**CYBER-ATTACK AS A NEW KIND OF PUBLIC EMERGENCY AND THE ISSUES OF CYBER GOVERNANCE IN VIETNAM**

**Mr. Nguyen Dinh Toan**

**Vietnam Administration of Seas and Islands**

**Email: dinhtoan78@gmail.com**

**Abstract:** Recently, along with the development of 4.0 technology, cyber-attacks have also become popular and had many hidden risks. This paper analyzes some case studies about cyber-attacks and illustrates ‘cyber-attack as a new kind of public emergency’. Following this, the paper offers some solutions for cyber governance in Vietnam**.**

**Keywords:** Cyber-attack,Public emergency, Cyber governance.

**1. Introduction**

Today, the rapid development of the Internet has a positive impact on economic development, education, health, culture and society. However, many people’s activities when using the Internet lead to risks, directly threatening national sovereignty, order and security, legitimate rights and interests of organizations and individuals. This phenomenon appears because the development of the Internet has created a ‘fertile ground’ for new types of criminals operating on the Internet, using social media as a means and tool to carry out personal schemes that are not only dark but also law-breaking behaviors, causing serious consequences to many aspects of the society. In particular, cyber-attacks target security, defense, economy and culture in many nations. With many sophisticated tricks, hackers use high technology to spread malicious codes to penetrate, and attack the state headquarters’ data system. At the same time, from negative and dark motives, some organizations and individuals thoroughly exploit social networks to fabricate, distort, slander, distribute fake news, etc. to poison, manipulate, do distract social spirit, causing economic damage. Facing that fact, protecting national security and protecting the rights and interests of people on cyberspace have been concerned and focused by many countries. This has also become a global issue.

There are many definitions of ‘cyber-attack’. According to Clarke and Knake (2010), cyber-war is “actions by a nation-state to penetrate another nation’s computers or networks to cause damage or disruption”. Similarly, Michael Hayden[[1]](#footnote-1) has spoken of cyber-war as the “deliberate attempt to disable or destroy another country’s computer networks” (Gjelten, 2010). However, some experts assert that there are no distinctions between the definition of cyber-war and the definitions of cyber-attack and cyber-crime (Hathaway et al., 2012).

The Shanghai Cooperation Organization has defined cyber-attacks as the inclusion of the use of cyber-technology to break political stability (Waxman, 2011). Furthermore, cyber-attack can be defined as an action that is performed with political or national security purposes to break the roles of a computer network (Hathaway et al., 2012).

In Vietnam, Clause 8 Article 2 of the Law on Cybersecurity 2018 regulates as following: “Cyber-attack is an act of using cyberspace, information technology or electronic means to sabotage or disrupt the operation of telecommunications networks, Internet networks, computer networks, information systems, or judgment systems, information management, databases, and electronic means”.

**2. Cyber-attack as a new kind of public emergency**

The first cyber-attack involved the Central Intelligence Agency (CIA) attacking a Soviet gas pipeline. In 1982, the CIA was accused of cyberattacks that disrupted a gas pipeline operation in Siberia. After that, the oil pipeline malfunctioned and exploded. Hacker groups can point to a specific military or civilian organization, probing for vulnerabilities, and armed attacks. Moreover, the Stuxnet attack devastated Iran's nuclear program, which was blamed on the United States and Israel. As a result, the decision to formalize the rules of cyber warfare is taken. Cyber-attacks are seen as a wake-up call and drive major changes in the way digital threats are handled (Leonard, T 2011). We have seen that the Organization for the Prohibition of Chemical Weapons had been affected by a recent cyber incident (Jabbari, 2018). Therefore, cyber-attacks have a strong influence on relationship between nations. It may cause armed conflicts. Some experts state that cyber-attacks should be considered as acts of war. Cyber-attacks are like armed attacks traditionally defined by war law (Hathaway et al., 2012).

Cyber-attacks are the cause of many crises of many companies in the world. It strikes the economy of companies. Some of them were bankrupted due to cyber-attacks. Additionally, due to cyber-attacks, there were many employees to lose their jobs.

Sony PlayStation Network (PSN) had to compensate users millions of dollars because of the cyber-attack. In April 2011, the PSN was launched by hackers. Multi-play gaming services, online games and other Sony contents were leaked. In which, there is personal information of 77 million players worldwide. Even the banking information of these accounts was compromised by hackers (Vnexpress, 2011). Immediately after the discovery of the incident, PSN as well as Sony Online Entertainment and Qriocity had to discontinue all services for about a month. To appease users, Sony had to be paid $ 15 million in compensation to affected people (Vnexpress, 2011).

Target - the second largest retail chain in the US, was the victim of a large-scale Internet attack in December 2013. Data of 110 million customers was stolen from November 27 to December 15. In which, up to 40 million customers have their information stolen (name, address, phone and email, bank account ...) and 70 million other customers have their information stolen almost completely (Kim Hung, 2014). More worrying, the agency that discovered the hacked Target was not Target. A security company in the United States accidentally discovered this, and at the same time they also discovered this group operated in Eastern Europe. The hackers stealthily installed malware on the victim's computer and then wrote down the credit card information. At the same time, they later offered $ 18 million in ransom for all of the data on black market websites (Kim Hung, 2014).

Cyber-attacks have influences not only the economy but also jobs. For instance, in November 2014, a Sony subsidiary, Sony Pictures Entertainment was attacked by a virus called ‘Guardians of Peace’. The damage was 100 terabytes (1TB equals 1000 GB), including important data that was stolen. The Internet attack by hackers this time took away many movie scripts, emails and personal data of 47,000 employees. Many employees were forced to quit their jobs because of the damage this time. In addition, Sony had to defer a few movies and pay up to $ 8 million in compensation to internal employees who were exposed (Dien San, 2014).

More importantly, Yahoo was bankrupted because of cyber-attacks. In 2014, Yahoo revealed that they had been subjected to an Internet attack affecting 500 million accounts. There is no need to argue much because they are not only hacked, but these accounts are also used to continue to deceive their relatives. Information such as name, date of birth, stolen cell phone caused a fever at that time. Regardless of Yahoo! Affirmed that the disclosure of this information would not affect the bank account but users of Yahoo decreased plunge (Ngoc Trang, 2016).

Before that, in 2012, the hacker group ‘Peace’ had sold 200 million user information with a password for $ 1900 on the Internet. The worst thing happened to Yahoo when they got hacked again, 32 million accounts affected, attackers used the same old method, hackers created malicious cookies on the Internet and login without Yahoo password (Bach Duong, 2016).

The sad ending when Yahoo! from a billion-dollar company sold himself for $ 4.5 million in 2017 to Verizon. In December 2018, Yahoo continued to admit that it had lost all 3 billion accounts to hackers in the past. This can be considered as the biggest attack in the history of the Internet (Truong Anh, 2016).

Cyber-attacks also attack the health of people and hospital’s systems. In 2017, an encrypted virus called WannaCry affected more than 230,000 computers globally. The National Health Service of the UK was affected. Following this, the Medical Service System was shut down, and ambulances must be rerouted. This is the UK's first time calling up an emergency committee caused by a cyberattack (Seattle Office of Emergency Management, n.d.).

Vietnam and Southeast Asian countries are considered to be dynamic countries with high growth rates of Internet applications but are also suffering heavy losses from criminal attacks network implementation (Dong A, 2020). Specifically, in October 2017, the leakage of personal information of 46 million mobile subscribers (related to home address, national identity card number, Sim card information, ...) in Malaysia poker has created a huge upheaval in community life. According to experts, this risk has been warned since 2014. However, when it occurs in practice, the danger level of the problem is fully recognized. In 2017 alone, Singapore suffered three major cyber-attacks, in which hackers attacked the entire network of the Ministry of Defense. In 2018, Singapore continued to suffer a lot of damage caused by cybercrime, typically hackers stealing personal information of 1.5 million people (Dong A, 2020)

In Vietnam, on October 30, 2016, the Department of Information Security (Ministry of Information and Communications) issued a coordination order requesting agencies, organizations and businesses to rush to scan and remove files. Large-scale targeted attack (APT) campaign targeting government agencies and key information infrastructure in Vietnam. More than 400,000 IP addresses were infected with more than 16 variants of the malware in this offensive (Dong A, 2020). According to a recent report by CyStack Company (operating in network security), in 2019, there were more than 560,000 attacks on websites globally, and Vietnam ranked 11th among countries with many websites being attacked in the world with more than 9,300 websites compromised. A series of such cases shows that protecting cybersecurity has become extremely urgent for all countries (Dong A, 2020)

Recently, cyber-attacks are becoming more frequent and sophisticated all over the world (Political Bureau of the Party Central Committee, 2018a). The nuclear centrifuges, air defense systems and electrical grids could be shut down. As a result, cyber-attacks could cause damages to national security (Hathaway et al., 2012). Additionally, cyber-attacks not only undermine valuable information but also cause economic losses (EKU, 2020). Cyber-attack can occur in anywhere, for example, banks, stores, hospitals, where have computer network. A cyber-attack destroys or disrupts the functionality of a computer network. Accordingly, the cyber-attack can be performed with whatever action that hackers desire, for example, bombing, cutting, infection, economic purpose (Hathaway et al., 2012).

In addition, cyber-attacks cause many consequences, for instance, scrambling financial records or incapacitating the stock market (Hollis, 2007), shutting off a nuclear reactor (Antolin-Jenkins, 2005), or opening a dam (Gellman, 2002), air traffic control system leading to plane crash (U.S. Government Accounting Office, 2013) and other physical and economic damages.

As a result, cyber-attacks are the infringements of national sovereignty on cyberspace, violations of national independence, autonomy, sovereignty and national interests on international information space.

Due to consequences that cause by cyber-attacks, we can see cyber-attacks are as new kind of public emergency.

**3. Legal framework for cyber governance and proposed network management in Vietnam**

**3. 1. International legal framework for cyber governance**

In September 2011, 47 member states of the Council of Europe released the ‘Declaration on Guiding Principle on Internet Governance’, of which the first principle is, “Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law. They must also ensure full respect for democracy and the rule of law and should promote sustainable development. All public and private actors should recognize and uphold human rights and fundamental freedoms in their operations and activities, as well as in the design of new technologies, services and applications.”

Cyberspace is borderless and thus, the clash of different cultures is almost unavoidable. Certainly, there is no absolute freedom. These are situations in which other human values need to be protected, possibly - case by case - justifying legal-based limitations. But such restrictions have to be imposed through the provisions of the law. But one thing we notice that restrictions have to be exceptions(Kleinwachter, 2012).

Recently, there are 138 countries in the world that have issued laws on cybersecurity, according to UN statistics. Notably, over the past six years, 23 countries have issued more than 40 legal documents and sub-laws on cybersecurity (Dong A, 2020). Although the names may differ from country to country, these laws have the common goals of creating a legal basis to protect the legitimate rights and interests of all citizens, as well as the activities of public authorities, organizations and businesses on the Internet environment. Simultaneously, along with the establishment of regulations that help regulate cyber-behavior, the laws also specify sanctions on cybersecurity breaches (Dong A 2020).

In the United States of America, the international strategy for cyberspace was published in May 2011. It consists of a set of activities across seven inter-dependent areas, including: Economy, Protecting networks, Law enforcement, Military, Internet governance, International development and Internet freedom (Schmidt, 2011).

According to the Government of Canada (2020), the cybersecurity strategy in this country was released in 2010, and it includes three pillars: (1) securing government systems: the roles and responsibilities are provided. Following this, the security of federal cyber systems is strengthened. Moreover, it enhances the awareness of cybersecurity throughout the government; (2) partnering to secure vital cyber systems outside the federal government: including a number of cooperative initiatives by actors; and (3) helping Canadians to be secure online: regulating cybercrime and citizenship privacy.

In May 2010, Japan published the cybersecurity strategy of Japan (NISC, 2018). It consists of three areas: (1) strengthening policies to deal with network attacks and establish a response organization; (2) establishing policies to adapt to changes in the information security environment; and (3) establishing active information security measures.

**3. 2. Legal framework for cyber governance in Vietnam**

In Vietnam, Law on Cybersecurity (regulating activities to protect national security and ensure social order and safety on cyberspace; responsibilities of relevant agencies, organizations and individuals) approved by the National Assembly on June 12, 2018, and effective from January 1, 2019. After one year of implementation, the Law has played an active role in implementing measures to protect network safety and security. In addition, that law prevents and handles violations of the law on cybersecurity promptly. In 2019, about 8,000 videos with malicious content, hundreds of fake accounts, thousands of sale links, illegal advertising were removed (Dong A, 2020). Many cases of using social networks to incite national hatred, calling for anti-government protests, distorting the lines, policies of the Party and State were discovered and handled appropriately. Awareness about cybersecurity of the people has gradually been raised. Moreover, the Law helps people daily access to healthy and useful information.

The above specific examples show that when the Law on Cybersecurity comes to life, it has played an important role in protecting the people’s legitimate rights, maintaining social order and protecting national security on the Internet environment. In order to continue to supplement and support the Law on Cybersecurity, on February 3, 2020, the Prime Minister signed to promulgate the Decree No. 15/2020/ND-CP (effective from April 15, 2020) that regulates on penalties for administrative violations in the fields of post, telecommunications, radio frequency, information technology and electronic transactions. Generally, along with the Law on Cybersecurity, the Decree will help promote the stronger role of the law on cybersecurity in detecting, preventing and handling violations on cyberspace. Following this, the most beneficiaries are people and agencies, organizations, businesses. It contributes to the protection of social order and safety.

However,Vietnam's information system still has many weaknesses and security gaps that are easy to be exploited, attacked, or penetrated. The fact is that disclosing and losing state secrets through the information system increased dramatically. The phenomenon of illegal exploitation and use of national databases and information resources and user personal data is complicated. Moreover, many new and modern services appeared, causing difficulties for the management and control of functional agencies (Le Van Thang, 2020). The above-mentioned fact has created many threats to information security of Vietnam. The hostile forces thoroughly used the information system to influence, intervene internally, steer policy, manipulate public opinion, infringes upon national independence and sovereignty on cyberspace, and waged information war against Vietnam (Political Bureau of the Party Central Committee, 2018b)[[2]](#footnote-2). Therefore, it can demonstrate that cyber-attacks are a new kind of public emergency in other countries and in Vietnam.

**3. 3. Recommend cyber governance in Vietnam**

To improve the effectiveness of information security in the coming time, it is necessary to pay attention to implement the following solutions synchronously:

***First,*** raising awareness about information security and ensuring information security (Political Bureau of the Party Central Committee, 2018c)[[3]](#footnote-3). It is important to be aware that information security is independence, sovereignty, national interests in the information space, safety, stable and strong development of the information field and the national information system. Information security is a central content of national security in the new condition, closely related to other traditional security issues such as internal political security, military security, and civil security as well as ideological, economic security, social security. The risk of information insecurity is a major and growing threat to national and international security. Therefore, ensuring information security is an important and regular task of the entire Party, the entire people, of the whole political system in which the People's Public Security Force is the core. To ensure information security, it is necessary to attach importance to and use synchronous measures of politics, law, science and technology, propaganda - education, organization - administration, economics, diplomacy and professional skills (Le Van Thang, 2020).

In the coming time, functional agencies should strengthen education, fostering and raising awareness of cadres, party members and the masses of the people; attach importance to propagating and disseminating to pupils and students about the dangers, insecurity factors, threats of information insecurity (Political Bureau of the Party Central Committee, 2018c)[[4]](#footnote-4). From there, raise awareness in using information services, especially services provided by foreign countries, improve political bravery, be able to recognize, receive information, self-defense, ‘immunity’ to fake and harmful information. The Ministry of Education and Training should build a plan to include content on identifying threats, factors causing information insecurity and responsibility for ensuring information security into the national education system, thereby educating awareness, responsibility, and raising awareness for the entire population on this issue.

***Second*,** establish national sovereignty in cyberspace, ensure to maintain national independence, autonomy, sovereignty and interests in international information space; effective protection and exploitation of national information resources (Political Bureau of the Party Central Committee, 2018a)[[5]](#footnote-5).

Vietnam needs to absorb international experience selectively, focus on research and establishment of national cyberspace (with infrastructure, services, legal framework) to early assert national ownership in cyberspace. Identify the constituent factors and promote solutions to effectively enforce national sovereignty on information space (Le Van Thang, 2020). Specifically, focuses should be on: (1) Developing hardware technology to ensure autonomy in means and equipment, especially the core network system, computers, telephones, information infrastructure; (2) Developing software technology to create its own software ecosystem, including: operating systems, search engines, social networks and Internet service applications. (3) Developing its own security technology and security inspection and monitoring system to proactively detect, prevent, and filter fake, bad and malicious information; (4) Building an integrated, interconnected and secure national database system (Big Data) to facilitate digital transformation and digital economic development; (5) Developing a modern, safe and responsible information communication and orientation system with its own offensive and defensive systems, especially the key information systems of the Party and State and in the security and defense fields; (6) Developing and perfecting institutions, policies, laws and service markets.

First of all, there should be a specific mechanism to focus resources to build on social networks, search engines, and Vietnam's own utility operating system that are compatible with the world and have a firm foothold in the free-market and in society (National Assembly of Vietnam, 2018). On the one hand, it affirms the national position, and ensures independence, autonomy and national sovereignty on cyberspace. Moreover, it limits dependence on foreign technology gradually. As a result, it improves security and autonomy in ensuring information security, ensuring national economic interests, facilitating the preservation and promotion of national cultural values, proactive in receiving information and facilitating in the Party and State's information and propaganda, effectively prevent bad and malicious information, increase the ability to ensure the privacy of users' personal information. At the same time, it is necessary to have a reasonable plan to exploit and protect the national information resources for socio-economic development, ensuring national defense and security (Le Van Thang, 2020).

***Third***, it needs to increase the Party’s leadership and direction, the centralized and unified management of the State, improve the effectiveness and efficiency of the state management on information security (National Assembly of Vietnam, 2018). Building and completing policies and laws on information security is focused (Political Bureau of the Party Central Committee, 2018b)[[6]](#footnote-6). Following this, it can create a legal environment to ensure safety and reliability for the digital economy, sharing digital data, and management of cross-border information service providers entering Vietnam (Le Van Thang, 2020). It needs to continue to develop laws to combat fake, bad and harmful information; personal information protection law. Additionally, it is necessary to build a mechanism to openly monitor, block and filter distorted and untrue information on cyberspace; regulate specifically and comply strictly with mandatory regulations on the use of real information when registering an account online. Moreover, it needs to build codes of conduct on cyberspace; regulations on the protection, inspection and use of national information resources and user personal data (Political Bureau of the Party Central Committee, 2018b).

***Fourth***, it is to ensure absolute security of important national information systems, important information systems for national security, improve defense capacity, and recovery from attacks on information systems. Additionally, it is to fight effectively against activities that violate cybersecurity by hostile forces and criminals (National Assembly of Vietnam, 2018)

The government needs to increase investment in modern infrastructure, the bandwidth that is wide enough to overcome congestion attacks, and have backup storage systems to redirect data against attacks and recover after a network attack (Le Van Thang, 2020). It needs to review regularly, detect and fix security gaps throughout the system, supplement specialized equipment and software capable of checking and controlling information security and safety in the telecommunications network environment, Internet, radio frequency. The government should develop and implement specialized technical solutions to inspect and detect risks of information insecurity. Importantly, the government should organize annual cyber-attack drills with the participation of government agencies, key economic groups, telecommunications and Internet service providers and agencies, relevant organizations, ensuring timely to handle threats causing insecurity and information insecurity in Vietnam.

It needs to focus on forecasting and implementing solutions to combat disabling: (1) activities of infringing information security of objects, especially attacks that paralyze national important information systems; (2) the intention to use artificial intelligence (Al) and big data to manipulate and incite public opinion and create conditions to promote the ‘color revolution’ in Vietnam; and (3) the conspiracy and intentions of hostile forces, hegemony to militarize information space, and launch information war on Vietnam (Political Bureau of the Party Central Committee, 2018b).

***Fifth****,* The government should focus the national resources on building and step by step developing the information technology industry, especially the information security industry (network security) of Vietnam (National Assembly of Vietnam, 2015).

With the current resources of Vietnam, it is necessary to focus on developing the information security industry in dual-use, combining the civil field with ensuring security and defense, public-private partners. The Vietnamese government should have a special mechanism to immediately implement short-cut and proactive solutions to step by step master and export information technology. Moreover, the government should encourage to research, develop and use Vietnam's own software and services to meet the information confidentiality requirements. Besides, the government should establish strong domestic information technology, telecommunications and Internet service providers, controlling the market, forming a force of service providers, capable of producing information security equipment by themselves.

The government should promulgate a mechanism to encourage, support and mobilize startups in cybersecurity technology startups, information technology enterprises, and domestic Internet and telecommunications service providers.

In the era of the industrial revolution 4.0, information security is increasingly becoming an important content of national security. Therefore, researching on information security and ensuring information security is always an urgent requirement today (Le Van Thang, 2020).

However, it is necessary to see that, in order for legal documents to play their role in reality, together with the participation of the political system, it is necessary for the cooperation and companionship of all people, as shown by consciously complying with the law when participating in social networks, be cautious before the unsubstantiated information, promptly detect signs of fraudulent or false information to warn the community, promptly report to authorities. It is a practical way for each person to protect themselves, contributing to protecting the healthy development of cyberspace, and protecting the peace and development of the country (Le Van Thang, 2020).

**References**

Antolin-Jenkins, V. (2005). Defining the parameters of cyberwar operations: Looking for law in all the wrong places?. *Naval L. Rev., 51*, 132-140.

Bach Duong. (2016). *Hacker rao bán 200 triệu tài khoản Yahoo! giá… 3 bitcoin [Hacker sold 200 million Yahoo! with price… 3 bitcoins]*. Retrieved October 2, 2020 from [https://khoahocphattrien.vn/cong-nghe/hacker-rao-ban-200-trieu-tai-khoan-yahoo!-gia-3-bitcoin/20160804111117550p1c859.htm](about:blank)

Clarke, R. A, & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins Publishers.

Dien San. (2014). *Hacker tấn công mạng máy tính hãng phim Sony [Hackers attacked Sony film studio computer networks]*. Retrieved October 2, 2020 from [http://antg.cand.com.vn/Khoa-hoc-Ky-thuat-hinh-su/Hacker-tan-cong-mang-may-tinh-hang-phim-Sony-334897/](about:blank)

Dong A. (2020). *Truyền thông, an ninh mạng và pháp luật [Communication, cybersecurity and legislation]*. Retrieved September 19, 2020 from [https://nhandan.com.vn/binh-luan-phe-phan/truyen-thong-an-ninh-mang-va-luat-phap-579963/](about:blank)

Gellman, B. (2002). *Cyber-attacks by Al Qaeda Feared: Terrorists at threshold of using Internet as tool of bloodshed, experts say*. Washington Post, June 27, 2002, at A1. Retrieved October 3, 2020 from [http://www.crime-research.org/library/Barton.htm](about:blank)

Gjelten, T. (2010). Extending the law of war to cyberspace. Retrieved September 19, 2020 from [http://www.npr.org/templates/story/story.php?storyId=130023318](about:blank), viewed.

The Government of Canada (2010). *Canada’s cyber security strategy: for a stronger and more prosperous Canada*. Retrieved September 19, 2020 from [http://publications.gc.ca/site/eng/379746/publication.html](about:blank)

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817-885.

Hollis, D. (2007). Why states need an international law for information operations. *Lewis & C Lark L. Rev., 11*,1023-1042.

EKU. (2020). *How to prepare emergency management for cyber-attacks*. Retrieved September 19, 2020 [https://safetymanagement.eku.edu/blog/emergency-management-for-cyber-attacks/](about:blank)

Jabbari, C. (2018). *The application of international law in cyberspace: State of play*. New York: Office for Disarmament Affairs, UN. Retrieved October 3, 2020 from [https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/](about:blank)

Kim Hung. (2014). *Ai đứng sau vụ đánh cắp dữ liệu Hãng Target? [Who was behind the Target Firm data theft?]*. Retrieved October 2, 2020 from [http://cadn.com.vn/news/135\_110604\_ai-dung-sau-vu-danh-cap-du-lieu-hang-target-.aspx](about:blank)

Kleinwachter, W. (2012). *Human right and Internet governance – MIND 4*. Berlin: Baku & Berlin.

Le Van Thang. (2020). *An ninh thông tin ở Việt Nam trong điều kiện hiện nay - Vấn đề đặt ra và giải pháp [Information security in Vietnam in current conditions - Problems and solutions]*. Retrieved September 19, 2020 from [https://snv.bacgiang.gov.vn/chi-tiet-tin-tuc/-/asset\_publisher/aRIn3er4plGA/content/an-ninh-thong-tin-o-viet-nam-trong-ieu-kien-hien-nay-van-e-at-ra-va-giai-phap](about:blank)

Leonard, T. (2011). *Cyber-attacks are an act of war: Pentagon to announce new rules of engagement against state sponsored hackers*. Daily Mail. Retrieved June 1, 2011 from [http://www.dailymail.co.uk/news/article-1392746/Cyber-attacks-act-war-Pentagon-issuenew-rules-hackers.html](about:blank)

National Assembly of Vietnam. (2015). *Luật An toàn thông tin mạng [Law on cyber information security]*. Hanoi.

National Assembly of Vietnam. (2018). *Luật An ninh mạng [Law on cybersecurity]*. Hanoi.

National Center of Incident readiness and Strategy for Cybersecurity (NISC). 2018. *Japan’s cyber security strategy*. Retrieved October 2, 2020 from [http://www.nisc.go.jp/eng](about:blank)

Ngoc Trang. (2016). *500 triệu người dùng Yahoo bị hackers tấn công [500 million Yahoo users were attacked by hackers]*. Retrieved October 2, 2020 from [http://thoibaotaichinhvietnam.vn/pages/quoc-te/2016-09-23/500-trieu-nguoi-dung-yahoo-bi-hackers-tan-cong-35921.aspx](about:blank)

Political Bureau of the Party Central Committee. (2018a). *Nghị quyết số 29-NQ/TW ngày 25/7/2018 về chiến lược bảo vệ tổ quốc trên không gian mạng [Resolution No. 29-NQ/TW dated July 25, 2018 on the strategy to protect the fatherland on cyberspace]*. Hanoi.

Political Bureau of the Party Central Committee. (2018b). *Nghị quyết số 30-NQ/TW ngày 25/7/2018 về chiến lược an ninh mạng quốc gia mạng [Resolution No. 30-NQ/TW dated July 25, 2018 on the national cybersecurity strategy]*. Hanoi.

Political Bureau of the Party Central Committee. (2018c). *Nghị quyết số 35-NQ/TW ngày 22/10/2018 về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới [Resolution No. 35-NQ/TW dated October 22, 2018 on strengthening the protection of the Party's ideological foundation, fight against wrong and hostile views in the new situation]*. Hanoi.

Schmidt, H. (2011). Launching the U.S. international strategy for cyberspace. Retrieved September 19, 2020 from [https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-usinternational-strategy-cyberspace](about:blank)

Seattle Office of Emergency Management. (n.d.). *Cyber-attack and disruption*. Retrieved September 19, 2020 from [https://www.seattle.gov/Documents/Departments/Emergency/PlansOEM/SHIVA/SHIVAv7.0-Cyber.pdf](about:blank)

Truong Anh. (2016). *Kết thúc một triều đại mang tên Yahoo và kế hoạch mới của Verizon [Ending a dynasty called Yahoo and new Verizon plans]*. Retrieved October 3, 2020 from [https://vietnamfinance.vn/ket-thuc-mot-trieu-dai-mang-ten-yahoo-va-ke-hoach-moi-cua-verizon-20160726142622039.htm](about:blank)

U.S. Government Accounting Office. (2013). Air traffic control: Weak computer security practices jeopardize flight safety. Grandview Heights, OH: BiblioGov.

Vnexpress. (2011). Mốc thời gian PlayStation Network bị tấn công và các lỗ hổng bảo mật [Timeline of PlayStation network hacks and security flaws]. Retrieved October 2, 2020 from [https://vnexpress.net/moc-thoi-gian-playstation-network-bi-tan-cong-va-cac-lo-hong-bao-mat-1544349.html](about:blank)

Waxman, C. (2011). Cyber-attacks and the use of force: Back to the future of article 2(4). *The Yale Journal of International Law, 36*(1), 421-458.

1. Former NSA and CIA director [↑](#footnote-ref-1)
2. Political Bureau of the Party Central Committee. (2018b). *Nghị quyết số 30-NQ/TW ngày 25/7/2018 về chiến lược an ninh mạng quốc gia mạng [Resolution No. 30-NQ/TW dated July 25, 2018 on the national cybersecurity strategy]*. [↑](#footnote-ref-2)
3. Political Bureau of the Party Central Committee. (2018c). *Nghị quyết số 35-NQ/TW ngày 22/10/2018 về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới [Resolution No. 35-NQ/TW dated October 22, 2018 on strengthening the protection of the Party's ideological foundation, fight against wrong and hostile views in the new situation]*. [↑](#footnote-ref-3)
4. Political Bureau of the Party Central Committee. (2018c*). Nghị quyết số 35-NQ/TW ngày 22/10/2018 về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới [Resolution No. 35-NQ/TW dated October 22, 2018 on strengthening the protection of the Party's ideological foundation, fight against wrong and hostile views in the new situation]*. [↑](#footnote-ref-4)
5. Political Bureau of the Party Central Committee. (2018a). *Nghị quyết số 29-NQ/TW ngày 25/7/2018 về Chiến lược bảo vệ Tổ quốc trên không gian mạng [Resolution No. 29-NQ/TW dated July 25, 2018 on the strategy to protect the fatherland on cyberspace]*. [↑](#footnote-ref-5)
6. Political Bureau of the Party Central Committee. (2018b). *Nghị quyết số 30-NQ/TW ngày 25/7/2018 về Chiến lược an ninh mạng quốc gia mạng [Resolution No. 30-NQ/TW dated July 25, 2018 on the National Cybersecurity Strategy]*. [↑](#footnote-ref-6)