CYBER SECURITY: CHALLENGES AND THE WAY FORWARD

Dr. Muhammad Riaz SHAD
National University of Modern Languages (NUML), Pakistan

Introduction

The rapid advancement of Information and Communication Technologies (ICT) since the mid-1980s has revolutionized the Information Infrastructure (II), which comprises communications networks and associated software and facilitates interaction among people and organizations. The prevalence of information at all levels of a society—individual, organizational and state—causes to label the contemporary era as "information age." This is particularly true for western industrialized nations, where critical infrastructures—communications, energy, transportation, banking, water and services—are increasingly dependent on Information Infrastructure. While the information revolution has created new opportunities, improved organizational efficiency and led to unprecedented global connectivity, it has brought about new unconventional vulnerabilities and threats bearing social, economic, political and security implications.

Cyber security, meaning the protection of computers, networks and data, is a serious concern of individuals and organizations, public and private as well as national and international. This concern becomes more serious as "the internet of things" expands. As the technology advances with a rapid pace, innovations in cyber-crime also take place. Microsoft security bulletins regarding vulnerabilities of its products and services show an ever growing number of bugs, viruses and other threats to cyber security. Scope for cyber-threat increases as cyber-space remains unregulated and cyber-crime is simple as well as inexpensive to commit. Above all, cyber-attack poses a technical challenge of identification of the responsible as it is concealed through the use of several networks. Thus, an easy escape from this problem does not exist. However,

serious cyber-attacks committed or backed by a state against another state can be prevented through international cooperation, if it could be achieved. This paper assumes that cyber security, apparently a technical issue, is to a great extent an economic and political matter. In view of this, the paper focuses on the social, economic and political, rather than technical, dimensions of cyber security.

1. Key Concepts

While the technical details of cyber security are beyond the scope of this study, the basic concepts are essential to understand in order to explain it as a socio-political phenomenon. These key concepts can be divided into two sets, each containing three interrelated concepts. First set comprises the concepts of cyber security, cyber space and cyber governance.

Cyber security, also called information technology security, refers to technologies, processes and practices "to prevent, detect and recover from damage to confidentiality, integrity and availability of information in cyberspace."[1] This general definition indicates that cyber security involves not only technical but also political and legislative measures.

Cyberspace refers to "the interaction of people, businesses and other entities over computer networks, namely electronic messages and commercial on-line services."[2] The most sizeable and visible manifestation of cyberspace is internet, which is ubiquitous as it is available everywhere at the same time.

Cyber (security) governance refers to "the development and application by Governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[3] It aims to discipline the behavior of internet developers and users through regulatory frameworks, involves both technical and legal measures, and operates within as well as between the states.

Second set comprises the concepts embodied in the nature and scope of cyber-attacks and the concept of critical infrastructure. *Cyber-attack* refers to "any act by an insider or an outsider that compromises the security expecta-

1 Jennifer L. Bayuk et al., *Cyber Security: Policy Guidebook* (Hoboken, New Jersey: John Wiley & Sons, 2012), 3.

2 Klaus W. Grewlich, *Governance in 'Cyberspace': Access and Public Interest in Global Communications* (The Hague, The Netherlands: Kluwer Law International, 1999), 19.

3 Jovan Kurbalija, *An Introduction to Internet Governance* (Geneva, Switzerland: Diplo Foundation, 2014), 5.

tions of an individual, organization, or nation."[4] Cyber-attacks can be categorized into four areas: cyber crime, cyber espionage, cyber terrorism and cyber war. It is useful to differentiate between these types of cyber attacks.

Cyber crime involves the use of computer networks by individuals alone or in groups to steal confidential data or cause disruption, mostly for financial gains. It includes criminal activities such as stealing of credit/debit card information and intellectual property theft as well as disruption to a website or service.

Cyber espionage refers to the use of computer networks to get unauthorized access to personal or confidential information held by individuals, governments or organizations for intelligence or certain operations.

Cyber terrorism is associated with a non-state actor/organization that uses computer networks for terrorist activities aimed at creating fear and panic or causing physical destruction.

Cyber war includes use of computer networks by a state against an adversary (state or non-state actor) for military operations designed to disrupt information systems or systems connected to information technology in view of political goals.

In technical terms, above-defined cyber-attacks take place in three forms: account takeover, impostor fraud and denial of service (DOS). *Account takeover* involves the use of malware to obtain a user's confidential information—IDs, PINs and passwords—for transferring money or doing other frauds. In *imposter fraud*, a fraudster presents himself to an authorized user as a person who is trustworthy or an authority, and requests a bank transaction, which seems normal to the bank. *Denial of service* (DoS) is a cyber-attack which makes networks or systems unavailable.

Serious cyber-attacks target *"critical infrastructures"* of an organization or a state. In this context, an infrastructure refers to "a framework of interdependent networks and systems, generally interlinked at many different levels, including industries, institutions and distribution capabilities that provide a flow of products or services."[5] Five broad sectors can be identified as critical infrastructures, particularly in modern developed countries: information and communication, banking and finance, energy, physical distribution (transpor-

4 Robin A. Gandhi et al., "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technology and Society Magazine*, February 2011.

5 Edward Halpin et al., eds. *Cyberwar, Netwar and the Revolution in Military Affairs* (Hampshire & New York: Palgrave Macmillan, 2006), 35.

tation networks) and human services.[6] Among these, information and communication infrastructure are vulnerable to cyber-attacks. Since other critical infrastructures are interconnected through information and communication networks, they are also vulnerable to cyber risks.

2. Range of Cyber-Attacks and the Motivations

Vital social infrastructures—electricity, finance, water, transportation, health and food—are increasingly dependent on ICT networks for their functioning, distribution and interconnectedness. This dependence results in both opportunities and vulnerabilities which can be exploited by people ranging from individuals to governments. "Information revolution" experienced by the contemporary world is boon as well as bane. It is bane because ICT has an "enabling function" for disruption, crime and state-level aggression. ICT dependence becomes more prone to vulnerabilities in times of social unrest, political tensions and other appalling events. The spectrum of cyber-attacks is quite broad, from individual activity, to activities of groups and non-state actors, to governmental actions. These attacks are driven by a range of motivations—from ideological campaigns, to financial gain, to political objectives.

Cyber-attacks perpetrated by different actors along a spectrum can broadly be divided into four types: hacking, serious and organized cybercrime, cyber-extremism and state-level cyber-aggression. These types of cyber-attacks vary with respect to the kind of target, attack methods and degree of impact.

a. Hacking

Hacking is the first in the range of cyber-attacks. It is done by a "script kiddie"—a person who is low skilled and, therefore, uses existing software tools to hack into computer networks. Hacking usually aims at fun, petty theft or revenge by a disgruntled insider. Besides, an individual hacker may be motivated by some ideological or political campaign at national or international level. Because hacking is a disorganized activity and has low-level consequences, it is far less threatening than other serious cyber-attacks. But some analysts consider it a serious cyber-attack not only because it may seriously perturb the affected but also because it may lead to more serious cyber-attacks.

b. Serious and Organized Cybercrime

As the internet has increasingly turned a significant source for financial and commercial activity, criminal's interest in it has increased accordingly. Presently, cyberspace is a tempting target for serious and organized crime,

6 Halpin et al., *Cyberwar, Netwar*, 35.

which is committed by organized and skilled mercenaries. Motivation behind such a crime is financial gain. Black market networks, for instance Darkmarket, are engaged in a variety of cybercrimes such as theft, buying and selling of personal data from bank accounts, credit cards, identity numbers and passwords as well as trade of botnets, meaning compromised computer networks. Likewise, organized criminal groups like Japanese Yakuza use cyberspace for a number of illicit activities: drug trafficking, money laundering, counterfeiting, bank frauds and piracy.

With "the migration of real-world organized crime to cyberspace," world economy suffers considerably. According to a 2014 report of the Center for Strategic and International Studies (CSIS), cybercrime cost the world economy around $445 billion per annum, while the total loss borne by major economies such as the US, China, Germany and Japan reached $200 billion a year.[7] Serious and organized crime stands as a challenge for law enforcement agencies, especially where it is transnational in character. While cyber criminals can operate transnationally without being detected, authorities across the world have yet to agree to cooperate with one another.

c. Cyber-Extremism

Cyberspace is becoming "the most important meeting place" for ideologically and politically motivated extremists, given their space in the physical world is narrowing and they have a transnational agenda. They use global "infosphere" for a number of activities: communications, propaganda, indoctrination/radicalization/recruitment, and training. Moreover, they exploit ungoverned cyberspace for disrupting the websites and networks of their enemies, stealing money and coordinating attacks in the physical-world. Use of cyberspace for their agenda is lucrative and convenient to extremists because it offers anonymity, it is cheap, and it provides transnational virtual reach.

d. State-level Cyber-Aggression

A state-sponsored cyber-attack is usually well funded, organized and conducted by highly skilled personnel. States have political, national security and strategic motivations behind such cyber-attacks. A new form of warfare has come of age in which cyberspace is strategically used to facilitate conventional military attacks. This kind of "cyber-enabled physical attack" first disrupts critical infrastructure to facilitate a physical attack on a military target. For instance, in 2007, Israel attempted a cyber-attack on Syria's air defense capabilities in order to launch an air strike in the country. Similarly, Russia allegedly

7 "Cyber crime costs global economy $445 billion a year: report," *REUTERS*, June 9, 2014, http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

made strategic use of cyberspace in the midst of its conflict with Georgia over South Ossetia in 2008.

An important dimension of Sino-US tensions is related to mutual accusations of cyber-attacks against each other. Neither state has officially acknowledged such attacks, even though both are reportedly engaged in research on cyber warfare. The U.S. is of the view that China is rapidly building capacity in cyber warfare and can disrupt its military forces' deployment or operations in case of a conflict.[8]

In recent years, states, particularly the U.S., have increasingly become concerned about cyber-attacks. In 2013, U.S. high-ranking officials acknowledged before Senate that "cyber attacks" and "digital spying" were more serious threats to national security than terrorism.[9] U.S. concern with regard to cyber threat is reflected in its federal government's allocation of $14 billion in 2015-16 fiscal year for cyber security.[10]

3. The Way Forward

Threat to information security or cyber security is serious and complicated, while states have so far failed to find a comprehensive and effective solution to the problem. Following facts give an idea about the seriousness and complexity of information security challenge:

a. Cyber offense is low-cost and easier, while cyber defense is expensive and harder. Fortinet pointed out in its 2013 Cybercrime report that a botnet—a network of compromised controlled by cybercriminals—costs $700 to establish or $535 to rent for a week.[11] On the other hand, states, particularly having ICT dependent infrastructures, spend billions of dollars on cyber security.

b. Cyber threat is serious because it involves multiple actors—individuals, organized and serious criminals, extremist groups and governments—and poses social, economic, political and security risks and challenges.

c. The threat is turning more serious as states' critical infrastructures are increasingly becoming dependent on information and communication in-

8 Dr Paul Cornish, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks* (PE 406.997) (Brussels: European Parliament, 2009), 15.

9 University of Maryland, "Cyber Security Primer," http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm

10 Andrea Shalal and Alina Selyukh, "Obama seeks $14 billion to boost U.S. cybersecurity defenses," *REUTERS,* February 2, 2015, http://www.reuters.com/article/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202

11 IT Governance, "What is Cyber Security?," http://www.itgovernance.co.uk/what-is-cybersecurity.aspx

frastructure. Billions of machines, such as computers, smartphones, tablets, ATMs and thermostats, are inter-linked, making different critical infrastructures inter-dependent.

d. Since regulation of cyberspace and critical infrastructures involves complications, an effective system for information security governance does not exist. This means information and communication systems have in-built vulnerabilities.

e. Major challenge to information security governance is the difficulty of attribution of cyber-attacks; cyber criminals cannot be detected.

f. Finally, cyber threat is transnational due to the borderless nature of cyber infrastructure.

In response to above-mentioned challenges to cyber security, states have adopted following measures:

I. States use technological tools to achieve three objectives with respect to cyber security: prevention, detection and response. Prevention includes governance, installation and awareness training with regard to technology. Detection means identifying any strange pattern in data traffic by monitoring and mining data. Response refers to the use of technological tools once cyber threat is detected. Technology enables an organization to deactivate its affected systems.

II. More nations worldwide are adopting national laws on cyber security governance and punishing criminals.

III. States have only a limited international cooperation on cyber security.

Two key observations from the preceding points are important to suggest the way forward:

First, technology does not ensure to overcome the issue of cyber security entirely. Attribution of cybercrime to a specific perpetrator is very difficult or almost impossible, because identity can be disguised. Traditional cyber security measures—anti-virus, encryption, firewalls and automated detection—simply repel the threat; they do not collect information regarding the perpetrator's identity. Hence, policing and accountability of perpetrators of cybercrime is extremely difficult. This lack of effective cyber deterrence encourages the wrongdoers to continue the cybercrimes. This means technological measures alone are insufficient to ensure cyber security.

Second, states are increasingly adopting self-regulatory legal mechanisms to achieve cyber security; however, national legal measures are not sufficient to deal with the problem. It is so because cyber threat is not bound by borders

as ICTs are globally interlinked. Likewise, cyber-crimes, whether in the form of serious and organized crime or terrorism or government-backed actions, are mostly transnational. Secondly, given that cyber-crime involves low-cost attacks which can easily and effectively be carried out even by people from poor nations, national legal mechanisms are insufficient to deal with transnational features of cyber security. Finally, certain cyber-attacks become an international relations issue when these are backed by governments as an extension of state conflict.

These observations indicate that international cooperation in cyber security is very important, while only technical and national legal measures do not constitute a complete solution. For instance, creator of "I-love-you virus" of 2000, a Philippines' young student whose act cost huge financial loss worldwide, could not be arrested under Philippines law.[12] International cooperation in cyber security has two dimensions. First is the formulation and implementation of an international regime that facilitates cooperation against cyber-crime across the nations. Second is the provision of "cyber security aid" in terms of technical or legal advice and financial assistance to those states which have weak cyber security capabilities and policies. In this case, role of International Telecommunications Union (ITU) needs to be strengthened as its Global Cyber Security Agenda aims to improve the capabilities of states and private organizations in cyber security.

However, achieving international cooperation in cyber security is a big challenge for international community. Cyber security is a "post-state" problem, but there has been little progress in understanding or resolving the problem beyond the state. Thus, we see a paradox: state can't effectively deal with cyber security issue, but state is expected to be responsible for it. This paradox shows the need for international cooperation. Lack of international cooperation in cyber security is associated with technical and legal factors, but, foremost, it is political in nature. Political factors responsible for dismal cooperation in cyber security can be identified from two examples of inter-state cooperation in this area, namely NATO and EU. The two entities, although different in terms of origin, have a long existence, sufficient to study hurdles in inter-state cooperation in cyber security.

Example of NATO shows the difficulty of adjusting cyber war concept within traditional security arrangements. The 2007 cyber-attack on Estonia reflected that Article 5 of NATO charter was hardly equipped to deal with

12 Mischa Hansel, "Cyber Security Governance and the Theory of Public Goods," *E-International Relations*, June 27, 2013, http://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/

cyber-attacks. More specifically, this attack highlighted two problems: attribution and retaliation, and characterization of cyber war as war. Use of force in retaliation to cyber-attack is problematic because of the attribution challenge. Given that the origin of cyber-attack can be masked, it is still unclear whether the 2007 attack on Estonia was backed by Russia as state. Retaliating against a state, from where a cyber-attack emerges, becomes misleading due to several reasons. First, a third party can exploit a pre-existing political tension between two states, as, for example, between Estonia and Russia or between China and Taiwan. Secondly, this will adversely affect inter-state trust, which carries vital importance in the context of political, diplomatic and treaty relations between states. In case of a cyber-attack, computer used for attack can be identified through Internet Protocol (IP), but this does not necessarily lead to the identification of person involved in attack. This means cyber-attacks can potentially be designed to appear come from a particular state. This ambiguity with regard to cyber attack's origin provides states a space for "plausible deniability."

Second problem that NATO's collective security doctrine seems unable to address is whether cyber war can be considered a war at all. While some experts opine that a cyber-attack can result in a serious incident suffice to be considered an act of war, others do not agree to equate the disruptive use of cyber space with war. In view of increasingly serious nature of cyber-attacks, such as DDoS, attacks on critical infrastructure and economic losses, cyber-attacks are being considered by some as state of war. However, this conception lacks consensus. Thus, NATO's example shows that the problem of attribution and its implications for retaliation and the problem of equating cyber war with a war in traditional sense of word are two political impediments on the way of international cooperation in cyber security.

Second notable example of international cooperation in cyber security is the Budapest Convention, officially known as the Council of Europe Convention on Cybercrime. In fact, this is the first international treaty that deals with crimes committed through internet. It was enforced in November 2001 and any state can joint it. It lists five cyber actions illegal and these should be investigated by authorized domestic agencies. These actions are unauthorized access, unauthorized interception, data interference, system interference and misuse of devices.[13] The Convention exempts states from investigating those crimes which clash with their public policies or security. Major political impediment the Convention faced was the interpretation of activities that fall in the category of online crimes. For instance, listing hate speech and violation of

13 Convention on Cybercrime, *Council of Europe,* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

copyright draws criticism and opposition from human rights activists, internet service providers and social media platforms like You Tube. Thus, cyber laws are criticized by some as "paper laws".

Few more factors account for the lack of international cooperation in cyber security. First, some states lack interest in addressing cyber-crimes alone or in collaboration with other states because of inadequate technical and financial capability. Second, some states are less vulnerable to cyber-crimes because their critical infrastructures are less dependent on ICTs or they have secure and reliant networks or lack intellectual property. This asymmetric vulnerability to cyber-crimes leads to varying interest in international cooperation in cyber security. Third, some states, like the U.S., do not agree to international agreements on cyber security because these will potentially limit the use of cyber space for military and intelligence objectives. In this case, there is a contradiction in the U.S. position as it is averse to the use of cyber technology by other states for military and intelligence activities, but it does so on its part. Fourth, another argument against international agreements on cyber security is that this would give an opportunity to oppressive governments for denying political, religious and economic freedoms to their people.

Conclusion

Notwithstanding with these impediments, states need to agree on international cooperation in cyber security of certain infrastructures. After all, there are many examples of international regimes aimed at protecting transnational activities from harmful acts. For instance, those involved in hijacking of civilian planes should be extradited or prosecuted according to an international treaty in the area of civil aviation. Although the issue of cyber threat cannot be entirely resolved, international community should develop political consensus on cyber security of, at least, civilian infrastructures. The discipline of International Relations has made great strides in addressing issues of war, peace, security and cooperation. However, its performance in focusing on cyber threats and their implications for inter-state relations is so far lackluster. Only realistic and dedicated efforts can lead to serious realization among states on the imperative of international cooperation in cyber security.