up the cyber security posture.

(b) Inadequacy of international provisions for investigation and access to cyber assets and collection of forensic evidence. Due to the trans-border nature of cyber-crimes, the apprehension of criminals, their extradition, seizure of computer hardware and collection of evidence, etc are big challenges.

(c) Lack of consensus on what constitutes a cyber-crime and the differing legal definitions of crime. At times it may happen that an act constituting a crime in one country may not be a crime in another (the aspect of dual criminality), e.g. the definition of *obscene and sexually explicit material* varies across various countries as per the social culture, and therefore what is considered *obscene* in India may *not be obscene* in US. In such cases, extradition of criminals becomes a challenge.

(d) The input costs to carrying out a cyber-attack are very low. Other than the hacking expertise, the only requirements are a good quality laptop and a high speed internet connection. Thus individuals, non-state actors and weaker nations are seeking resort to cyber-crime instead of kinetic means, which are cost prohibitive.

(e) Technologies like the Dark Web, IP spoofing, etc are instrumental in providing anonymity to the cyber-criminals.

(f) The ever increasing desire of governments, private organisations and individuals to migrate to more and more online services keeps expanding the crime landscape in cyberspace.

(g) The cyber awareness amongst masses is very poor, and it will remain so. It is a difficult task for the government machinery in any country to enhance cyber security awareness of its population.

(h) Lack of expertise in law enforcement department and judiciary.

(j) Lack of harmony between Nation States in cyber laws and investigation of cyber-crimes.

17. Regulations, judiciary and international mutual cooperation have not been able to keep pace with technological advancements. Not all Nations have laws which are adequate to address these issues. When the issues elevate to transnational level, the problems get amplified. These can be resolved through a common framework for understanding the specifics of the problem and plausible solutions. Apropos, it is the necessity of the current times and the changing cyber scenarios that an international framework is worked out that is legally binding on all countries. The pitfalls of absence of such an internationally binding document are:-

(a) Regulatory gaps of a country can create offender havens with the potential to impact other countries.

(b) Hurdles in international cooperation, especially with regards to aspects related to dual-criminality, extradition, collection of cyber evidence, etc.

(c) Problems are multiplied exponentially when more than two countries are involved, e.g. the criminal may belong to one country, at the time of committing crime he may be physically present in the second country, the machine(s) that he has used for the crime may be in some other countries, and the impact of crime may be in few countries (other than covered before). Such situations are very complex to handle, from the perspective of fixing responsibility, collecting evidence from multiple machines in different countries, seeking extradition, etc.

(d) Laws of nation states may remain archaic in the absence of a reference modern international law.

(e) Cyber criminals will continue to exploit these gaps and conduct crimes with impunity, knowing very well that they can escape the law.

(f) Cyber- attacks by rogue states and cyber terrorism will increase due to lack of consensus amongst the global community.

International Efforts in Fight Against Cyber-crime

18. Certain efforts have been made at international level by the United Nations (UN) and some regional organisations like the OECD (Organisation for Economic Cooperation and Development), CoE (Council of Europe), etc.[34]

(a) From 1983 to 1985 the OECD carried out a study to ascertain feasibility of harmonizing criminal laws to curb cyber-crime. It resulted in a study report called *"Computer-related Crime: Analysis of Legal Policy"*.

(b) The CoE drafted *Recommendation 89(9)* and adopted it on 13 Sep 1989. It highlighted the importance of quick response to cyber-crime and need for harmonizing the law being transborder in nature.

(c) In 1990, the first European Working Party on Information Technology (IT) crime was established.

(d) The OECD adopted recommendations regarding security of Information Systems in 1992, and requested members to establish adequate regulations to tackle cyber-crime.

(e) The *UN Manual on the Prevention and Control of Computer Related Crime* was published in 1995.

(f) The CoE adopted *Recommendation No R (95)13* which guided the states and their investigating authorities. The major issues included were search & seizure, technical surveillance, obligations to cooperate with investigation authorities and international cooperation.

(g) The Budapest Convention on Cyber-crime was drafted in 2001 by the CoE, and was opened for signatures by member states on 23 Nov 2001.[35]

(h) The International Telecommunications Union (ITU) launched *Global Cybercrime Agenda (GCA)* initiative in May 2007.[36]

(j) In 2013, NATO prepared the *Tallinn Manual*.[37]

(k) In 2013, *UN Office on Drugs and Crime* (UNODC) published a *Global Report on Cyber-Crime.*[38]

(l) The UNODC also maintains a Global Programme on Cybercrime *(to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance)*, Open-ended Intergovernmental Expert Group on Cybercrime *(to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States)* and a detailed *Cybercrime Repository*.[39]

19. Details of above mentioned documents/ guidelines are discussed below:-

(a) **UN Manual on Prevention and Control of Computer Related Crime.**[40]

(i) The UN Manual, published in 1995 provides a discussion on cyber-crimes, their methods & complexities, and the need for international cooperation on solving trans-border cyber-crimes. It discusses aspects such as the "*jurisdiction issue, transborder search of computer data banks, mutual assistance in transborder computer-related crime, extradition, transfer of proceedings in criminal matters*," etc.[41]

(ii) It has suggested various methods to achieve international cooperation in this domain, and maintains that such a *"strategy is necessary, both immediately and in the long term, to ensure international cooperation and to foster the political will to create a secure information community and the universal criminalization of computer crime"*.[42]

(iii) It acknowledges the dire need for enhanced international cooperation in fighting cybercrime and states: *"The international elements in the commission of computer crime create new problems and challenges for the law. Systems may be accessed in one country, the data manipulated in another and consequences felt in a third country………How can it be determined in which country the crime was actually committed? Who should have jurisdiction to prescribe rules of conduct?.......These issues are to be addressed by all countries"*[43]

(iv) The UN Manual, thus, is more like a guiding document and not binding on any country.

(b) **<u>The Budapest Convention 2001</u>.**[44]

(i) The Budapest Convention was drafted by the CoE and serves as a common criminal policy to fight cyber-crimes against society, through cooperation between States to facilitate detection, investigation and prosecution. The Convention came into force in Jul 2004 and as of Nov 2018, 61 States have ratified it. India and Brazil have not yet signed stating that they were not involved in the drafting process, and Russia has refused to sign on grounds that it will affect its sovereignty. The Convention covers the areas of unauthorised access, unauthorised interception, data interference, misuse of computer devices, electronic forgery, electronic fraud, child pornography and copyright offences. However, it does not address certain cyber-crimes such as*access with intent to commit or facilitate commission of offence, denial of genocide and crimes again humanity, offences involving protected computers, fraud and related activity in connection with electronic mail, harassment utilizing means of electronic communication, cyber terrorism, identity theft, publishing or transmitting of material containing sexually explicit act, racist and xenophobic material,* etc. The convention is based on the cyber-crime methods used in those days, and is outdated; it and fails to address the new age cyber-crimes based on identity theft, phishing, terrorist use of Internet, spam, botnets and cyber-attacks against critical information infrastructure like telecom, banking & finance, railways, air-traffic, water supply, etc.

(ii) The aim of this Convention is "*facilitating detection, investigation and prosecution (of cyber-crime) at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation*". The Convention is a weak document for implementation as the actions related to mutual cooperation (which is the genesis of this document) are subject to many conditions and leave a lot of room for Nations to decide to cooperate or not, despite being signatories; e.g. it uses phrases like:-

> *(aa) "Each Party may reserve the right not to apply or to apply only in specific cases or conditions"*
>
> *(ab) "does not extradite him or her to another Party, solely on the basis of his or her nationality"*

(ac) "provided that they are punishable under the laws of both Parties concerned"

(ad) "Extradition shall be subject to the conditions provided for by the law of the requested Party"

(ae) "mutual assistance conditional upon the existence of dual criminality"

(af) "reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled"

(ag) "assistance shall be governed by the conditions and procedures provided for under domestic law"

(ah) "declare that it avails itself of the reservation(s) provided for"

(aj) "Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe"

(c) In 2004 the **NATO set up a Cooperative Cyber Defence Centre of Excellence (CCD-CoE)** which was granted the status of an International Military Organisation in 2007 post Estonia attacks. The mission of CCD-CoE is to *"enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation"*[45]

(d) The **International Telecommunications Union (ITU) launched *Global Cybercrime Agenda (GCA)*** in May 2007[46] for a framework where international response to cyber-crime and cyber-security could be harmonised. The GCA submitted its report on cyber security and cyber-crime legislations in Aug 2008, which highlighted aspects such as *“loop holes in current legal frameworks, the need for international cooperation (being a transnational problem), need for a global strategy and the critical role of the ITU in formulating the same, etc”*.

(e) In 2013, ***UN Office on Drugs and Crime*** **(UNODC)** published a ***Cyber-Crime Report***. Key findings of the report are:[47]

(i) Diversity of national laws has led to emergence of cluster of countries that are not suited to the global nature of cybercrime.

(ii) Traditional methods of interaction for international cooperation are time consuming and hence not suited for investigating transnational cybercrimes as time is of essence in collection of cyber forensic evidence.

(iii) In the growing world of cloud computing and data storage, the definition of terms like evidence location needs a relook to build consensus.

(iv) Analysis of national regulatory frameworks reveals inadequate harmony in core cybercrime offences, investigation powers and admissibility of electronic evidence.

(v) LEA in developing countries need long term assistance in combating cybercrime.

(vi) Cyber security aspects need strengthening in all countries to obviate occurrence of cybercrimes.

(vii) Countries that responded to questionnaire, reported between 30% (Americas) to 70% (Europe) cybercrimes which were transnational in nature:-

> *(aa) "One country from Eastern Europe noted that 'around 80 per cent of the cybercrime acts inspected by [domestic law enforcement authorities] are related to more than one country.'*
>
> *(ab) Another, from West Africa, stated that most of the victims targeted by cybercrime perpetrators within its territory were located 'outside of national boundaries.'*
>
> *(ac) Other countries said that most reported offences were 'initiated outside' of their territory.*
>
> *(ad) Still others observed that 'in most cases we act as a conduit.'*
>
> *(ae) Countries noted that the use of proxy servers, and the growing influence of social media, was among the factors behind an increasing number of cases involving a transnational dimension.*
>
> *(af) One country even reported that perpetrators are fully aware of jurisdictional issues and purposefully use internet resources, such as mail servers, located abroad in an attempt to hide evidence of their illegal activities."*[48]

(viii) The report also discusses options to strengthen fight against cybercrime- collated through a questionnaire which was circulated to nations. Major options that resulted from the survey are:-

> *(aa) "The development of international model provisions on criminalization of core cybercrime acts, with a view to supporting States in eliminating*

safe havens through the adoption of common offence elements.

(ab) The development of international model provisions on investigative powers for electronic evidence, with a view to supporting States in ensuring the necessary procedural tools for investigation of crimes involving electronic evidence.

(ac) The development of model provisions on jurisdiction, in order to provide for common effective bases for jurisdiction in cybercrime criminal matters.

(ad) The development of model provisions on international cooperation regarding electronic evidence, for inclusion in bilateral or multilateral instruments, including a revised United Nations Model Treaty on Mutual Legal Assistance, in line with suggestions in the Discussion Guide for the Thirteenth Congress on Crime Prevention and Criminal Justice.

(ae) The development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters, with a view to providing an international mechanism for timely cooperation to preserve and obtain electronic evidence.

(af) The development of a comprehensive multilateral instrument on cybercrime, with a view to establishing an international approach in the areas of criminalization, procedural powers, jurisdiction, and international cooperation.

(ag) The strengthening of international, regional and national partnerships, including with the private sector and academic institutions, with a

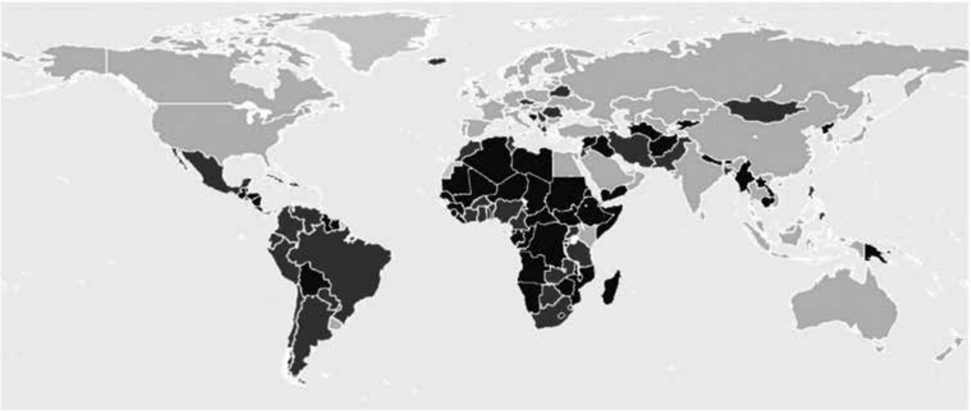
> *view to delivering enhanced technical assistance for the prevention and combating of cybercrime in developing countries."*[49]

(f) **The Tallinn Manual.** Tallinn Manual[50] was prepared by an International Group of experts in 2013 at the invitation of NATO office. An explanatory document was later released called the *Tallin Manual 2.0*[51]which expands on the version 1. Both the documents have no legal sanctity and are to be taken as opinions of the experts on the subject. **These documents explain how international law applies to cyber conflicts and cyber warfare between States. It does not address the issue of cyber-crimes per-se.**

(g) **South African Development Committee (SADC) Model Law.**[52] The SADC Model Law was drafted in 2013 with a view to formulate and harmonise ICT policies, regulations and legislative framework in the Sub-Sahara African countries. It deals with cyber offences like illegal access, illegal interception, data spying, forgery, fraud, child pornography, pornography, identity theft, racism, spam, stalking, etc, but does not address crimes such as aiding or abetting, corporate liability, offences involving protected computers, misleading domain names, infringements of copyright, damage to computer system, cyber terrorism, sending offensive messages, violation of privacy, internet gambling, etc.

(h) **African Union (AU) Convention on Cyber Security and Personal Data Protection.** The AU adopted a *Convention on Cyber Security and Personal Data Protection* in Jun 2014[53] that was a guideline for member States to strengthen the cyber security laws and protect critical infrastructure against cyber-attacks. It sought to harmonise synergy between members to handle this cyberspace menace. It was not a binding document, but an effort to get everyone thinking on similar lines, and extend cooperation in handling of cyber-crimes.

(j) In 2018, **ITU published the *Global Cyber-security Index (GCI)*** report. The report highlighted the cyber-security commitment of nations across the globe (in the five domains of legal measures, technical measures, organisational measures, capacity building and national/international cooperation) as shown in the figure below. Light blue represents highest level of commitment, and dark blue- the lowest. 54 countries were rated in the high category, 53 in medium and 87 in low category.[54]



The colours in the heat map above indicate differences in the level of commitment with high, medium, and low scores in a range of colours from light blue (peak commitment) to dark blue (low commitment). This is also reflected in the GCI groups in section 4.2.

(k) **<u>European Union</u>.** Europe began regulating social media and technology companies in May 2018 when the GDPR (General Data Protection Regulation) took effect. The intent of these new laws is to give citizens more control over their data that the service providers collect. New regulations stipulate that companies must collect only minimal data which is required for the application to function; they should get explicit consent from users for every possible use of their data; if the data of a company is hacked it has to report within 72 hours. Yahoo, Facebook, Uber - these are just a few companies that were hacked in the past, but did not make it public for months. Companies that do not comply with the laws have to pay fines up to 4% of the company's global annual revenue or € 20 million (about US$ 24.5 million), whichever is higher.[55] EU has issued several directives in respect of cyber-crime, as given below:[56]

(i) 2001 – Framework Decision on combating fraud and counterfeiting of non-cash means of payment

(ii) 2002 – ePrivacy Directive

(iii) 2011 – Directive on combating the online sexual exploitation of children and child pornography

(iv) 2013 – *Directive on Attacks Against Information Systems*

(v) The *European Cyber-Crime Centre (EC3)* started operating in 2013 and acts as the central agency in fight against cyber-crime, strengthening the legal and security framework through collaboration amongst member countries.

(vi) Global Alliance against Child Sexual Abuse

(vii) In addition, the *European Network and Information Security Agency* has been set up for sharing of good practices related to cyber security.

20. **<u>International Discussions and Collaboration Efforts</u>**

(a) Chatham House, Royal Institute of International Affairs is an independent policy institute based in London. A detailed discussion was held at the Chatham House in 2012 on International law pertaining to cyber-crimes, and participants included government officers, lawyers, cyber experts, etc.[57] The forum deliberated specifically on the aspects of cyber warfare that can be waged by Nations and how to handle such situations using the United Nations' legal framework. The discussants came to a conclusion that thereare certainly grey areasthat need to be addressed. They also discussed whether cyber security and cyber warfare should be handled by military or by the homeland security. The panel drew parallels with the cold war era and a similar strategy of mutual assured destruction as is applicable to use of nuclear weapons.

(b) A research paper (2015) on cyber warfare lists the various challenges in applying traditional laws to cyber war.[58] The first issue it deliberates is the definition of cyber-war and cyber-warfare. It differentiates between the two by stating that *while cyber warfare is use of cyber-attacks with warfare like intent, cyber war would be a situation where the only domain being fought is in cyberspace*- the moment we add kinetics it becomes a war where cyber warfare was also used.[59] It analyses the Tallin manual also and brings out that the Tallin Manual was developed based on the laws of only four nations, viz, US, UK, France and Germany, and thus is very restrictive in its outlook as it fails to be applied to other countries whose laws may be at large variance with those of these four countries.[60] It also highlights the challenge that not all members of the group may agree to a particular aspect while formulating the manual, and thus leads to problems.[61] The aspect of applying international weapons treaties to cyber weapons has also been analysed, and the study concludes that due to the distinct nature of cyber weapons (e.g. the list of cyber weapons, if drawn out, may become redundant in a very short time due to advancements in technology) it is difficult to apply the existing treaties in their current form, to cyber weapons.[62]

(c) In Dec 2016 a meeting of the Ministers of Justice of the Americas was held to discuss the implementation of Budapest Convention on Cyber-crime.[63] It is worthy to note that the Convention was drafted in 2001 and came into force in 2004. However, 12 years down the line we were having international discussions on its implementation! It clearly shows that the Convention lacks necessary framework for an effective implementation in the changed technical and socio-economic landscape.

(d) A research paper published by the Chatham House, London in Jul 2018[64] has analysed the efficacy of cyber-crime laws in GCC countries (Gulf Cooperation Council- political and economic alliance of six Middle Eastern countries—Saudi Arabia, Kuwait, United Arab Emirates, Qatar, Bahrain, and Oman).The study brings out the following:-

(i) The laws focus more on restricting freedom of expression than actual cyber-crimes, aim being to have stronger control over social media.

(ii) The definition of crimes that classify as cyber-crime is well covered, but for investigation and prosecution, they rely on traditional laws, which are inadequate to handle the specific nature of cyber-crimes.

(iii) Laws are vaguely worded, leaving scope for misinterpretation and misuse, and are at variance with international human rights regulations.

(iv) Revision of these laws is urgently required.

(v) GCC countries should join international forums such as the Budapest Convention.

A Global Treaty and Regulatory/Legislative Framework to Combat Cyber-Crime.

21. Cyberspace is being touted as the 5th domain of war- after land, sea, air and outer space. The UN accepts *Crimes Against Peace and Security of Mankind* as crimes under the international law. Apropos, crimes in cyberspace against peace and security of mankind should also be considered as crimes under framework of international law. Internet and

computer based business, commercial activities and communications transcend international borders creating a new virtual space of human interaction which is devoid of regulations and legislations. Inimical elements, whether criminals, hate mongers or non-state actors/terrorists are exploiting this facet and they carry out cyberspace criminal activities with impunity- the rising graphs of cyber-crimes are a testimony to that. Systems across the globe follow differing set of rules; it thus becomes convenient for cyber criminals to take advantage of the absence of uniform legislation that is applicable and legally binding to all Nation States.

22. We see that there have been efforts to bring synergy in handling of cyber-crimes in various pockets across the globe. However, a major factor that seems to be stalling an international consensus on the subject is that some Nation States are themselves engaged in unethical activities in cyberspace, either related to gathering of intelligence on adversary nations, or keeping a tab on dissent within the country. It therefore suits them that there is no internationally binding legislation through which they can be held accountable and questioned for their actions by relevant global authorities. Unlike other treaties like the Chemical Weapons Convention, Non-Proliferation Treaty, etc where a number of Nation States have openly committed to abide by these regulations to support global peace, committing to a legislation banning unwanted activities in cyberspace is a big question as it will mar their own strategic interests.

23. There is no international organisation (like the Interpol) to address the peculiar nature of trans-border cyber-crimes. The existing documents are just guidelines, not binding on anyone, and treaties are also seeking voluntary compliance. There is no international regulatory framework through which efficient control and investigation of cyber-crimes can be ensured for the global community.

24. Apropos, what is required is a truly international framework comprising of ***legal measures, technical measures, organisational measures, capacity building and national/international cooperation*** (in line with the ITU GCI Report discussed earlier), that can be deterrence to cyber criminals, rogue states and cyber-terrorists who commit computer based crimes with impunity, especially transborder crimes. The frameworkshould be able to do the following at the minimum:-

(a) Create a well-defined legal framework that can facilitate efficient business, e-commerce and communications across the globe through use of internet and computer systems.

(b) Define, penalise and proactively prevent cyberspace criminal activities that would harm individuals, organisations, society or the State at large.

(c) Assist investigation of cyber-crimes including seizure of hardware/software, collection of forensic evidence across States and extradition of criminals.

(d) Provide for review of the framework at a regular frequency to keep abreast of the technological, societal and legal developments.

(e) Provide fairness as well as firmness in dealing with cyber-crimes involving Nation States.

(f) Be acceptable to all to ensure self-compliance by individuals and States.

(g) Provide platform for sharing of technology, procedures, etc to strengthen the cyber infrastructure.

(h) Provide for a global cyber policing organisation with appropriate authority.

(j) Create a well-defined legal framework that can facilitate efficient business, e-commerce and communications across the globe through use of internet and computer systems.

(k) Achieve uniformity in definitions of cyber-crimes.

(l) Define, penalise and proactively prevent cyberspace criminal activities that would harm individuals, organisations, society or the State at large.

(m) Ensure assured access to the computer systems used in cyber-crime to law enforcement agencies of victim nation(s).

(n) Ensure assistance to law enforcement agencies of victim nation(s) in collection of cyber forensic evidence, seizure of material, etc.

(o) Enable expeditious extradition of cyber-criminal(s) to the victim nation, to be tried under their law.

(p) Provide for a global cyber policing organisation with appropriate authority, akin to Interpol.

(q) Provide for an International Cyber Court akin to the International Court of Justice (ICJ).

(r) Provide fairness as well as firmness in dealing with cyber-crimes involving Nation States.

(s) Be acceptable to all to ensure self-compliance by individuals and States.

(s) Provide platform/forum for sharing of technology, procedures, etc to Strengthen the cyber security posture of critical

IT infrastructure.

(t) Provide for review of the framework at a regular frequency to keep abreast of the technological, societal and legal developments.

References (Endnotes)

1 https://www.technadu.com/biggest-cyber-crimes/9094/, Accessed 13Apr 2019

2 http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

3 https://www.timesofisrael.com/israel-uses-17-tons-of-explosives-to-destroy-syrian-reactor/

4 http://large.stanford.edu/courses/2015/ph241/holloway1/

5 https://www.oneindia.com/2012/08/22/china-s-hand-in-india-s-power-blackout-1057676.html

6 https://cyware.com/news/3-cyber-attacks-that-rocked-industrial-control-systems-817fee48, Accessed 18 Apr 2019

7 Baezner, Marie & Patrice, Robin, Cyber and Information warfare in the Ukrainian conflict, Center for Security Studies (CSS), ETH Zürich

8 https://www.wired.com/story/russian-hackers-attack-ukraine/

9 https://cyware.com/news/3-cyber-attacks-that-rocked-industrial-control-systems-817fee48, Accessed 18 Apr 2019

10 https://www.darkreading.com/perimeter/inside-the-north-korean-hacking-operation-behind-swift-bank-attacks--/d/d-id/1332969, Accessed 18 Apr 2019

11 https://ifflab.org/cyber-crimes-in-the-history-of-cyber-attacks/, Accessed 13 Apr 2019

12 https://www.bbc.com/news/world-us-canada-40538061, Accessed 18 Apr 2019

13 https://www.computerweekly.com/news/252437089/Russia-compromised-core-router-in-US-energy-attacks, Accessed 18 Apr 2019

14 https://timesofindia.indiatimes.com/city/pune/north-korea-hand-in-cosmos-bank-cyber-heist-unsc-panel/articleshow/68605160.cms, Accessed 13 Apr 2019

15 https://www.technadu.com/biggest-cyber-crimes/9094/, Accessed 13Apr 2019

16 https://www.technadu.com/biggest-cyber-crimes/9094/, Accessed 13Apr 2019

17 https://ifflab.org/cyber-crimes-in-the-history-of-cyber-attacks/, Accessed 13 Apr 2019

18 https://ifflab.org/cyber-crimes-in-the-history-of-cyber-attacks/, Accessed 13 Apr 2019

19 https://learn.g2crowd.com/cybercrime-statistics, Accessed 13 Apr 2019

20 https://www.varonis.com/blog/cybersecurity-statistics/, Accessed 13 Apr 2019

21 https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/, Accessed 13 Apr 2019

22 http://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/, Accessed 13 Apr 2019

23 https://cybriant.com/2018/03/2018-cybercrime-stats/, Accessed 13 Apr 2019

24 https://www.itu.int/en/ITU-D/Partners/Pages/Call4Partners/CYBLDCStats.aspx, Accessed 29 May 2019

25 https://www.csoonline.com/article/3219165/gartner-worldwide-

information-security-spending-to-hit-93b-in-2018.html, Accessed 29 May 2019

26 https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf, Accessed 28 May 2019

27 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, Accessed 29 May 2019

28 https://www.huffpost.com/entry/thoughts-on-iot-and-finan_b_11298656, Accessed 29 May 2019

29 https://www.networkworld.com/article/3198474/cisco-to-network-engineers-get-comfortable-with-software-it-s-here-to-stay.html, Accessed 29 May 2019

30 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, Accessed 29 May 2019

31 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf, p 18, Accessed 29 May 2019

32 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf, p 17, Accessed 29 May 2019

33 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf, p 20, Accessed 29 May 2019

34 https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/ CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf, Accessed 17 Apr 2019

35 Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680081561, Accessed 16 Apr 2019

36 https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf,

Accessed 29 May 2019

37 Available at http://csef.ru/media/articles/3990/3990.pdf, Accessed 17 Apr 2019

38 https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, Accessed 11 May 2019

39 https://www.unodc.org/unodc/en/cybercrime/index.html

40 Available at http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_ UN_Guide.pdf, Accessed 17 Apr 2017

41 Available at http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_ UN_Guide.pdf, p 21-25, Accessed 17 Apr 2017

42 Available at http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_ UN_Guide.pdf, p 4, Accessed 17 Apr 2017

43 Available at http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_ UN_Guide.pdf, p 19-20, Accessed 17 Apr 2017

44 Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680081561, Accessed 16 Apr 2019

45 Bogdanoski, Mitko, 2013, Cyber Terrorism– Global Security Threat(https://www.researchgate.net/publication/252195165_CYBER_TERRORISM-_GLOBAL_SECURITY_THREAT?enrichId=rgreq-14f411ff03cd369f82b998f51689c441-XXX&enrichSource=Y292ZXJQYWdlOzI1MjE5NTE2NTtBUzo5OTA4NjkwMDQwMDEzMEAxNDAwNjM1NTY3NDQ3&el=1_x_2&_esc=publicationCoverPdf) Accessed 28 Apr 2019

46 https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf,

Accessed 29 May 2019

47 https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, p xi-xii, Accessed 11 May 2019

48 https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, p 183-184, Accessed 11 May 2019

49 https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, p xiii-xv, Accessed 11 May 2019

50 Available at http://csef.ru/media/articles/3990/3990.pdf, Accessed 17 Apr 2019

51 Available at https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf, Accessed 17 Apr 2019

52 Available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf, Accessed 16 Apr 2019

53 African Union Convention on Cyber Security and Personal Data Protection, 27 Jun 2014 (https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf) Accessed 16 Apr 2019

54 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf, Accessed 29 May 2019

55 Adam, Chiara, 24 Jun 2018, Three social media regulations the US needs to import from Europe (http://thehill.com/opinion/technology/393840-three-social-media-regulations-the-us-needs-to-import-from-europe) Accessed 26 Jul 2018

56 https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en, Accessed 17 Apr 2019

57 International Law: Meeting Summary: Cyber Security and International Law, 2012, Chatham House, London (https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf) Accessed 27 Apr 2019

58 Robinson, Michael, Jones, Kevin and Janicke, Helge, 2015, Cyber warfare: Issues and challenges, Computers & Security · March 2015 (https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges/citation/download) Accessed28 Apr 2019

59 Robinson, Michael, Jones, Kevin and Janicke, Helge, 2015, Cyber warfare: Issues and challenges, Computers & Security · March 2015, p 14 (https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges/citation/download) Accessed28 Apr 2019

60 Robinson, Michael, Jones, Kevin and Janicke, Helge, 2015, Cyber warfare: Issues and challenges, Computers & Security · March 2015, p 37 (https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges/citation/download) Accessed28 Apr 2019

61 Robinson, Michael, Jones, Kevin and Janicke, Helge, 2015, Cyber warfare: Issues and challenges, Computers & Security · March 2015, p 38 (https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges/citation/download) Accessed28 Apr 2019

62 Robinson, Michael, Jones, Kevin and Janicke, Helge, 2015, Cyber warfare: Issues and challenges, Computers & Security · March 2015, p 43 (https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges/citation/download) Accessed28 Apr 2019

63 OAS Meetings of the Ministers of Justice or Attorneys General of the Americas 9th Meeting of the Working Group on Cybercrime,

12-13 Dec 2016, Washington DC Agenda item “International legal frameworks“ (http://www.oas.org/juridico/pdfs/cyb9_coe_cyb_oas_dec16_v1.pdf) Accessed 27 Apr 2019