Transactions on Machine
Learning and Data Mining
Vol. 13, No. 1 (2020) 43 - 59

P-ISSN: 1865-6781, E-ISSN 2509-9337
ISBN 978-3-942952-78-1

ibai Publishing
www.ibai-publishing.org

COVID-19 & Cyber Security Challenges US, Canada & Korea

Eduard Babulak[1], James Hyatt[2], Kim Kyu Seok[3] and Jang Sun Ju[3]

[1] Liberty University, Lynchburg, VA 24502, USA
[2] Fort Hays State University, Hays, KS 67601, USA
[3]Sungkyunkwan University, Suwon, South Korea
babulak@ieee.org
hyattphd08@gmail.com
tuffever@naver.com
wkd4861@gmail.com

Abstract. Globalization and ubiquitous Internet have made significant contribution to mankind while bringing business, education and health closer to every home on the planet. However, in the process of dynamic development and innovation to the Information Communication Technologies (ICT) and Internet, in conjunction with the fast developments in Computing Industry and Artificial Intelligence, the Cyber Security has become of critical importance to governments, businesses, industries, health and academia worldwide. Given current spread of COVID-19 with its impact on economies, business, industries, health and nations security in US, Canada and South Korea the importance of Cyber Security has become paramount. Millions of people lost their jobs, many people died, many are seriously ill, and the morale is quite low worldwide. It is in time like these that criminals and outlaws are exploiting any possible vulnerability that could give an opportunity for effective cyber-attack(s). The principal author, lived, worked and studied in South Korea, Canada and US, working with co-authors in times of earlier and current Cyber Security related issues in South Korea, Canada and US. Past twenty years may have brought most valuable and fascinating technologies to mankind worldwide, but at the same time the global mobility, seamless connectivity and free sharing of information and goods among the nations worldwide also promoted new dimension of computational challenges, such as cyber security.

Keywords: Cybersecurity, Cyber-attacks, Threats, Cyberwar, Cyber-economy, Cyber-culture, South Korea, USA, Canada.

1 Introduction

The use of Internet today, has become essential for most of the people and somehow contributes to a make life more convenient with easy access and sharing of information at any time, from anywhere with anyone. In some way Internet brought positive as well as negative impacts.

Given the ubiquitous connectivity and easy access to Internet, number of financial, government and industrial organizations were subject to security attack(s) from various sources. These events have made big impact on cyber security awareness not only for the industrial, business, and government organizations.

With the integration of more distributed or aggregated renewables and the wide utilization of power electronic devices, the smart micro grid is facing new stability and security challenges [1-2]. Cyberspace is often understood as everything related to Internet and computer communications infrastructures. Given the current statistics the Cyber security issues are becoming very critical to any organization worldwide [3-4]. The paper discusses cyber security issues in the Republic of Korea, US and Canada. These three countries in particular, have put lot emphasis on developing proper strategies and policies on how to prevent and avoid any possible cyber-attack(s) and its negative impact on nation's security and its economic wealth.

The National Cyber Security System (NCSS) of South Korea came under criticism when North Korean cyber-terrorists attacked the office computers and servers of major South Korean broadcasting and financial companies on March 20, 2013. The NCSS had evolved up to that time by addressing problems that arose from incidents dating to the January 25, 2003 Internet crisis, the March 4, 2011 distributed denial of service (DDoS) crisis, and other events occurring between those attacks. The above 2013 cyber-terrorism incident magnified the limits of NCSS leadership, expertise, and collaborative systems, while revealing that past reforms were nothing more than stopgap measures [5].

The paper is organized as follow. Section one presents an introduction, section two introduces cyber security and digital identity with subsection on Cyber Security and second on Digital Identity. Section three describes cyber security issues in South Korea, with subsection presenting an example of Phishing Attacks in South Korea. The fourth section discusses the situation in Canada and US. The section five presents conclusions.

2 Cyber Security and Digital Identity

Our Third Millennium is the era of ubiquitous access 24/7 to digital information via fast Internet, Artificial Intelligence, Humanoid Robotics and Smart Computational Cyberspace. Given the complexity and seamless connectivity among billions of computational devices worldwide, the cyber security and digital identity have become a common household name. This section provides an overview of cyber security and digital identity.

2.1 Cyber Security

The cyber security today has become the essential to any business, government or organization worldwide. Cyber threats can be divided into three categories: cyber-crimes, cyber security, and cyber warfare. [8]

Over the past decade, there has been incredible R&D on cyber security technologies by U.S. government which includes NSF, DARPA, Navy, and the Arm Forces. However, current technology is not sufficient enough to protect the vital infrastructure. The main reason for this deficiency is the lack of severe systematic methodologies for developing and examining the next generation on cyber security as well as lack of experimental infrastructure.

Until now, new security technologies have only been examined and validated in small scale private research facilities, which is not so quite representative of large operational networks or of the portion of the Internet that could be opened to an attack.

In order to make rapid progress of improvement in defense against attack, the state of the art security mechanisms must be enhanced. This requires development of large scale security test beds containing new frameworks and standards for validating that these test beds are trustworthy and useful. According to [6], current deficiencies and impediments to evaluating network security mechanism lack of scientific rigor, lack of representative network data [7]. Main challenging parts of these actions are the complexity of interaction among infrastructure such as protocol types, topology methods and the network traffic.

2.2 Digital Identity

Figure 1, without authentication no user can be provided of service in which in our cyber space, this security mechanism level of requirement become higher each day. Every not sophisticated password or group of secure mechanism can be broken eventually.

The Figure 2, illustrates the Trust Framework with its basic components. Cross sector digital identity project was one of the major huge projects in Microsoft in 2011. The goal of the project was to bring together private and public participants to demonstrate within POCs (Proof of Concepts), key NSTIC concepts and to identify barriers to adoption across variety of domains.

Figure 2 illustrates general motivation behind the cyber-attacks. The US Cyber Emergency Response Team (CERT) contributes to education of young generation to be aware of the use of personal computers with regards to cyber security. The new generations of cyber-attacks are somehow ahead of existing security technology solutions implemented today.

Most IT/Security professionals are well aware of the growing sophistication of cyber threats and the types of attackers they face. Nearly two-thirds of those surveyed feel their companies will be targeted by a cyber-attack in the next six months. Professionals working in larger organizations (more than 500 employees) are significantly more concerned than those in companies of 100- 500 workers.

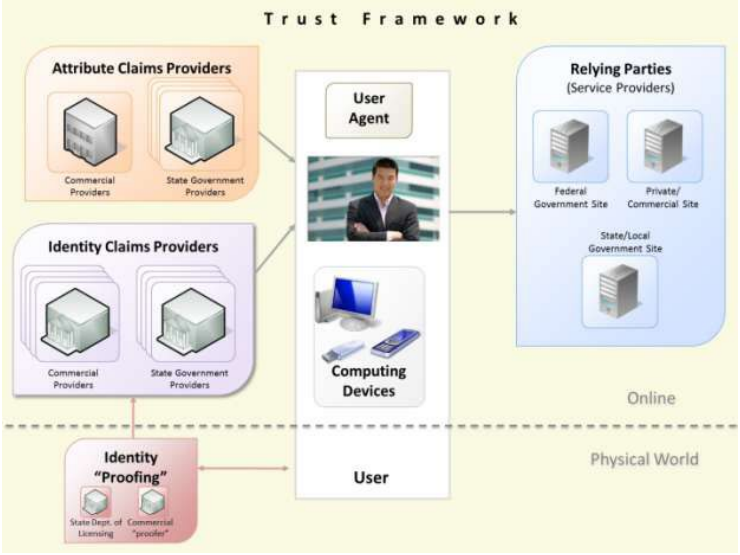


Fig. 1. Cross-Sector Digital Identity Project [10]

Over half of the respondents in every market segment surveyed, feel they will be targeted by a cyber-attack in the next six months, though there were some significant differences in a few key segments. Perhaps understandably, government security professionals feel they are most likely to be attacked (74%) compared to a significantly smaller percentage (though still a majority) of respondents in the retail industry (55%). This is consistent with a 2010 study conducted by the Ponemon Institute [8-10]. The Ponemon Institute study found that "83 percent of respondents believe their organization has been the target of an advanced threat; 71 percent believe they have seen an increase in advanced threats over the past 12 months."

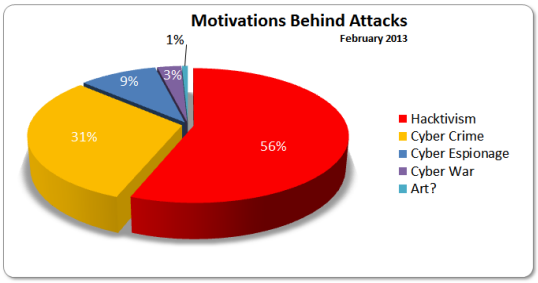


Fig. 2. Motivation of hackers [2]

Two-thirds of the study participants believe the increase in cyber-attacks is neither due to "media hype" nor perceived weaknesses in their defenses, but rather the result of a growing number of hackers, as well as better organized criminal groups and nation state perpetrators. 61% of respondents feel that they are most likely to be attacked by

Anonymous and/or other hacktivists, for example, those behind such public attacks as those on HBGary Federal, Sony and the Stratfor security consultancy. These attacks can do tremendous damage to the companies' brand and bottom line. Overall, respondents feel that threats from organized crime, foreign nations and cybercriminals, are a greater threat than disgruntled employees and corporate competitors.

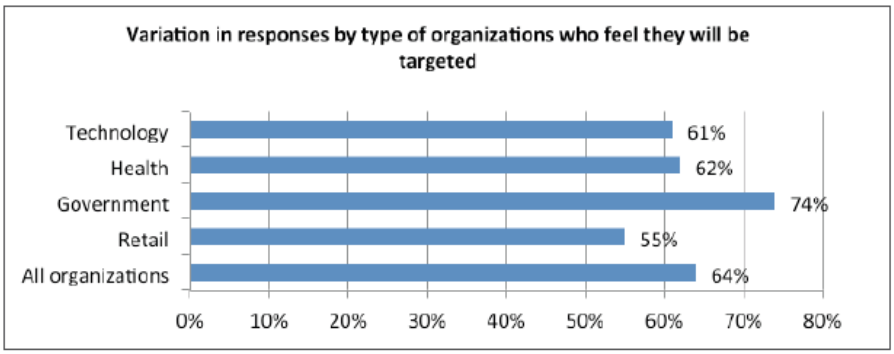


Fig. 3. Organization's Response to Cyber Attacks [23]

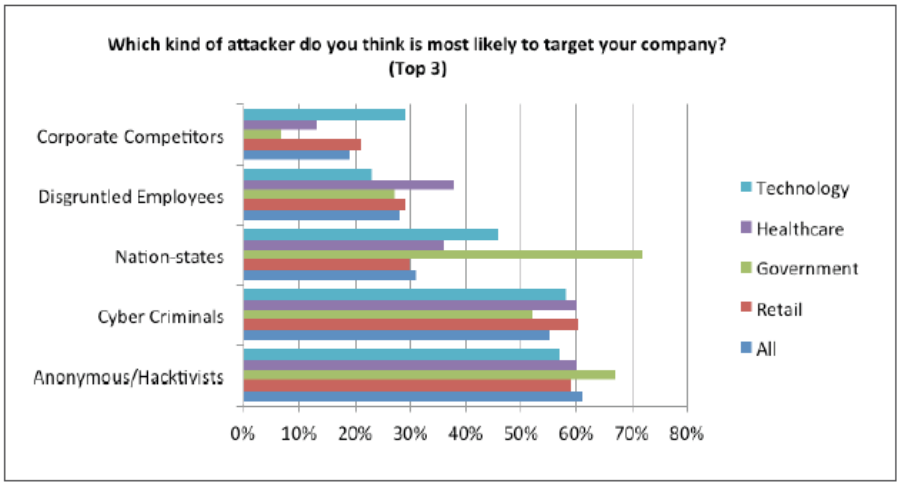


Fig. 4. Industry Cyber Attackers Categories [24]

The IT and security professionals are not confident that their current cyber security is highly effective at protecting their most important and most vulnerable machines. Overemphasizing security can restrict freedom and stifle entrepreneurial potential. Conversely, liberty in cyberspace without an appreciation of cyber security presents rising commercial and governmental costs as well as unacceptable threats to national security [6].

As shown in the table, South Korea still have not reached level compared to US and Canada. With US generous support, the South Korea experienced very dynamic and successful economic growth and has become one of the major player on the world martket stage. South Korean complanies like Samsung, Hunday, LG and others have rich the market in most of the countries worldwide. Korean Telecomm have been on eof the driving forces in developing 3, 4, and 5 G Communication Networks Infrastructures in South Korea and worldwide.

Table 1. Comparison of Cyber Security Policies.

REGION	SOUTH KOREA	USA & Canada
Recognizes Awareness as a Problem	Yes	Yes
Specifies Target Population	No	Yes
Specifies Types of Cyber Security Threads	No	Yes
Provides Suggestions for Defense Against the Attacks	No	Yes
Provides for Voluntary Compliance	Yes	Yes
Action Emphasis for Cyber Security is on Policy Maker	No	No
Seek Uniformity of Criminal Sanctions	No	Yes

3 Cyber Security status in South Korea

South Korea has one of the most advanced technology in mobile and wireless communication system in the world. As the numbers of cyber-threats increasing, the South Korea is reinforcing its cybersecurity infrastructure [6-8]. Most importantly, the government and corporations are facing unexpected attacks to their systems. South Korea is attempting to enhance its cyber combat capabilities as North Korea continues to pose a growing security attack with its advanced electronic warfare technology and skills.

South Korea has one of the highest speed network systems had many industrial banks attacked by especially North Korean and China. Also in Canada, the government had started to pay more of attention to the security of the network system due to so many trial attacks were from China. Trust framework is to describe a brief concept of secure communication between user and service provider.

In addition, experts claim that [4] South Korea has not paid much attention to cyber-attack possibilities while North Korea has systematically developed thousands of electronic warfare specialists and improved cyber combat capabilities. Official said "We have drawn up plans to strengthen the cyber command to respond to newly emerged security challenges such as cyber warfare and cyber terrorism," [1-2] under condition of anonymity because he was not authorized speak to media. He also noted that "Ensuring cyber security is no longer a matter of choice but is an issue of top priority that impacts national security". [3] Nong Hyup Bank, a large commercial bank organization in Korea, suffered from extremely massive denial of service in April 12th last year paralyzing the banking network for a week.

Fig. 5. S. Korea 8th-largest origin point for DDoS attacks: Akamai [18]

Moreover, this event had exposed vulnerabilities of thousands of financial institutions and utilities that rely on network to keep economy on going. Furthermore, it is also believed to have attacked major South Korean government and business websites including Cheong Wa Dae, the National Assembly, the Ministry of National Defense, Shinhan Bank and Korea Exchange Bank.

Despite of such events, critics pointed out that the country's efforts to tackle the new threat are still lackluster considering a lack of military training programs, the insufficient number of specialists and budget allocations for cyber capabilities.

Security experts also have stressed out a point that North Korea could attack the online networks of South Korea's core financial, traffic, aviation and power supply centers anytime they want to, so all citizens should be educated about the possibility of cyber terrorism. Lee Ho-Woong, the head of Security Response Center at Ahnlab emphasized cyber-attacks are getting more complicated.

Figure 4, shows use of electrical power difference between the North Korea and South Korea. North Korea despite of having limited power energy resource, they have managed to develop very sophisticated task force to promote cyber security attack on South Korea as well. North Korea which have also the world's biggest hacking organization group may run out of resource in the near future. Contrarily Korea which have been developed since last 50 years have highest "speed" of network but still remains various holes in the network resulting in open to variety of cyber threats.

Fig. 6. N. Korea launches Cyber Attack to steal S. Korea's War Plans [19]

Recent statement [4] states: "Advanced persistent threat that uses a combination of various IT technologies in a systematic manner for economic and political purposes has been a major and continuing trend for some years now." Since number of attacks increased, thus attack method gets much more advanced each time. As a result the government agencies had taken necessary steps to boost the cyber security readiness. A group of state-funded hackers from North Korea are reported to have hacked a South Korea's military database last September to gain access to 235 GB of sensitive data, including war plans. The leaked data includes 'Operational Plan 5015' which is considered as classified [19].

A South Korean intelligence official says North Korea is believed to have stolen the personal information of an estimated one-point-six million South Korean officials through Internet hacking over the past five years. The source said the National Intelligence Service (NIS) and other authorities have looked into a multitude of recent personal data theft incidents and have traced a number of the hacking routes to North Korea.

The main targets hacked were Web sites of South Korean security organizations and university alumni groups. The NIS found that the North had databased resident registration numbers, addresses, phone numbers and email addresses of South Korean officials. The intelligence official said North Korea used the email addresses of key South Korean officials to hack into government Web sites and to steal government documents [20].

Figure 5 illustrates the example of DDoS cyber-attack on South Korea. Inside the Korean telecommunication infrastructure there are number of vulnerabilities in the network. Eavesdropping, network collision events occur every day in Korea. In order to achieve users satisfaction, not only providing fast speed network but also with secure network topology is essential.

Bank technology officials, pointed out that the South Korean Central Bank had increased computer security measures after the attack on Nong Hyup Bank. The finance ministry had launched a Cyber Security Center for 24-hour vigil of the government's finance and economic agencies, Kang Cheol-won, head of security at

Bank of Korea, said. Kwon Tae-young, senior adviser at the local think tank Korea Research Institute for Strategy, said that South Korea should also focus on bolstering its capabilities to deal with two new security domains: space and cyberspace.

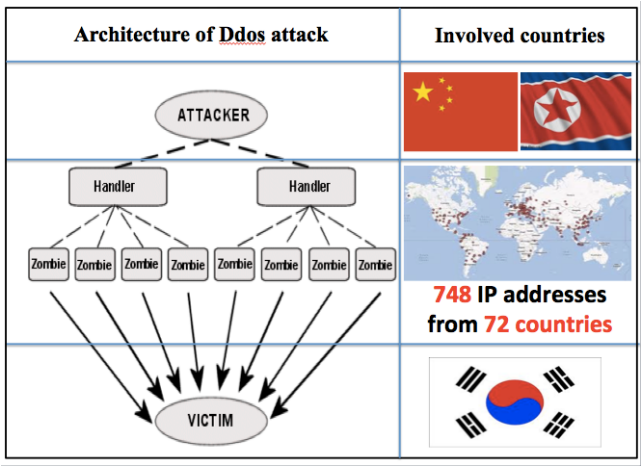


Fig. 7. Korea DDos cyber-attack issue [5]

Beginning from the 20th Century, the United States had gone through enormous growth on economics and industrial business [8-10]. Moreover, the United States had tremendous improvements in advanced technology. During this time, the government needed to collaborate in variety of ways in order to serve national interests and meet requirements of the security. Acceleration in information system technology allowed communication between individuals and states despite of the position of where they are. However, advantages are not always positive. In other words, the benefits to the whole country overshadowed questions and concerns about how these capabilities might be used for specific purposes. These breakthroughs granted new opportunities to organizations, nations or individuals a new skill for perpetrate crime, espionage, sabotage.

Historically, government usually collaborated only on key technological innovations, like nuclear power, to utilize efforts for the common good. Today, government agencies often seem to pursue separate (perhaps counter-productive) policies, in lieu of cooperating effectively to address incoming cyber threats to our local and global network systems.

The United States government has unique insights into the cyber threats but cannot seamlessly share these insights with the very industries that own and operate over ninety percent of the telecommunications' infrastructure and operations. This is further exacerbated by the common misperception that these threats are technical and tactical level attacks best handled at the unit or individual domain level.

This bifurcated approach has resulted in the loss of precious years while the cyber threat vectors and activity levels have grown exponentially. Furthermore, the United

States as a whole has yet to put in place systemic approaches, tradecraft, technologies, and end-to-end solutions across government, academia, and industry. [6]

The prevalence of data security concerns emerging across all sectors is making it clear to many that the United States' cyber security intelligence is lacking in several areas. To address this urgent need, the INSA report included several guidelines that may inspire more thoughtful discussion on key issues and help create more effective data protection practices. "While there is a great deal of focus on current cyber security issues, there is little focus on defining and exploring the cyber threat environment at a higher level," noted INSA analysts.

Moreover, according to the Network World, the Department of Homeland Security has been given jurisdiction in the cyber security area in recent years, still the agency may be short of experience and expertise needed to orchestrate a proper solution. "Ultimately, INSA's Cyber Council would like to see a meaningful partnership among all relevant government agencies and the private sector to ensure seamless sharing of threat information, timely analytical judgments and reasoned, measured responses to clear threats," the report stated.

Experts believe that enhancing national cyber security is still a challenging task that is constantly growing in size and complexity. However collaborative efforts plus experts come in one agreement may provide significant push in to the right track.

Fig. 8. China vs. US mutual accusations [22]

Between China and US not only communication is often but also behind the network, 70 percentage of cyber threats to US are namely from China, illustrated in Figure 6.

3.1 Example of attacks in Korea (Phishing)

As time goes on new attacks develop in Korea. Especially voice phishing has been attacked in Korea to huge numbers of customers. However current numbers of voice phishing attacks are decreasing where SMS and Internet phishing has been increased. According to report by KISA, hackers phish financial industries as about 73%, and

27% others related to government. Moreover, not much law has been restricted on phone calls from miscellaneous numbers.

Fig. 9. Current Phishing status in Korea

What Korea has done and Results

Since numbers of attacks have increased, Korea government has proposed following statements on attacks

- Identification of international incoming call and SMS messages (since May 09 2012)
  - ※ Korea major telecommunication organization has been running PSTN methods for international calls
- 「Prevention of out of law attacks to finial industry」(December, since 2012)
- 「Guide to prevention incoming fake call number」(since July, 2012)

Current phishing attacks (Figure 7) involve numbers of financial industry and same as its website to let users feel confused. Following Figure 8., illustrates real examples of phishing on smartphones. Many researches are on how to prevent smartphone phishing messages and sites. Below Figure 9-10, shows comparison of phishing internet sites on smartphones.

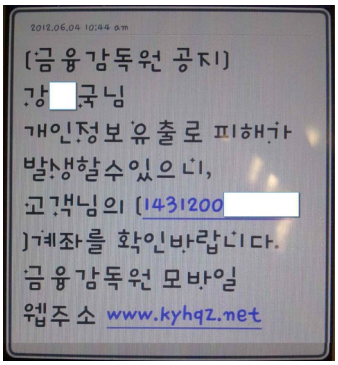
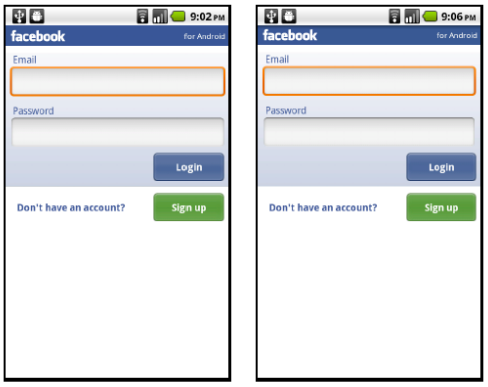
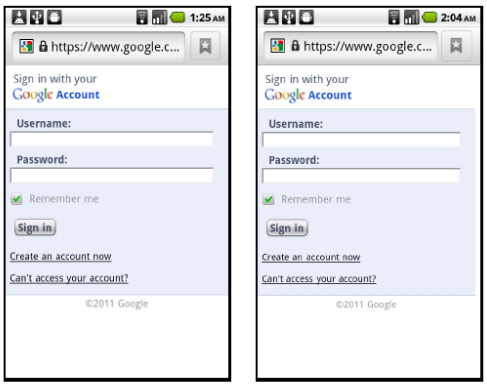


Fig. 10. Smartphone Phishing attack in South Korea



(a) Real Facebook login. (b) Fake Facebook login.

Fig. 11. Comparison of phishing internet sites on smartphones.



(a) Real browser. (b) Our fake browser.

Fig. 12. Comparison of phishing internet sites on smartphones.

Voice phishing attacks occur usually from outside of Korea to avoid network trace and use Korea own financial industry number or government related to confuse users
Major impersonate organization :

1. investigative agency(26%)
2. bank(16%)
3. public institution(6%)
4. parcel service(5%)

Also attackers use easy of change in incoming call such as VoIP and use technical weak point of the call connection.

4 Cyber Security in Canada & USA

Over few years, many issues based on cyber threats have been arose in Canada. As in other zones of commerce and theatres of operation, Canada and the United States are deeply integrated in cyberspace. Both nations derive benefits from cybersecurity cooperation. Canadians should not underestimate the benefits they gain from US willingness to share advanced capabilities for cyber operations. The US Department of Homeland Security's Cyber security and Infrastructure Security Agency (CISA) and the FBI have issued a joint statement accusing hackers based in the People's Republic of China (PRC) of attempting to steal research relating to Covid-19 [1].

Canada draws a clear net benefit from close cooperation with the United States in cyberspace because both the nature of the evolving threat and the nature and cost of countering this threat are increasingly more difficult for a state to address on its own. At the same time, as it cooperates with the United States and other close allies, the Canadian government faces the challenge of finding a balance between security and the Canadian definition of freedom [5].

Professionals note that Canada needs to develop better strategies for handling cyber-attacks. Canadians have become accustomed to hearing about Chinese hackers more than others lately that they tried to break into federal departmental and House of Commons computer systems or that Chinese cyber espionage was at least partly responsible for Nortel’s downfall [8-12].

A U.S. report pointed to a single building in Shanghai (occupied by Unit 61398 of the People’s Liberation Army) as being the center of sustained cyber-attacks on targets in the U.S., Canada and Britain. Last year, the government also introduced the Protecting Children from Internet Predators Act. It was widely denounced as being overly invasive and counters to personal freedoms, as it would have required internet providers to allow for police access to personal online communications without a warrant. Canadians would not abide overreaching from the government or authorities into their personal lives, which are carried out more than ever online. The Mandiant report revealed that three servers linked to the alleged Chinese hackers were located in Canada, and used to funnel data back home.

Fig. 13. Canada and the U.S. Announce Joint Cyber security Action Plan

When asked what industries the Canadian organizations belonged to or where in the country they were located, a Mandiant spokesperson said the company would "not be providing that level of detail." ″It lines up with what we already suspected to a high degree," said Martin Rudner, distinguished research professor emeritus at Carleton University. He added that "suspicions that a dedicated People's Liberation Army unit was engaged in mainly industrial espionage" have been circulated for at least a year. In a statement faxed to The Associated Press, China's Foreign Ministry dismissed the report as "groundless," and the country's Defense Ministry denied any involvement in the cyber-attacks.

The New York Times reported that the Canadian arm of Telvent, now owned by Schneider Electric, was one of the companies affected by the multi-year attack. The company designs software for remote access to energy production and distribution systems in the oil and gas industries. The attack itself was revealed to customers in September. Canada's problem, said Professor Rudner, is that the country not only lacks the necessary talent to defend from comprehensive cyber-attacks, but few programs and resources are in place for cyber security training. In the U.S., for example, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a part of the Department of Homeland Security, offers a number of training courses designed "to improve the security posture of control systems within the nation's critical infrastructure". The department considers companies involved in such sectors as energy, communications, banking and more to be part of America's critical infrastructure.

In 2005, Public Safety Canada established the Canadian Cyber Incident Response Centre (CCIRC) with similar goals to help owners and operators of the country's critical infrastructure reduce the risk of cyber-oriented threats. One of the organization's goals was to share "standards, best practices, awareness, and education," according to the Auditor General's Fall 2012 report. The report was critical of the CCIRC's efforts, finding the organization had progressed slowly in making such information available. ″It was scathing on how little was being done," said Professor Skillicorn. These responsibilities have since been shifted to another department within Public Safety Canada following the introduction of Canada's Cyber Security Strategy in 2010.

Aside from programs operated by the National Research Council and National Resources Canada, which are not accessible to civilians, according to Professor Skillicorn and Professor Rudner, neither knew of training or education initiatives in Canada similar to those in the U.S. or U.K. ″To get training, one has to have access to the federal system," Professor Rudner said. Public Safety Canada, which oversees matters of cyber security affecting the government, did not respond to a request for comment in time for publication.

Canada government not only needs to enhance cyber security level against attempts from others, but also it is essential to educate people of how much it is important of having a warning of security issues.

This is not first time that foreign entities namely, China have been accused of illegally gaining access to Canadian corporate interests. As reported by the Wall Street Journal and Financial Post in 2011, hackers, apparently from China, had unfettered access to the computer network of former Canadian telecommunications giant Nortel for over a decade, until the company's bankruptcy in 2009.

According to reports, Chinese hackers were alleged to have targeted law firms involved in BHP Billiton Ltd.'s takeover bid for Saskatchewan's Potash Corp. such companies that deal in natural resources relevant to Chinese state interests with the intent of influencing negotiations [12-17]. The Mandiant report comes on the same day that Apple Inc., revealed some of its employees' computers had also been infiltrated by hackers, according to the Wall Street Journal, using the same malware used to target Facebook Inc. last week. The malware, some security experts believe, originated in China. Therefore this leaves the government in a strange position. Security issues continue, whether they arise from Shanghai or domestically.

5 Conclusions

In this paper authors discuss important issues related to cyber security in South Korea, United States and Canada region. Given current COVID-19 related crisis, the cybersecurity in South Korea, Canada and US have become the government priority. Their Computer Emergy Response Teams (CERTs) monitor all possible cyber-attacks and implement a real-time cyber-attack database, while implementing proper countarmesures. CERTs work hand-n-hand with the National Security Agencies to make sure that the Cyber-Attack Database is up-todate, providing proper access to authorised personnel in real-time. The autors promote further research and creation of multinational research teams to design more sofisticated and robbust cybersecurity in the region of South East Asia, North America and worldwide.

Acknowledgments

The authors are grateful for the generous support received from colleagues at the Liberty University, Fort Hays State University in US, and Sungkyunkwan University in South Korea. This work was sponsored by the research security grant awarded in South Korea.

References

1. Chinese hackers attacking Covid-19 researchers, US warns, Network Security Volume 2020, Issue 5, pages 1-2, May 2020.
2. Wenchao Meng Xiaoyu Wang Shichao Liu, Distributed Control Methods and Cyber Security Issues in Microgrids, 1st Edition, Paperback ISBN: 9780128169469, Academic Press, 296 pages, 20th March 2020.
3. Vladlena Benson, John McAlaney, Emerging Cyber Threats and Cognitive Vulnerabilities, 1st Edition, Paperback ISBN: 9780128162033, Academic Press, 259 pages, 21st September 2019.
4. RasimAlguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat, Cyber-physical systems and their security issues, Computers in Industry, Volume 100, pages 212-223, September 2018.
5. James Andrew Lewis, Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States, Discussion Paper No: IDB-DP-457, Inter American Development Bank, July 2016.
6. Alexander Moens, Seychelle Cushing, and Alan W. Dowd (2015). Cybersecurity Challenges for Canada and the United States. Fraser Institute.
7. Julian Jang-Jaccard, Surya Nepal, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences Volume 80, Issue 5, pages 973-993, August 2014.
8. Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jarbi, David Lyon, and R.B.J. Walker (2014). After Snowden: Rethinking the Impact of Surveillance. International Political Sociology 8, 2: 121–144. DOI: 10.1111/ips.12048.
9. Canada, Parliament, Senate, Standing Senate Committee on National Security and Defence [SSCNSD] (2014). Transcript of Proceedings. 41st Parl., 2nd sess. Meeting No. 18.
10. Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay (2014). Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. RAND Corporation.
11. Young Do Kim, Jin Sung Kim, Kyung Ho Lee, Major issues of the national cyber security system in South Korea, and its future direction, pages 435-455, Korean Journal of Defense Analysis, Volume25, Issue number 4, December 12th, 2013.
12. Cilluffo, Frank J., and Sharon L. Cardash (2013). Cyber Domain Conflict in the 21st Century. Journal of Diplomacy & International Relations 14, 1: 41– 47. EBSCOhost (87977324).
13. Gjelten, Tom (2013). First Strike: US Cyber Warriors Seize the Offensive. World Affairs 75, 5: 33–43. EBSCOhost (92026925).
14. Collins, Sean, and Stephen McCombie (2012). Stuxnet: The Emergence of a New Cyber Weapon and its Implications. Journal of Policing, Intelligence, and Counter Terrorism 7, 1: 80–91. DOI: 10.1080/18335330.2012.653198.
15. Cox, James (2012). Canada and the Five Eyes Intelligence Community. Canadian Defense & Foreign Affairs Institute.
16. Brenner, Joel (2011). America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. Penguin Press.
17. Barford, P., M. Dacier, T.G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen (2010). Cyber SA: Situational Awareness for Cyber Defence. In Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang, eds., Cyber Situational Awareness: Issues and Research (Springer): 3–14.
18. S. Korea 8th-largest origin point for DDoS attacks: Akamai https://en.yna.co.kr/view/AEN20180702006000320 accessed June 20, 2020.

19. N. Korea launches Cyber Attack to steal S. Korea's War Plans https://www.cybersecurity-insiders.com/north-korea-launches-cyber-attack-to-steal-south-koreas-war-plans/ accessed June 21st 2020.
20. NK Stole 1.6 Mln S.Koreans' Personal Data via Hacking http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=64969 accessed June 19, 2020.
21. NK Stole 1.6 Mln S.Koreans' Personal Data via Hacking http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=64969 accessed June 19, 2020.
22. Bruno Mascitelli, Mona Chung: Hue and cry over Huawei: Cold war tensions, security threats or anti-competitive behaviour?, Research in Globalization, Volume 1, 2019, 100002, ISSN 2590-051X, https://doi.org/10.1016/j.resglo.2019.100002.
23. Deloit on Cyber crisis management: Readiness, response, and recovery, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf accessed June 18, 2020
24. Red Team on the Top 6 Industries At Risk For Cyber Attacks, https://www.redteamsecure.com/blog/the-top-6-industries-at-risk-for-cyber-attacks/ accessed June 19, 2020