Cyber Security and International Law

Khatuna Burkadze*

Abstract

In terms of carrying out cyber attacks and cyber warfare, cyber threats represent one of the main challenges for the international and national securities. Nowadays, it is necessary to examine international legal aspects of cyber security. Therefore, the main goal of the paper is to explore issues related to international regulations of cyber operations in order to ensure security of cyber space and avoid cyber threats. Besides, the article elaborates the definition of the term "cyber-attacks" as well as the types of attacks in cyber space. However, it should be mentioned that the use of force is strictly limited in the international law according to the Charter of the United Nations. This Charter was adopted in 1945 when the creation of cyber space was the matter of future rather than considerations of those times. Consequently, the central question of the paper is the following: Could cyber attack be equated to armed attack according to the international law? Answer to this question can provide insights for defining rules of cyber operations in case of cyber attacks.

Keywords: cyber security, cyber space, cyber attacks, cyber warfare, cyber operations, cyber defense.

Introduction

It is difficult to respond to cyber attacks when it is uncertain who or what has engaged in the attack (Murphy, 2011, p.29). 2015 National Security Strategy of the United States says: "We are shaping global standards for cyber security and building international capacity to disrupt and investigate cyber threats. We are fortifying our critical infrastructure against all hazards, especially cyber espionage and attack. We will defend ourselves, consistent with U.S. and international law, against cyber attacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity. We will assist other countries to develop laws that enable strong action against threats that originate from their infrastructure. Globally, cyber security requires that long-standing norms of international behavior —to include protection of intellectual property, online freedom, and respect for civilian infrastructure—be upheld, and the Internet be managed as a shared responsibility between states and the private sector with civil society and Internet users as key stakeholders" (National Security Strategy of the US, 2015, pp.3-13).

According to the Cyber Security Strategy of Georgia large-scale cyber attacks launched by Russia against Georgia in August 2008 have clearly demonstrated that the national security of Georgia cannot be achieved without ensuring security of its cyberspace. These attacks showed that the protection of cyberspace is as important for national security as land, maritime, and air defenses (Cyber Security Strategy of Georgia, 2012-2015, p.2).

Given the anonymity of the technology involved, attribution of a cyber attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber attack to a specific server in another state, this can be an exceptionally time-consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used these as 'zombies' in conducting attacks (Graham, 2010, p. 92.).

When one state develops a new military technology, other states are threatened. In response, they must take action to enhance their own security. This often results in arms racing, where states find themselves continually developing more and better weapons in order to stay ahead in the competition for relative security. What makes weapons and other military technologies especially threatening is not merely their destructive potential, but that their purpose can be difficult to discern (Rueter, 2011, p.30).

The global community is fast becoming "wired". By the beginning of the next millennium some 100 million individuals enjoy access to the internet. Indeed, over the past decade the number of users has almost doubled annually(Schmitt,1998-1999,p.886).

Traditional arms regimes would likely fail to deter cyber attacks because of the challenges of attribution, which make verification of compliance almost impossible. If there are to be international norms of behavior in cyberspace, they may have to follow a different model (Murphy, 2011, p.29).

Global interconnectedness brought about through information technology gives States and non-State actors a powerful potential weapon. Military defense networks can be remotely disabled or degraded. Flooding an Internet site, server or router with data requests to overwhelm its capacity to function—so-called "denial of service" attacks—can be used to take down major information networks (Waxman,2011,p.45).

In spite of the abovementioned facts currently international community does not have a common strategic view about cyber threats, cyber attacks, cyber warfare and cyber operations. On the one hand, we need consensus concerning the aforesaid issues in terms of creating new information and communication technologies and on the other hand, inter-national and national cyber defense capabilities must

*Associate Professor at the International Black Sea University, Tbilisi, Georgia
E-mail: khburkadze@ibsu.edu.ge

be increased by the international organizations and states.

Cyber Space and Cyber Threats

Contemporary security threats are characterized by, among other things, asymmetry and flexibility. However, in the modern world, security threats transcend the limits of the physical domain, physical security and freedom of the individual and impinge on the economic, intellectual and privacy domain. In addition to activities and relationships in the physical domain of reality, using services available over the global network — the Internet — we communicate, exchange information, perform tasks, have fun and make purchases in a parallel, virtual reality. In the Internet information cloud we leave traces of our activities, traces that connect us to other people, institutions, companies and organizations. By leaving behind this information, we unintentionally reveal more about ourselves than we would have wanted (Djordjijevic, 2011, p.35).

Cyber-based threats are evolving and growing and arise from a wide array of sources. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including hackers, disgruntled employees, foreign nations engaged in espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others (Cyber Security – Threats Impacting the Nation, 2012, p.3).

The nation's critical infrastructure operates in an environment of increasing and dynamic threats, and adversaries are becoming more agile and sophisticated. Terrorists, transnational criminals and intelligence services use various cyber tools that can deny access, degrade the integrity of, intercept, or destroy data and jeopardize the security of the nation's critical infrastructure (Cyber Analy-sis and Warning,2008,p.7).

Cyberspace has become a parallel universe in which the criminal, terrorist and unlawful combatant can operate with a high degree of impunity. Adding to the challenge, the privacy services provided in the form of user anonymity and data encryption make it difficult for law enforcement, intelligence organizations and militaries to attribute actions, whether lawful or not, to specific individuals or state actors (Bret and Wingfield,2011,p.39).

Professor Michael Schmitt noted that cyber threats differ in four ways from traditional threats: (1) computer networks are a new target category, with computer network attacks capable of providing the same results as striking the traditional target with a kinetic weapon; (2) an attack does not have to use kinetic force and can solely involve a command from one computer to the target system; (3) the intended results are often not kinetic and could simply involve the manipulation of data or disruption of a service; and (4) cyber threats are not constrained by political boundaries or geography (Schmitt, 1998-1999, p.888).

As for methods to determine the source of a possible attack — Determining the source of an act within the required time to mount an effective response is often impossible because of such factors as spoofing identities and the lack of bilateral or multilateral agreements for sharing data about the paths that messages take in crossing one or more national borders. Given the way the Internet messaging protocols are designed, this is the norm rather than the exception. However, such factors are not showstoppers in determining culpability. There are many other methodologies that may be used to establish culpability, such as those that take advantage of open source, human and signals intelligence. The impossibility of reliable trace-back does not preclude the use of all other sources and methods to build a clear mosaic of responsibility, possibly after the fact (Bret and Wingfield, 2011, p. 39).

Cyber Attacks and Cyber Warfare

Today telecommunications give fighting forces incredible capabilities to be proactive and adaptive, and to take meaningful response. Today's war fighters expect and demand reliable, fast, interoperable, and protected communications. Telecommunications also enable the acquisition of information concerning the disposition, objectives, and vulnerabilities of the enemy to gain a strategic advantage, creating war fighting disciplines such as Communications Intelligence (COMINT), Electronic Warfare (EW), Electronics Intelligence (ELINT), Foreign Instrumentation Signals Intelligence (FISINT), Imagery Intelligence (IMINT), Open Source Intelligence (OSINT), and Signals Intelligence (SIGINT). High-speed communications cannot occur, however, without computers, and the pervasive use of computers in almost every device inextricably link telecommunications, computers, and the war fighting capability of any modern military force (Tubbs, Luzwick, Sharp,2002,p.8).

Information Operations (IO) and Information Warfare (IW) compose the modern construct that embodies and demonstrates the dependency of modern warfare on telecommunications and computers (Tubbs, Luzwick, Sharp,2002,p.8).

As for the terms which are related to "cyber attack" and “cyber warfare”, the U.S. Department of Defense defines "cyberspace operations" as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace” (Lord, 2009, p.4.).

Definition of the Department of Defense of “computer network attack" (CAN) is "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves” (Brown and Tullos, 2012).

Cyber warfare raises issues of growing national interest and concern. Cyber warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary’s ability to do the same. Some major problems encountered with cyber attacks, in particular, are the difficulty in determining the origin and nature of the attack and in assessing the damage incurred (CRS Report for Congress, Cyber warfare, 2001, p.2).

On balance, cyber warfare may favor nations robust in IT, but the Internet is a prodigious weapon for a weaker party to attack a stronger conventional foe. And Internet-dependent nations have more to lose when the network goes down (Geers, 2011, p. 27).

In the future, the ultimate goal of warfare — victory — will not change. And the advice of Sun Tzu and Clausewitz will still apply. However, the tactics of war are radically different in cyberspace, and if there is a war between major world powers, the first victim of the conflict could be the Internet itself. There will be two broad categories of cyber attacks during a major war: military forces: The attacks would be conducted as part of a broader effort to disable the adversary’s weaponry and to disrupt military command-and-control systems; civilian infrastructure: these would target the adversary’s ability and willingness to wage war for extended periods, and may include an adversary’s financial sector, industry and national morale (Geers, 2011, pp. 26-27).

The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery. A key feature of this approach is that it limits “cyber-attacks” to those hostile acts that are intended to harm critical cyber systems—thus restricting the definition based on the objective of the attack (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue & Spiegel, 2012, p. 824).

Types of Cyber Attacks

The current cyber threat environment is dramatically changing and becoming more challenging with every tick of the clock. Cyber attacks have risen to unprecedented levels of sophistication and frequency. The significant number of viruses, worms and other forms of malware, coupled with the dramatic growth of botnets and the continuous rise in the number of cyber attacks, combine to confirm the significance and severity of the problem (Coleman, 2010).

There are various types of cyber attacks: denial of service, distributed denial of service, exploit tools, logic bombs, phishing, sniffer, Trojan horse, virus, vishing, war driving, worm, zero-day exploit. The growing number of known vulnerabilities increases the potential number of attacks. By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging from defacing web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations’ systems; or destroy systems (Cyber Analysis and Warning, 2008, p.8).

Distributed Denial of Service (“DDOS”) attacks have been the most prevalent form of cyber-attack in recent years. In these attacks, coordinated botnets—collections of thousands of “zombie” computers hijacked by insidious viruses—overwhelm servers by systematically visiting designated websites. The attack in Burma, described above, was a DDOS attack, as was the attack on a Falun Gong website inadvertently aired on China Central Television. There are several other recent examples of such attacks—a few of which we describe here to provide a sense of the varied ways in which such attacks may be carried out (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue & Spiegel, 2012, p.837).

Another form of cyber-attack is a semantic attack, in which the attacker surreptitiously inputs inaccurate information in a computer system. More sophisticated than the DDOS attack, a semantic attack causes the computer system to appear to operate normally, even as it fails (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue & Spiegel, 2012, p.838).

The malware that can attack and hack into these financial systems has a value much like any commodity. A “herder,” or commander, of a botnet makes use of malware to infect and control other computers. Botnets are sold and rented just like any commodity, with prices based on supply and demand. A new industry has therefore emerged as one of the fastest growing sectors in the criminal world. Professional skills are required to hack into a computer and run a botnet (Butrimas, 2011, p.12).

The year 2007 marked a watershed in cyberspace. The Estonian example demonstrates that a cyber attack on a nation’s infrastructure, initially fueled by a grassroots patriotic base, can later attract professional cyber criminals. It’s a potent combination. Targeting and attack information was provided on websites to those who wanted to use their computers to enter the fray. Botnet managers that had used malware to infect unsuspecting computers directed their “zombie” computer armies to “open fire” against listed Estonian banking, government and press sites (Butrimas, 2011, pp.12-13).

Estonian officials are declaring that their country is the first to fall victim to cyber warfare. Prime Minister Ansip and other Estonian public officials alluded to Article V of the NATO Treaty, which states that an attack on one of its members shall be considered an attack against all and enables these nations to exercise the right of self-defense recognized by Article 51 of the Charter of the United Nations. Most EU member states - including Estonia - also belong to NATO (Steven Lee Myers, 2007).

Estonian Defense Minister Jaak Aaviksoo, meanwhile, discussed the situation with NATO officials and later stated the following during an interview with British newspaper the Guardian: "At present, NATO does not define cyber attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defense, will not automatically be extended to the attacked country. Not a single NATO defense minister would define a cyber attack as a clear military action at present. However, this matter needs to be resolved in the near future" (Steven Lee Myers, 2007).

Large-scale cyber attacks launched by Russia against Georgia in August 2008 have clearly demonstrated that the national security of Georgia cannot be achieved without ensuring security of its cyberspace. In the course of the Russian-Georgian war, Russian Federation engaged in targeted and massive cyber attacks against Georgia alongside land, aerial and naval assault. These attacks showed that the protection of cyberspace is as important for national security as land, maritime, and air defenses. According to Internet technical experts, it was the first time a known cyber attack had coincided with a shooting war (Markoff,2008).

A growing strand of cyber scholarship suggests the Estonian and Georgian incidents are harbingers of future cyber conflict. Within a broader spectrum of cyber attack, strategists highlight low-intensity cyber warfare as an increasingly prevalent and threatening form of conflict (Watts,2011,p.72.).

Cyber Security and Its Activities

Attacks resulting in the incapacitation or destruction of the nation's critical infrastructures could have a debilitating impact on national and economic security and on public health and safety. To protect the nation's critical computer-dependent infrastructures against cyber threats and attacks, law and policy have identified the need to enhance cyber security and establish cyber analytical capabilities (Cyber Analysis and Warning, 2008, p.10).

As cyber security expert Paul Kurtz notes: "You can have a small piece of code that can do a whole of a lot of damage or just a little bit of damage depending on how you choose to use it." The most important weapons of cyber war are the "cyber warriors" that conduct it. But it can be equally difficult to identify a cyber warrior. Many militaries have officially-designated cyber warfare units, yet responsibility for both cyber offense and cyber defense can easily be spread throughout various security and intelligence agencies, and even into the private sector. Even when cyber warriors are recognizable, it is nearly impossible to distinguish between their offensive and defensive intentions and abilities. This is because the same knowledge and tools that cyber warriors use to defend against attacks, such as firewalls and intrusion detection programs, can be used to circumvent those same protections (Rueter, 2011, p.42).

According to the 2015 Cyber Strategy of the United States Department of Defense, DoD sets five strategic goals for its cyberspace missions: build and maintain ready forces and capabilities to conduct cyberspace operations; defend the DoD information network, secure DoD data and mitigate risks to DoD missions; be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber attacks of significant consequence; build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages; build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability (Cyber Strategy of the United States Department of Defense, 2015, pp.7-8).

Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior. As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyber attacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. The deterrence of state and non-state groups in cyberspace will thus require the focused attention of multiple U.S. government departments and agencies. The Department of Defense has a number of specific roles to play in this equation (Cyber Strategy of the United States Department of Defense, 2015, p.10).

According to the 2014-2017 Cyber Security Strategy of Estonia, the main cyber security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Estonian state, the economy and the population. Therefore, the key fields on which the Cyber Security Strategy focuses are ensuring vital services, combating cybercrime more effectively and advancing national defense capabilities. Additional supporting activities will include: shaping the legal framework, promoting international cooperation and communication, raising awareness, and ensuring specialist education as well as the development of technical solutions (Cyber Security Strategy of Estonia, 2014, p. 6).

As for Georgia, the Georgian Cyber Security Strategy is a principal document outlining state policy in the area of cyber-security, reflecting strategic goals and guiding principles, and laying down action plans and tasks. Based on this Strategy, the Government of Georgia undertakes actions facilitating safe operation of state agencies, private sector and the public in cyberspace, secure electronic transactions and unhindered functioning of Georgian economy and business (Cyber Security Strategy of Georgia, 2012-2015, p.2).

Conclusion

International community will have to achieve consensus about governing cyber attacks, cyber warfare and cyber operations. These issues are significant for the national security of states, especially, in terms of developing new information and communication technologies which can increase cyber risks as well.

Based on the cases of cyber-attacks including the Estonian and Georgian cases, the protection of cyber space is a part of defense and security policy. In order to implement an effective cyber policy for avoiding cyber threats, it is important to enhance cyber defense capabilities and carry out cyber security activities. In parallel, states need cooperation on the aforesaid issues in the framework of international organizations.

In this context, the contribution of the North Atlantic Alliance is significant because NATO approved its first cyber defense policy in January 2008 following the cyber attacks against Estonia. The North Atlantic Alliance is responsible for the protection of its own communication networks. NATO promotes cyber education and ensures cyber security activities. Nations are and remain responsible for the security of their communication networks which need to be compatible with NATO's and with each other's. (Cyber Security, 2015). In spite of the foregoing, the following questionable and problematic issue should be outlined: Could the Alliance define cyber attack as a clear military action for using Article 5 of the North Atlantic Treaty?

NATO recently enhanced cyber defense capabilities. However, in order to use collective or individual defense operations against online warfare, it is necessary to achieve agreement regarding new interpretation of armed attack under Article 51 of the United Nations Charter for the international recognition of existing attacks in cyber space and promoting timely effective cyber security measures.

References

Bret M. & Wingfield T. (2011). International Legal Reform Could Make States Liable for Cyber Abuse. per Concordiam, Journal of European Security and Defense Issues, Volume 2, Issue 2, retrieved October 15,2015,from:http://www.marshallcenter.orgmcpublic-web/MCDocs/files/College/F_Publications/perConcordiam/pC_V2N2_en.pdf, p. 39

Brown G. and Tullos O. (2012). On the Spectrum of Cyberspace Operations. retrieved October 10, 2015, from: http://smallwarsjournal.com/print/13595

Butrimas V. (2011). An Unsettling Trend. per Concordiam, Journal of European Security and Defense Issues, Volume 2, Issue 2, retrieved October 2, 2015, from: http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V2N2_en.pdf, pp.12-13.

Murphy J. F. (2011). Mission Impossible? International Law and the Changing Character of War. International Law Studies, Volume 87, Editors: Raul A. “Pete” Pedrozo and Daria P. Wollschlaeger, p.29.

National Security Strategy of the United States. (2015). retrieved October 10, 2015, from: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf, pp.3-13.

Cyber Security Strategy of Georgia. (2012-2015). retrieved October 10, 2015, from: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Georgia_2012_National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf, p.2.

Graham D. (2010). Cyber Threats and the Law of War. Journal of National Security Law & Policy, Vol. 4, p. 92.

Rueter N. (2011). The Cyber Security Dilemma. Duke University, p.30.

Schmitt M. (1998-1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, Volume 37, pp.886-888.

Waxman M. (2011). Cyber Attacks as “Force” Under UN Charter 2 (4). International Law Studies, Volume 87, Editors: Raul A. “Pete” Pedrozo and Daria P. Wollschlaeger, p.45.

Djordjijevic N. (2011). Defending Cyberspace. per Concordiam, Journal of European Security and Defense Issues, Volume 2, Issue 2, retrieved October 15, 2015, from: http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V2N2_en.pdf, p.35

Cyber Security – Threats Impacting the Nation, GAO (Government Accountability Office of the US) -12-T, April, 2012, p.3

Cyber Analysis and Warning, GAO (Government Accountability Office of the US) - 08, July 2008, pp.7-8

Tubbs D., Luzwick P., Sharp W. G. (2002). Technology and Law: The Evolution of Digital Warfare. International Law Studies, Volume 76, Editors: Schmitt Michael and O’Donnell Brian, p.8.

Lord W.T. (2009). Cyberspace Operations: Air Force Space Command Takes the Lead. High Frontier, The Journal for Space & Missile Professionals, Volume 5, p.4.

CRS (Congressional Research Service) Report for Congress, Cyber warfare, 2001, p.2.

Geers K. (2011). Heading off Hackers. per Concordiam, Journal of European Security and Defense Issues, Volume 2, Issue 2, retrieved October 2, 2015, from: http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V2N2_en.pdf , pp.26- 27.

Coleman K. (2010). Cyber threats worsen every second, stronger measures necessary to address more frequent and sophisticated attacks. retrieved October 2, 2015, from: http://www.defensesystems.com/Articles/2010/04/26/Digital-Conflict-Cyber-Defense.aspx

Lee Myers Steven, Estonia Accuses Russia of Computer Attacks, New York Times, May 18, 2007, retrieved November 24, 2015, from: http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?h

Markoff J. Before the Gunfire Cyber attacks, New York Times, August 12, 2008, retrieved October 10, 2015, from: http://www.nytimes.co Hathaway O., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W. & Spiegel J. (2012). The Law of Cyber Attack. California Law Review, p. 824. m/2008/08/13/technology/13cyber.html?_r=1&em

Watts S. (2011). Low-Intensity Computer Network Attack and Self-Defense. International Law Studies, Volume 87, Editors: Raul A. “Pete” Pedrozo and Daria P. Wollschlaeger,p.72.

Cyber Strategy of the United States Department of Defense.(2015).pp.7-10.

Cyber Security Strategy of Estonia. (2014). p. 6.