BIGMUN 2018
Disarmament and International Security (DISEC)

Research Report

Topic 3: Member states' cyber security against major foreign attack

Ronas T. Kesmez and Maria H. Katz

Introduction

As the world is becoming increasingly digitalized and networked, more business value and personal information are migrating into digital form on globally interconnected technology platforms. As a result, the number of cyber-attacks is surging, as the information is more easily accessible. So much so that within the first half of 2017, almost 2 billion data records around the world were stolen or lost by cyber-attacks and 918 data breaches, compromising 1.9 billion data records, resulted in the number of lost, stolen or compromised records to increase by 164 percent, compared to the same period in 2016.[1] This new international security challenge poses a threat of cyber-conflict between states. Cybercrime and state-sponsored cybercrime activities are one of the largest global dangers to today's society and economy. Every year, $400 billion is lost globally due to cyber-attacks. Therefore, the need to increase stability in cyberspace and respond to large-scale cyber incidents is urgent, and a precondition for building a strong trusted digital space.[2]

Key Terms

Cyber Security – Technologies, processes, and practices designed to protect computers, networks, programs and data from attack or unauthorized access.[3]
Cyber-attack – A "deliberate exploitation of computer systems, technology-dependent enterprises, and networks. Cyber-attacks use malicious code to computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as identity theft."[4]
Ransomware – A malicious software designed to limit or block access to computer systems until a sum of money is paid[5], often paid in bitcoins, a form of digital currency or cryptocurrency kept on a public ledger in the cloud, ensuring the criminal's anonymity.[6]
Spear phishing – an email spoofing attack, targeting specific organizations or individuals, seeking unauthorized access to sensitive information. Often conducted by perpetrators for financial gain, trade secrets or military information.[7]
Data record – "The structure of a database. Many unique data fields are the unique components used to make the structure. Many data records make a data file and many data files make a database."[8]
Global Cybersecurity Index (GCI) – a multi-stakeholder initiative measuring the commitment of individual countries to cybersecurity, analyzed through five categories: legal measures, technical measures, organizational measures, capacity building, and cooperation.[9]

---

[1] Graham, Luke (20/09/2017). Visited 08/01/2017. Available at: https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html
[2] Jaansalu, Liis (22/12/2017). Visited 08/01/2017. Available at: http://www.consilium.europa.eu/en/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/
[3] Rouse, Margaret (November). Visited on 03/01/2017. Available at: http://whatis.techtarget.com/definition/cybersecurity
[4] Techopedia. Visited on 03/01/2018. Available at: https://www.techopedia.com/definition/24748/cyberattack
[5] Trend Micro. Visited on 07/01/2018. Available at: http://www.trendmicro.dk/vinfo/dk/security/definition/ransomware
[6] Investopedia. Visited on 07/01/2018. Available at: https://www.investopedia.com/terms/b/bitcoin.asp
[7] Rouse, Margaret. Visited on 08/01/2018. Available at: http://searchsecurity.techtarget.com/definition/spear-phishing
[8] The Law Dictionary. Visited on 07/01/2018. Available at: https://thelawdictionary.org/data-record/
[9] Global Cybersecurity Index. Visited on 09/01/2018. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Main Body

Background

Digital technologies have become indispensable to our economy, in finance, health, energy and transport sectors. Consequently, as more information is becoming available online, we are more susceptible to incidents that could disrupt the supply of essential services society has become reliant on. The cyber threat is evolving and becoming more pervasive as cyber intrusions become more common and sophisticated. Origins of cybercrime are criminality, terrorism, and state-sponsored cyberattacks. Companies and businesses are targeted for trade secrets, intellectual and corporate data, universities for their research and development, citizens are targeted by identity thieves and fraudsters for financial gain[10], while "hacktivists", gaining unauthorized access to computer files and networks, make political statements by piercing firewalls.

Cybercrime costs the global economy more than US$400 billion per year.[11] To ensure the safety of the global economy, cybersecurity is therefore at the top of the international agenda. Governments and businesses worldwide are searching to find better defense strategies against cyberattacks. Despite these efforts, cybercrime is likely to increase due to technical innovations, the expanding number of available online services and the development of the Internet of Things[12], enabling communication between machines (M2M) increasing hackers' ability to manipulate appliances. [13]

Past incidents[14]

Recent years have seen an extraordinary number of cybersecurity meltdowns. Such attacks included the breach of the spy tools of the elite NSA-linked operation, the 'Equation Group' by the hacking group known as Shadow Brokers. The group offered a sample of the NSA data and attempted to auction it off, as well as leaked parts for Halloween and Black Friday. More recently, in April 2017, Shadow Brokers released a Windows exploit known as 'EternalBlue' since used to infect targets in two high-profile ransomware attacks. One of these attacks was WannaCry, aimed at hundreds of thousands of targets, including public utilities and large corporations. The ransomware is specifically known to have temporarily crippled the National Health Service hospitals (NHS) of the United Kingdom. Eventually, a flaw was found and ultimately used to render the malware inert to stop its spread. The ransomware did, however, manage to net almost 53bitcoins, approx. $130000. US officials believe the attack to be a North Korean government project. The second ransomware attack stemming from the 'EternalBlue' release, hit targets worldwide about a month after WannaCry. The malware, Petya, infected networks in multiple countries, including US pharmaceutical company Merck, Danish shipping company Maersk and Russian oil giant Rosneft.

Further contributing to the cybercrime industry, WikiLeaks published a data trove, 'Vault 7', with over 8700 documents stolen from the CIA comprehending of documentation of alleged spying operations and hacking tools. This could have severe consequences for the CIA, both in terms of its reputation and public image and its operational abilities. Collectively, Vault 7 and the releases of

[10] FBI. Visited on 07/01/2018. Available at: https://www.fbi.gov/investigate/cyber

[11] Newman, Lily Hay (01/07/2017). Visited on 07/01/2018. Available at: https://www.wired.com/story/2017-biggest-hacks-so-far/?mbid=email_onsiteshare

[12] The interconnection via the internet of computing devices embedded in objects, enabling them to send and receive data.

[13] Gabel, Detlev, and Liard, Bertrand, and Orzechowski, Daren (01/06/2015). Visited on 07/01/2018. Available at: https://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important

[14] Newman, Lily Hay (01/07/2017). Visited on 07/01/2018. Available at: https://www.wired.com/story/2017-biggest-hacks-so-far/?mbid=email_onsiteshare

the Shadow Brokers has led to debates concerning the governmental development of digital spying tools. The industry has spread to politics and political campaigns. Days before the French presidential runoff in May, 9GB of emails from Emmanuel Macron were leaked. Shortly after the Macron Campaign released a statement confirming the breach and cautioning that not all content was legitimate. The operation is believed to be an attempt by the Russian-government-linked hacker group 'Fancy Bear'. Other significant cyberattacks include Fireball, Delta Charlie, and Skype.

The 198 Million Voter Records Exposed is an example of an incident not driven by malicious intent. In June 2017, a researcher discovered a publicly accessible database containing personal information for 198 million US voters over the past 10 years. The host of the database, Deep Root Analytics, had misconfigured it so that more than a terabyte of voter information was available to anyone on the internet. Exemplifying the cybersecurity risks, the firm said that only the data was only accessed by the discovering researcher, however, there has been no proof of this.

Current action in the field

The United Nations telecommunications agency reported in 2017 that only half of all countries have a cybersecurity strategy, 38% of countries have a published cybersecurity strategy and 12% of governments are developing one. The 10 most committed countries are Singapore, United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France, and Canada. The International Telecommunication Union (ITU) released its second Global Security Index in 2017, demonstrating the overall cybersecurity commitment of ITU's 193 member States.[15] This index is used to measure the status of cybersecurity worldwide. The Index shows improvement and strengthening on the five pillars of the ITU Global Cybersecurity Agenda: legal, technical, organizational, capacity building and international cooperation. The ITU express that prevention and mitigation measures to reduce the risks posed by cyber-related threats should also be put in place, and encourage governments to consider national policies taking into account cybersecurity and emphasizing the importance of private citizens to be smart online.[16]

Relevant Countries

France – France's biggest bank, BNP Paribas's property arm was hit with the ransomware virus, EternalBlue. The country's presidential elections were also affected by the Macron campaign hack.

The 10 most committed countries are Singapore, United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France, and Canada. Ranking based on countries' legal, technical and organizational institutions, their educational and research capabilities, and their cooperation in information-sharing networks, using the GCI.

Singapore – The CSA is a national agency that oversees cybersecurity strategy, operation, education, outreach, and ecosystem development in Singapore, as part of the Prime Minister's Office and managed by the Ministry of Communications and Information.

United States – The Department of Homeland Security ensuring cybersecurity in the nation.

[15] UN News Centre. Visited on 09/01/2018. Available at: http://www.un.org/apps/news/story.asp?NewsID=57119#.WlYPkCPONAZ

[16] UN News Centre. Visited on 09/01/2018. Available at: http://www.un.org/apps/news/story.asp?NewsID=57119#.WlYPkCPONAZ

Relevant Organisations

Desktop Central - "is an integrated desktop and mobile device management software that allows you to automatically patch Windows, Mac, and Linux endpoints and perform various other operations to secure your network against cyberattacks."[17]

FireEye – Award-winning, cyber security provider with intelligent security. Has over 5300 customers in over 67 countries.

CSA – the Cyber Security Agency of Singapore

Paladion – a global leader in artificial intelligence driven managed detection response services.

Other companies include EY, Deloitte, PwC, KPMG, IBM, and Accenture.

Relevant UN Resolutions

A/RES/64/211
Resolution adopted by the General Assembly on 21 December 2009 during the Sixty-fourth session, on *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.*
Organizations and individual owners and users of information technology, Governments have a collective responsibility to ensure and enhance the stability, security, and continuity of the Internet and information technologies. Encourages member states to share their best practices to assist other Member states in the achievement of cybersecurity.
Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

A/72/315
Developments adopted by governments, Report of the Secretary-General on 11 August 2017 during the Seventy-second session, on *Developments in the field of information and telecommunications in the context of international security.*
General Assembly invited all Member States, taking into account the assessments and recommendations contained in in report of the Group and Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), to continue to inform the SG of their views and assessments on information security and efforts taken on a national level to strengthen information security and promote international co-operation, and international efforts to strengthen information security at the global level.
Available at: http://undocs.org/A/72/315

A/71/172
Developments adopted by governments, Report of the Secretary-General on 19 July 2016 during the Seventy-first session, on *Developments in the field of information and telecommunications in the context of international security.*
General Assembly invited all Member States, taking into account the assessments and recommendations contained in in report of the Group and Governmental Experts on Developments

[17] Manage Engine. Visited on 09/01/2018. Available at: https://www.manageengine.com/products/desktop-central/secure-network-from-ransomware-and-cyber-attacks.html?gclid=EAIaIQobChMIn_v3y-7L2AIV6CnTCh1NGQzrEAAYAiAAEgLFQ_D_BwE

in the Field of Information and Telecommunications in the Context of International Security (A/70/174), to continue to inform the SG of their views and assessments on information security and efforts taken on a national level to strengthen information security and promote international co-operation, and international efforts to strengthen information security at the global level. Available at: http://undocs.org/A/71/172

Cyber security strategy documents for individual countries:
https://ccdcoe.org/cyber-security-strategy-documents.html

National cyber security organization for individual countries:
https://ccdcoe.org/national-cyber-security-organisation.html

Bibliography

FBI. Visited on 07/01/2018. Available at: https://www.fbi.gov/investigate/cyber

Gabel, Detlev, and Liard, Bertrand, and Orzechowski, Daren (01/06/2015). Visited on 07/01/2018. Available at: https://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important

Global Cybersecurity Index. Visited on 09/01/2018. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Graham, Luke (20/09/2017). Visited on 08/01/2018. Available at: https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html

Jaansalu, Liis (22/12/2017). Visited 08/01/2018. Available at: http://www.consilium.europa.eu/en/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/

Manage Engine. Visited on 09/01/2018. Available at: https://www.manageengine.com/products/desktop-central/secure-network-from-ransomware-and-cyber-attacks.html?gclid=EAIaIQobChMIn_v3y-7L2AIV6CnTCh1NGQzrEAAYAiAAEgLFQ_D_BwE

Newman, Lily Hay (01/07/2017). Visited on 07/01/2018. Available at: https://www.wired.com/story/2017-biggest-hacks-so-far/?mbid=email_onsiteshare

Investopedia. Visited on 07/01/2018. Available at: https://www.investopedia.com/terms/b/bitcoin.asp

Rouse, Margaret. Visited on 08/01/2018. Available at: http://searchsecurity.techtarget.com/definition/spear-phishing

Rouse, Margaret (November). Visited on 03/01/2018. Available at: http://whatis.techtarget.com/definition/cybersecurity

Techopedia. Visited on 03/01/2018. Available at: https://www.techopedia.com/definition/24748/cyberattack

The Law Dictionary. Visited on 07/01/2018. Available at: https://thelawdictionary.org/data-record/

Trend Micro. Visited on 07/01/2018. Available at: http://www.trendmicro.dk/vinfo/dk/security/definition/ransomware

UN News Centre. Visited on 09/01/2018. Available at: http://www.un.org/apps/news/story.asp?NewsID=57119#.WlYPkCPONAZ