Solutions to Proactively Prevent and Respond to Non-traditional Security Risks, Focusing on Ensuring Cybersecurity and Information Security in the Context of a Fast-moving World under the Impact of the Fourth Industrial Revolution

Assoc. Prof, Dr. Van Thanh NGUYEN

Abstract: *In the context of a fast-moving world under the influence of the 4.0 Industrial Revolution, non-traditional security issues have become destabilizing factors affecting national security, and also pose new challenges to regional and international peace and stability. United Nation statistics show non-traditional security is facing dozens of threats. In particular, there are issues that need special attention and effective solutions to proactively prevent and respond such as terrorism, drugs, hackers, environmental disasters, epidemics, human trafficking, illegal migration, especially violations of cyber sovereignty, cyber security, high-tech crime, etc. In this article, the solutions emphasized by the author include human resources, material resources, policies, especially technological solutions.*

Keywords: *industrial revolution 4.0, non-traditional security, cyberspace, network security.*

1. Impacts of the Fourth Industrial Revolution

Human history has undergone four industrial revolutions. The first Industrial Revolution in 1784, originated in Scotland, was characterized by mechanization with hydraulic machines and James Watt's invention of steam engine (announced in 1775), opened the era of mechanical production. Mankind transitioned from agricultural civilization to industrial civilization. The Second Industrial Revolution, originated in the USA from 1871 to 1914, was characterized by electric motors, transportation, chemistry, steel production and electro-mechanical production and moved to the automation stage. The Third Industrial Revolution also originated in the USA in 1969 with the advent of information technology (IT), using electronics and IT to automate production, catalyzed by semiconductors,

supercomputers, laptops (1970 and 1980), Internet (1990s). The Fourth Industrial Revolution (FIR) started from the German government's CNC project. This term was first used in 2011 at the Hannover Fair and officially recognized the concept and connotation at the 46th World Economic Forum (WEF), January 20, 2016.

The Fourth Industrial Revolution was characterized by the following aspects:

The breakthrough of science and technology based on digital technology platform that integrates "smart" technology to optimize production processes and methods, leveraged by AI (artificial intelligence); 3D printing technology, biotechnology, new materials, automation technology, Robotics, internet of things technology (IoT) and Internet of services (IoS). The characteristic of FIR is cyber-physical production systems (CPS), first introduced by Dr. Jame Truchat, CEO of National Instrument in 2006, in which smart devices work together over a wireless network or through the "cloud".

The scale of development is unprecedented in history, the growth is exponential, and the impact on the economy and the ecological environment is enormous. In order to reach 50 million users, it took the phone 75 years; 38 years for radio, 13 years for television, only 4 years for the Internet and 3.5 years for Facebook. Economically, it affects consumption, production, productivity and prices. The world economic map and the power map of businesses are also being re-established. For example, 3D printing technology is worth US$3.1 billion/year, an increase of 35% compared to 2012; increase of 32% on average to reach US$21 billion in 2020.

The impact of FIR's emerging technology on all aspects of social life. Digital technology IoT (internet of things) through a system of connection technologies and different platforms which is an integrated part of the future Internet that includes current and evolving Internet and network developments with a dynamic global network infrastructure based on physical and virtual "things" interoperability protocols using smart interfaces that are seamlessly integrated into the information network. IoT perspective includes: (i) IoE: Internet of energy; (ii) IoS: Internet of services; (iii) IoM: Internet of Mobility; (iv) IoP: Internet of people, (v) Io: Internet of things. IoT will change the way an economy operates, creating new business models. IoT will change the way an economy operates,

creating new production and business models. Hyper connectivity through IoT and cloud computing will enable the global and near-instant transfer of information and communication, creating previously unimaginable ways of delivering goods and services.

Artificial Intelligence (AI): A computer system that demonstrates behavior that requires intelligence (Smart). Classification: (i) Systems that think like humans (neural networks and cognitive architecture); (ii) The system acts like a human (automatic reasoning); (iii) Rational thinking system (reasoning, optimization); (iv) Rational action system (intelligent software, Robot achieves goals through cognition, planning, communication, decision and action). Four widespreads: (i) sensors everywhere, (ii) connection everywhere; (iii) data everywhere, (iv) service everywhere.

2. Non-traditional security: characteristics, risks and challenges

- Concepts of non-traditional security

Non-traditional security is a relatively new scientific concept in the field of security. Professor Mely Caballero Anthony, Secretary General of the Alliance of Research Institutions on non-traditional security in Asia (NTS-Asia), said that, in a broad sense, non-traditional security "refers to the shift away from the military and State focus of the traditional security model." NTS-Asia defines: "Non-traditional security issues are challenges to the survival and prosperity of people and states, arising mainly from non-military sources, such as terrorism, climate change, depleted resources, infectious diseases, natural disasters, illegal migration, food shortages, migrant smuggling, illegal drug trafficking and transnational crime. These dangers are often transnational in scope, defy unilateral remedies, and require a comprehensive response – political, economic, social, as well as the use of humanitarian military force".

At the 6th Summit of the countries of the Association of Southeast Asian Nations (ASEAN) and China on November 1, 2002, the phrase "non-traditional security" officially appeared in the "ASEAN – China Joint Declaration on cooperation in the field of non-traditional security" and unified in the awareness that: "non-traditional security issues such as illegal drug trafficking, human trafficking including trafficking of women and children, piracy, terrorism, arms smuggling, money laundering, international economic crimes and cybercrime, have become important

destabilizing factors, affecting regional and international security, and is posing new challenges to regional and international peace and stability."

In each specific field, traditional security issues and non-traditional security issues have mutual impact and are intertwined. However, it is necessary to be clearly aware of the differences in some key aspects between traditional security and non-traditional security as follows: Traditional security emphasizes ensuring national security by using military means. The main point is that political and diplomatic measures are only supportive. Non-traditional security measures are more diverse and mainly non-military in nature, with cooperation and coordinated action; promote economic development, progress and social justice, implement social security...

Traditional security is centered on national sovereignty, emphasizing on external threats. Non-traditional security is people-centered, emphasizing ensuring that each individual in the community enjoys basic rights and favorable conditions to develop their capabilities. Therefore, non-traditional security threats can come from both outside and inside, emphasizing threats from within each country.

Non-traditional security is the expansion of the concept of traditional security, the concepts of national security. In fact, non-traditional security issues have evolved or arisen for a long time, but now have new characteristics and are considered a new type of security threat such as terrorism, illegal immigration, lack of water resources, ecological environment, drug smuggling... are being globalized and networked with various methods and tactics, and the consequences are much more different than before.

Non-traditional security and traditional security under certain conditions can transform each other, typically ethnic minority issues, religious conflicts, economic crises... within a country can cross national borders and spread abroad, becoming a transnational, global problem, affecting the stability and security of other countries, other regions. In addition, non-traditional security and traditional security together impact and influence the development of security strategies and policies of each country to respond to their threats and challenges.

- Characteristics of non-traditional security:

There are a number of characteristics, including: (i) Non-traditional security is clearly transnational. (ii) Non-traditional security is non-governmental in nature, (iii) Non-traditional security relatively overlaps with

traditional security challenges; (iv) Non-traditional security is becoming global; (v) Non-traditional security is both violent and non-violent. The nature of violence has non-military characteristics such as terrorism, drug trafficking, transnational organized crime, and non-violent nature such as environmental pollution and worsened ecology issues, financial and currency crisis, epidemics, floods, natural disasters, resource depletion...

- Threats of non-traditional security

According to the United Nations, non-traditional security includes 10 threats: (1) terrorism, (2) drugs, (3) piracy, (4) money laundering, (5) hackers, (6) environmental disasters, (7) epidemics, (8) human trafficking, (9) illegal migration and (10) ethnic and religious extremism. Non-traditional security was then widely used and popularized in many international forums on political, security, defense, economic and social issues; in defense and security strategies of many countries and territories, as well as in regional and international security cooperation forums.

Some top risks threatening in the near future are forecasted as follows: (1) Extreme weather events (e.g. floods, storms, etc.); (2) Failure of mitigation and adaptation to climate change and sea level rise; (3) Major natural disasters (e.g. earthquakes, tsunamis, volcanic eruptions, geomagnetic storms); (4) Massive biodiversity loss and ecosystem collapse; (5) Ecological damage and disasters caused by humans; (6) Failure of climate change mitigation and adaptation; (7) Weapons of mass destruction; (8) Crisis of water and energy resources; (9) Human security (related to human rights) due to the development of AI (Artificial Intelligence).

The dangerous nature of non-traditional security threats is not only manifested to the extent of destruction and devastation to human life, but also poses many challenges to social stability, the survival of the whole community, the actual effectiveness of global cooperation and integration. It even raises military security concerns. Natural disasters, earthquakes, tsunamis, storms, floods, epidemics, depletion of natural resources... increasingly challenge the achievements of modern science, technology and human abilities and efforts. Terrorism, transnational crime, high-tech crime, financial problems, energy security, food security... are severely testing the operating capacity of governments and the stability of governments, political institutions and economies, including the richest and strongest economies, as well as the feasibility and sustainability of international links.

The connotation of the non-traditional security issue is "dynamic" and can continue to be expanded through time. It is not a coincidence that the way of raising the non-traditional issue among countries, regions and communities has certain differences. Identifying certain specific issues within the context of non-traditional security issues only has a relative meaning, on one hand, to serve the planning and development of security policies and strategies of the country and other bilateral and multilateral security commitments in international cooperation and association, on the other hand, to compare differences from traditional security issues of each country as well as each region and around the world.

3. Awareness of sovereignty and security in cyberspace

The concept of sovereignty appeared in 1648 by the Westphalian system which defined that states have sovereignty over their territories and internal affairs that other countries cannot intervene. The principle of sovereignty is closely linked to international law and is related to equality, therefore, each country is equal to each other according to international law and has no right to impose on any other country.

Regarding the concept of network security and cyberspace, the Cyber Security Law 2019 stipulates in Article 2 as follows:

(1) Cybersecurity is the assurance that activities in cyberspace do not harm national security, social order and safety, and the legitimate rights and interests of agencies, organizations, and individuals.

(2) Cyber security protection means to prevent, detect, stop, and handle cyber security violations.

(3) Cyberspace is the connecting network of information technology infrastructure, including telecommunications networks, Internet networks, computer networks, information systems, information processing and control systems, and databases; is a place where people perform social behaviors that are not limited by space and time.

(4) National cyberspace is cyberspace that is established, managed and controlled by the Government.

Physically and technically, "cyberspace" has three layers: Physical transmission infrastructure includes information technology hardware devices that are logically connected to each other, creating different types of networks; core service infrastructure and services that create protocols for storing, processing, and exchanging information, mainly including standard

regulations, operating systems, platform technologies such as software technology, network technology, interfaces, communication methods, protocols, information processing transmission, control... application software with the creation of shared libraries and services; information technology application system and database, application software so that digital information is created, stored, processed and exchanged to serve life's needs and impact people's awareness.

Regarding social nature, "cyberspace" is a special human social environment that converges all 6 elements: (1) policies and laws; (2) technological capacity; (3) information content; (4) human resources; (5) organizational structure; (6) human consciousness in cyberspace, creating a special human social environment.

In particular, policies and laws are regulations and codes of conduct that regulate behavior and relationships between individuals, organizations, state management agencies, countries, and international organizations when participating in cyberspace. It creates a legal corridor to ensure the safe and effective operation of cyberspace, paving the way for technology development.

Technological capacity is applied technology and the ability to research and develop new technology for information technology infrastructure, software, services, etc., which constitute cyberspace, including all types of base technology such as network technology, electronic technology, semiconductors, microprocessors, software technology... In addition, there are also technology standard regulations, communication methods and interfaces between layers of a certain technology.

From a theoretical perspective, since 1994, some international scholars have mentioned the relationship between cyberspace and national sovereignty or the relevance of applying theories in international relations to the Internet. The rapid development of science - technology and the Internet is accompanied by the emergence of issues of safety, information security, network security, network espionage, risk of conflict, and cyber war between countries in international relations. These issues pose requirements for managing and protecting territory and national interests in cyberspace, also commonly understood in the term "space sovereignty". There are many opinions that national sovereignty exists in cyberspace because of the existence of essential infrastructure for cyberspace to form

and cyberspace sovereignty can be considered an extension of territorial rules in sovereignty.

From a practical perspective, at the global level, the 2003 Declaration of Principles of the World Summit on the Information Society (WSIS) articulated that policy authority on public policy issues related to the Internet belongs to the sovereign right of nations. The reports of the United Nations Group of Governmental Experts (UNGGE) in 2013 and 2015 emphasized that state sovereignty and international norms and laws originating from sovereignty apply to the state's conduct of activities related to information and communication technology; the principle of sovereignty is the basis for enhancing security in the use of information and communications technology by countries.

Regarding cyberspace sovereignty in Vietnam, from a theoretical perspective, since 2014, the Party and State of Vietnam have issued many documents addressing the issue of "ensuring sovereignty and national security" on the basis of content on risks and measures to ensure safety, security, and protection of national secrets in cyberspace, such as Documents of the 13th Party Congress, Resolution No. 29-NQ/TW, July 25, 2018 of the Politburo, 12th tenure on "Strategy to protect the Fatherland in cyberspace"; Resolution No. 30-NQ/TW, dated July 25, 2018 of the Politburo on "National Cyber Security Strategy", etc. It can be seen that the Party's resolutions and directives, as well as the State's legal regulations all agree on the guiding viewpoint on ensuring information safety and security and protecting national sovereignty in cyberspace.

4. Threats to cyberspace today

Currently, the security situation in cyberspace and high-tech crimes in the world and in Vietnam is complicated. In aviation security, the number of cyber attacks targeting aviation information systems has tended to increase in frequency, scale and complexity. According to the European Aviation Safety Agency (EASA), on average each month there are about 1,000 cybersecurity incidents in the aviation sector worldwide. According to the survey results report of cybersecurity company Immuniweb in 2020, up to 97% of the world's top 100 airports have not met cybersecurity testing requirements, vulnerable to cyber-attack. From 2019 to 2020, the number of cyber attacks on airlines increased by 530%, of which in 2020, there were 755 cyber attacks on airlines, 150 attacks on airports; mainly

to steal personal and credit information for fraud, extortion, and property appropriation. Details are as follows:

(1) In January 2016, the hacker group "Babylon APT" posted ads on the online black market, selling information about security holes in the network systems of a series of major airlines in the world such as Delta Airlines, United Airlines, Japan Airlines…;

(2) In early August 2016, the computer network system of Delta Airlines in the US "had a serious network problem", the airline's flight information display system was disrupted and had to perform procedures for passengers manually, causing delays of nearly 3,000 flights and cancels of more than 740 flights worldwide, with an estimated material damage of nearly 100 million USD in 3 days of service disruption;

(3) In September 2019, aircraft manufacturer Airbus confirmed that it had suffered many cyber attacks and illegal intrusion into its network system;

(4) In November 2020, Brazilian aircraft manufacturer Embraer was encrypted and demanded ransom;

(5) In February 2021, hackers attacked the International Aviation Telecommunications Company (SITA) stealing customer personal data...

More dangerously, some hacker groups supported by foreign governments conduct cyber attacks on airlines and airports of other countries with the aim of sabotaging and influencing politics, diplomacy, economy. Most recently, there was a cyber attack on the information system of the Russian Federal Air Transport Agency (Rosaviatsia) in March 2022 that deleted more than 65 Terabytes of data and made Rosaviatsia 's website inaccessible for a period of time.

Overall, cyber security challenges include:

Firstly, cyberspace attacks sabotage and cause disruption of information technology infrastructure systems, activities of agencies, organizations and individuals. The attack targets are important information systems such as e-Government; road and air traffic control systems, electricity and water supply, and high-tech agricultural control systems; airports, railway stations, ports, banks...

According to the 2017 Global Information Security Index Report of the International Telecommunications Union (ITU) of the United Nations, Vietnam ranked 120 out of 193 countries in the world, 10 out of 11 Southeast

Asian countries, 23 out of 29 countries in the Asia-Pacific region in terms of capacity to ensure network information security. (This result is based on locating the IP addresses that launch the attacks. In some cases, the IP addresses used by hackers may be proxy addresses to hide their actual location).

Second, cyber attacks target the databases of agencies, organizations, and large economic corporations to collect and steal information and data. In July 2016, Vietnam Airline's website was also attacked by hackers and consequently a lot of customers' personal information was exposed. On March 8, 9, and 10, 2017, hackers attacked and changed the website interface of Tan Son Nhat International Airport, Da Nang, Phu Quoc, and Rach Gia.

Third, attacks aimed at taking control of computers and digital devices, illegally accessing information technology systems of agencies, organizations and businesses, gaining remote control and changing the interface websites or databases... to blackmail or discredit these organizations. The information network system of our country's aviation industry has also been a top target of cyber attacks and terrorism.

Fourth, taking advantage of Internet connection, there are emerging such crimes as frauds to appropriate property through multi-level business and e-commerce activities are emerging; fraud and theft in card and electronic payment activities; theft, buying and selling credit card information to appropriate property; gambling and organizing gambling via the Internet; theft of social network user accounts to fraudulently appropriate property; propagating and distributing depraved publications, organizing prostitution brokerage, and distributing depraved photos and private images to humiliate others.

Fifth, high technology crimes are increasingly causing great damage to the development of each country and around the world. According to forecasts of the Vietnam Computer Emergency Response Center (VNCERT), the trend of exploiting and attacking IOT devices such as cameras and smart TVs is one of 5 cyber attack trends.

5. Solutions to proactively ensure the cyber security in the current context

5.1. General solutions

Firstly, perfecting and enhancing the capacity to ensure safety, network security and national network information for agencies, departments,

branches and localities, key infrastructure projects with network connections and important economic corporations

(1) Completing the information infrastructure system and information technology equipment to ensure network security and safety and national network information for central and local agencies; key infrastructure projects and important economic corporations with network connections. Nationally important information systems are identified and appropriate, continuous protection measures are applied from the design, construction, development, operation and use stages. (2) Concentrating the entire society's resources in ensuring network safety and security and national network information. (3) The State ensures funding for safety, network security and national network information.

Second, building a healthy cyberspace environment. Awareness and capacity to ensure safety, cyber security and national cyber information of the entire society are enhanced. Users have basic knowledge about security in the network environment; regularly update the situation and level of information security risks to be able to effectively prevent themselves. The information network system ensures security standards.

Domestic information technology enterprises are strong, dominate the market, and are not dependent on foreign products. The mainstream press plays a key role in shaping public opinion to be able to resist bad and toxic information in cyberspace.

Mobilizing the strength of the entire political system and the entire population in the fight to counter false information and anti-propaganda rhetoric in cyberspace.

Third, building a specialized force capable of proactively dealing with all risks occurring in cyberspace. A specialized force to ensure information security and national cyberspace security under the Ministry of Public Security; a force performing defense tasks in cyberspace under the Ministry of National Defense; an information security force under the Ministry of Information and Communications that are capable, ready, and proactive in dealing with all risks occurring in cyberspace.

Fourth, international cooperation in the fields of ensuring safety, information security, and network security is expanded and strengthened: (1) Expanding international cooperation with countries around the world to ensure safety and security of national networks and network information,

enlist the support of the international community to fight against the false allegations of hostile forces against Vietnam. (2) Participating in international conventions and agreements on ensuring safety and security of national networks and network information, preventing and combating cybercrime in accordance with the guidelines, guidelines, policies and laws of the Government, Party, and State. (3) Effectively and practically deploying protocols and cooperation agreements on cybercrime prevention signed with other countries.

5.2. Specific solutions

Data encryption: For important and intimate information, users should encrypt before sending. The purpose of encrypting information is to avoid attacks of hackers.

Updating software: One of the effective solutions to avoid losing information is to install software. Users should install and regularly update anti-virus software, attack warning software, system monitoring software...

Installing anti-virus software: Installing anti-virus software is also a solution recommended by experts. Users should scan for viruses before downloading software to their devices. Some online tools help check online malware such as: virus total, 6scan security, sitecheck.

Using software of clear origin: Ensuring that all software and applications on the user's device have a clear origin will help limit the risk of information insecurity.

Controlling permissions on the device: Clearly divide permissions to members and relatives on the device that the user owns.

Turning off Wifi, Bluetooth, and NFC connections when not in use: Remember that after accessing the network, users must turn off Wifi, Bluetooth, and NFC connections to avoid the risk of passwords, documents, and personal information being leaked./.