Science and Technology Trends
Governance Systems for Cybersecurity

Cybersecurity Governance Framework in Vietnam: State of Play, Progress and Future Prospects

Candice Trân Dai

1. Introduction

Vietnam has made tremendous progress over the past decades in the field of Information and Communication Technology (ICT). The country moved fast and emerged as a dynamic player in the global ICT landscape. It has become an attractive location for IT outsourcing and ICT hardware production as well as one of the fastest growing digital economies in the world. With a total population of 94,93 million, the Internet penetration rate in Vietnam has reached 53% and the E-commerce rate penetration is to date 35% (We are social, 2017), both statistics showing that the country enjoys plenty of scope for further development in this area. Since the country was connected to the global Internet network in 1997, and especially at the turn of the Millennium, it has embarked on the path of an accelerated and relatively comprehensive development of the ICT sector, largely driven and supported by a proactive governmental policy.

Vietnam appears to be a very good example of a country that has chosen a proactive ICT development strategy that is reflected not only by the tangible dynamism of the Vietnamese information society and by the strong enthusiasm of the Vietnamese population for new digital tools, products and services but also consequently by the growing exposure of the country to cyber threats. In the case of Vietnam, cyber threats are internal as well as external in the sense that the country faces malicious acts in cyberspace from its territory but also directed from outside. According to data from collaborative platforms of IT security specialists and reports from companies specializing in information systems security, which monitor and produce statistics on malicious activities in cyberspace on a global scale, Vietnam's situation is as follows: the country belongs to the top ten countries in the world with the highest malware encounter and infection rates (Microsoft, 2016) for January-June 2016 period, it ranks third in the top 25 countries in the world with the highest number of suspected botnet[1] IPs for the year 2016 (Daily Botnet Statistics, 2017), it reaches the fourth place among the top 5 countries for spam sending, and the third place among the top 5 countries for

Asia Center, Maison de la Recherche de l'INALCO 2 rue de Lille 75007 Paris, France
E-mail: C.TranDai@centreasia.eu

1 A botnet is a set of compromised computers, often referred to as "zombies", infected with malicious software, which allows an attacker to control them.

dictionary[2] attacks (Project Honey Pot, 2017). Noteworthy progress has been made regarding the overall cybersecurity situation of Vietnam in recent years, as shown by the results of Vietnam's Information Security Index performed by the Vietnam Information Security Association (VNISA) with the country reaching 59.9 per cent for the year 2016 as compared to 47.4 percent in 2015, 39 percent in 2014 and 37.3 percent in 2013. Nevertheless, Vietnam has to cope with an increasing number of cyber incidents[3].

While Vietnam nurtures strong ambition to reach its digital potential, it faces several obstacles and challenges to achieve its goals. Besides the need for further improvement of overall IT infrastructures to support the growing digital economy, or the need to further expand advancement in reducing the digital divide within the country, one of the important key factors in driving digital advancement lies in digital confidence. How much users trust digital products and services can be either a growth enabler or a significant impediment with regards to the digital economy. The stakes are high because the country remains extremely vulnerable and permeable to cyber attacks and cybercrimes, which could eventually affect the development potential of the ICT sector in the country and contravene the strong ambitions of the Vietnamese government in this field. This is particularly critical as Vietnam considers ICT as a strategic lever for economic development and as the country strives for reaching the next level of digital maturity by leveraging on digital transformation and digital innovation. In the context of great exposure to cyber threats, the Vietnamese authorities have been thriving in recent years to tackle cybersecurity gaps in the country. The issue of cybersecurity has thus become a top priority for the Vietnamese government, which is well aware of the country's weak capacity in this area and the fact that the systems in place, whether organizational, regulatory or technical, do not offer sufficient and adequate protection against malicious acts in cyberspace.

This paper aims at reflecting the progress accomplished by Vietnam in dealing with the issue of cybersecurity by highlighting the formulation of cybersecurity policy and strategy in the making, implementation and work in progress so far, as well as challenges and opportunities.

2. Policy and Strategy

It is only in recent years that Vietnam has undertaken to take better control of the country's vulnerability in cyberspace and to enhance the country's cybersecurity capability. The first landmark initiative regarding cybersecurity in the country dates back to the year 2010 with the release of a dedicated government roadmap, i.e. the Prime Minister's Decision No. 63/QĐ-TTg of January 13, 2010 ratifying the "Digital Information Security Development Project to 2020", with a planned investment of USD 42 million between 2010 and 2020.

Previous initiatives in this domain were all but scattered and area-focused: they did not encompass a holistic policy and strategy although they did include various cybersecurity aspects. We may for instance refer to the various decrees and laws that were passed at the beginning of the 2000s such as, among others: Decree No. 26/2007/ ND-CP of February 15, 2007 detailing the implementation of the Law on Electronic Transactions regarding digital

2 The attack of passwords by dictionary is a form of attack directed against passwords in clear, not against the encryption of passwords. The attacker is trying words that actually exist in a dictionary. This method is based on the fact that many people use common words for their passwords.

3 According to Vietnam Computer Emergency Response Team (VNCERT), the number of cyberattacks of all sorts in Vietnam for the year 2016 increased four fold as compared to 2015.

signatures and digital signature certification services; Decree No. 90/2008/ND-CP dated August 13, 2008 on Anti-spam ("Decree 90")[4]; Decree No. 64/2007/ND-CP dated April 10, 2007 on the application of information technology in the operation of State agencies; Decree No. 73/2007/ND-CP dated May 8, 2007 on the research, production, trading and use of crypto codes to protect information not falling within the scope of State secrets; the Law No. 51/2005/QH11 of November 29, 2005 on E-transactions, the Law No. 67/2006/QH11 of June 29, 2006 on information technology.

2.1. Digital Information Security Development Project 2010-2020

The "Digital Information Security Development Project to 2020" issued in 2010 sets forth Vietnam's overall objectives in the field of cybersecurity to be achieved by 2020 into a breakdown of four main areas: ensuring network security and information infrastructure so that they are in line with the needs of ICT development; ensuring the safety of data and information technology applications so that they comply with safety standards; training certified cybersecurity specialists and raising public awareness on information security; and improving the legal framework for information security and computer-related crime. The document further details the objectives to be attained during the period 2010-2015 such as: ensuring the security of national information infrastructures, which encompasses security techniques and equipment provision for internal networks of public institutions and national databases; building information security surveillance and alarm systems; ensuring the security of databases and applications of ICT in public institutions from central to local level as well as in the private sector, with the objective of 100% of government websites of all levels having effective solutions against security incidents as well as emergency plans in case of incident and 100% of electronic transactions platforms having taken measures to ensure the security of information; assuring the training of human resources, with the objective of issuing national certificates for 80% of administrators of important information systems of the government and effective training of one thousand cybersecurity professionals according to international standards; and improving the legal environment, especially regarding computer crime and encryption.

The 2010 roadmap also highlights the need to "improve mechanisms and government policies on information security", to "build and strengthen institutions in the field of information security", to "encourage and support the development of local information security products" and to "promote cooperation at home and abroad". Regarding the development of local cybersecurity products, the document focuses on investment and support for R&D of products, solutions and service models to complement imported cybersecurity products together with the support of local cybersecurity businesses as well as R&D and exploitation of open source technologies. As far as international cooperation is concerned, the document stresses the importance of sharing and exchanging information between countries not only at regional level but also at global level. It also calls for the reinforcement of cooperation between the various national institutions involved in cybersecurity.

2.2. Network Information Security Plan 2016-2020

Further to the "Digital Information Security Development Project to 2020", the Prime Minister's Decision No. 898/QĐ-TTg of May 27, 2016 ratifying the "Network Information Security Plan 2016-2020" provides for more specific tasks to be achieved during the period 2016-2020. Compared to the previous

4 This Decree had been amended by Decree No. 77/2012/ND-CP ("Decree 77") issued on October 5, 2012.

intermediate roadmap, which brought out rather basic and broad objectives, this second 5-year roadmap introduces additional features and highlights some current priorities. The new guidelines that have been emphasized revolve primarily around the following areas: reinforcement of the cooperation with the private sector and the role of Vietnamese companies in the domestic information security market; and enhancement of critical information systems security and cyber resilience capacity. There is clearly a call to the private sector, and especially the main associations representing the IT sector in Vietnam, such as the Vietnam Information Security Association, the Vietnam Software and IT Services Association, the Vietnam Association for Information Processing, the Vietnam Internet Association and the Vietnam E-commerce Association, to play an active and leading role in boosting the country's cybersecurity capability. Vietnamese companies, especially ICT and Internet operators, are hence expected to take all appropriate and effective measures to reinforce the protection of critical information infrastructures and to coordinate with the Ministry of Information and Communications (MIC) in this regard. The roadmap advocates the support to investment, training and development of human resources for small and medium enterprises operating in the field of cybersecurity. Moreover, Vietnamese companies are encouraged to foster R&D, production and supply of cybersecurity solutions, products and services. On this point, the Network Information Security Plan 2016-2020 sets out a target of "developing at least five Vietnamese brand name information security products widely used in the domestic market" by 2020. The Ministry of Science and Technology (MOST) shall play a preeminent role in funding and supporting market development of domestic cybersecurity solutions.

The roadmap highlights the task of ensuring the security of national important information systems and information systems of government agencies by insisting on cyber resilience and business continuity. It further emphasizes the objective of upgrading general information security awareness in the country by increasing awareness campaigns, expanding cybersecurity training and drills, as well as enhancing government agencies officials' awareness and training. Further to that, the roadmap introduces the idea of establishing a network of cybersecurity experts to support and advise the competent authorities regarding protection of the national information framework. The stress is also being laid on the need to "update the system of national standards and technical regulations relating to information security" and to "establish a framework model of network information security management system in accordance with international practices". In this domain, evaluation and assessment of information systems security management are to be carried out on a regular basis. It is worth mentioning that the roadmap sets a goal of "putting Vietnam out of the list of 20 countries with the highest rate of malware and spam spreading in the world". As mentioned before, Vietnam belongs to the world top countries for malware encounter and infection rates, suspected botnet IPs, spam sending, and dictionary attacks. Consequently, the country suffers from a bad reputation in this area and this may impact the overall digital attractiveness of the country. There is therefore a need to preserve trust in Vietnam's digital economy. In this respect, we may note that the roadmap highlights the objective of promoting the application of digital signatures. In line with the previous 5-year roadmap, the Network Information Security Plan 2016-2020 additionally reasserts the promotion of national and international cooperation in the field of cybersecurity, including with domestic and foreign enterprises.

2.3. Emergency Response Plan to Secure National Network Information Security

While the "Digital Information Security Development Project 2010-2020" and the "Network information security plan 2016-2020" outline various guidelines and objectives to enhance Vietnam's cybersecurity capability, the Vietnamese policy-makers have also come up with more practical policy and strategy documents which tend to reflect an increasing awareness and stronger engagement regarding cybersecurity issues.

The Prime Minister's Decision No. 05/2017/QĐ-TTg of March 16, 2017, ratifying the "System of emergency and rescue plan to ensure the safety of the national information network", is a very good example of this evolving policy approach as it provides for an emergency response in case of serious cybersecurity incidents impacting national networks. The plan aims at addressing serious network security issues which fall under specific conditions and meet distinct criteria. Firstly, the information system subject to security incident must have been classified as a level 4 or level 5 information system[5] or it must have been included in the list of national important information systems. Secondly, the information system subject to security incident must have encountered one of the following problems: system services are interrupted; confidential data or State secrets are likely to be disclosed; integrity of important data of the system is not guaranteed and not recoverable; system control is lost; or the incident is likely to occur on a large scale or cause chain effects, compromising other level 4 or level 5 information systems. Thirdly, the management of the information system is not able to control and handle the problem. The emergency response plan further details the procedures for security incidents report, serious cybersecurity incidents remediation as well as initial rescue plan deployment and emergency rescue plan implementation.

Regarding organization and management, a National Steering Committee for Emergency Response will be established with the task of directing the Ministry of Information and Communications, the Ministry of Public Security (MPS), the Ministry of Defense (MOD) and other concerned ministries, branches and localities in emergency rescue work to ensure security of the national network. The Ministry of Information and Communications is the standing body assisting the National Steering Committee for Emergency Response. It is to decide on the rescue options and assume the prime responsibility for, and direct the urgent rescue work to ensure the security of the national information network; to direct the Vietnam Computer Emergency Response Team (VNCERT) to receive, collect and process information and reports on cybersecurity incidents and propose rescue plans. The VNCERT shall remain the National Coordination Unit for Emergency Response and is part of the National Emergency Response Team together with the Authority of Information Security of the Ministry of Information and Communications; the Network Security Department, the High-Tech Police Department for Prevention and Combat against High-tech Crimes of the Ministry of Public Security; the Department of Information Technology, General Staff Department of the Ministry of Defense; as well as with a number of units specialized in responding to network security incidents of ministries, ministerial-level agencies, government-attached agencies, provincial-level People's Committees, telecommunications and Internet enterprises.

Besides the National Emergency Response Team, the emergency plan stresses the compulsory

5 According to Decree No. 85/2016/ND-CP dated July 1, 2016, of the Government on the security of information systems by classification, the classification of the country's information systems comprises 5 levels, of which level 4 and level 5 concern the most critical ones regarding Defense systems, security systems, e-government systems, information infrastructure systems and industrial control systems.

participation of a certain number of organizations to the National network information security rescue network, which comprises notably the Vietnam Internet Network Information Center (VNNIC), the Central Post Office, enterprises providing Internet and telecommunications infrastructure services; organizations and enterprises providing data center services and leasing of digital information storage space; organizations managing and operating national databases; and organizations and enterprises managing and operating important information systems and industrial control systems in the fields of energy, industry, health, natural resources and environment.

The "Emergency response plan to secure national network information security" appears to be very ambitious as it aims at endowing the country with a multidisciplinary incident response team, coordinated at national level and capable of mobilizing various relevant organizations, both in the public and the private sectors, and according to specific procedures and deployment schemes. It shall be noted that additional organizations may join the National network information security rescue network on a voluntary basis, providing they bring out relevant cybersecurity capabilities. It is worth mentioning that the Ministry of Information and Communications is also tasked "to act as the principal body or to designate a coordinating agency acting as the national focal point in coordination with functional units of other countries or international organizations in responding to and handling inter-country incidents". This point is quite important as cyber incidents are very often transnational by nature and require international cooperation and coordination.

3. Implementation and Work in Progress

Vietnam's cybersecurity roadmap implementation is currently based on three main pillars: the first pillar covers the area of institutional framework for cybersecurity, the second pillar concentrates on the legal architecture for cybersecurity and the third pillar focuses on the training and development of human resources specialized in cybersecurity.

3.1. Institutional Framework

Vietnam has embarked in recent years on the reorganization of its institutional framework for cybersecurity, which is reflected not only by the creation of new dedicated organizational units, but also by the search for better coordination of governmental agencies dealing with cybersecurity at national level. The three major governmental agencies in charge of cybersecurity in Vietnam are the Ministry of Information and Communications, the Ministry of Public Security and the Ministry of Defense.

The Ministry of Information and Communications has one dedicated authority, the Authority of Information Security (AIS), and two dedicated units, the Vietnam Computer Emergency Response Team (VNCERT) and the National Electronic Authentication Center (NEAC), which constitute its outpost for cybersecurity. The AIS, which was formally established following the Decision of the Ministry of Information and Communications No. 1281/QĐ-BTTTT of September 9, 2014, officially took office in October 2014. The main functions of the AIS are as follows[6]: "formulation of laws, regulations and policies relating to information security; implementation of technical and procedural measures; guiding and supporting governmental agencies and other organizations to enhance and protect their information systems; giving out early

6 Source: Ministry of Information and Communications.

warning regarding information security; ordinating activities on preventing SPAM in Vietnam; monitoring and inspecting the protection activities regarding information security; evaluating information security level in organizations and critical information infrastructures; raising awareness; improving capacity; cooperating with international organizations". The Vietnam Computer Emergency Response Team (VNCERT), which was established under the Prime Minister's Decision No. 339/2005/QĐ-TTg of December 20, 2005, has had its functions, tasks and organizational structure redefined by the Decision No.1778/QĐ-BTTTT dated 26 October 2015. As an operational cybersecurity unit, although the VNCERT is primarily in charge of monitoring, warning, coordination and rescue, it has also been playing an active and leading role in the formulation of legal documents relating to cybersecurity, as well as regarding cooperation with foreign CERTs counterparts, promoting and coordinating incident response activities nationwide, or participating to the elaboration of technical standards. VNCERT is a multifaceted operational unit, whose role may be upgraded as its scope of intervention has gained prominence in recent years and as its perimeter of action has expanded. Like the VNCERT, the National Electronic Authentication Center (NEAC) is a specialized unit placed under the supervision of the Ministry of Information and Communications. Following Prime Minister's Decision No. 1592/QĐ-TTg of September 9, 2014, NEAC officially took office in December 2014. It is primarily contributing to the strengthening of the institutional architecture for electronic transactions, including authentication of digital signatures and electronic authentication by building and implementing a national Public Key Infrastructure (PKI) plan in Vietnam that will be the foundation for its National Electronic Authentication Framework (NEAF). The goal is to build a nationwide infrastructure for effectively securing electronic transactions and securing trust in e-commerce and e-government.

The Ministry of Public Security has three main entities dedicated to cybersecurity and information security: the Department of Network Security (referred to as "A68") and the Department of Information Security and Communications (referred to as "A87") which both depend on the General Department of Security of the Ministry of Public Security; and the Police Department for Prevention and Fight against High-tech Crime (referred to as "C50") which is supervised by the General Department of Police. The Department of Network Security, which was officially established rather recently, i.e. after the announcement on August 28, 2014 by the Ministry of Public Security, oversees the management and administration of information systems security and cybersecurity. The Department of Information Security and Communications is focusing on contents control and management, including for instance illegal sale of personal data online. As for the Department for Prevention and Fight against High-tech Crime, it is specialized in the fight against cyber criminality, including for instance online fraud and financial crime.

The Ministry of Defense has two main entities focusing on cybersecurity, the Information Technology Department and the Government Cipher Committee. The Information Technology Department is placed under direct supervision of the Joint General Staff of the People's Army of Vietnam; it oversees IT and secure electronic information management. The Government Cipher Committee is a specialized unit placed under direct supervision of the Minister of Defense. It is responsible for State management of encryption communications and networks; strategy, policies and legal documents regarding encryption; as well as research, development, production, importation and use of encryption solutions and products.

While new institutional entities dedicated to cybersecurity are being created or reorganized, the need for better coordination between the various government agencies responsible for cybersecurity has also been taken into account. On this matter, we may note that the Ministry of Information and Communications introduced in 2014 a proposal related to the coordination of government action on the issue of cybersecurity. The idea was to provide for the modalities and scope of coordination of the action of the Ministry of Information and Communications, the Ministry of Public Security and the Ministry of Defense.

3.2. Legal Framework

Improving the legal framework for data protection, information security and the prevention and punishment of computer-related crime constitute the second pillar of Vietnam's cybersecurity roadmap. While the country's overall regulatory architecture for cybersecurity had long been insufficient, the Vietnamese government has been particularly active on that front in recent years. There has been an abundance of new and re-drafted regulations; several pieces of legislation have already been implemented while other regulations are in the making and being drafted.

Among the main recent texts that ought to have a major impact on the local context of cybersecurity, the Law on Network Information Security is undoubtedly a fundamental text. The Law No. 86/2015/QH13 on Network Information Security was passed on November 19, 2015 by the National Assembly and took effect on July 1, 2016[7]. It is the first dedicated law in Vietnam regarding cybersecurity. In essence, the Law on Network Information Security contains provisions, which address cybersecurity, information systems security, personal data security and contents security. It should be noted that this approach is part of a vision of the issue of cybersecurity from the perspective of information security, meaning that a political distinction is made between the notions of "information security" and "information systems security". For the Vietnamese regime, as for other states in the world, such as China and Russia, cybersecurity policy is inseparable from the concept of information security. It therefore refers to informational content of which information and communication technologies are the vectors and which are envisaged as a source of potential threat to political stability. The apprehension of the issue of cybersecurity thus goes far beyond the purely technological dimension. This policy approach is well reflected by Article 3 of the Law which introduces several definitions such as "network information security" being defined as "the protection of network information and information systems against any illegal access, use, disclosure, interruption, amendment or sabotage in order to ensure the integrity, confidentiality and availability of information". The Law on Network Information Security aims at being a foundational policy and regulatory document for the country's overall cybersecurity strategy. Key aspects of the Law include assurances for four building blocks, i.e. "network information protection", "protection of personal information", "information system protection" and "prevention of network information conflicts"; as well as regulatory frameworks for "civil cryptography", "standards and norms of network information security", "network information security business", "human resource development for network information security" and "state management of network information security".

Among the key new developments brought out by the Law, we may note visible efforts towards

7 English translation of the Law is available on the Ministry of Information and Communications Website: http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf

the introduction of a unified law regulating data privacy, which was previously addressed within various laws and decrees including the Law on E-Transactions, the Law on Information Technology, the Law on Protection of Consumer Rights, Decree No. 52/2013/NĐ-CP on E-Commerce and Decree No. 72/2013/NĐ-CP on Management, Provision and Use of Internet Services and Online Information, or the Civil Code. Together with the Decree No. 85/2016 / ND-CP of July 1, 2016, on "Safety Information System by Level", which provides details regarding criteria, competence, order and procedures for determining security levels of information systems and for ensuring the security of information systems for each level, we may also note that the Law on Network Information Security recalls the current new existing framework of five distinct levels according to the potential damage and impact on production, public benefits, social order and safety, national defense and security. Additionally, the Law provides for a whole new set of regulatory frameworks regarding civil cryptographic products focusing on trading in civil encryption products, procedures to get business licenses for trading in civil cryptographic products and services, importation and exportation of civil cryptographic products, responsibilities of companies trading in civil cryptographic products and services, responsibility of organizations, individuals using civil cryptographic products and services. Furthermore, the Law details the regulatory framework regarding businesses providing network information security products and services including business license and permit procedures for trading in network information security products and services. Section 4 of the Law entitled "Prevention of Network Information Conflicts" is quite short, very broad and rather vague as compared to other sections of the document, especially as it is mentioned that the government will have to provide further details regarding "responsibilities of organizations and individuals in prevention of network information conflicts" as well as "prevention of network use for the purpose of terrorism". This section is nevertheless quite interesting as it aims at addressing other dimensions of cyberspace which relate more to strategic aspects of cybersecurity. This shows at least that the Vietnamese authorities are considering those aspects as well and that additional output may be expected.

The Law on Network Information Security appears to be a clear engagement towards codifying the regulations on cybersecurity, especially as previous regulations had been scattered throughout different pieces of more general legislation. As it appears throughout the document, additional documents and regulatory inputs are in the making in order to further clarify the scope, applicability and responsibility regarding several aspects of the Law. Apart from the Law on Network Information Security, several regulatory measures have been introduced in recent years, in particular Decree No. 25/2014/NĐ-CP of April 7, 2014, on the "Provisions on preventing and combatting crimes and other violations of the law which use high-tech". The decree provides in particular a whole set of measures applicable in the event of the detection of a high-tech crime and specifically intended for research and investigation. It has to be put in perspective with the ongoing process of reviewing the country's new Penal Code, which was initially scheduled to come into force on July 1, 2016[8], and which shall include criminal penalties for violations relating to cybersecurity and for cybercrime acts. In addition to these specific regulations, it shall be reminded that Vietnam has been continuously working on improving the security of electronic transactions and is conducting further efforts regarding electronic payments and card-based payments.

8 The National Assembly has issued a resolution to delay the implementation of the revised Penal Code.

3.3. Human Resources Development

The third main pillar, which underpins the Vietnamese government's roadmap on digital information security by 2020, focuses on the training and development of human resources specialized in cybersecurity. The Prime Minister's decision No. 99/QĐ-TTg of January,14, 2014, ratifying the plan "Training and development of human resources for information security to 2020", also called "Project 99", constitutes the cornerstone of the Vietnamese government's strategy in this area. By 2020, Vietnam has set out the following objectives: training of 2000 graduates at bachelor's and higher levels; sending 300 teachers and researchers for training abroad, including 100 people at Ph.D. level; sending 1500 cybersecurity personnel for short-term training abroad; organization of short-term cybersecurity training for 10,000 cybersecurity officers in public institutions. It also involves the ongoing training of 2,000 cybersecurity personnel in government agencies of strategic importance. To ensure the training of cybersecurity specialists, Vietnam has decided to encourage the opening of ad hoc specialties in the universities of the country, which is accompanied by a policy of encouragement and incentives for the development of enrollment of students in courses offering specializations in information and communication technologies and cybersecurity. The emphasis is also placed on monitoring the quality of the training provided, in the context of a desire to upgrade the curriculum. Some of the leading institutions in this area include FPT private university (FPT University), which is part of the Vietnamese ICT firm FPT, and the Posts and Telecommunications Institute of Technology (PTIT), which is supervised by the Ministry of Information and Communications. Several Vietnamese universities had previously initiated computer security training courses, but they did not offer full dedicated degree courses, and rather combined them with courses in computer science and information systems. It is expected that no fewer than eight key institutions will integrate "Project 99" to train cybersecurity specialists through dedicated curricula.

Additionally, it is worth mentioning that the Vietnamese authorities have engaged in upgrading the general awareness of the Vietnamese population regarding cybersecurity. The Prime Minister's Decision No. 893/QĐ-TTg of June 19, 2015, on "Approving the project on communication, discipline, awareness and responsibility for information security to 2020" highlights the various means by which the country is expected to raise general cybersecurity awareness, with a particular emphasis on the youth, encompassing for instance educational materials on information security to be integrated into informatics and extracurricular activities from junior to senior high school; information security contests to be organized for different target groups of students of universities, colleges, professional secondary schools; as well as the mobilization of traditional and online media on covering the topic of cybersecurity and developing and broadcasting dedicated awareness programs. This initiative is quite interesting and particularly welcome as it reflects the crucial necessity to raise the Vietnamese population cybersecurity awareness and knowledge level[9]. So far, the objectives of the new cybersecurity awareness roadmap to 2020 appear to be quite ambitious and include notably the following: less than 50% of information security incidents occur because of poor awareness of cybersecurity risks; more than 80% of civil servants, officials and officials of state agencies and organizations are educated about basic habits, responsibilities and skills to ensure information security when using information technology; more than 80% of officials and employees of enterprises

9 According to the ESET Vietnam Cyber-Savviness Report 2015, "When compared with other Asia-Pacific markets, Vietnam comes in last in terms of cyber-savviness behind Malaysia, Singapore, India, Thailand, Hong Kong and Indonesia, in that order."

providing telecommunication and information technology services are educated about cybersecurity risks and procedures for rescue coordinating and troubleshooting; over 50% of users in general, over 60% of high school students and over 70% of university students are educated about the basic risks and skills relating to cybersecurity.

4. Conclusion

As Vietnam has embarked upon the daunting task of revamping and upgrading its cybersecurity policy and strategy with a clear and tangible acceleration in recent years, especially since the last four years, it is facing a challenging work as far as implementation is concerned. As a matter of fact, while strategy and planning documents provide for guidelines and broad outlines, the decisive part of the work concerns the operationalization of the policy framework. In reality, a well-designed policy does not automatically imply successful implementation. This is even more critical when it comes to cybersecurity.

There is no doubt that Vietnam has made positive progress in addressing the issue of cybersecurity by working out the conception of a national cybersecurity governance framework throughout several policy and legal documents. The key determinant of success will rest upon effective coordination of all stakeholders, further clarification on legal aspects and continuous evaluation and assessment of cybersecurity policies. It is worth mentioning that the Vietnamese government tends to have a much more proactive position towards the role of the private sector in the field of cybersecurity and that closer and better coordination with private companies, especially those involved in the ICT and digital sectors, has been emphasized in most recent policy documents. Furthermore, economic and business aspects of cybersecurity are well taken into account as it is shown by support to R&D&I and expansion of the domestic information security market. Regarding legal aspects, the Law on Network Information Security would need further details and sub-legislation guidelines, especially regarding more precise scope of applicability as well as more precise compliance requirements. The issue of civil cryptographic products is bound to pose some challenges for businesses but also for individuals, therefore clear compliance and application requirements ought to be further defined, so as to keep balance between security and privacy. More generally speaking, how new cybersecurity and information security rules may be interpreted or enforced require further developments. As to operationalization of cybersecurity policies, it shall be implemented in a dynamic way that reflects the evolution of the cyber threats landscape. As future cyber risks and threats are evolving, there is a need on the part of policy-makers to focus on regulatory and administrative flexibility together with the design of a set of relevant standards, whether technical or non-technical.

As mentioned before, one very welcome and positive initiative is the Prime Minister's Decision on "Approving the project on communication, discipline, awareness and responsibility for information security to 2020", which shows that cybersecurity-related education and training has become a priority for the Vietnamese government. As far as cybersecurity is concerned, the technology side is indeed only one part of the equation, the human side remains of utmost importance. In any new endeavor, and especially regarding cybersecurity, resistance to change remains a fundamental human characteristic, which may act as a hindrance towards enhancing awareness and responsibility. Beyond cybersecurity awareness, there is also a need for cybersecurity literacy, i.e. an actual and practical understanding of cybersecurity and a culture of information security

that becomes part of an organization mindset, whether public or private. Simply put, ICT&D and cybersecurity shall no longer be apprehended as distinct issues.

In the case of Vietnam, the challenge is also that of a developing country, which must combine the promotion of ICT and the development of its digital economy with the security of information systems and the structuring of a cybersecurity policy and strategy, while composing with a lower investment capacity than that of more industrialized countries in this domain and other competing priorities. Vietnam has therefore very clearly chosen an active policy of international cooperation, not only with other countries in the Asia-Pacific region but also with countries in other regions of the world. In this respect, it may be noted that most of the policy and legal documents relating to cybersecurity include a section dedicated to international cooperation. Whether bilateral or multilateral cooperation, Vietnam has been engaged for several years in a collaborative approach to the issue of cybersecurity. There is a clear opportunity for Vietnam to benefit from the experience and expertise of the most advanced countries in this field so as to take advantage of best practices and avoid many pitfalls.

What could be described as a cybersecurity "new deal" in Vietnam has been clearly nurtured by notorious cyber incidents in recent years in the country, which undoubtedly acted as wake-up calls. Additionally, it should be more generally understood as a political will to preserve and consolidate the development potential of the ICT&D sector in the country, the objectives being that "information and communication technologies serve as an important driving force, helping to ensure the country's growth and sustainable development"[10] and that they act as "an important driving force for stimulating the development of the knowledge-based economy and for improving national competitiveness in the process of international integration"[11].

References

Daily Botnet Statistics (2017), Botnet Statistics for the year of 2016. Retrieved from <http://botnet-tracker.blogspot.fr/2017/01/botnet-statistics-for-year-of-2016.html>

ESET (2015), Vietnam Cyber-Savviness Report 2015: Cybersecurity, User Knowledge, Behaviour and Attitudes in Vietnam. Retrieved from <https://static1.esetstatic.com/fileadmin/Images/INT/Press/2015/2015-12-22/ESET_Vietnam_Cyber_Savviness_Report_Dec_2015.pdf>

Microsoft (2016), Microsoft Security Intelligence Report (SIR), Volume 21 | January through June 2016. Retrieved from <https://www.microsoft.com/security/sir/default.aspx>

Ministry of Information and Communications (2014). Vietnam ICT White Book 2014, Information and Communications Publishing House.

Project Honey Pot (2017), Project Statistics. Retrieved from <https://www.projecthoneypot.org/statistics.php>

Tran Dai C. (2014). La cybersécurité : talon d'Achille du Vietnam dans le domaine des TIC, Les Grands Dossiers de Diplomatie n° 23, Géopolitique du cyberespace, enjeux mondiaux, pp.54-57.

Tran Dai C. (2015). La cybersécurité au Vietnam : formulation et mise en œuvre d'une nouvelle stratégie, Hérodote n°157, Les enjeux géopolitiques du Viêt Nam, pp. 126-140.

Vietnam Internet Network Information Center (2014). Report on Vietnam Internet Resources 2014, Vietnam Internet Network Information Center.

We are social (2017), Digital in 2017: Southeast Asia. Retrieved from <https://wearesocial.com /blog/2017/ 02/ digital-southeast-asia-2017>

10 Decision of the Prime Minister No. 1755/QD-TTg of September 22, 2010, on the "Plan to make Vietnam a country strong in information and communication technologies".

11 Resolution No. 36-NQ / TW dated July 1st, 2014 of the Politburo on the "Application and development of IT and communications to 2030".