VFAST Transactions on Education and Social Sciences
http://vfast.org/journals/index.php/VTSE@ 2015 ISSN(e): 2309-3951;ISSN(p): 2411-0221
Volume 3, Number 1, January-December, 2015

pp. 141–146

UNDERSTANDING THE SIGNIFICANCE OF CYBER SECURITY THREATS

ATTIQ UR REHMAN[1]
Area study centre for Africa, north and south America
[1] QUAID-I-AZAM UNIVERSITY ISLAMABAD
MIRZA_ATTIQ@HOTMAIL.COM

ABSTRACT: In the age of globalization, rapidly emerging digital infrastructures of states are open for the clandestine and malicious activities of virtual warriors. The dependency on cyberspace has revealed the digital vulnerabilities of states before their rivals. Hence, the national security of state, presently, is wrestling with the cyber security threats. The protection of core national values and sensitive infrastructure of states are under question. Therefore, the safety and security of digital assets of states have become one of the most serious concerns for the policymakers. The international cyber culture across has declared the national government of states more insecure and unprotected. The combination of offensive and defensive capabilities of state is the key instrument in the cyberspace for the security, and protection of their cyber borders. In this way, the central theme of the work attempts to highlight the significance of cyber security threats by elaborating the strategic dimension of global cyberspace.

Keywords: Cyber Security; Cyber Crimes; Safety and Security; Virtual Warriors; Information Communication Networks; Cyber Terrorism; Cyber Warfare; Digital World; National Security.

1. Introduction

The structure of internet system has emerged as a one of the prevailing security domains in international politics due to the rapidly emerging security challenges. The cluster of security threats has fabricated a complex strategic environment globally in which the states are becoming vulnerable and defenseless. The increasing dependency of international system on cyberspace, in this way, has posed serous security threats to contemporary state structure. The wide usage of internet has become an essential component of society, politics and economics. The growth of cyberspace in all spheres of life raised the critical questions of cyber security and the protection of national cyber borders. In this way, safe and secure computer network has become the basic need of society. The development of a trustworthy communication networks based on incredible accuracy, security of information and sensitive data has become the demand of the citizens of every nation.

On one side, the widespread usage of internet has revolutionized the international society by facilitating and providing the nations with the upgraded and advanced means of communication. On the other, the global fast interconnectivity has posed the risks to digital survival of mankind, because the organized criminal activities, politically motivated hackers, and cyber intruders have caused the unthinkable consequences such as economic espionage, financial loss, theft of sensitive data and secret information. Therefore, the disguised internet users with fake IDs, and threats of devastating effects of internet are no more unusual and alien features of international cyberspace. As a result, the frequent attacks on cyberspace from anonymous sources backed by political objectives have created internationally an ambiguous security environment in which all states are equally vulnerable and defenseless. Therefore the rapidly growing digital infrastructure of states has raised critical questions, regarding the safety and security of internet users to state governments.

The powerful and vulnerable information communication networks have fabricated an utterly new strategic environment in which it is not easy to justify the digital status of the world. It is still controversial question whether the internet is a blessing or a curse. Has the internet facilitated the traditional state system or it deliberately declared the vulnerabilities of leading state's structure. The increasingly growing cyber-attacks on information communication networks have challenged the traditional values of international system. The combination of merits and demerits of internet has formulated a challenging global cyberspace in which the appreciable performance along with the security of Information Communication Technology (ICT) is under question.

In short, cyber security threat has become one of the potential security threats to international system today. The strategic dimensions of cyberspace have inaugurated a new competition among states which reflects an ambiguous and dichotic state behaviors. On one side, states are fighting in cyberspace in order to defeat their rival forces by empowering their digital offensive capabilities. In reaction, the security pundits of states are busy in building the cyber forces in order to formulate the robust cyber deterrence against their covertly working cyber enemies. On the other, the national leaders are keenly interested in taking bilateral and multilateral initiatives for the global cyber security.

Domestically, the security of legitimate internet at domestic level, and the protection of national interest at international level are the potential challenges of cyber world. The effective legislative measure at national level along with the bilateral and multilateral initiatives could be adequate countermeasures in order to fight the war against emerging cybercrimes. In this way, cyber security has become an undeniable fact of the world. Therefore, a number of writers try to portray the future of international system without even addressing the fundamental questions relevant to cyberspace. The existing literature on cyberspace tried to associate the concept of cyber terrorism, information warfare, and cyber warfare with cyberspace without explaining the evolution and conceptual origin of cyber world. The primary objective of this work is to highlight the contemporary status of virtual world while focusing the historical bases of cyberspace. Moreover, the study attempts to evaluate the potential challenges of rapidly emerging cyberspace. At the end, the work will attempt to architect the future of international computer network in computer oriented politics.

2. What is Cyberspace?

The term cyberspace was firstly used by William Gibson in his science fiction novel *Neuromancer* in 19984 (Libicki 2007: 05). Later the idea was flourished by Neil Stephenson in his work *Snow Crash* in 1989. Both writers tried to portray the different dynamics of universe for mankind by challenges the conventional wisdom of virtual world. So, the ideas of science-fiction writers got public appreciation and general acceptability. The directors and producers of film industry started thinking about the cyber future of the world by following the fiction writers. The rapidly growing computer systems and communication networks materialized further the ideas of writers and vision of filmmakers.

The term cyberspace is not solely associated with the internet and the linked computers, but it also includes the electronic devices and the mechanisms either directly or indirectly linked to it (Fischer 2009: 11). Further the term incorporate the software that help in smooth functioning of operating systems, stored data, and devices which transfer the data from one computer to another. Moreover, cyberspace contains all the structures such as the cables, routers, servers, networks and the satellites, which is involved in internet transmission. Therefore, cyberspace has its own mapping techniques and methods for running the internet communications (Fischer 2009: 11). Additionally, the term cyberspace infrastructure usually refers to four elements which include the hardware used in internet, telecommunication structure, associated operating systems and the digital devices such as desktop or laptop computer (Fischer 2009: 11). The threats to one component of the cyberspace endangered the whole structure. Usually, the malware affect the efficiency of operating system by targeting its performance.

An analytical survey of nontraditional security threats suggested that the Cyber security is not a new dimension of world politics. Historically, the demise of Soviet Union and the end of Cold War marked a new chapter in the history of mankind by highlighting the significance of nontraditional security threats. Cyber security is one of them. Even before the tragic event of 9/11, the leading policymakers and the security analysts in their studies had been raising the serious concerns regarding the vulnerabilities of computer networks.

Presently, internet has entered in all the spheres of life and increased the dependency of mankind on online communication networks. So the web of information communication networks has covered the whole world into a global village. The social interactions, business deals, economic transactions, governmental activities, social and political campaigns on internet have inaugurated an age of internet. The escape from World Wide Web (www) is not only hard but impossible today. The fundamental objective of constructing the global web of information network was only to facilitate the people across the borders by establishing a peaceful society, but the widespread accessibility of internet developed it as a weapon for criminals and hackers. Presently, cyberspace emerged as a potential challenge, because it is difficult to control the hostile conquest in the cyber world. The easy and friendly virtual conquests hampered the traditional security paradigms of security

3. Challenging Future No doubt, the tragic incident of 9/11 has shaken the international security, but the threats of cyber-attacks even before the war on terror had raised the serious security concerns internationally. In post 9/11 era, the computer-mediated conflicts have surrounded the whole world. The safety and security of cyber borders of states has become a global problem, because the friendly conquest in cyber world is a gravest threat to the sovereign values of every state. Therefore, cyber security threats are strictly associated with the international communication networks. All the states are equally vulnerable in cyberspace because the attacks on official websites and national information systems are not unusual incidents of contemporary international system. Moreover it is not easy to calculate the cost of the loss caused by cyber-attacks.

The adequate security measures are essential to reduce the possibilities of cyber security threats because the multidimensionality of cyber-attacks has jeopardized security of the entire world. The criminal attempts in cyberspace can exploit the technical shortcomings of global web of networks. In order to strengthen the cyber defense, the state officials are busy in developing appropriate cyber policies and adequate cyber laws to minimize the likelihood of cybercrimes in future.

In this way, the development and enhancement of a national cyber security program has become a fundamental demand of every state, because the disguised hackers and cyber criminals have impeded the defense—the state's abilities to protect the critical digital infrastructure and sensitive information. Therefore, it is essential for state officials to contain the overcoming wave of cyber threat before it produce unthinkable consequences in the form of cyber terrorism and cyber warfare in future. As such catastrophic effects of cyber-attacks could be capable enough to inflict unthinkable damages to any nation. In this way, the cyber security is becoming one of the potential threats to the traditional security apparatus of states. There are three reasons which have shifted the cyber security at alarming level. First of all, the global interconnected network of public and private organizations. Secondly, the dramatically increasing internet users around the world, and thirdly, the sophistication in offensive techniques of criminals in cyber world (Fischer 2009: 01).

The primary responsibility of state authorities is to protect the legitimate internet users from the mischievous acts of cyber world before it has become a nightmare for whole mankind. The security pundits are keenly interested in preventing the influence of criminals, terrorists, hackers, spies from the cyber borders of the nation because it is undeniable truth that the world of cyber beings is evolving faster than ever by providing the new avenues and opportunities to the cyber criminals. In the progressing virtual world, the threats of fraud, crimes, and harassing acts are less likely to diminish in the society. The inadequate response of security experts will welcome the massive cyber-attacks in future. The insecure and vulnerable spots of internet are likely to be exploited by independent hackers and politically motivated cyber criminals.

Consequently, the motivation of terrorists after the 9/11 incident has been vividly exposed to the whole world. So, the potential terrorist groups or anti-globalization networks can launch an attack anywhere in the world. As it is accepted by a security scholar, Professor Neil Barret, from Royal Military College of Science (now the Defense College of Management and Technology) in UK, "we are going to have to start seriously considering that terrorists are going to get involved in hacking."(Streeter and Warren 2005: 244). In this way, in order to protect the digital infrastructure along with valuable computer-oriented intellectual properties of states, it is essential to understand the nature of challenges of cyberspace before formulating the countering strategies.

4. Cyber Security a Potential Threat. The cyber-attacks on critical infrastructure and sensitive digital assets of states have reached into its zenith by leaving the contemporary leading law enforcing agencies of states unprotected and unsafeguarded. The sensitive information of states, financial networks, digital command and control systems, and government institutions are under attack by the illicitly functioning cyber criminals. The anonymously working virtual warriors attacking with bogus IDs portrays awful picture of world politics in which all states need to declare the cyber security laws. The covert operations of cyber warriors has gained the momentum to launch unthinkable and unmanageable damages to the key infrastructure of states, which could not be less than a digital pearl harbor and cyber 9/11. In this way, the devastating effects of bloodless cyber skirmishes has become more severe threats then the dangers of nuclear and conventional attacks of rivals.

The age of cyberspace has challenged the traditional wisdom of security by inaugurating the cyber race in international system. No doubt, the state authorities are keenly interested in building the cyber forces which capable to launch preemptive operations against the potential rivals in cyberspace, but still the subs-state actors, militants and the illegitimate internet users has acquired the expertise to penetrate the cyber border of a state (Cavelty 2008: 138 – 140).

With the infancy the prominent cyber security threats which need serious attentions of cyber centric policies in order to strengthen the exiting cyber defensive mechanisms of states. The proper understanding of aforementioned characteristics of cyber world is the principle element for the development of an apposite cyber security strategy. The effective strategies cannot only prevent the hostile efforts of penetrations but it will also augment the existing national security mechanisms of states.

5. Cyber Security VS National Security. The defense of cyber borders of states has become one of the most severe threats to the national security mechanism of state. The rapid emergence of netizens (the citizens of virtual world) jeopardizes the cyber borders of states, which provides equally opportunities to the cybercriminals to carry their malicious activities in the digital world. The national security mechanisms are failing to recognize the nature of cyber-attacks, the threats in cyberspace are difficult to categorize. The identification of internal and external attacks is a staid challenge to the state authorities working on national security domains. Under national security mechanism, the governments treat domestic and foreign threats separately. Usually, the assigned departments are responsible to handle the internal and external threats to the states. Presently, the distinction of threats in cyberspace is impossible to define (Neack 2007: 15).

The easy conquest in cyberspace through digital ballistic missiles has fabricated a complex security environment for national security experts. The attempts to prevent the penetration efforts of cyber criminals have become a difficult task for state officials. The traditional notion of national security has engulfed the challenge of cyber security threats. The establishment of cyber deterrence by the formulation of defensive cyber forces of IT professionals is the prerequisite for cyber security. The effective mechanism for the identification, execution, and prosecution of cyber intruders can support the digital dimension of national security of states. The effective security mechanism in response to the overwhelming wave of cyber-attacks can overcome the digital deficiencies of states. The mobilization of internet-centric organs of national security mechanism can curtail the emerging wave of widespread malpractices of cyberspace. The rigorous nature of cyber security threats can be effectively managed by embarking an intensive debate among the national security experts in order to determine the security of cyber network.

6. Prospects of Hostile Cyberspace. The unthinkable growth and popularity of internet across the globe has dramatically changed the structure of international system. Henceforth, the future of international system is portraying a horrifying picture in which the states will be more unguarded and fragile before the threats of cyber warfare and cyber terrorism. The strategies in the information warfare in the virtual world, unlike the physical warfare strategies, will hinder the traditional security mechanisms of states. The cyber warriors will prefer to develop offensive capabilities for the ruinous, containment, penetrating and massive striking in the cyberspace (Erbschloe 2001: 3-7). The abilities to attack on information networks and capability to disable the digital command and control systems from rivals demands the development of defensive and counteroffensive competencies. Therefore, the protection of sensitive information along with the availability of a safe communication network has become a serious question for the security architecture of the military in the contemporary digital age. The protection of the military systems and the insurance of security readiness of virtual troops, coupled with the effective deployment of counter measuring forces and plans can ensure the electronic security of armed forces.

Besides the devastating consequences of cyber warfare, the unthinkable and unimaginable costs of terrorism in the cyberspace are becoming an inevitable future of the world. In future, the exploitation of information networks and communication technologies will become the most effective tool of terrorist organizations. In this regard, the terrorist access to the internet will inflict the sense of insecurity to the state authorities (Colarik 2006: 35). The evolving illicit networks of religiously extremist and ideological fundamentalist individuals can potentially diminish, disrupt and ultimately destroy the cyber assets of states in future. Therefore, in order to eliminate the threats of e-Jihad and digital extremism, the constant patrolling of digital boundaries and perpetual monitoring of illegal activities can empower the investigating capabilities of the states which can strengthen the domestic cyber security of the states. Additionally, the active involvement of IT companies working in private sectors can augment the role digital forces of states. In order to identify the potential weaknesses and their remedies in cyberspace can minimize the threats of cyber terrorism.

Besides the threats of cyber warfare and electronic terrorism, the threats of economic espionage, theft of sensitive and classified data needs absolute security which is utterly a new phenomenon. In this way, the establishment of a secured and protected cyber has become of one of the serious concern of defense planners of the states which are rapidly developing their e-infrastructures.

7. Way Forwards. The development of a national cyber security plan is an essential demand of every state that intends to develop the digital infrastructure. In order to build a stable and secure cyberspace, a combination of national and international approach can be effective and viable. The implementation of following steps can address the contemporary cyber challenges to the international cyberspace.

7.1. National Level

The digitally growing states need a reliable defense system which can identify and counter the cyber threats while overcoming the vulnerabilities. A protected and secured information communication network can secure the social, political and economic digital structures of the nations. So, an effective computer based early warning system could be helpful. At domestic level, the states should focus on the development of an early warning cyber system in order to secure the critical national infrastructure. Moreover, the formulation of a cyber-force can also defend the national cyber border of the states. Such force can also work as anti-cyber terror force in order to eliminate the suspicious or harassing online activities. In this way, a defensive cyber network could save a state in cyber world.

At national level, the state should develop its defensive capabilities for the identification of potential threats to the cyber borders by taking the legislative reforms—the policies and laws related to cyberspace, the involvement of computer industry along with the anti-malware organizations. Moreover, the promotion of cyberspace awareness campaigns, cyber-crime training centers, feedback from academia can be an awakening call to the most vulnerable states in the virtual world. The series of high profile and trained IT professional should be hired by the states for the formulation of effective counter measure against the cyber security threats.

The law enforcement agencies should be empowered to overcome the cybercrimes while the identification and prosecution of domestic hackers or virtual criminal can be controlled by the cyber-force. The units of such hi-tech force can control the awful uses of communication networks by seizing the activities of organized cyber-criminal gangs. Moreover, the collaboration between states officials and academia can explore the unknown dimensions of cyber defense which can better the performance of the architecture of cyber security.

7.2. International Level

The promotion of an international cyber security campaign can brought a dramatic change because the multilateral cooperation in the form of agreements can protect the global cyberspace. Convention on Cybercrimes introduced by EU is the first international agreement which gathered the 45 member states (with few non-member states) at Budapest, Hungry in its 109th session and signed a convention on cybercrimes. The 48 articles of the convention focused the techniques and strategies to counter cybercrimes by harmonizing the legislation at national level, developing the investigating skills, with establishing the international cooperation (Blane 2003: 01). Besides the EU efforts, several states are signing the agreements bilaterally to combat the growing cyber-attacks. Additionally, the regional efforts to prevent the potential cyber security threats are also under consideration. The Organization of American States (OAS) is agreed with the Latin American and Caribbean Internet Addresses Registry (LACNIC) on strengthening of internet security. Apart from all the discussed initiatives, a more comprehensive approach based on international cooperation for information sharing and cooperative agreements to enhance the global cyber security is required to downplay the overcoming wave of cybercrimes.

The global approach will not be helpful, though, in enhancing the state's capabilities against the cybercrimes but it will also introduce robust cyber deterrence by securing the cyber borders. The sharing values at international level will neutralize the hidden cyber ballistic missiles. No doubt, the multilateral initiatives have been taken by the states, but improved security cooperation will overcome the obstacles of security threats in cyberspace.

In short, there are several ways to overcome the cyber risks and cyber vulnerabilities which include the promotion of cyber education, research oriented computer reforms in academia, adopting the national and international reforms in exiting cyber defense. For sure, the international challenge of cyber security needs international cooperation. States should be activated at national and international level for the building to a secured and protected cyberspace. Moreover, the advancement of information defense structure can serve the guard the cyber borders of the states. The development of information warfare defense organizations, training of cyber combatants, the active cooperation between national and international defense organizations, testing the cyber defensive abilities, and assimilating the less-dependent information structures can be concrete steps which can effective ensure the survival in toxic cyberspace ((Erbschloe 2001: 10).

8. Conclusion. The future of the world is rapidly falling in cyber domain. The growth of internet is one of the most prominent achievements of IT, and it has become a commonly known phenomenon today. The rapidly growing digital infrastructure has increased the state's dependency on computer networks overdramatically. In response to the increasing malpractices in cyberspace, every state needs to reform its cyber defense system while integrating the national security with the international cyber security framework because the collapse of worldwide computer network will cause the serious and incredible consequences. Such collapse will ultimately lead to huge loss to society and everyday life.

In order to determine the sophisticated cyber security apparatus, all states need to share their defensive capabilities in the war against cyber-crimes. As the harassing characteristics of cyberspace are the real concerns of security consultants. To securing the cyber borders has become a global challenge. All states are equally vulnerable before the cyber criminals and illicit hackers. Hence, cyberspace is an international problem which is demanding the collective response of all the states for the establishment of a protected worldwide internet communication network. The rapidly emerging digital infrastructure of states has revealed the state's vulnerabilities and declared the national governments defense unsecured. A single state cannot effectively work in isolation as no state can build a virtual wall to keep its own network safe keeping (keeping in view the extensive sharing of information in every field of life). An international alliance would be the best strategy which can formulate international standards related to cyber laws. In this way, a global war against cybercrimes can secure the future of mankind.

The state authorities must understand the significance of cyber security. Cyber weapons are extremely dangerous for the digital social, political and economic infrastructure of the state. In the contemporary age of globalization, the modern nations are rapidly depending upon internet which is on the one hand facilitating the states to run their economic, social and political system. On the other hand, the addiction of communication networks made states vulnerable before their rivals. The covert hostile attack in the cyberspace can inflict the inconceivable consequences for any state. Consequently, the worse scenarios can be resulted in financial crisis, political instability and social unrest which can create a chaos anytime anywhere. So, in order to overcome the clandestine exploitation of cyberspace, all states should share their expertise by taking global initiatives. The global approach will ultimately secure all the states.

REFERENCES

[1]. Blane, V. J. (2003). *Cybercrime and Counterterrorism: Current Issues.* New York: Novinka Books.

[2]. Cavelty, M. D. (2008). *Cyber – Security and Threat Politics: US Efforts to Secure the Information Age*. New York: Routledge.

[3]. Colarik, M. A. (2004). *Cyber Terrorism: Political and Economic Implications*. London: Idea Group Publishing.

[4]. Fischer, A. E. (2009). *Creating a National Framework for Cybersecurity: An analysis of issues and options.* New York: Nova Science Publishers.

[5]. Erbschloe, Michael. (2001). Information Warfare: How to Survive Cyber Attacks. New York: McGraw – Hill.

[6]. Libicki, C. M. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

[7]. Neack, Laura. (2007). *Elusive Security: States First, People Last.* Plymouth: Rowman & Littlefield Publishers.

[8]. Streeter, Michael and Warren, Peter. (2005). *Cyber Alert: How the World is Under Attack from a New Form of Crime.* London: Vision Papperbacks.