საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა ქვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

11

THE GLOBAL CYBER DOMAIN AND NEW CHALLENGES

KHATUNA MSHVIDOBADZE

EXPERT OPINION

2013

GFSIS საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

KHATUNA MSHVIDOBADZE

THE GLOBAL CYBER DOMAIN AND NEW CHALLENGES

11

2013

The publication is made possible with the support of the US Embassy in Georgia.

Editor: Jeffrey Morski

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN 978-9941-0-2681-2

Introduction

The rapid growth of dependence on information technology and its increasing development has given rise to a global system of systems. Within the information space, the inter-dependent communication networks, computer systems and existing databases of the Internet infrastructure allowed for the creation of a new global cyber domain which, along with numerous advantages, has led to new threats.

It is rather difficult to pinpoint the exact date of the invention of the Internet, although the idea of a packet-switched network (a digital inter-network communication method that groups all transmitted data irrespective of content, structure and type into suitably sized blocks) originated in the early 1960s when the then-United States Advanced Research Projects Agency (ARPA), later the Defense Advanced Research Projects Agency (DARPA), made significant advances in the development of computer networks that could be linked together through what would become the Internet. The demonstration of the implementation of this idea dates to October 29, 1969 when a post-graduate student programmer at UCLA, Charles S. Kline, transmitted the first Internet message, "login." ARPANET then connected just two computers at the University of California, Los Angeles (UCLA) and Stanford University. Today, there are approximately 2.5 billion Internet users.[1]

At the time, it was difficult to imagine that just four decades later, the global packet inter-connection network would become a significant challenge for security. The history of the creation of ARPANET rests on the establishment of the Lincoln Laboratory at the Massachusetts Institute of Technology (MIT) in 1951 and the conception of the Intergalactic Computer Network introduced by the American computer scientist, Joseph Carl Robnett Licklider.[2] Licklider's "Galactic Network" concept defined a new type of social interaction, achievable via a global computer communication system, in which access to data and information was available to the general public. Even then, his conception represented the notion of today's Internet.

The adoption of the term *Internet* itself dates back to 1974 when the term was first used in Vinton Cerf, Yogen Dalal and Carl Sunshine's publication (RFC 675), *Specification of Internet Transmission Control Program*. The names of American computer scientists, Vinton Cerf and Robert Kahn, are associated with the creation of networking Transmission Control Protocol

and Internet Protocol (TCP/IP) computer communication protocol suite and the first commercial system for an electronic mail system.

It is difficult to compare new discoveries and the technological advances made by humans over thousands of years. Nonetheless, it is at least safe to say that none of the technological advances heretofore have made such an impact on humanity so rapidly and in such a large scale as this technological achievement has.

Internet technology has greatly influenced the broad masses of the world in several areas. The original purpose of its creation was scientific advancement and research. Therefore, the security of this immense system of systems became a critical challenge only at a later stage. The emergence of a new information space has also somewhat contributed to a unified perception of the world: a space where political boundaries do not exist.

New Challenges

In 2010, only a few decades after the creation of a new virtual dimension, the authors of the recommendations on the new strategic concept of the North Atlantic Treaty Alliance (NATO) wrote: "The next significant attack on the Alliance may well come down a fibre optic cable;" in other words; the Internet.[3] The new strategic concept for NATO also highlights the following circumstance: "Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."[4] Given the current reality, a question arises: has our own technology brought us into a dead end in terms of security?

Today, certain states, and especially developed countries, are faced with new, more difficult threats. Cyber spies, cyber soldiers, cyber terrorists and groups supporting one force or ideology or another have found their place in the virtual world.

Cyber threats endanger not only technologically advanced countries but less developed states as well. Potential target countries take cyber security very seriously. These countries elaborate cyber policy in accordance with their cultural, social, economic, geographic and political circumstances. They seek effective ways, create and amend strategic documents, tactics and approaches.

Cyber crimes against individuals, businesses and governments are an everyday occurrence. Cyber warfare already poses a threat with national security analysts looking for more effective, consistent strategies and international agreements aimed at counteracting.

Cyber attacks may be equivalent to special operations and aerial attacks. In contrast with the financial and human resources necessary for the training and equipment of special forces or air forces, hackers, computers, botnets or the development of other types of cyber and information weapons require much less time and money. This could potentially endanger a country's critical infrastructure, economy and the psychological state of the population. The employment of cyber weapons against opponents is much cheaper than military and political intervention. "You could fund an entire cyber warfare campaign for the cost of replacing a tank tread, so you would be foolish not to," stated Bill Woodcock, the Founder and Research Director of Packet Clearing House, a non-profit research institute.[5] With minimum expenses, cyber criminal groups and countries can destabilize the economy and critical infrastructure of a target country. To this day, experts argue regarding the way cyber attacks should be defined – as a criminal act or as an act of war.

With the existence of the Internet, active individuals equipped with computer skills frequently develop into well-trained "hacktivists," hacker-terrorists and hacker-warriors. In addition, these individuals are scattered throughout the world.

It should also be noted that cyber threats pose a danger not only to open systems but closed systems as well. Closed systems are networks that are not directly connected to the Internet, but are, nonetheless, vulnerable, as illustrated by the examples of Stuxnet and Wikileaks. Stuxnet was a computer worm that destroyed a thousand centrifuges at the Nanantz nuclear enrichment lab in Iran. Wikileaks is an organization that placed the United States' national security in grave danger by publishing tens of thousands of highly classified US state documents provided to it by the former US Army Private Bradley Manning. The Internet is not the only way to access computer systems; although it is a broad and open road.

The information space has also contributed to the establishment of a rebellious Internet generation. The active employment of this space brought about social mobilization in various countries. As with crime and war, political activism and debates relocated to cyberspace and the social media.

The latter gave impetus to mass protests in the Arab countries. The active use of cyberspace made feasible the public mobilization in Russia on December 10, 2011, when tens of thousands of people protested the results of the parliamentary elections.

Interestingly, this sort of activity already has a two-decade history. The first large-scale employment of the Internet in a conflict situation took place during the Chechen wars. The Chechens managed to use cyberspace so effectively that afterward, then-Prime Minister of Russia, Vladimir Putin, stated: "We surrendered this terrain some time ago ... but now we are entering the game again."[6] The Chechens managed to communicate successfully with influential Western journalists and supply them with relevant information. They conveyed the information before the Russian propaganda machine disseminated its own version. The Chechens became particularly adept at the distribution of images depicting acts of violence committed by the Russian troops. The Russian side publicly denied the existence of these facts. Chechen separatists even managed to raise funds deposited by their supporters in their bank account in California.[7]

Subsequently, Internet use became a so-called "rule" in almost all types of conflict. The engagement of non-conventional forces in conflicts drew mixed reactions and reflections worldwide. A new trend of wide Internet use and connectivity has been established although the public has yet to see the maximum potential of cyberspace during conflicts. Internet use during hostilities is a modern method that frequently engages ordinary citizens as well as warriors fully or partially armed with cyber weapons. This development renders three types of effects: first, various groups that do not act on behalf of the state; second, government forces utilizing new strategies for action or forming and employing cyber militant groups; third, the development of a new type of fighter called individual cyber warriors. Some countries are not only tolerant toward cyber criminal groups but also hire them against target countries. For instance, the Russian Business Network (RBN) is seen as the principal actor in the cyber attacks carried out against Georgia in 2008. Soon thereafter, Stephen Spoonamore of Global Strategic Partners told *InternetNews.com* that RBN was and perhaps still remains a group of cyber criminals that maintains close ties with the Russian government.[8]

For revisionist countries, such as Russia and China, cyber espionage presents the principal means of obtaining economic, military and technologi-

cal advantages over status-quo countries, mainly the United States. Meanwhile, within the country, information control, cyber repression and undemocratic legislative initiatives serve as substantial leverage for maintaining social and political order. Sub-national groups, such as al-Qaeda and Anonymous, also sometimes act as revisionist forces. Regardless of radical disparities among them, these revisionist states and sub-national groups share one common standpoint – undermining the dominant positions of the United States and its allies. In the modern era, in the international political arena, cyber power will be one of the preconditions defining this dominant role. Cyber technology is seen by Russia and China as a crucial means to achieve revisionist objectives. Al-Qaeda uses this technology for research purposes, information storage and communication. Anonymous uses to cyber attacks to express contradictory ideological attitudes.

Numerous cyber weapons of various types directed against individuals, governments and organizations are being developed on a daily basis. Currently, the international community, or at least a part of it, is seeking effective ways to combat cyber attacks, to identify the most effective technical, legal and political strategies against this threat and where to draw the line between crime and war.

Georgia in Cyberspace

In some countries almost everything is connected to the Internet. Although a country like Georgia may not be as connected as, for instance, Germany, France, the United States and other developed countries, this offers little comfort. Georgia is a part of this global system and its crucial infrastructure is largely dependent on the Internet. The information space reaches beyond established national boundaries at the speed of light, although the standards are set by technological leaders.

For instance, security standards, with which Georgian banks must comply, have clearly not been defined by them but by the large banks in Frankfurt, London and New York. It is significant to note the decisions taken by international banks with regard to Georgian banks during the cyber attacks carried out against the country in 2008. Kenneth Corbin writes on *InternetNews.com*: "The attackers struck hard at Georgia's banking system, overwhelming financial sites with so many fraudulent transaction attempts that it became impossible to tell the good from the bad. Sensing that the system was under siege, international banks shut down service. As

a result of the spillover effect, several days passed without a single transaction being processed inside Georgia."[9] By the same principle, the Tbilisi International Airport must comply with the standards established by the International Air Transport Association (IATA).

Given the global systems and in accordance with international standards established in this regard, for instance, for the security purposes of banking and air systems, countries are obliged to take appropriate measures in accordance with established cyber security norms.

Many other significant processes are managed via Industrial Control Systems (ICS), many of which are connected to the Internet. ICS expert, Joseph Weiss, writes: "[Industrial] control systems are the backbone and mission critical components of global industrial infrastructures such as electric power, oil and gas, chemical, pharmaceutical, water, metal refining, auto manufacturing, transportation,"[10] and many other systems to the extent that any vital process that is controlled by such a system connected to the Internet is vulnerable to cyber attacks.

Part Three of the Threat Assessment Document of Georgia, published in September 2010, which expounds on transnational threats, also highlights the dangers from cyber attacks. The document states, "During the August 2008 war the Russian Federation in parallel with land, air and sea attacks carried out [a] concentrated and massive cyber assault on Georgia," which demonstrated that "the use of computer technologies to carry out cyber attacks represents a real threat in the globalized world."[11]

Russia's cyber attack in 2008, which was executed on a par with kinetic warfare, gave impetus to the Georgian government to take certain steps toward cyber defense. In 2008, Russia carried out attacks using both Soviet-era tanks and 21st century fiber optic cables. Cyber attacks deactivated the government's information and communication channels, news portals, financial transactions and Internet connections. Attacks carried out in cyberspace accomplished some missions previously conducted by aviation and artillery. Following the bitter experiences of 2008, the Georgian government took a number of successive steps in terms of Georgia's cyberspace security. The Law on Information Security entered into force, defining information security standards for private and public organizations. In 2010, the Data Exchange Agency was established under the Ministry of Justice whose main objective is the development of e-governance, the establishment of data exchange infrastructure and the formation of a unified

government network in Georgia. The Agency is also authorized to develop information and communication standards in the public sector and establish and implement information security policy.[12]

Under the auspices of the Data Exchange Agency, the Computer Emergency Response Team (CERT) was established. The team operates seven days a week, 24 hours a day. As stated on the official web page of the team, the CERT is authorized to implement the monitoring of Georgian cyberspace and respond to crucial computer incidents observed in the government network and critical infrastructure.[13] Before and during the war of August 2008, the bulk of Georgia's Internet traffic passed through Russia while following the August events, the new Poti-Varna fiber-optic line "Caucasus" carries approximately 90% of Internet traffic.

On May 17, 2013, the president of Georgia signed a document detailing the Cyber Security Strategy and the Cyber Security Action Plan of Georgia. The document calls for the coordinated work of state agencies and the development of collaboration mechanisms between state and private sectors. Moreover, the document stresses the need for international cooperation and the establishment of educational resources. The Action Plan is envisioned until the year 2015.[14]

Recently, the Georgian CERT gained international recognition for the discovery of and rapid response to the Win32/Georbot Trojan virus created for espionage purposes against Georgia. The virus was characterized with a high penetration ability into computer systems and was able illegally to access all types of documents, conduct video and audio recordings via personal computers, independent of their users, as well as to transmit information from a user's desktop to the bot's control computer. The Trojan targeted state and critical infrastructure computer networks. In addition, in certain cases, computers in the banking sector, non-governmental organizations and private companies were also infected.[15]

Georbot aimed to uncover and steal documents using security-associated terms and subsequently transmit these data to the control server. The Georgian CERT created and infected false documents in order to mislead the assailant, thus identifying the attacker. Using reverse engineering, the Georgian CERT gained full access to the command and control servers, deciphered communications mechanisms and analyzed the virus files. Based on the information obtained, it became possible to identify individuals and organizations involved. Further investigations revealed traces of Russian hackers and Russian government organizations.[16]

In the international arena, on June 6, 2012, Georgia ratified the Council of Europe Convention on Cyber Crime. Although Georgia signed the Convention in 2008, due to the fact that the Treaty calls for not only international cooperation for the purposes of conducting cyber investigations but also for the harmonization of the Georgian legislation with the norms established by the Convention, there was a four-year delay. The adoption of the Law on Information Security accelerated the ratification of the Convention by Georgia. The Convention entered into force for Georgia on October 1, 2012.[17]

Clearly, since 2008, Georgia has taken significant steps in enhancing cyber security although the fight against this crucial problem calls for the implementation of a deliberate, consistent cyber policy prioritized at the state level. In order to combat this problem effectively, relevant measures must be taken within the country – government computer networks must be equipped with genuine software, government computers must feature appropriate security systems and government officials must be familiarized with the elementary rules of cyber security. It is essential to enhance cooperation among government and business organizations, widely implement educational programs and raise public awareness. It is vital to establish a sensor system for the prevention of advanced attacks and to develop a large-scale cyber counter-intelligence plan and self-defense strategies. In this regard, inter-agency coordination and communication is a priority. It is essential that the legislative framework within the country not only be developed but also enforced. Coping with this problem also requires close international cooperation.

Conclusion

The original purpose of the creation of the Internet did not take into account the development of security measures. The invention of the Internet was motivated by the need to provide a more favorable environment for scientific activity. However, today, the security of computer networks requires constant provision and implementation of new safety measures.

The creators of the Internet would have never fathomed that the increasing development of web-technology would give rise to such a large-scale system of systems whose security would become such a significant challenge. Within this hard-to-control environment, along with the numerous advantages, new challenges have emerged. People and money have trans-

ferred to the cyber world. Accordingly, crime, espionage, terrorism and war have all found their place in this new area.

This vast technology has increased the dependence of governments, businesses and individuals on the Internet and the computerization of almost everything. The cyber reality has generated new challenges, not only technical, but also political and legal.

To some extent, all countries are becoming increasingly dependent on the Internet and they benefit from it and may also become victims of its misuse. No country, regardless of its size or resources, will be able to neglect information technology. For instance, in contrast to 2008, Georgia's dependence on Internet technology has considerably increased, which has enhanced not only the significance of its cyberspace security but also its share and responsibility in terms of ensuring the security of the global cyberspace.

References

1 *Internet World Stats*, "Usage and Population Statistics." Undated. Retrieved from www.internetworldstats.com/stats.htm on August 10, 2013

2 Leiner, Barry, Vincent Cerf, et.al., *A Brief History of the Internet,* The Internet Society, undated. Retrieved from www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet on August 8, 2013

3 North Atlantic Treaty Organization, *NATO 2020: Assured Security; Dynamic Engagement, Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO,* Brussels, 17 May 2010, p. 45. Retrieved from www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf on August 7, 2013

4 NATO, *Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon,* November 19, 2010. Retrieved from www.nato.int/cps/en/natolive/official_texts_68580.htm on August 10, 2013

5 John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008. Retrieved from www.nytimes.com/2008/08/13/technology/13cyber.html on August 4, 2013

6 Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," *SC Magazine,* August 27, 2008. Retreived from www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ on August 5, 2013

7 *Ibid*. Retrieved from www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ on August 8, 2013

8 Kenneth Corbin, "Lessons From the Russia-Georgia Cyberwar," *Internetnews.com*, March 12, 2009. Retrieved from www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm on August 10, 2013

9 *Ibid.*. Retrieved from www.internetnews.com/government/article.php/3810011/Lessons+From+the+RussiaGeorgia+Cyberwar.htm on August 4, 2013

10 Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats.* New York: Momentum Press, 2010

11 Alexander Melikishvili, "Georgia's New Threat Assessment Document identifies Russia as a Main Threat," *Eurasia Daily Monitor,* October 25, 2010. Retrieved from www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=37077&tx_ttnews%5BbackPid%5D=27&cHash=3ebccbc084, on August 10, 2013

12 *Data Exchange Agency.* Retrieved from www.dea.gov.ge/?action=page&p_id=5&lang=geo on August 5, 2013

13 *Data Exchange Agency, CERT.GOV.GE*. Retrieved from www.dea.gov.ge/?action=page&p_id=120&lang=eng on August 5, 2013

14 Decree of the President of Georgia On the Cyber Security Strategy of Georgia and the Approval of the 2013-2015 Action Plan on the Implementation of the Cyber Security Strategy of Georgia. May 17, 2013. Retrieved from www.nsc.gov.ge/files/files/legislations/kanonqvemdebare%20normatiuli%20aqtebi/cyber%20security%2017%20may.pdf on August 10, 2013

15 Data Exchange Agency, "Cyber Espionage against Georgia" October 24, 2012. Retrieved from http://dea.gov.ge/uploads/CERT%20DOCS/CERT.GOV.GE.pdf and attached PDF file on August 5, 2013

16 *Ibid.*

17 Council of Europe, Treaty Office, *Convention on Cybercrime,* undated. Retrieved from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG on August 10, 2013