CYBERSECURITY MAINTENANCE IN VIETNAM IN 4.0 ERA

Van-Thang LE, Phuong-Lan NGUYEN, Quoc-Dung NGO
People Security's Academy of VietNam

Abstract: The rapid growth of Industry 4.0, especially the development of Internet of Things (IoT) is leading a unprecedented revolution in the cyber-physical systems and has brought rich utilities to users. It is envisaged that the number of interconnected devices will exceed 50 billion by 2020 [1], with an estimate of about 8 devices per person. Such an enormous amount will deeply impact our digital lives in many application domains, for example, transportation, healthcare, smarthome, smartcity, medical and healthy equipment, energy management, etc. In this perspective, at least 30 cities and provinces such as Hanoi, Ho Chi Minh City, Da Nang…are looking forward to turning themselves into smart cities [2]. Therefore, the IoT is becoming increasingly popular as a powerful tool of cybercriminals. According to Gartner analysts, 25% of cyberattacks will have involved IoT devices by 2020 [3]. In this paper, we present the Vietnamese vision and the People Security's Academy efforts in order to prevent the cybersecurity problems in Vietnam in the 4.0 era.

Keywords: Cybersecurity, Vietnam, 4.0 era, People Security's Academy of VietNam.

I. INTRODUCTION

The digital transformation following the Industrial Revolution 4.0 is taking place strongly in Vietnam, affecting all areas of life. On the one hand, the Industrial Revolution 4.0, a fusion of digital, physical and biological technologies, the internet of things and artificial intelligence, has a strong impact on production, making a sharp change in production methods. To take advantage of this Revolution, Vietnam is now striving for sustainable development on the basis of improving growth quality, to increase labour productivity and competitiveness to move up in the global value chain. However, on the other hand, the ability to connect infinitely in the digital era is posing challenges to cybersecurity. Every day, the world has to face to thousands of cyber-attacks. The

number of cyber-attacks has grown steadily and rapidly during the last few years. Damage from these attacks amounted to trillions of dollars due to data theft or attacks aimed at critical systems.

In Vietnam, cybersecurity issues are in an alarming state. A series of targeted attacks on the airport system, banks, websites are typical evidence. Cybersecurity threats in Vietnam are currently focusing on 4 types, including denial of service, phishing (information theft fraud), deface and malware. In recent years, these threats target on organizations, individuals, banks to steal sensitive information and also to extort. Besides, with the evolution of technology, information systems are faced with new threat stemming from artificial intelligence platforms.

Particularly in 2016, 7.000 websites/web portals were attacked in Vietnam. A lot of devices connected with the Internet are exposed to security vulnerabilities that lead to the risk, allowing hackers to exploit and escalate privilege. On 29 July 2016, a hacker group launched an attack on the website of Vietnam Airlines with client information leaked and on-flight information screens at Vietnam's 2 biggest airports [4], Tan Son Nhat International Airport and Noi Bai International Airport. Independent security expert Nguyen Hong Phuc said the hackers had shared three links leading to files that contain personal data of over 400,000 members of Vietnam Airlines' frequent passengers club, Golden Lotus. According to Mr. Phuc, this information may have fallen into the hands of the hackers four days before the attack.

The hackers also targeted at the financial sector. Typically, in August 2016, a customer of Vietcombank, one of the biggest banks in Vietnam, lost more than 22.000 USD via Internet Banking transaction. On the next day, Viecombank's shares fell by VND 150,000 ($6.7 USD) per share to VND 54,500 ($2.45) per share at the end of the session. The bank's market capitalisation therefore fell by VND 4 trillion ($180 million). After that incident, the bank has made significant changes to its online banking policies in order to prevent similar incidents. According to the top online security firm BKAV, cyber-attacks including the rise of ransomware cost Vietnamese users VND12.3 trillion or more than $542.8 million in 2017. This year saw strong attacks from

ransomware and malware containing cryptocurrency mining tools, causing losses that were more than 18% up from 2016. More than 1,900 computers in Vietnam were infected by the global WannaCry attack in May. WannaCry is a ransomware, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. Meanwhile, a cryptocurrency mining malware which appeared on Facebook has infected more than 23,000 computers in Vietnam. As cryptocurrencies became popular worldwide, hackers were prompted to launch attacks on computers to turn them into mining tools.

In 2018, the damage caused by computer viruses to Vietnamese users reached a record of VND 14,900 billion, equivalent to US $642 million, 18% more than the damage of 2017. According to Bkav's research, more than 60% of agencies and enterprises in Vietnam are infected with malicious code. The main reason is that agencies and enterprises have not yet equipped with comprehensive antivirus solutions for all computers in the intranet. Therefore, as long as a computer on the network is infected with malicious code, all the other computers on the same network will be attacked and infected. In addition to slowing down the machine, the Cryptocurrency-Mining Malware also has the ability to update and download other malicious codes to erase data, steal personal information or even perform APT attacks.

About 2 decades ago, the terminology “Internet of Things” occurred and, nowadays, became one of the most important pillars of the Industry 4.0. According to the International Telecommunication Union [5], Internet of Things is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies. In a Cisco’s report, more than 50 billion devices will be communicating with each other by 2020 [1]. IoT devices deliver substantial benefits to end users, but also bring unprecedented security challenges. IoT devices typically possess low processing capabilities, limited memory and storage and minimal

network protocol support. It is a significant challenge to design complex and comprehensive security measures. Using these weaknesses, in 2016, the first wave of IoT device attacks brought down the Internet. The Mirai Botnet hacked into some Internet of Things devices - in this case mainly routers and Internet Protocol (IP) cameras - and transformed the devices into botnets. The centrally-controlled IoT botnets flooded Dyn's, a Domain Name Services (DNS) provider [6], traffic causing a disruptive bottleneck that blocked Internet access for millions of users worldwide. Overall, IP addresses of Mirai-infected devices were spotted in 164 countries, such as Brazil, Vietnam, China [7].

COUNTRY	% OF MIRAI BOTNET IPS
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Table 1: Top countries of origin of Mirai DDoS attacks

Nowadays, Vietnam has about 350,000 IoT devices on the internet including mostly routers and IP cameras. According to The Vietnam Information Security Association (VNISA), more than 50% of those might be affected by information security loopholes [8]. In the context of 4.0 era, these IoT devices open tremendous opportunities for a large number of novel applications that promise to improve the quality of our life. However, in parallel with the development of IoT technology, there exists security issues of information leaking, disruption to operation or, in some scenarios, even loss of life when anything can be a spy device to collect information and interact

with users anytime, anywhere. Moreover, Vietnam's Prime Minister Nguyen Xuan Phuc has approved the sustainable smart city development plan for the 2018-2025 period and beyond towards 2030 [9] with a view to improving the livelihood of city residents. At least 30 cities and provinces such as Hanoi, Ho Chi Minh City, Da Nang…are looking forward to turning themselves into smart cities. Therefore, securing IoT devices has become a big challenge not only for Vietnam's government but also for all nations in the world. Before presenting our research to deal with IoT device security issue, the next section presents an overview of Vietnam's cybersecurity protection measures.

II. VIETNAM CYBERSECURITY PROTECTION MEASURES

Vietnam's Cybersecurity protection measures are based on three main factors that are policies, human and techniques.

Human factor is incorporated in any system and has a strong impact on the operation of that system. There are three main actors that we can mention which are: system administrator who is responsible for the configuration and reliable operation of information system, system operator who is responsible for the running of information system and ensuring that the system operates properly, user who utilize the resources provided by information system such as computer, network etc. Generally, the user lacks the technical expertise, the importance of the data, software, system within an organization and required knowledge to prevent cyber-attacks. Somehow, the user could be considered as an "Insider threat" or the weakest point. Indeed, when a cyber-attack happened, most of the time the breach is caused due to an employee's misjudgement, carelessness or simply lack of knowledge. To minimize the cyber-attacks consequences caused by human factor, companies, organization have to continuously educate and build detailed guidelines for their employees to follow.

Since 2014, the Vietnamese Prime Minister has issued the decision No. 99/ QĐ-TTg approving the plan "Training and development of human resources for information security to

2020", abbreviated as "Project 99". According to the project, by 2020, Vietnam has set out the following objectives: sending 300 teachers, researchers for training cybersecurity abroad including 100 PhD level; 2,000 graduates at bachelor's and higher levels with cybersecurity major; 1,500 trainees and 10,000 government officers for cybersecurity short-term training. To ensure these objectives, eight key universities including People's Security Academy (PSA) were chosen to open a new speciality focusing on information technologies and cybersecurity. To encourage these universities, 22 million USD, not including the abroad education, was granted for equipping cutting-edge cybersecurity devices and labs.

Additionally, The Prime Minister's has also issued the Decision No. 893/QD-TTg dated June 19, 2015 on "Approving the project on communication, discipline, awareness and responsibility for information security to 2020" to mainly promote the general awareness of the Vietnamese population regarding cybersecurity. There are many contests and educational materials integrated into informatics and extracurricular activities from junior to senior high school. These initiatives have attracted a lot of young people's attention as well as teachers and professional secondary schools.

Policy factor reflect the legal frameworks such as laws, decrees, circulars, guidelines, procedures related to the development of cybersecurity regulations. These frameworks may not be exhaustively address to all national or international cybersecurity aspect, but it provides important practical guides for organizations, companies and cyberspace users to promote the confidentiality, integrity and availability of public and private information, systems and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security. In recent years, cybersecurity risks and cyber-crimes pose more and more serious threats to nations in the world, therefore, legal frameworks are becoming more necessary than ever. In the last decade, developed countries such as Canada, Belgium, France, Germany, Italy, United Kingdom, United States of America etc. have introduced

their national legal framework in which they mention clearly measures to protect cybersecurity in terms of national security.

In this perspective, Vietnam has introduced numerous Laws, decrees and circulars that could be mentioned as follows:

- Law of E-transactions, 51/2005/QH11, promulgating 29/11/2005
- Law of Information Technology 67/2006/QH11, promulgating 12/07/2006
- Decree No. 26/2007/ND-CP of February, 15th, 2007 detailing the implementation of the Law on e-transactions of digital signatures and digital signature certification service;
- Decree No. 27/2007/ND-CP of February, 2nd, 2007 on e-transactions in financial activities;
- Decree No. 90/2008/ND-CP of August, 13th, 2008 on anti-spamming;
- Law of Network information security of November, 19, 2015 providing regulations on network information security activities, rights and responsibilities of organizations, companies and individuals in securing network information security, civil cryptography and government management in network information security. This one took effect on July, 1, 2016 and made an important contribution to ensuring network information security.

However, this Law has not met requirements caused by complex changes of cybersecurity in terms of national security. Therefore, the Law of Cybersecurity was approved by the National Assembly on June 12, 2018 and took effect on January 1, 2019. Compared to the Law of Network Information Security of November 19, 2015, the Law of Cybersecurity, has 7 chapters and 34 articles, clearly defines the important following points:

- Defining acts of violating national security on cyberspace.
- Specifying the organization who has the responsibility for handling cybersecurity attacks.
- Determining standards and technical regulations on cybersecurity.
- Determining measures for cybersecurity protection as follows:
    + Cybersecurity evaluation;

+ Cybersecurity condition evaluation;

+ Cybersecurity verification;

+ Cybersecurity monitoring;

+ Cybersecurity incidents responding and troubleshooting;

+ Cryptography;

+ Preventing, suspending the telecommunication and internet services in accordance with law;

+ Requesting to remove illegal or not truth information in cyberspace that violate national security, social order and safety, legitimate rights and interest of people and facilities;

+ Collecting data that violate national security, social order and safety, legitimate rights and interest of people and facilities in cybersecurity;

+ Blockage and limiting the operation of information system; suspending or withdrawing the information system operation, domain names according to Law;

+ Prosecuting, investigating cases according to Criminal Procedure Law;

+ Other measure according to the national security law and the administrative violation law.

Technical factor is the use of cybersecurity devices such as firewall, virtual private network (VPN), intrusion detection/prevention system (IDS/IPS), antivirus (AV) …; defense models such as defense in depth, centralized defense model…, cryptography algorithms such as private-key, public-key algorithms to ensure three components of the CIA triad referring to Confidentiality, Integrity and Availability.

The Vietnamese government considered this factor the most important measure in ensuring cybersecurity. There were a lot of key projects at national level scheme backed and funded by government toward production of important cybersecurity devices such as firewall, virtual private

network (VPN), intrusion detection/prevention system (IDS/IPS), anti-malware (AV) …. In general, these projects are carried out by a group of experts including researchers and industrial experts and gave promising results. Otherwise, key domestic organizations and corporations such as VNPT Corporation [10], Viettel Corporation [11], BKAV Corporation [12], Vietnam Cyberspace Security Technology JSC (VNCS) [13] and so on have invested huge amounts to develop cybersecurity products.

In this perspective, People Security's Academy (PSA) has cooperated with Vietnam Posts and Telecommunications Group, commonly abbreviated as VNPT, to develop an adequate solution to protect IoT devices in using Artificial Intelligence and Big Data. The objective of this cooperation is to protect about 200.000 IoT devices produced by VNPT against cyber-attacks. This is also the main contribution of PSA to prevent the cybersecurity problems in Vietnam in the 4.0 era. Next section presents PSA A.I Toolkit, a beta version for monitoring IoT devices for VNPT.

III. IOT DEVICE PROTECTION WITH PSA A.I TOOLKIT

According to Cisco, there will be about 50 billion IoT connected devices worldwide by 2020. Such an enormous amount will deeply impact our digital lives in many application domains, for example, transportation, healthcare, smarthome, smartcity, medical and healthy equipment, energy management, etc.

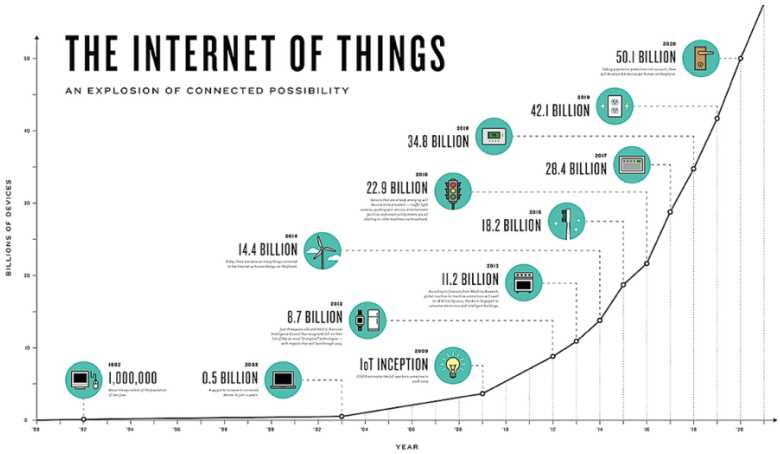

Figure 1: IoT connected devices by 2020 [1]

In order to give a better understanding, we will present our work applied for Routers. Routers are essential in providing reliable network connectivity between IoT devices and a successful attack allows cybercrime could perform exploit and escalate privileges of these devices to take control of the whole network. The worst recorded cyber-attack on Router happened in 2016 and was clocked at 1.1 terabytes per second (TBps) [6] as presented in the first section. In recent years, there has been a lot of research on information security for routers, especially deep learning applications in detecting malware on these devices. Studies can be mentioned as [14], [15], [16], .

These methods can be divided into two main classes: static and dynamic approach . Static approach [17] is useful for analyzing device that consists in detecting malware in firmware source code or executable files without executing them. This approach uses techniques like control-flow-graph (CFG), data-flow-graph (DFG), symbolic execution (SE) to analyze every single executable and able to identify malware characteristics such as API (Application Programming Interfaces) call, n-grams, Printable String Information (PSI), Function Length Frequency (FLF), opcodes (operational codes) [18].

Dynamic approach [19] consists in monitoring the whole device during its run-time to detect abnormal behaviors. To perform this approach, the most important part is to collect all of the data from device network and operating system. Then, these data will be analyzed with machine learning models to detect if there is any abnormal behavior. The result of this step will be warned to network administrator afterwards. PSA A.I Toolkit is also based on this approach to able to monitor the whole devices of VNPT as required. The PSA A.I Toolkit's architecture is presented by figure 2 and composed by 4 main modules as follow:

- *The Agent Management Center (AMC):*

This is the most important module of PSA A.I Toolkit and is responsible for the installation of Agent into VNPT IoT devices. Different from Personal Computer (PC) that use mostly x86 processor, we can find a lot of platform of processor installed into IoT devices such as MIPS, ARM,

PowerPC etc [20]. Therefore, agent must be developed in a manner that could be cross-compiled for multi-platform of processors.

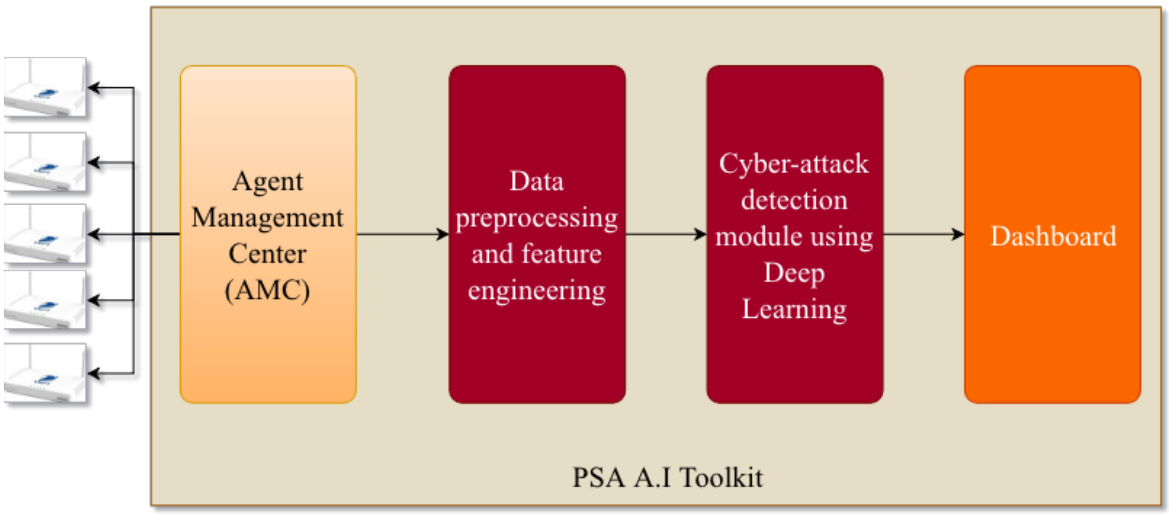

Figure 2 PSA A.I Toolkit architecture

Definition 1: An agent is a computer system that is situated in some environment, and that is capable of autonomous action in this environment in order to meet its design objectives [21].

Figure 3 Agent description

In real setting, we have to identify hardware architecture, processor and the version of firmware for each IoT device. Based on collected information, a selection of corresponding agent is automatically made by AMC before installing it into device. Figure 2 gives a short description of an agent that can interact with IoT device to collect data including network behavior, system-call behavior. In general, to reduce a COTS router firmware image to less than 8 megabytes, vendors have customized theirs firmware image by removing “unnecessary” packages. Hence, Busybox is widely used in embedded systems because it combines tiny versions of many common

UNIX utilities into a single small executable [22]. Therefore, such system can not integrate sophisticate tools to monitor system-call because Busybox does not have enough utilities and a lot of libraries are also missing. Thanks to Landley [22] with different pre-built Busybox versions, we can customize them to get more utilities. Therefore, our agent doesn't store collected data but transfer it to AMC at a predetermined time-step (about every 60 seconds). The collected data are stored in a temporary database before being moving to the data preprocessing and feature engineering module.

- *The Data preprocessing and feature engineering module:*

Before using the system-call sequences and network behavior as inputs to PSA cyber-attack detection module that based on Deep learning algorithms, we have to convert data into numerical feature vectors. Figure 4 shows a sample of raw network behavior (Pcap) and system-calls behavior.

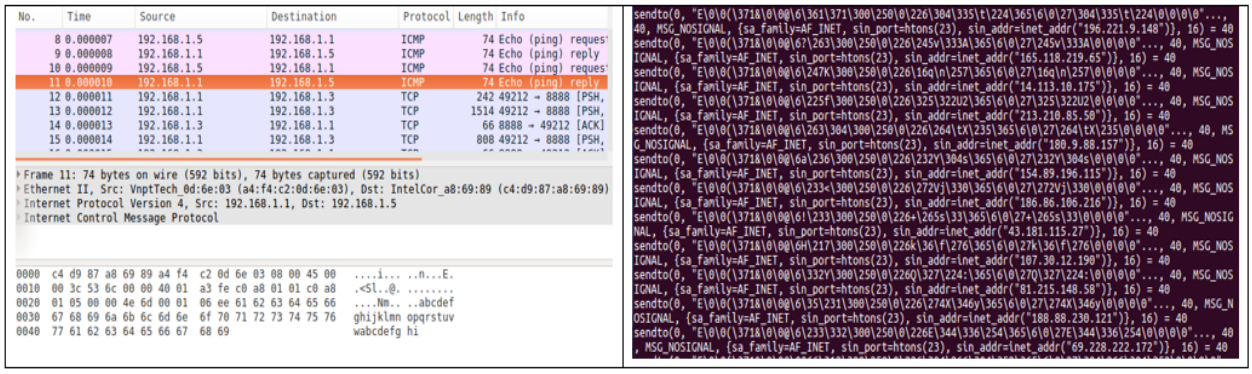

Figure 4: Raw Pcap and system-call data

At this stage, we used Skip-gram and Principal Component Analysis (PCA) algorithms to transform these raw data into required format by PSA cyber-attack detection module afterwards.

- *The Cyber-attack detection module:*

After the data preprocessing step, we feed the data as inputs into Deep Neural Network to determine which behavior is abnormal and others. In this module, we used Convolutional Neural Network (CNN) combined with Long short-term memory (LSTM) [23] to train data and to generate

cyber-attack detection model. Convolutional neural network is a specific type of artificial neural network that uses perceptrons, a machine learning unit algorithm, for supervised learning, to analyze data. There are three main types of layers to build a CNN:

+ Convolutional layer: A convolutional operation refers to extracting features from the input image and multiplying the values in the filter with the original pixel values

+ Pooling layer: The pooling operation reduces the dimensionality of each feature map

+ Fully-connected layer: The fully-connected layer is a classic multi-layer perceptrons with a softmax activation function in the output layer.

Long Short-Term Memory networks – usually just called "LSTM" – are a special kind of neural network, capable of learning long-term dependencies. They were introduced by Hochreiter & Schmidhuber (1997), and were refined and popularized by many people in following work. They work tremendously well on a large variety of problems, and are now widely used. LSTM are explicitly designed to avoid the long-term dependency problem. Remembering information for long periods of time is practically their default behavior, not something they struggle to learn. The architecture of proposed neural network is shown in Figure 5.

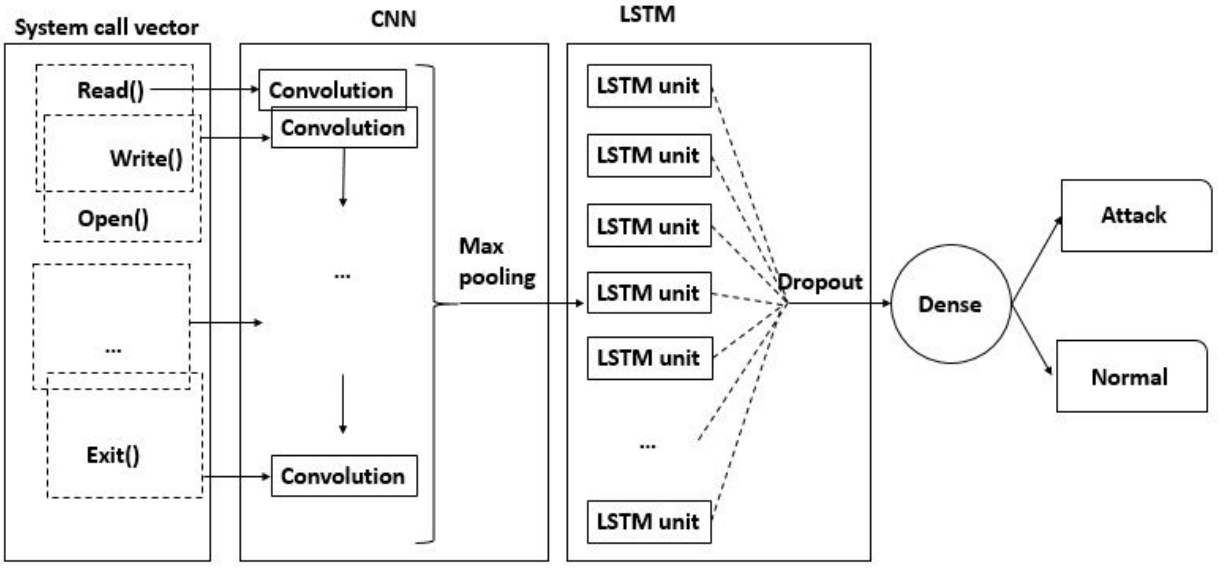

Figure 5: PSA cyber-attack detection module architecture

- *The Dashboard module:*

PSA A.I Dashboard displays a collection of visualizations for monitoring the whole network situation in real time. This module gives at a glance the information that administrator needs to make key decisions. The primary view was built with a simplification of the Human Machine Interface (HMI) as shown by figure 4. Each circle, column represents an aggregation of cyber-attacks by threat, by port and by Internet Protocol addresses. Interaction is a crucial component of most elements on the Dashboard, administrator can get more details by clicking or by hovering on display elements.

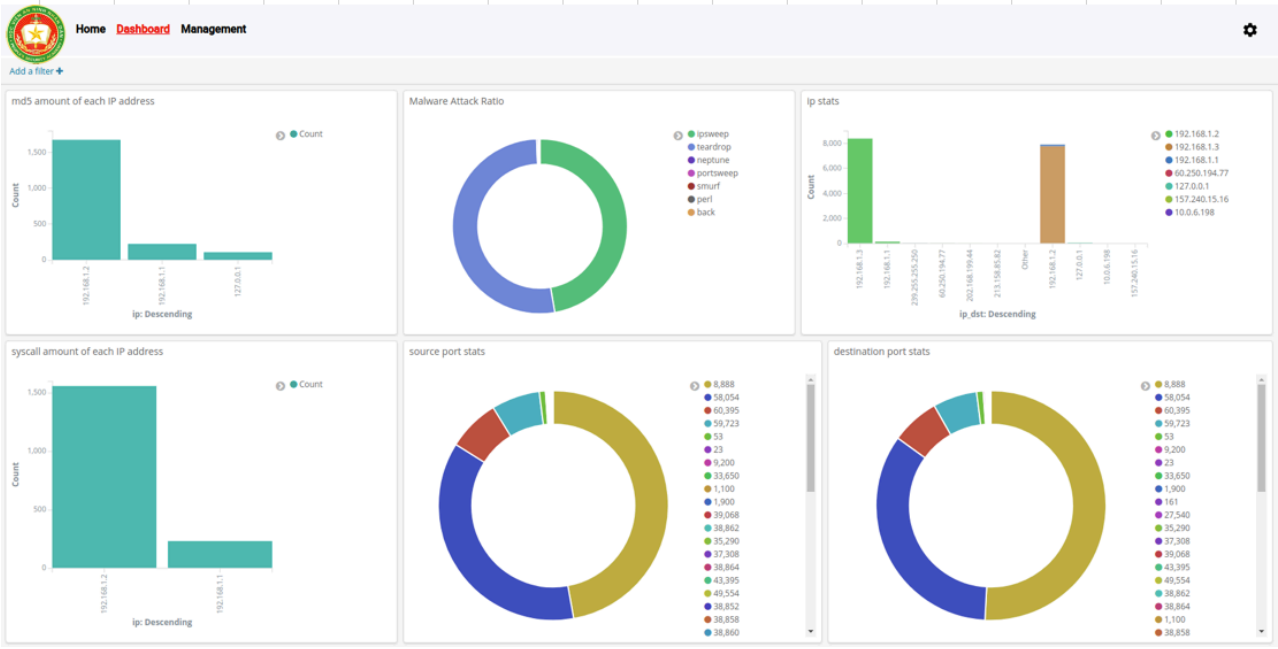

Figure 6: PSA A.I Dashboard

IV. CONCLUSION

Globally, cybersecurity has become the most dangerous threat to national security. To ensure the country's sustainable development, Vietnam has made efforts to upgrade cybersecurity policy and strategy with a clear and concrete acceleration in recent years. These efforts created a strong basis of legal frameworks and guidelines for organizations, companies and individuals to participate into the development of cybersecurity. Consequently, Vietnam government tends to be

more and more proactive and the sharp result could be mentioned is the Cybersecurity Law that took effect on January, 01, 2019. Although this Law would need further details and sub-legislation guidelines, especially the scope of cybersecurity protection measures, but it marked as the first legal document in term of national security in cyber-space.

In the point of view of PSA, human is the most important factor, playing a key role in ensuring national cybersecurity. To achieve this goal, PSA has been providing the best conditions to develop cybersecurity, such as funding research labs, organizing seminars, supporting necessary conditions for students and lecturer/researchers. As a result, PSA A.I Toolkit appeared as an inevitable consequence. In the process of cooperating with VNPT, PSA A.I Toolkit has been released to test and achieved cyber-attack detection results with accuracy about 95%. In the short-term, PSA continues to improve PSA A.I Toolkit to deploy in real life and cooperate deeper with VNPT in training security personnel. In parallel, PSA aims at becoming a reputable organization in securing IoT systems.

REFERENCES

[1] "Cisco Internet of Things, 2015, [Accessed: 10- Sep 2018]."

[2] "Smart cities in southeast ASIA." Produced for world cities summit 2018 in collaboration with the centre for liveable cities, Singapore, Jul-2018.

[3] "Gartner, 2016, Available at: https://www.gartner.com/newsroom/id/3291817

[4] Brett Davis, Hacking Attack At Vietnam Airports Another Chapter In South China Sea Dispute, https://www.forbes.com/sites/davisbrett/2016/08/13/hacking-attack-at-vietnam-airports-another-chapter-in-south-china-sea-dispute/#64a588716e35 , [Accessed: 10- Sep- 2018]."

[5] "Overview of the Internet of things, Recommendation ITU-T Y.2060." International Telecommunication Union, 2013.

[6] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas, "DDoS in the IoT: Mirai and other botnets," in *IEEE Computer Society*, 2017, vol. 50, pp. 80–84.

[7] D. Ben Herzberg, Dima Bekerman, and Igal Zeifman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis , https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html."

[8] "Việt Nam, Israel share experience in cyber security, https://www.vietmaz.com/2018/07/viet-nam-israel-share-experience-in-cyber-security/." .

[9] "Vietnam approves sustainable smart city development plan, http://vovworld.vn/en-US/news/vietnam-approves-sustainable-smart-city-development-plan-667949.vov

[10] "VNPT Corporation, http://www.vnpt.vn/en/Home.aspx, [Accessed: 10- Nov- 2018]."

[11] "Viettel Corporation, http://viettel.com.vn/en, [Accessed: 10- Nov- 2018]."

[12] "BKAV Corporation, http://www.bkav.com/, [Accessed: 10- Nov- 2018]."

[13] "Vietnam Cyberspace Security Technology JSC (VNCS) , http://vncs.vn/en/

[14] Hamed HaddadPajouh, Ali Dehghantanha, Raouf Khayami, Kim-Kwang Raymond Choo, “A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting,” 2018.

[15] Christopher D. McDermott, Farzan Majdani, Andrei V. Petrovski, “Botnet Detection in the Internet of Things using Deep Learning Approaches,” presented at the International joint conference on neural networks 2018, Rio de Janeiro, Brazil.

[16] Shun Tobiyama, “Malware Detection with Deep Neural Network Using Process Behavior,” presented at the 2016 IEEE 40th Annual Computer Software and Applications Conference, 2016.

[17] Dehghantanha, A., Azmoodeh , A. and Choo, K.-K.R, “Robust Malware Detection for Internet Of (Battlefield) Things Devices Using Deep Eigenspace Learning,” presented at the IEEE Transactions on Sustainable Computing, 2018.

[18] Huy Trung Nguyen, Quoc Dung Ngo, and Van Hoang Le, “IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier,” presented at the International Conference on Information Communication and Signal Processing (ICSP 2018), Singapore, 2018.

[19] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C., “IoTPOT: A Novel Honenypot for Revealing Current IoT Threats,” *Journal in Information Processing*, vol. 24, pp. 522–533, May 2016.

[20] Jonas Zaddach and Andrei Costin, “Embedded Devices Security and Firmware Reverse Engineering,” *BlackHat*, 2013.

[21] M. Wooldridge, *An Introduction to Multiagent System*, Second edition. John Wiley & Sons, 2009.

[22] “Project - BusyBox, https://busybox.net/downloads/BusyBox.html

[23] Jinpei Yan, Yong Qi, and Qifan Rao, “Detecting Malware with an Ensemble Method Based on Deep Neural Network,” presented at the Security and Communication Networks, 2018.