Cyber (In) Security: A Challenge to Reckon With

Sitara Noor [*]

Abstract

Recent developments in the cyber domain have exposed the dangers of a largely apathetic behaviour towards the looming threats of cyber warfare. Calls for more rigorous corrective measures have been made, as some states have begun to view such breaches as a top national security threat. Such threats have also changed the dynamics of state behaviour, giving way to subtle aggressions with potentially destabilising and far-reaching consequences. These transgressions have also brought to the fore numerous challenges of cyber security that find their origin in scant technical understanding, the absence of a legal framework, and an overall complex strategic environment. This calls for the institution of some rules of the game to ensure the freedom of the Internet, while at the same time protecting critical cyber infrastructure through a normative approach that can pave the way for some concrete measures for regulating state behaviour.

Keywords: Cyber Warfare, Cyber Security, Information Technology, Digital Networks, Security Threat, National Security

Introduction

The information revolution has transformed the lives and works of people all over the world as global Internet connectivity skyrocketed over the past two decades, resulting in an increased reliance and dependency on digital networks in both the civilian and military sectors. According to the International Telecommunication Union's (ITU) estimates, three billion people, or forty per cent of the world's population was using the Internet at the end of 2014, as compared to the eight per cent figure in 2001.[1]

[*] Ms. Sitara Noor is an Islamabad based security analyst and currently pursuing her M.Phil in International Relations from National Defence University.

The Internet revolution did not come alone; it brought along with it the associated challenges of cyber age, giving rise to recurring debates about cyber warfare and cyber security. The extent of these challenges is evident from the fact that these terms have become a buzzword in strategic circles over the past few years. However, relatively little attention has been paid to identify what cyber warfare and cyber security constitute, and what challenges they have brought along in a highly digitalised world. When John Carlin alluded to, "the icy chill of digital winds" in his classical essay *A Farewell to Arms* in 1997, hardly anyone took it as a major national security concern, or even worthy of serious attention at the policy level.[2] However, the trend is changing fast, with the emergence of continuous debates in scholarly circles as well as policy corridors to address the matter as a priority issue, particularly with regard to national security.

This study aims to delve into the ongoing debate about cyber threats and its impact on national security. It tries to bring to the surface various domains where cyber-related challenges need to be untangled for more clarity about the issue itself. It would further address some areas that need immediate attention, as intensified cyber-related threats and challenges are unfolding, and would create grave vulnerabilities if left unattended, particularly related to national security.

Cyber Challenge: Gauging the Threat

A cyber attack may range from a malware or phishing attack to hacking attempt or data leakage. With the advent and abundance of new technologies like smart phones and cloud computing, cyber vulnerability has increased manifold and poses a greater challenge. There is no universally accepted definition of cyber attacks, which makes it somewhat difficult to define the parameters in which cyber challenges can be confined. There are, however, a range of views and ideas to address what constitutes a cyber attack.

At the regional level, the Shanghai Cooperation Organisation (SCO) raised concerns over the potential dangers associated with misuse of new technologies.[3] According to the Tallinn Manual - a study conducted by an international group of experts in the aftermath of cyber skirmishes on

Estonia – a cyber attack is defined as: "A cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[4] A more comprehensive yet focused definition of cyber attacks can be found in a Yale University study, according to which: "A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose."[5] For the purpose of analysis, this definition helps to distinguish cyber warfare from a simple cyber crime and the use of cyber means for espionage without affecting the network itself, hence constraining focus within some parameters and frames of reference, wherein lies the complexity of the issue.[6]

The absence of an internationally accepted definition and a corresponding legal framework has apparently made the use of cyber attacks easier by state and non-state actors. One can trace a number of cyber attacks and hacking attempts in the past years. A major cyber attack surfaced as early as 1988, when Morris Worm came to be known as one of the first recognised worms to affect the global cyber infrastructure.[7] It largely affected computers in the US. Almost a decade later in 1998, Indonesia fell victim to the first major state-level cyber attack when its official websites were allegedly hacked by Chinese hackers.[8] However, a new precedent was set in April 2007, when Estonia experienced an organised cyber war, whereby a three-week wave of distributed denial-of-service (DDOS) attacks resulted in the collapse of its information technology infrastructure. The alleged Russian involvement in these attacks unleashed a debate regarding whether such a breach constitutes a military attack, as it virtually brought all of the Baltic States' financial activities to a standstill for many days.

Later, the emergence of the Stuxnet[9] in October 2010, and its infamous attack on the Iranian nuclear facilities proved to be a game changer for the cyber warfare debate. On the one hand, it brought to the fore the involvement of a state entity in a substantial cyber attack, and on the other hand, it highlighted the extent of catastrophic consequences. The advent of Stuxnet, which is by far the most sophisticated cyber attack, can justifiably be termed as crossing the Rubicon in the cyber sphere, where the security debate entered an altogether new phase. It demonstrated that the mere

creation of an 'air gap' in the computer networks would not guarantee security from a cyber attack.[10] Its sheer complexity and sophistication was sufficient proof to ensure that it had state backing, allegedly by the US and Israel. Later, in August 2012, came a financial setback, when the computer network of Saudi Aramco was struck by a self-replicating virus – the most destructive act of computer sabotage on a company to date – infecting as many as 30,000 of its Windows-operated devices.

If the situation was less complicated earlier, Edward Snowden's revelations presaged a new era of cyber security challenges. According to the *Washington Post's* revelation about the US's black budget, the US intelligence services carried out 231 offensive cyber operations in 2011, where the Internet was used as a theatre for "spying, sabotage and war."[11] This was manifested in the form of the Flame virus and the most recently discovered worm the Mask, which are now known as being used for espionage and data collection for the past several years.

The growing number of such negative developments indicates that cyber warfare has come of age. Subsequently, the global community has realised the challenges that threaten digital infrastructures and has gone to the extent of naming cyber threats as a top-priority national security challenge. According to the *2014 Worldwide Threat Assessments of the US Intelligence Community*, cyber security challenges surpass the threat of terrorism.[12] In 2010, the Pentagon established Cyber Command as a sub-unit of Strategic Command, one of the nine Combatant Commands of the US's Unified Command System, which envisioned a cyber offensive and defensive policy.[13] This trend caught on in state behaviours all over the world, and a number of states developed their cyber security strategies to counter the threat. China's military doctrine advocates to utilise a combination of cyber and electronic warfare capabilities at the early stages of a conflict.[14] According to a United Nations Institute for Disarmament Research (UNIDIR) report, thirty-three states have included cyber warfare in their military planning and organisation, and another thirty-six states have incorporated only defensive capabilities.[15] This report acknowledges the fact that the knowledge of cyber defence capabilities can also be utilised in offensive operations.[16]

There is, however, a realisation that security against such an undefined and ambiguous threat becomes a difficult task, as its parameters are not clearly defined. Whereas there is no universally accepted definition of cyber attack or cyber warfare, there is some unanimity of views as to what the measures for cyber security should be. According to the ITU, cyber security is defined as:

> The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.[17]

It further states that cyber security is aimed at ensuring the security of an organisation as well as the user's assets in view of the potential risks present in the cyber domain. The aforementioned definition construes the broader objectives of cyber security. In this regard, recognising that the nuances of cyber technology are different from other kinetic means, one can also borrow the 3S concept from the discipline of nuclear studies, whereby safety, security and safeguards can be applied to the cyber domain. In this context; safety could ensure that people and systems are safe from harmful computer malwares and viruses; security would mean the ability to ensure the security of hardware and software through tangible and non-tangible measures against malevolent attacks; and safeguards would mean the non-diversion of dual-use cyber technology for harmful objectives.

Challenges to Cyber Security

As the instances and magnitude of cyber attacks and cyber warfare have increased over the years, a lot of discussion on measures and counter-measures is being generated, as more states come up with their distinctive yet oft-conflicting approaches. Unfortunately, the debate is still not free of ambiguity. There are a number of challenges that are a centerpiece of the ongoing deliberations and need to be taken into serious consideration. Some of these prevailing and emerging challenges,

surrounding the contemporary cyber security debate, fall in the domains of technical, legal and politico-strategic areas.

Technical Challenges

The foremost challenge in cyber security lies in the technical domain. It has becomes difficult to understand the particular nature of a cyber attack and then to find a solution due to the ever-changing nature of cyber threat. Every time when a cyber attack occurs, its parameters are different from its predecessor. This makes it an ever-evolving phenomenon, where each time a lot of thought and effort goes into decoding and defining its technical dimensions. In order to carry out a cyber attack, all that is required is a smart brain and a working computer connected to the Internet, and this combination of resources is enough to wreak havoc. It becomes even harder, sometimes impossible, to detect an attack in advance and even pre-empt when it has state backing, as was the case with the Stuxnet and the Flame virus. Therefore, the dual-use nature of cyber-related technology poses a major challenge, which makes it difficult to distinguish between its offensive use and conventional or productive use.

The identification or tracing down the origin of a cyber attack has become even more complicated with the involvement of non-state actors.[18] A state actor has access to more resources, and can thus carry out concealed efforts, whereas a non-state actor would rely more on a hit-and-run tactic. The emergence of cyber mercenaries[19] in collusion with state or non-state elements creates an even more troubling situation, making it difficult to attribute the origin of the attack to just one source since there are no cyber radars to detect the direction of an attack. As is evident in the case of the Stuxnet virus attack on the Iranian nuclear facilities, the authorities initially denied even the existence of the deadly virus, let alone confirm the verification of its origin, which essentially requires a referent object. Successful verification can only occur against a tangible object; and the cyber domain does not have that capacity. The evolving administrative and governance systems that oversee the Internet make the attribution of a cyber attack extremely challenging, a fact acknowledged by many technical experts.[20]

Legal Challenges

The prevalence of technical issues in the realm of cyber security adds to its legal challenges. In the legal domain, it is important to determine the role of international law in cyber warfare and its application for the sake of cyber security. This debate raises two concerns, primarily about the legality of cyber war. The logical question that comes to mind is about the relation between cyber warfare and kinetic warfare. Is the former, essentially an offshoot of conventional military warfare? If so, how could existing laws that govern traditional kinetic war apply to war in the cyberspace, given the challenges it brings along, which are fundamentally different from traditional wars? Although the objectives of cyber warfare may be the same as that of a kinetic war, such as damaging the adversary but the means applied are inherently different.[21] Its impact would also be different, as the applied means may not have the ability to distinguish between military and civilian targets, hence inflicting indiscriminate damage. Such an indiscriminate response would be considered unlawful. According to the law of war, only three categories of individuals can be targeted during a combat: combatants, civilians directly participating in hostilities, and civilians who act in a continuous combat function.[22] Can a form of war that fails to make this important distinction be governed under the same legal principles?

Armed conflict between nations, or 'international armed conflict' is largely governed by two bodies of international law-*jus ad bellum*, the body of law that governs the question of when a nation may resort to the use of armed force, and *jus in bello*, the body of law that regulates the behaviour of a state party involved in an armed conflict.[23] Over the years, the United Nations (UN) Charter has established itself as the primary source of *jus ad bellum*, which prohibits the use of force. This brings into focus the applicability of Article 2(4) of the UN Charter, which states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[24] This refers to the principle of non-intervention, and questions the very nature and legality of cyber attacks. It is further complemented by the international customary laws' norm of non-

intervention. Although there is an ongoing debate on the principle of non-intervention, the predominant view is that this principle only addresses armed forces, excluding economic and other political intimidations. However, there is no definitive view about whether a cyber attack is a part of it, or it excludes an armed attack.

In the aftermath of the cyber attack on Estonia, as some viewed it as an attack on a North Atlantic Treaty Organisation (NATO) member, NATO invoked Article V of its Charter of collective defence. At the 2008 Bucharest Summit, NATO leaders agreed to develop certain systems and structures so that Estonia-like situations could be prevented and countered.[25] Similarly the Stuxnet, the Flame, and its counterparts are unprovoked attacks that go against the principle of non-intervention. However, sans forensic footprints providing technical evidence, legal action against any such act becomes virtually impossible.

Secondly, assuming that an attack has been determined to be a cyber attack, does it invoke the right of self-defence under Article 51 of the UN Charter? In the literal sense, an armed conflict should involve use of conventional arms. However, if it is analysed in view of the landmark judgment by the International Court of Justice (ICJ) about the legality of nuclear weapons in self-defence, it can be applied, "to any use of force, regardless of the weapons employed."[26] This judgment justifies self-defence, but opens up another debate, as the likely response also needs to be constrained within some guidelines and governing principle. The right of self-defence under Article 51 of UN Charter itself requires the application of condition of necessity and proportionality in response to any aggression. There is at least some consensus at an intellectual level in favour of the use of defensive armed forces if the impact of a cyber attack is equivalent to a conventional military attack.[27] This, however, becomes tricky in cyberspace. For instance, how and to what extent would Iran have responded, if it could identify the origin of the Stuxnet? The virus did cross a red line and caused physical damage to its nuclear installation to a level that Iran had shown intent to respond militarily. This purpose was achieved without firing a single bullet. So does the application of a different means to achieve the same objective quash the legitimacy of Iranian kinetic response?

Further, it begs the question of the applicability of International Humanitarian Law (IHL) and its probable role in cyber warfare. Although cyber warfare is largely considered to be subject to the existing rules of IHL, its applicability in entirety is debatable due to the very nature of cyber war itself, as some rules of IHL become difficult to apply.[28] An isolated cyber attack cannot be governed under IHL principles, if it fails to establish a link with an armed attack, which is an important pre-requisite of the applicability of IHL. Moreover, it does not allow the employment of any type of weapon with unlimited objectives that diminishes the distinction between civilian population and combatants.[29]

International and Regional Legal Frameworks Governing Cyberspace

There is no singular and all-encompassing international legal instrument that covers all necessary concerns associated with cyber security challenges. There are segments of appropriate international law covering norms and acceptable behaviour of information technology in trade and communication through the Internet, but these laws are by no means fit to govern state behaviour in terms of using cyber space as a disruptive tool of war, or to cover the law of international armed conflict.[30] Therefore, the existing laws and international legal instruments provide only a fragmentary assistance to deal with cyber challenges. Different elements of these legal instruments offer some solace, but without a significant measure to deal with any non-compliance, they leave behind many caveats to deal with.

At the regional level, various organisations have developed a framework and guidelines to be observed. NATO, for instance, in the aftermath of the Estonian episode, held its first meeting in 2008 at the Bucharest Summit to address cyber attacks. It led to the creation of two new NATO divisions, namely the Cyber Defence Management Authority (CDMA) and the Cooperative Cyber Defence Centre of Excellence (CCDCOE).[31] NATO's CCDCOE undertook a study under an International Group of Experts, who produced a manual on the law governing cyber warfare known as the Tallinn Manual. This detailed study did not attempt to establish new norms and rules; rather, it examined the

applicability of existing norms. In this way, it was an effort in *lex lata*, not *lex ferenda*, which means an exercise in the extant law and not an attempt to create law.[32] It did not fill the legal loopholes, but prescribed some solution within the existing legal boundaries.

The Council of Europe (CoE), on the other hand, has taken a more comprehensive and direct approach, and developed the first international treaty on crimes related to the Internet and other computer networks, which goes by the name of the 2001 Council of Europe Convention on Cybercrime, commonly known as the Budapest Convention.[33] The Convention calls for increased cooperation among signatory states for the investigation of cyber crime emanating from a foreign land. However, it does not mandate the requested country from which the information has been sought to actually share information. It also fails to address the attacks made by state parties. It is also criticised for being a largely European Convention, although it does not bar the participation of other regions.

There is also a lack of consensus among global actors as to what approach and standards should lead the cyber security debate and initiatives due to the divergence of interests, with the European countries emphasising the human rights aspects of cyber security, based on their characterisation of Internet freedom as a fundamental right, contrary to the Russian and Chinese positions which emphasise Network Sovereignty as the leading principle as a way forward.[34]

This divergent approach has led to a rather meek response at the UN. There have been a number of resolutions on the broader agenda item of; "developments in the field of information and telecommunications in the context of international security".[35] The UN General Assembly (UNGA) Resolution 57/239 notably talks about the creation of a global culture of cyber security, but without demanding any specific action. Resolutions 55/63 and 56/121 of the UNGA establish a broad framework on countering the criminal misuse of information technologies.

There are a number of other regional arrangements that have addressed the issue of cyber security at length, and have come up with some regional

solutions and guidelines. These regional bodies include the Commonwealth of Independent States' (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001), the CIS's Model Laws on Computer and Computer-related Crime (2002)/Electronic Evidence (2002)/Harare Scheme (2002/2011), the SCO's Agreement on Cooperation in the Field of Information Security (2009), the League of Arab States' Convention on Combating Information Technology Offences (2010), the ITU/Caribbean Community/CTU Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010), the ITU/Secretariat of the Pacific Community Model Law on Cybercrime (2011), the East African Community (EAC) Legal Framework for Cyber laws (2008), The Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime (2011), The Common Market for Eastern and Southern Africa (COMESA) Cyber Security Draft Model Bill (2011), the African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa (2012), and The Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2012).

Politico-Strategic Challenges

Given the challenges at the legal and technical fronts, a third set of challenges lies in the politico-strategic domain. It would be erroneous to equate emerging cyber war with the Cold War in the strategic and political domains, as cyber phenomena come with entirely different dynamics. On the one hand, it brings out some puzzling paradoxes. The first paradox is related to the very nature of cyber technology that has expanded and flourished as a tool of globalisation. Technology, particularly information technology, has become the wheel of a globalised and technology-dependent world. In order to deal with this challenge, one oft-repeated solution is to revert back to indigenisation or to usher in a dawn of a "Cybered Westphalian Age",[36] where modern democracies could first define and then protect their cyber frontiers. After the Stuxnet, states realised the need for safety measures, as the common cyberspace with infinite boundaries had become a repeated victim of grab-and-go cyber attack incidents.[37]

The second paradox relates to the attempt to foster national security without compromising democratic principles, as the principles of security and accessibility work contrariwise, resulting in detrimental consequences for one another. This has further increased the perception gap among various global actors and has resulted in varying and mostly contradictory approaches to deal with these challenges. Russia and China, for instance, have focused on establishing a broad international oversight of the Internet, which in their view would create deterrence against the malicious use of cyberspace in the case of war. On the other hand, the US is not willing to rule out the offensive use of cyber technology.[38] The leaked Presidential Policy Directive 20 that was never published officially stated that its Offensive Cyber Effects Operations (OCEO): "…can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."[39]

On the one hand, these paradoxes highlight the complexity of the issue itself, and on the other, they expose the decision makers' predicament in the face of a cyber-related security challenge. In the absence of credible evidence due to technical shortcomings, it would be a troublesome task to take into account all possibilities about the origin and motivation of the attack. This complexity further expands into the danger of miscalculated escalation due to an inherent chance of error, not to mention the legal, political and moral implications of such a miscalculated decision.

Squaring the Circle

It is certainly important to find an answer to the number of questions associated with this ongoing debate, despite the fact that cyber warfare has yet to achieve the status of full-blown activity. However, there is no denying the fact that its very nature demands special attention, particularly if cyberspace as a fifth dimension of warfare is crowded with fifth-generation tactics of war, where non-state actors can acquire the capability to impose their will on state actors. Hence there is need to develop common approaches to curb the growing risks of cyber conflict and subsequent destabilisation. The following are some proposed measures to this end.

- The most important step in this regard would be to establish regulatory oversight to address the legal loopholes in the prevailing setup. It is important to fill these caveats and legally define what constitutes a cyber attack, and to determine the red lines in this domain. This gap can be bridged first by demystifying the existing legal structure and then adding new elements where needed. In this regard, there is a need to develop and adopt a formal treaty or convention that would foster a consensus on the basic and universally accepted principles and rules covering the cyber sphere. This becomes even more necessary with the exponential increases in cyber attacks on security and financial infrastructures of states in the absence of a governing set-up. A number of states have developed national cyber-security strategies, but this does not override the need to have an international framework since cyber warfare is quintessentially a transnational activity with trans-boundary impacts. A greater international cooperative framework in the form of a multilateral treaty is required to effectively curb the criminal use of cyberspace. Such a framework should ideally develop a global common nomenclature to demystify some of the existing principles. It would help to establish international cooperation for investigation and prosecution of such activities, and would create some much-needed cyber-deterrence.

- There is a need to establish an international reporting system of cyber-related events. Based on the principles of Incident and Trafficking Database (ITDB) that was developed for the illicit trafficking of nuclear and radiological materials at the International Atomic Energy Agency (IAEA), there could be an international Cyber Security Incident Database (CIDB) under the UN, where all countries would be able to report minor or significant cyber attacks. This would keep a check on global cyber activities and encourage the states to report any incident and acquire global help in return. Sharing of information at such a forum would go a long way in breaking a gridlock of silence on this front.

- There is a need to adopt and nourish a normative approach to ensure global cyber security. Several states have taken some voluntary measures at the national level. Such voluntary measures can be institutionalised and expanded into some Confidence Building Measures (CBMs) to ensure their compliance with international norms of peace and security. Such CBMs exhibiting transparency can be a useful tool among states such as the US and China, India and Pakistan, which can engage in a number of CBMs in the cyber domain to enhance regional security.[40] A cyber element can also be added to some existing CBMs to enhance their utility. For instance, since the signing of the 1988 India-Pakistan Non-Attack Agreement on nuclear installations, at the beginning of each year the two countries exchange lists of their nuclear installations. This is lauded as the most successful of CBM between the two nuclear rivals, and one that has withstood the pressures of various crises. Article 1 of Non-Attack Agreement prohibits an attack or damage to each other's nuclear facilities. However, it does not categorically include or address a cyber attack.[41] It is therefore proposed that the cyber dimension may be incorporated in the existing agreement for more clarity. It may also be expanded to secure other critical infrastructures such as aviation and the nuclear command and control system.

The measures proposed above do not work in isolation. Each one complements the other and is necessary for a stronger response to the abuse of cyberspace. Therefore, there should be a concerted effort to take effective measures in all the given areas to create and strengthen a global cyber security regime.

Conclusion

The exponential increase in cyber attacks over the years has brought to surface a number of challenges that have changed the dynamics of conventional war. In view of the growing cyber threats, a number of conventional tools of war fighting have become meaningless in a number of ways, if not irrelevant altogether. It has virtually taken the warfare much farther from the Clausewitzian concept of use of military force as a

means to extend foreign policy objectives. Its application, in essence, is closer to Sun-Tzu's concept of indirect warfare, where a war could be fought and won without "laying siege to the cities".[42] This makes prevention even more difficult, as the traditional boundaries between offence and defence are blurred. In light of this, it becomes necessary to have strong legal foundations based on technical realities. This would certainly not be possible without the global community coming together to espouse universally agreed principles and codify some norms and rules. Global cooperation and necessary information sharing would help the world to stay a step ahead of cyber-spatial warriors and criminals.

Notes and References

1. ICT Statistics, "The World in 2014: ICT Facts and Figures," accessed March 24, 2015, http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

2. John Carlin, "A Farewell to Arms," *Wired*, Issue no. 5.05, May 1997, accessed January 10, 2014, http://www.wired.com/wired/archive/5.05/netizen.html.

3. *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*, 61st Plenary Meeting, December 2, 2008.

4. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), 106.

5. Oona A. Hathaway, Rebecca Crootof, et al., "The Law Of Cyber-Attack," *California Law Review* (2012): 10.

6. Ibid, 11-15.

7. "A Timeline of Cyber Attacks," *NATO Review Magazine*, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.html.

8. "Chinese Protesters Attack Indonesia Through Net ," *BBC News*, August 19, 1998, accessed March 15, 2014, http://news.bbc.co.uk/2/hi/science/nature/154079.stm.

9. Norton Antivirus Company defines the Stuxnet as, "a computer worm that targets industrial control systems that are used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar

operations." In 2010 it ravaged Iran's Natanz nuclear facility and destroyed its centrifuges, accessed March 24, 2015, http://us.norton.com/stuxnet.

10. David E. Sanger, "Iran Fights Strong Virus Attacking Computers," *New York Times*, September 25, 2010.

11. "U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show," *The Washington Post*, August 30, 2013, accessed March 02, 2014, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

12. James R. Clapper, Director of National Intelligence, Statement for the Record, "Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence , January 29, 2014, accessed March 15, 2014, http://online.wsj.com/public/resources/documents/DNIthreats2014.pdf.

13. Mark Thompson, "Panetta Sounds Alarm on Cyber-War Threat," *Time*, US, October 12, 2012, accessed March 26, 2014, http://nation.time.com/2012/10/12/panetta-sounds-alarm-on-cyber-war-threat/.

14. "China's National Defense in 2004," Information Office of the State Council of the People's Republic of China, 2004, accessed March 12, 2014. http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html.

15. James A. Lewis, Katrina Timlin, "Cyber security and Cyber warfare, Preliminary Assessment of National Doctrine and Organization," UNIDIR Resources, 2011, accessed March 26, 2014, http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

16. James A. Lewis, Katrina Timlin, "Cyber security and Cyber warfare, Preliminary Assessment of National Doctrine and Organization," UNIDIR Resources, 2011, accessed March 10, 2014, http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

17. Overview of Cyber Security ITU-T X.1205, Telecommunication Standardization Sector of ITU Series X: Data Networks, Open System Communications and Security (04/2008), accessed April 01, 2014, http://www.itu.int/rec/T-REC-X.1205-200804-I.

18. The non-state actors are defined as "*non-sovereign entities that exercise significant economic, political, or social power and influence at a national, and in some cases international, level*", Report on the series of seminars held in 2006-07 on "*The Role of Non-state Actors in International Politics*" hosted by the National Intelligence Council (USA) and Eurasia Group, accessed April 10, 2015, https://fas.org/irp/nic/nonstate_actors_2007.pdf. In the cyber domain, however, a non-state actor can be a citizen of a state but it conceals its identity in the virtual world. It may range from an ordinary citizen to a cyber espionage agents or a cyber terrorist. See for example: Johan Sigholm, " *Non-State Actors in Cyberspace Operations"* Captain, Ph.D. student, Swedish National Defence College, accessed April 10, 2015, http://www.ida.liu.se/~g-johsi/docs/JMS_4-1_Sigholm_Non-State_Actors_in_CyberOps.pdf.

19. Merriam Webster dictionary defines a mercenary as "*a soldier who will fight for any group or country that hires him*." A cyber mercenary can be defined as an individual or a group of experts who can offer their skills to anyone who will pay them a good amount of money. Kaspersky, the anti-virus company, has uncovered various cyber mercenaries, who can run full-scale surveillance assaults, such as Icefog discovered in 2013 and Desert Falcons in 2015. For details see: Pierluigi Paganini, "Icefog – Kaspersky discovered the group of cyber mercenaries", *Security Affairs*, September 27, 2013.

20. Dr. Jeffrey Hunker, Bob Hutchinson, Jonathan Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution," Institute for Information Infrastructure Protection, January, 2008, accessed April 02, 2014, http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf, also see "'Flame' Virus explained: How it Works and Who's Behind it," accessed April 02, 2014, http://rt.com/news/flame-virus-cyber-war-536/.

21. A good debate on means based definition and objective based definition is made in Oona A. Hathaway, Rebecca Crootof, et al., "The Law Of Cyber-Attack," *California Law Review*, 2012, 11.

22. Oona A. Hathaway, Rebecca Crootof, et al., 40.

23. Herbert Lin, "Cyber conflict and international humanitarian law," *International Review of the Red Cross*, Volume 94, Number 886, Summer 2012, 523. accessed February 25, 2014, http://www.icrc.org/eng/assets/files/review/2012/irrc-886-lin.pdf.

24. Charter of the United Nations, Chapter I: Purpose and Principles, accessed February 25, 2014, http://www.un.org/en/documents/charter/chapter1.html.

25. "NATO Agrees Common Approach to Cyber Defence," accessed February 25, 2014, http://www.euractiv.com/infosociety/nato-agrees-common-approach-cyber-defence/article-171377.

26. International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, advisory opinion, 1996, Article 39, accessed April 20, 2014, http://www.icj-cij.org/docket/index.php?sum=498&code=unan&p1=3&p2=4&case=95&k=e1&p3=5.

27. Oona A. Hathaway, Rebecca Crootof, et al., 26.

28. Summary of ICRC presentation on the application of IHL to cyber warfare and new technologies, November 8, 2012, accessed April 02, 2014, https://www.icrc.org/en/war-and-law/conduct-hostilities/cyber-warfare.

29. Marco Sassòli, "Legitimate Targets of Attacks under International Humanitarian Law," Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge, January 27-29, 2003.

30. Meeting Summary: Cyber Security and International Law, Mary Ellen O'Connell, Louise Arimatsu, May 29, 2012.

31. Rex B. Hughes, *NATO and Cyber Defence: Mission Accomplished?*, *ATLANTISCH PERSPECTIEF*, April 2009, accessed April 02, 2014, http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf .

32. Myrna Azzopardi, "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on its Treatment of Jus ad bellum Norms," *ELSA Malta Law Review*, (Edition III, 2013), 174-184.

33. *Text of the Convention on Cybercrime, Budapest, 23.XI.2001.* Accessed April 03, 2014, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

34. Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," *International review of the Red Cross*, Volume 94 Number 886 (Summer 2012).

35. See, *e.g.*, G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19,

2006); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Jan. 8, 2008); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Jan. 9, 2009); G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Jan. 14, 2010) .

36. Chris C. Demchak, Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, (Spring 2011), 32-61.

37. Ibid, 36.

38. Joseph Nye, "The Mouse Click that Roared," *Project Syndicate*, September 09, 2013, accessed March 12, 2014, http://www.project-syndicate.org/commentary/addressing-the-cyber-security-challenge-by-joseph-s--nye#o4xpVYeRh1gitusW.99.

39. Glenn Greenwald and EwenMacAskill , "Obama Orders US to Draw up Overseas Target List for Cyber-Attacks", *The Guardian*, June 7, 2013, accessed March 20, 2014, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

40. Prof. Götz Neuneck, "*Confidence Building Measures - Application to the Cyber Domain*," IFSH, University of Hamburg, accessed March 12, 2014, www.ifsh.de and www.armscontrol.de Also see, Brig. Tughral Yamin, "*Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan*," Sandia Report, SAND2014-4934, 2014, accessed May 05, 2014, http://www.sandia.gov/cooperative-monitoring center/_assets/documents/SAND2014-4934.pdf.

41. *Text of the Non Attack Agreement between India and Pakistan*, Centre for Non Proliferation Studies.

42. Sun Tzu, *The Art of War, Chapter III, Attack by Stratagem*, accessed April 12, 2014, http://www.chinapage.com/philosophy/sunzi/sunzi-e.html.