Who is responsible for Cybersecurity?

Student Name: Ruochen Pi
Student Number: 500055496

4. *Cybersecurity isa joint responsibility of the government and private sector.*

Critically analyse the previous statement. Use at least two nation states as case studies to argue how the state and private sector have responded to the current cybersecurity landscape and where the responsibility of security systems and assets should lie.

Keywords: cybersecurity, government, private sector, China, Ukraine, responsibility

Abstract

Context:
Network security incidents occur frequently all over the world, including attacks on government agencies and private enterprises. There are attacks for political needs, there are attacks for money.

Purpose:
The purpose of this study is to discuss the responsibility of cyber security, explaining the view that cyber security is a shared responsibility of the government and the private sector.

Methods:
This study is a subjective and objective combination of research, which refers to the relevant network security laws of various governments and the large and small network security incidents in the world. Take case as the center, think and discuss the responsibility of network security diversely. Classify and discuss the incident, including different attackers and attacked parties, different purposes, different public harm degree, etc.

Conclusion:
It is concluded that network security is the common responsibility of government and private sector, and the proportion of responsibility is different according to different scenarios.

Introduction

Cybersecurity is a joint responsibility of government and private sector.
In today's globalized and digital world, developed countries and developing countries regard cyber security as one of the priority areas of national security.

Cybersecurity is mainly reflected in two aspects. The first one is the network level, which is

including attack and defense, namely cyber defense and cyber deterrence. The second one is information level, which is including information protection and information supervision.

Cybersecurity also covers four parts. The first one is system security, such as system collapse and damage to the system storage, processing and transmission of the message caused by damage and loss. Second, network security, such as user password authentication, user access control. Third, information communication security, such as preventing and controlling the consequences caused by illegal and harmful information transmission, to avoid the large cloud free spread of information on the public network out of control. The fourth one is information content security, such as to avoid attackers using system security loopholes for eavesdropping, impersonation, fraud and other activities that harm legitimate users.

Argument

Network security is the common responsibility of the government and the private sector.
For different network security incidents, the government and the private sector should bear different responsibilities. For example, if the attackers are hacker groups, and it involves the national government or critical infrastructure defense, the state needs to defend, then the power of the private sector is not enough to interfere with the national government or critical infrastructure; If the attacker is a state, whether it is a government, a company or an individual, then the defender must be a state power. The private sector can often assist governments in their cybersecurity efforts.

According to different scenarios, this study collected different cases to analyze. There are 3 cases, which is including government cybersecurity incidents between nations for political purposes, private sector cybersecurity incidents between nations for financial purposes, and private sector cybersecurity incidents in the country for financial purposes. In different real events, how is the responsibility for network security divided?

Research

Case 1 Political factors drive cyber attacks

This is a government cybersecurity incidents between nations for political purposes.
Cybersecurity is particularly important for the young independent State of Ukraine, which has been the victim of cyber-attacks many times over the past few years. There have been a number of cybersecurity incidents in Ukraine in recent years, for example, In March 2014, Ukraine's national telecommunications system was hit by a cyber attack. On December 23, 2015, attackers hacked into the computer system of Ukraine's national grid and shut down the corresponding control equipment, resulting in a power outage lasting three hours. In 2016, the biggest airport in Ukraine was shut down by hacker, and at the same time, one of the hacker group, attacked Ukraine's STB

TV station. All in all, the most famous case of Ukraine cybersecurity is the "Russian-Ukrainian" cyber war (*Streltsov, L,2017*).

In a love-hate relationship with Russia, as early as 2012, Ukrainian government websites were regularly hacked by Russians with sophisticated malware, starting a war of public opinion
In fact, back in 2012, when Russia and Ukraine were fighting each other rather than actually fighting each other, Ukrainian websites, especially government websites, were regularly hacked. In 2013 Ukrainian system administrators discovered the infiltration of advanced malware, such as Red October, Miniduke, NetTraveler, etc (Kateryнchuk, P. 2019).

Ukraine finally saw what a massive and full-scale technical attack looked like when the rhetoric turned into a real war in 2014. Ukraine's national Space Agency found that some of its satellite systems had been hacked, that Russia had special forces targeting critical data, and that NATO and Ukraine had been targeted through a series of searches for information about politicians. They falsified Wikipedia searches for Ukraine's country profile and falsified scores of social media posts to discredit Ukraine. Even in the 2014 Ukrainian presidential election, the official website was hacked and the results of the vote were tampered with (*McCrory, D. 2020*).

In addition to the weapons of public opinion, Russian hackers attacked 50 substations of Ukraine's power system. Most of Ukraine's communications infrastructure operates through controlled lines and switches (*Sullivan, J. E., & Kamensky, D. 2017*). This is a disadvantage because it is extremely vulnerable to enemy control. The event left 200,000 people living in darkness. It became known as the Ukrainian power grid incident (*McCrory, D. 2020*).

In the case of attacks on Ukraine, Russia's cyber operations have sometimes been coordinated with those of its armed forces. Nowadays, network warfare and actual combat have already moved towards the trend of integration, and today's network attack may be brewing a big entity "conspiracy", it is unknown. No network security, no national security. No informatization, no modernization

In face of these attacks, what did the Ukrainian government and private sector do and take responsibility?
For Ukrainian government:

1. The Ukrainian government has made great efforts to develop domestic Cybersecurity In April 2016, and published the New Ukrainian Cybersecurity Strategy (*National Security and Defense Council of Ukraine. n.d.*).
   It will design new standards for Ukrainian cyber security and accelerate cyber security research and development activities.
2. Ukraine government has great international cooperation in the field of cyber security.
   On February 7, 2018, America and Ukraine signed the Ukrainian Cyber Security Cooperation Act (*Streltsov, L. 2017*).
   A. Demanding that the United States provide advanced security for Ukrainian government computers and technical support for Ukraine,
   B. Reducing its dependence on Russian technology;

C. Help Ukraine expand its capacity to share cybersecurity information and cooperate on international responses.

3. Government support the development of cyber security, recruits cyber volunteers to form cyber forces (*Cyberberkut. n.d.*).
   In February 2015, the Department of Information Policy of Ukraine published a new page on its official website called "Ukrainian Information Forces" to recruit Ukrainian online volunteers.
   Using the power of Ukrainian netizens to send the right message to the world against Russia's propaganda war.

For private sector:
Ukraine's cyberattack capabilities are not to be sniffed at. Ukraine's private sector, or civil society, also has extremely powerful cybersecurity capabilities. U.S. Assistant Secretary of Homeland Security Stuart Baker has said Ukraine is not a powerful country, but it has some sophisticated hackers. If there is one area that fits its size, it is cybersecurity (*Alien removals under Operation Predator - Govinfo.gov. n.d.*).

In Ukraine, these private sectors are pro-government, protected by the state, and have sophisticated hacking and cyber security defenses. They often work with the Ukrainian government, taking charge of cyber security in the course of international cyber warfare, and launching attacks when necessary.

Case 2 Network attack event

This is a private sector cybersecurity incidents between nations for financial purposes. Cyber-attacks are well known and often happen in different countries. This case is a domain name attack in China. At around 0:00 on August 25, 2021, a denial-of-service attack was launched on China's national domain name resolution nodes, affecting the Sina Weibo account and some.cn websites *(Charles Riley. n.d.)*. After handling, services were restored to normal by 2 am, the China Internet Network Information Center (CNNIC) said in a notice *(Charles Riley. n.d.)*. But at about 4 a.m., the nation's domain name resolution node was again hit by the largest denial-of-service attack in history, affecting some web site resolution and causing slow or interrupted access. At the time of the announcement, the attack was still ongoing and the NDS service had gradually resumed *(Charles Riley. n.d.)*. The Ministry of Industry and Information Technology has launched a special emergency plan for the security of the Domain name System to further ensure the resolution of the country's domain names. The original intention of the attacker is to attack the private server domain name of a game to achieve their own goals. Denial-of-service attacks, or denial-of-service attacks, are often used by hackers to make a target machine stop providing services or resources, according to Interactive Encyclopedia. These resources include disk space, memory, processes, and even network bandwidth, preventing normal users from accessing them *(Encyclopedia.com. 2021, November 14)*.

In this case, the country's private sector suffered illegal cyber attacks by foreign hackers for financial purposes. There are many similar incidents in China. According to the statistics, in the

first half of 2021, the number of hosts controlled by Trojan horses and botnets in China reached 6.93 million, according to sample monitoring (*Science Net news channel. 2013, September*). That's a big drop from last year, but still a staggering number. The vast majority of the 6.93 million hosts were controlled by foreign servers, with U.S. addresses accounting for one-third of the 15,000 Trojan and botnet control servers. A large number of Chinese websites have been implanted with hidden attacks such as "back doors" and "dark links". 16,000 overseas IP controls 33,000 websites in China by embedding "back doors", a huge number.

In this kind of case, the responsibilities of the government and the private sector for network security also play a common role.

For Chinese government:
The Ministry of Industry and Information Technology of the Chinese government has launched a special emergency plan for the security of the domain name System to further ensure the resolution of domain names in the country. First, the government helped Sina Weibo solve the existing problems and held a press conference (*Science Net news channel. 2013, September*). Subsequently, in order to prevent the recurrence of relevant time, the government formulated relevant policies and corresponding countermeasures

For Sina Weibo application program, which is a private sector, and .cn website operators:
The private sector also took responsibility. First of all, although it happened in the early hours of the morning, the private sector's technicians found the problem and reported it to the system. The private sector then acknowledges the problem and apologizes, compensating users accordingly. Then it turns to the government to help solve the problem. Finally, as well as after the replay, to prevent similar incidents. This is all the efforts made by Sina Weibo and .cn website operators in this event.

Case 3 Information leakage event

This is a cybersecurity incidents within a country for financial purposes. I experienced this case myself, deeply realized the importance of cybersecurity, multiple potential dangers of personal information leakage, and understood that network security is the responsibility of both government and the private sector.

In 2020, during Chinese New Year, 538 million Weibo user information was sold on the dark web (*Global, A. C. n.d.*).
Weibo, the most-used app in China and the international equivalent of Twitter, is a social networking and microblogging service that allows users to update graphic messages of up to 200 characters plus multiple photos or videos.
The application side identifies that the attacker illegally called the interface to obtain user information, but others point out that the data source was through the draglibrary, not the API interface. At the same time, some non-public information is not available through the API. The

leaked information includes users' id numbers, mobile phone numbers, bank card numbers and other private information. Because I was also one of the victims of this event, I received a number of fraudulent phone calls around March 2020, including false winning news notification, remittance notification, etc.

In this case, it was the joint action of the public security department, the information department and other departments of the country that finally caught the suspect, which is what we glad to see. We have to admit that when we enjoy the speed, convenience and intelligence of the Internet, we have consciously or unconsciously sold our privacy. At any time, the large and small information leakage events happening all the time. There are some more significant events, for example, on March 31, 2020, Marriott International group disclosed the personal information of 5.2 million customers, and this is the second major data breach at Marriott in as these years (l*rmax, M, 2020, April 13*). For another example, on Oct. 17, 2020, the U.K. privacy regulator imposed its largest-ever fine, when British Airways (British Airways PLC, BAY.LN) was fined 20 million pounds ($25.8 million) for a 2018 data breach that affected over 400,000 customers (*BBC. 2020, October 16*).

In this case, the Chinese government and the private sector also shared responsibility.
For Chinese government:
These incidents are under constant efforts by every countries' governments to reduce them. For example, on October 13, 2020, China submitted to the 22nd Meeting of the Standing Committee of the 13th National People's Congress a draft of the Personal Information Protection Law, which attracted much attention, for deliberation. Violators of the Personal Information Protection Law can be fined up to 50 million yuan (*China Briefing News. 2021, September 16*). There are also international agreements on network security incidents between governments. Law is a cost threshold for the occurrence of illegal activities, which plays a role in preventing network security criminal activities and punishing the perpetrators of network security criminal activities.

For private sector:
As with case2, private companies bear some of the burden. Although they do not do a good job of network security defense, but they always detect the network operation status, and immediately respond to emergencies. At the same time, network operators have established a network information security complaints, reporting system, public complaints, reporting methods and other information, timely acceptance and processing of complaints and reporting about network information security. In this case, the private sector also actively cooperated with the government in the investigation.

Analysis and Critical Thinking

According to the above case, we can analyze that there are multiple scenarios in which the country undertakes the responsibility for network security. There are three main points.

1. If the attacker is an ordinary hacker, the target of the attack is an individual with a small audience, just like an individual cold, who catches a cold who will be treated, which is figured out from case 2.

2. If the attacker is a hacker group, and the target is an individual, with a large audience, like the flu, the country needs to be concerned, which is figured out from case 3.
3. If the target is a nation, even an individual, as was the case with SARS, the nation should launch a high-level response, which is figured out from case 1.

Therefore, the security responsibility of the state in cyberspace is mainly divided into four parts:

The first is national defense, mainly against overseas organized threats to the overall operation of China's Internet, critical infrastructure and national security.
The second is space governance, which takes safeguarding China's economic development as the starting point to handle and coordinate security incidents that damage the interests of a large range of users and affect the operation of key infrastructure.
The third is cyber diplomacy. We need to establish a broad transnational cooperation mechanism on cyber security to reflect our voice and influence in the world.
The fourth is comprehensive deterrence, to improve our own monitoring capabilities and build defensive tools and capabilities so that others will not dare or be able to attack us.
These are the four responsibilities of the state. Of course, the responsibility of the state needs to be borne by specific entities.
China has such a principle that whoever is in charge is responsible for it, who runs it and who accesses it. When a network security incident occurs, it occurs on which entity, who should be responsible for the specific.

The security responsibility of the private sector is mainly divided into four parts:

The first is network operation security protection.
Security level protection system, such as the determination of professional network security person in charge, standardized operation, the development of private sector internal network security management system, data classification, data backup encryption, strengthen the prevention of computer viruses and network attacks and other harmful network security behavior of technical measures. Network security incident emergency plan and security risk disposal, specifying that network operators shall formulate network security incident emergency plan and timely deal with security risks such as system vulnerabilities, computer viruses, network attacks and network intrusions. It is prohibited to engage in or assist in activities endangering cyber security.
The second is personal information protection.
To protect the legitimate rights and interests of citizens, the core of network security is personal information protection system. For example, it does not violate laws and administrative regulations or the agreement between the parties to collect and use personal information, and it deals with the personal information kept by the parties in accordance with regulations and the agreement of users. For example, the private sector does not illegally sell or provide personal information to others. For example, network operators collect and use personal information with the consent of those collected
The third is assistance and reporting.

For enterprises, network security law also involves a more important responsibility, is to assist and report responsibility. For example, when discovering security defects, loopholes and other risks in network products and services, it shall promptly report them to the relevant competent authorities. For example, when an incident occurs that endangers network security, it will be reported to relevant competent authorities in accordance with regulations. For example, the management of information posted by users should be strengthened to prevent improper comments from harming society. For example, it provides technical support and assistance to public security organs and state security organs in safeguarding national security and investigating crimes in accordance with the law.

Conclusion

To sum up, cybersecurity is a joint responsibility of the government and the private sector. There are also many problems in the overall environment of global network security. For example, in the manufacturing industry, it is difficult for many private sector enterprises to interact with national security departments.

In terms of academic research, the articles on network security around the world are more theoretical and less practical, lacking guidance and foresight. Taking the country as the theme, the government and the private sector can jointly shoulder the responsibility of network security. Advance may be attacked, retreat may be defended. To build a complete network ecosystem, the government, enterprises, organizations and individuals in cyberspace can form benign interactions, and the state and the private sector are the guarantee of peace.

Referencing and Bibliography

CASE 1

Streltsov, L. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. Eur J Secur Res 2, 147–184 (2017). https://doi.org/10.1007/s41125-017-0020-x

Katerynchuk, P. (2019). Challenges for Ukraine’s cyber security: National dimensions. Eastern Review (Łódź, Poland), 8, 137–147. https://doi.org/10.18778/1427-9657.08.05

McCrory, D. (2020). Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States. The RUSI Journal, 165(7), 34–44. https://doi.org/10.1080/03071847.2021.1888654

Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. European Journal for Security Research, 2(2), 147–184. https://doi.org/10.1007/s41125-017-0020-x

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. The Electricity Journal, 30(3), 30–35. https://doi.org/10.1016/j.tej.2017.02.006

The Working Group at the NCCC at the NSDC of Ukraine approved the draft cybersecurity strategy of Ukraine. National Security and Defense Council of Ukraine. (n.d.). Retrieved November 14, 2021, from https://www.rnbo.gov.ua/en/Diialnist/4838.html#:~:text=The%20purpose%20of%20the%20Cybersecurity,deterrence%2C%20cyber%20resilience%20and%20interaction.

Cyberberkut. (n.d.). Cyber Berkut: Кибер Беркут. rus. Retrieved November 14, 2021, from http://www.cyber-berkut.ru/en/index_02.php.

Alien removals under Operation Predator - Govinfo.gov. (n.d.). Retrieved November 14, 2021, from https://www.govinfo.gov/metadata/pkg/CHRG-108hhrg92347/mods.xml.

CASE 2

Charles Riley. (n.d.). Chinese internet hit by biggest cyberattack in its history. CNNMoney. Retrieved November 14, 2021, from https://money.cnn.com/2013/08/26/technology/china-cyberattacks/index.html.

Encyclopedia.com. (2021, November 14). " Gale encyclopedia of e-commerce. encyclopedia.com. 26 Oct. 2021 . Encyclopedia.com. Retrieved November 14, 2021, from https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/denial-service-attack.

Science Net news channel. (2013, September). Sciencenet - National Responsibility for Cyber Security. Retrieved November 14, 2021, from http://news.sciencenet.cn/sbhtmlnews/2013/9/278424.shtm.

CASE 3

Global, A. C. (n.d.). China: Weibo admits to leak of personal data on millions of users. Business & Human Rights Resource Centre. Retrieved November 14, 2021, from https://www.business-humanrights.org/en/latest-news/china-weibo-admits-to-leak-of-personal-data-on-millions-of-users/.

lrmax, M. from, Lrmax, Christopher Escobedo Hart | Nov 04, 03, S. C. | N., 28, E. B. | O., Michael Vizard | 1 day ago, & Richi Jennings | 1 day ago. (2020, April 13). Marriott Data Breach

2020: 5.2 Million guest records were stolen. Security Boulevard. Retrieved November 14, 2021, from https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/.

BBC. (2020, October 16). British Airways fined £20M over Data Breach. BBC News. Retrieved November 14, 2021, from https://www.bbc.com/news/technology-54568784.

The PRC Personal Information Protection Law (final): A full translation. China Briefing News. (2021, September 16). Retrieved November 14, 2021, from https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/.