Zeszyty Naukowe SGSP 2021
2021, Nr 80 (tom 1), s. 199–216
ISSN: 0239-5223

DOI: 10.5604/01.3001.0015.6485

WERONIKA JAKUBCZAK, PHD, ASSOCIATE PROFESSOR
The Main School of Fire Service, Warsaw, Poland
e-mail: wjakubczak@sgsp.edu.pl
ORCID 0000-0003-1501-5064

HON-MIN YAU [姚宏旻], PHD
National Defense University, Taoyuan City, Taiwan
e-mail: cf22517855@gmail.com
ORCID 0000-0003-3737-0438

TRENDS IN CYBERSECURITY REGULATIONS OF TAIWAN (REPUBLIC OF CHINA) – PHASES OF PROMOTION OF MAJOR CYBER SECURITY PLANS AND PROGRAMS IN THE NATIONAL CYBER SECURITY PROGRAM OF TAIWAN (2021–2024)

ABSTRACT

The authors of the article focus on the main trends observed within cyber security regulations of Taiwan (Republic of China). In fact, Taiwanese governmental websites faced approximately 5 million attacks every day in 2021 [8]. Despite these attacks, the Taiwanese government operates in a steady way to improve its cyber capability, progressing on its cyber security increase path. The main document behind it in the form of strategic regulation is the National Cyber Security Program of Taiwan (NCSP 2021–2024). It explains the structure of the entities responsible for cyber security and describes both goals that have been accomplished and the ones that are/will be implemented.

In particular, Taiwan focuses on providing higher cyber security protection standards, including critical infrastructure elements, private-public cooperation, the use of new technologies, and scouting for new talents. International collaboration is also highly valued as an example of joint cyber exercises between Taiwan and the USA in 2019.

KEYWORDS

cyber security, cyberspace, cyberattacks, Republic of China, Taiwan, critical infrastructure, cybercrime

Received: 29.11.2021; Reviewed: 27.12.2021; Accepted: 17.12.2021

TRENDY W REGULACJACH DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA NA TAJWANIE (REPUBLIKA CHIŃSKA) – ETAPY PROMOCJI GŁÓWNYCH PLANÓW I PROGRAMÓW DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W NARODOWYM PROGRAMIE BEZPIECZEŃSTWA CYBERNETYCZNEGO TAJWANU (2021–2024)

ABSTRAKT

Autorzy artykułu skupiają się na głównych trendach obserwowanych w strategiach cyberbezpieczeństwa Republiki Chińskiej. Tajwańskie strony rządowe miały około 5 milionów ataków dziennie w 2021 r. Mimo to działają one w sposób stały, podążając ścieżką wzrostu cyberbezpieczeństwa. Głównym dokumentem, który za nim stoi, w postaci regulacji strategicznej, jest Narodowy Program Cyberbezpieczeństwa (2021–2024). Część – Fazy promocji głównych planów i programów bezpieczeństwa cybernetycznego. Powyższy dokument przedstawia rozwój strategii cybebezpieczeństwa między 2001 a 2021 r. Wyjaśnia on strukturę podmiotów odpowiedzialnych za cyberbezpieczeństwo oraz opisuje zarówno cele, które zostały zrealizowane, jak i te, które są/będą wprowadzane w życie.

W szczególności Tajwan koncentruje się na zapewnieniu wyższych standardów cyberbezpieczeństwa, w tym elementów infrastruktury krytycznej, współpracy prywatno-publicznej, wykorzystaniu nowych technologii i poszukiwaniu nowych talentów. Współpraca międzynarodowa jest również wysoko ceniona, jako przykład można wymienić wspólne cyberćwiczenia Tajwanu i USA w 2019 r.

SŁOWA KLUCZOWE

cyberbezpieczeństwo, cyberprzestrzeń, cyberataki, Republika Chińska, infrastruktura krytyczna, cyberprzestępczość

Przyjęty: 29.11.2021; Zrecenzowany: 17.12.2021; Zatwierdzony: 17.12.2021

INTRODUCTION

The purpose of this article is to explain the evolution of the cyber security trends in Taiwan (the Republic of China) with respect to various "Phases of Promotion of Major Cyber Security Programs and plans" defined by its government's cyber security policy. The language and the structure of this article are as used in the strategic documents of Taiwan related to cyber security and it was protected in order to highlight the specific nature of the aforementioned documents. Digitalization and technology evolution stimulate new threats to emerge and old ones to evolve in dangerous directions and scales. Despite the COVID-19 pandemic, globalization does not slow down [4]. Cyberattacks are getting more dangerous nowadays since both civilians (private and public) and the military use elements of cyberspace infrastructure and cyber technologies [3]. Moreover, many parts of them are to be recognized as critical infrastructure – the most important part of the infrastructure that ensures that a state can function, such as power plants, power grids, financial sector, medical sector, emergency systems, airports, communication and command systems used by police, firefighters and military personnel, etc. In all of the systems mentioned above that the use of software and hardware can be targets of cyberattacks – a cybercrime, terrorist attack, or emanation of cyberwarfare [5].

By official statements, Taiwanese governmental websites faced approximately 5 million attacks every day [8] or 20–40 million attacks per month [1] in 2021, and Taiwan is initiating various measures to defend itself in the digital domain. In fact, the main document describing these efforts in the form of legal regulation is National Cyber Security Program (NCSP 2021–2024) [6]. It explains the structure of the entities responsible for cybersecurity and describes both goals that have been accomplished as well as the ones that are/will be implemented. In particular, to understand how Taiwan has become such a resilient country, it is crucial to understand the idea and consistency behind the implementation of the great goals described in Phases of Promotion in the NCSP.

The situation mentioned above highlights that Taiwanese are working on providing higher standards of cybersecurity protection, including critical infrastructure elements, private-public cooperation, use of new technologies, and scouting for new talents. International collaboration is also highly valued as the example of joint cyber exercises between Taiwan and the USA in 2019 [2].

In order to increase the readiness of its cyber security, Taiwan has been intensely working on the creation and maintenance of the very complex system that could provide it. The system above has been developed for many years, and its first organizational and strategic aspects were put into operation as of the year 2001. Hence, as a part of this research, the authors also analyzed the text of the previous NCSP of Taiwan, however, due to the brief nature of this paper, the main focus will be put upon the evolution of cyber security introduction, maintenance of the top level of its provision and process of continuous improvement in this field.

METHOD

The authors used the analytical method in order to present the most important aspects of trends in cyber security regulations of Taiwan with respect to various phases of promotion of major cyber security plans and programs documented in the NCSP 2021–2024. The primary research methodology was based on an analysis of the results of scientific investigations of the text of the NCSP 2021–2024 and a synthetic description of the key conclusions drawn from the review of the literature and aforementioned strategic documents. Generally, the research methods used in this paper included a critical analysis of the strategic documents, literature, comparative analysis, and analysis of the available data.

PHASES OF PROMOTION OF MAJOR CYBER SECURITY PLANS AND PROGRAMS IN TAIWAN

Since 2001, the National Center for Cyber Security Technology (NCCST) has accomplished a successful promotion of 5 different phases where the major cyber security plans or programs have effectively improved the completeness of Taiwan's cyber security. Each of them was implemented within an originally introduced 4-year period. Please find below figure the information on these particular phases accomplished since 2001.

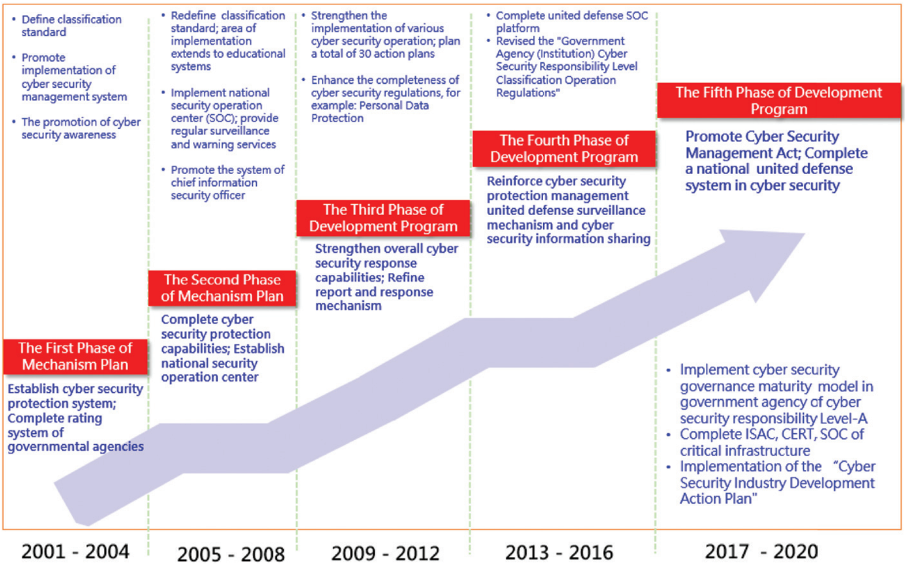
• Define classification standard
• Promote implementation of cyber security management system
• The promotion of cyber security awareness
The First Phase of Mechanism Plan
Establish cyber security protection system; Complete rating system of governmental agencies
• Redefine classification standard; area of implementation extends to educational systems
• Implement national security operation center (SOC); provide regular surveillance and warning services
• Promote the system of chief information security officer
The Second Phase of Mechanism Plan
Complete cyber security protection capabilities; Establish national security operation center
• Strengthen the implementation of various cyber security operation; plan a total of 30 action plans
• Enhance the completeness of cyber security regulations, for example: Personal Data Protection
The Third Phase of Development Program
Strengthen overall cyber security response capabilities; Refine report and response mechanism
• Complete united defense SOC platform
• Revised the "Government Agency (Institution) Cyber Security Responsibility Level Classification Operation Regulations"
The Fourth Phase of Development Program
Reinforce cyber security protection management united defense surveillance mechanism and cyber security information sharing
The Fifth Phase of Development Program
Promote Cyber Security Management Act; Complete a national united defense system in cyber security
• Implement cyber security governance maturity model in government agency of cyber security responsibility Level-A
• Complete ISAC, CERT, SOC of critical infrastructure
• Implementation of the "Cyber Security Industry Development Action Plan"
2001 - 2004
2005 - 2008
2009 - 2012
2013 - 2016
2017 - 2020

Fig. 2. The promotional phases of cyber security in Taiwan
Source: NCSP 2021 to 2024

Many milestones have been accomplished. In particular:

1. The First Phase of Mechanism Plan (NCSP 2001–2004) – The Cyber Security Protection System and Complete Rating Mechanism for Government Agencies were established.

In 2001 the Executive Yuan[1] promulgated the "Mechanism Program of Security in Establishing National Information and Communication Infra-

[1] The Executive Yuan is the executive branch of the government of the Republic of China (Taiwan). The Premier is its leader. *The Executive Yuan. Structure and Functions.* https://english.ey.gov.tw/Page/E43650B2CB14861B.

structure" (Phase 1 Mechanism Program), with the vision of "ensuring a national safe and reliable information and communication environment" [6].

Construction of a cyber security protection system shall be recognized as the key achievement of Phase I. Detailed accomplishments are as follows:

1) The National Information and Communication Security Taskforce (NICST), NCCST (technical staff unit – a competent authority of national cyber security construction and policies) were established.
2) Promotion of the cyber security management system for essential government agencies involved in the functional and economic aspects of the country; provision of the corresponding cyber security support and work requirements for agencies through the establishment of cyber security crisis notification and early warning mechanisms and responsibility level classification standards; conducting external cyber security audits against designated agencies.
3) Promotion of cyber security training for information personnel; an increase of public awareness of cyber security, etc.
4) Conduct full review and revision of relevant cyber security legal regulations; introduce national technical standards and specifications; product inspection and guarantee mechanism.
5) Establishment of Information Security Management System (ISMS) for the critical infrastructure (CI) system, the introduction of cyber security control programs (early warning, notification mechanism, and personnel training of the security operation center).

2. The Second Phase of Mechanism Plan (NCSP 2005–2008) – Improvement of the Capabilities of Cyber Security Protection, Establishing a National Security Operation Center.

After completing the Phase 1 Mechanism Plan, the Executive Yuan approved the "Mechanism Program of Security in Establishing National Information and Communication Infrastructure (2005 to 2008)" (Phase 2 Mechanism Program) in 2004. The hope is to strengthen the overall capacity for cyber security, and the critical achievements include:

1) Establish a National Security Operation Center (N-SOC) to monitor the well-being of Taiwanese cyberspace and provide early warning information for core government agencies to achieve 24-hour protection.

2) Establish the Chief Information Security Officer (CISO) mechanism for central government agencies and designate each deputy head of the ministries in charge of cyber security operation as the CISO concurrently; implement cybersecurity-related plans in the regional government units.
3) Expand the cybersecurity implementation plan to lower levels of the government hierarchy and further extend the installations of cyber security systems from essential government agencies to the education system.
4) Introduce general-level Information Security Management. System (ISMS) into the education system and supervise county-level (city) education network centers to establish its own version of ISMS.
5) Enhance the effectiveness of operations through regular government audits. Government agencies introduced internal audit systems to implement cyber security-related management work and continue to conduct external cyber security audits for public and private organizations providing auditing recommendations.
6) Extend the specified areas of protection in the national-level cyber security plan; strengthen the formulation of cyber security plans that promote online transaction security and protect people's personal data.

3. The Third Phase of Development Plan (NCSP 2009–2012) – Strengthening the Overall Response Capability of Cyber Security; Improvement of the Report and Response Mechanism

The Phase 3 development program was issued in January 2009. The presented vision focusing on building "a safe and reliable smart nation; a secure and qualified digital life" was to create cyber security requirements for the private sector and gradually strengthen their cyber security defense mechanism. The main achievements were:

1) Improve management procedures for security breach detection, identification, analysis, and response, shorten incident report timeline, and strengthen emergency handling, response, and recovery capabilities.
2) Implement cyber security governance and evaluation plan upon agencies identified as A-level and B-level organizations; specify requirements for agencies to allocate designated information security systems and manpower according to their organizational characteristics; classify information systems to match corresponded information security requirements.

3) Adopt a "plan-do-check-act" (PDCA) planning model to improve the overall information security management of government agencies, and mitigate potential operational risks of domestic government agencies and private enterprises by certified with international security standards verification procedure (i.e. ISO 27001).
4) Increase reliability and security of e-commerce, strengthen online transactions identity authentication mechanism, promote the use of Public Key Infrastructure (PKI) certificate services.
5) Promote the use of third-party appraisal by business institutions, strengthen cyber security auditing of enterprises in accordance with the latest laws and regulations, encourage businesses to strengthen personal data protection, establish cyber security management system, conduct internal audits and subcontract a third party authority to conduct external cyber security audits.
6) Support the cyber security research, encourage higher education systems to offer cyber security courses, enrich cyber security professional research talents, develop key cyber security technologies, and provide value-added applications in the industry.
7) Strengthen cyber security ideas, risk awareness activities form educational organizations at all levels, inspect the security of important cyber assets, conduct public security inspections and Catch-the-Flag competitions, to increase the national level of cyber security awareness.

4. The Fourth Phase of Development Plan (NCSP 2013–2016) – Strengthening the United Defense Monitoring Mechanism for Cyber Security Protection Management, and Intensifying Cyber Security Intelligence Sharing

"National information and communication security development program (2013 to 2016)" (Phase 4 development program) was approved by the Executive Yuan in 2013. Its vision is as follows: "building a safe cyber security environment; stepping towards a high-quality cyber society" to strengthen the counter-reaction capabilities of the central government against cyber-attacks. The aims of the program were:

1) Construction of national policies and its environment: continuously improve and revise information security policies; promote reasonable manpower and budget mechanisms for information security in govern-

ment agencies. Annually evaluate information security service vendors; prepare and operate the "National Center for Cyber Security Technology", promote administrative legalization and security verification of information and communication equipment, actively communicate with international and domestic certification organizations, and regularly review projects.

2) Cyber security protection and information sharing: establish a governmental cyber security governance structure, assess the maturity of cyber security governance of government agencies at the level of A, B, and C; build an Institute of Watch Internet Network (iWIN) network content protection agency to strengthen the mechanism of network content security management; introduce cyber security offensive and defensive situational and actual drills; promote governmental cyber security management systems, and improve governmental cyber security management operations; develop cyber security infrastructure security settings and continuously update the Government Configuration Baseline (GCB) for different systems; increase capabilities in collecting cyber security threats by intelligence, and strengthen information analysis and sharing mechanism.
3) Industrial development and technological upgrade: set up cyber security protection technology research capacity and strengthen the competitive advantage of emerging cyber security independent technologies; intensify the cooperation between enterprises and academic institutions, application of emerging technological practices of cyber security; strengthen the applications of crime investigation, digital evidence preservation, digital forensic laboratories; use of modern key technologies (mobile devices and applications, wireless networks, and Secure Software Development Lifecycle (SSDLC), etc.), to build a corresponding security detection mechanism.
4) Talent cultivation and international exchanges: promote cyber security professional training and certification mechanism, and plan to establish the registration and certification mechanism of cyber security professionals; introduce the evaluation system for cyber security functional capabilities and encouragement of various categories of personnel to complete cyber security function training regularly and pass courses evaluation.

5. The Fifth Phase of Development Plan (NCSP 2017–2020) – Promotion of the Cyber Security Management Act; Completion of National Cyber Security United Defense System

The Phase 5 Program was approved in 2017 as a response to the threats and challenges of information and communication security. To achieve the goal mentioned above the Taiwanese Government decided to promote the development of a digital nation and innovative economies and upgrade cyber security to the level of national security protection under the policy direction of "Cyber Security is National Security." The continuous improvement and implementation of various cyber security protection measures are necessary while facing complex and changing cyber security threats.

The vision of the 5th phase is "building a safe and reliable digital country" with three key aims – Building a National Cyber Security United Defense System, Improving the Overall Cyber Security Protection Mechanism and Strengthening the Development of Independent Cyber Security Industries.

The Taiwanese also included 4 key promotional strategies, and they are:

- Completing Cyber Security Infrastructure – Cyber Security Management Act was passed,
- Building a National Cyber Security United Defense System,
- Promoting the Independence of the Cyber Security Industry,
- Nurturing High-Quality Cyber Security Talents.

Eleven specific measures have been formulated to gradually promote national cyber security defense-in-depth and united defense system in order to stabilize the security defense line of national digital territory.

The strategic document includes a long list of current implementation priorities and promotion results. However, the most important aspects are as follows:

1) Complete cyber security infrastructure, and this includes:
   - Cyber Security Management Act was passed in 2018.
   - The Ministry of Economic Affairs and the National Communications Commission jointly promote security testing, certification, and verification for information and communication products (i.e. testing laboratory certification, cyber security testing service).

2) Construct national cyber security united defense system

- The cyber security united defense system of Taiwan is based on the core of eight major Critical Infrastructure (CI) sectors[2]. Conduction of horizontal cross-domain united defense, forming a "Three-layered Cyber Security United Defense Architecture," is promoted to mitigate the impact of CI operation disconnection due to cyber security attacks. Establishment of Security Operation Center (SOC) of domestic-level and various CI-sector-level, Computer Emergency Response Team (CERT), Information Sharing and Analysis Center (ISAC) and other united defense mechanisms. These systematic and institutionalized deployments enable cyber security information collection and sharing; incident report and response; integration, sharing and application of intelligence, and establishing a complete defense line.
- Strengthening local government cyber resilience: cyber security protection of the local government and its affiliated local offices helps them construct a safe information and communication operating environment to establish a reliable cyber security environment. Create promotion of cyber security regional united defense; corporation of a local united cyber security protection network; cooperation between a local government with nearby academic research institutions to jointly cultivate future cyber security talents for the government and academia. Six regional ISACs have been established and become members of the National Information Sharing and Analysis Center (N-ISAC) – information can be quickly shared with local governments' representatives. SOCs of 6 regions have completed the collection of cyber security information of neighboring counties and cities and conducted a comprehensive analysis to grasp suspicious and malicious behavior.

[2] "The eight critical infrastructure domains defined by the Office of Homeland Security, Executive Yuan, include Government, Energy, Water, Hi-Tech Industrial Parks, Information and Telecommunication, Transportation, Banking and Finance, Emergency Services, and Public Healthcare". National Cyber Security Program of Taiwan (2017 to 2020), 2016.

3) Boost the independence of the cyber security industry

In 2019, "Procuring Principles for Information and Communication Security Independent Products" were introduced. The aim was to promote the independent development of the national cyber security industry and increase the domestic autonomy rate. As a result, many entities were encouraged to adopt different products of cyber security – central and local agencies (institutions), public schools, government-owned enterprises, and administrative, legal persons.

In addition, the Ministry of Economic Affairs has established an integrated cyber security service platform (SecPaaS) and promoted the matching services of domestic cyber security products and certified services. Focused upon acceleration of cyber security industry development, the government has also created good conditions and development environment for the cyber security industry players in Taiwan, so that the participants can quickly accumulate various capabilities and have room for growth in the early stages of development. That includes support for cyber security startup community; promotion of knowledge; establishing an environment for cyber security trends and technology exchanges among the industry, academia, and research circles.

4) Cultivating high-quality cyber security talents

The Taiwanese Ministry of Education added in 2018 an electronic-information discipline cluster, setting up an "Information and Communication Security Discipline" to the original public-funded studying abroad examinations to provide admitted students with the opportunity to study overseas. Since 2019, it promoted the establishment of 5 cyber security master programs in 4 colleges and universities and gradually established a systematic cyber security talent cultivation system that is accompanied by a diversified training model.

- Since 2016 training course of "Taiwan Cool Hacker" has been promoted. To support the development of cyber security technical and practical skills among talented teachers from the academy and industry were invited to work within the Mentor system. That enabled to instruct cyber security practices and technology and provide the experience of cyber security competition through apprenticeship—an opportunity to participate in more specialized and advanced studies for gifted students. Since 2017 a new type of cyber security summer school program (Advanced Information

Security Summer School, AIS3) has started. It aims to cultivate high-level cyber security talents. Through the diversified practical training model, the Taiwan cyber security students have been ranked among the best during international cyber security competitions in recent years.

- To help with cyber security industry talents development, the Ministry of Economic Affairs has started special classes since 2017, subsidizing 400 hours of full-time cyber security training per trainee and training unit providing successful employment matching services after the completion of the course. The development of cyber security talents uses various cyber security training models in the market to set up on-the-job classes for short-term cyber security training in different industrial fields. In addition, the Industrial Bureau provides subsidies to the enterprise-appointed trainees, immediately strengthening the industry's cyber security level.

It is essential to mention that in the forenamed strategic document, the Taiwanese legislators analyzed and addressed cyber security trends in other countries. That was presented as part of The Second. Global cyber security threat and international policy trends, B. Development trends of international cyber security policies. In particular, countries such as the USA, Japan, Singapore, and Germany were considered.

FUTURE OUTLOOK – THE SIXTH PHASE

In February 2021, the Taiwanese government released the latest phase, the sixth phase of the NCSP 2021–2024. The vision is to create a resilient and secure "smart nation". Taiwan wishes to become the pivotal cyber security center and build a smarter and active cyber defense. Given that from the manufacturing of personal protective equipment to the fabrication of semiconductor chips, Taiwan has become an essential player in the global supply chain ecosystem due to its effective handling of the pandemic. Hence, Taiwan continues to invest and enhance its capability in the cyber security domain in order to ensure its continued prosperity in this new level of digitalization now and in the Post COVID-19 world. These Taiwanese efforts outlined above could be described as follows:

First, the prevalence of using Industrial Control Systems (ICS) becoming unavoidable vulnerability for the modern society, and the water that bears a boat is the same that swallows it up. Hence, Taiwan continues to enhance its regulations, procedures, training, and security standards in order to mitigate the risk brought by modern society's reliance on ICT devices.

Second, the Taiwanese government also focuses on creating a friendly and innovative environment to support the development of cyber security talents and industry. Today, cyber security is just like an essential utility service, which is an intrinsic part of the necessities of our modern society. Without cyber security, any advanced technology would still become void due to the loss of users' trust in its service. Taiwan understands credibility is the prerequisite of successful ICT service. Therefore, it has utilized a strategy that focuses on constructing a sounder and healthier cyber environment by advancing people's knowledge of information security technology.

Third, as the geopolitical tension places Taiwan in a unique position of studying cyberattacks originating from the other side of the Taiwan strait, Taiwan has continued to leverage this unusual situation and transform itself into developing the cyber security industry. After all, the one who knows you best is often your enemy. This characteristic has made Taiwan one of the frontrunners in cyber security studies.

Finally, the NCSP 2021–2024 has also continued to consolidate the aforesaid advantages with a vision of making Taiwan's cyber security service in the international space. In order to accelerate the digitalization of Taiwan via the Digitalization of Taiwan's economic activities by the Digital Nation and Innovative Economic Development Program (DiGi+, 2017–2025), the Taiwanese government invested heavily in improving both the software and hardware of Taiwan's cyber security. DiGi+ means to promote the digital economy via improving infrastructures, regulations, governance, and city management. Cyber security has become not only a commodity but also a vital necessity. In short, Taiwan is determined to contribute to safeguarding the global cyber environment meaningfully and is looking forward to any opportunity for international collaborations.

As this article is just a brief introduction to the researched matter – the authors will elaborate on this aspect in future papers.

CONCLUSIONS

It is clear that Taiwan follows a long-term strategy with appropriate adjustments being made every four years to reflect the development of ongoing threats in cyberspace. In dealing with cyber security, setting appropriate horizontal goals is very important as this will guide a state's cyber security policy moving steadily toward a better future. Taiwan's approach is vast and long-term-oriented, still, the strategy has to be general enough to let the structures and legal regulations operate smoothly.

To sum up, due to the limitation of attribution, nations and states in the past could often claim no knowledge of cyberattacks originated from their territory in order to circumvent their responsibility to any cyber incident. Hence, the discussion of cyber security in the policy circle often focused on "exploiting" cyberspace instead of "protecting" cyberspace. However, just like air pollution, cyber security is a transnational problem, and no country is able to be exempt from its impact. Therefore, the international community needs to work together to ensure the well-being of this global domain, and it may also be time for us to change the mindset from thinking about states' right to exploit cyberspace to states' obligation to protect cyberspace.

The new global health situation creates a reality that people need to work remotely and factories manufacture intelligently and automatically. Hence, the safeguard of one's ICT assets, including IoTs, AI, communication network, and smart city or manufacturing grids, becomes Taiwan's critical mission of "build Taiwan as a safe and resilient smart country." Likewise, Taiwanese President, Tsai Ing-Wen, expressed clearly in May 2020 at her second term of the presidency that her "National security is cyber security 2.0" is not only "improving the capacity of cyber security industry" as the mid-term and long-term development objective for national cyber security infrastructure, but also creating an attractive environment to encourage domestic and foreign companies to invest in Taiwan's cyber security industry. Hence, this is to say that in an analogy of protecting the international environment, this will suggest an alternative way forward for the international community to deal with cyber pollution.

By introducing several documents of strategic importance, Taiwan has proven that it follows the most important cybersecurity trends and can address the most demanding threats. Furthermore, the Republic of China

(Taiwan) continuously enhances its regulations, procedures, training, and security standards. The main goal of the aforesaid is to build resistance to the risks brought by modern society's dependence upon ICT devices.

In particular, Taiwan successfully introduced and developed national policies (including the government bodies) and worked on the cyber security protection and information sharing. Industrial development and technological upgrade was an important part of the process as well. Furthermore, with respect to ever-growing threats, Taiwan recognized the necessity to invest in training and selecting talents that could positively impact the development of cybersecurity. Last but not least, the Republic of China (Taiwan) put a lot of attention to the development of cooperation between the public and private sectors to improve cybersecurity.

REFERENCES

1. Cheung E., Ripley W., Tsai G., CNN Business, *How Taiwan is trying to defend against a cyber "World War III"*, 2021, https://edition.cnn.com/2021/07/23/tech/taiwan-china-cybersecurity – intl-hnk/index.html.
2. Department of Information Services, Executive Yuan, 2019, *Taiwan and US co-hosting multinational cybersecurity exercise*, https://english.ey.gov.tw/Page/61BF20C3E89B856/0f357b66-7ed3-4123-98c6-b91097b82536.
3. Jakubczak R., Martowski R.M., *Powszechna obrona terytorialna w cyberobronie i agresji hybrydowej*, Warsaw 2017.
4. Jakubczak W., *Condition of Cybersecurity in Poland – Selected Aspects*, "Przedsiębiorczość i Zarządzanie" 2016, Issue No.: 5.1.
5. Lehto M., *Cyberspace and cyber warfare* [in:] Dimitrov K.,] (ed.), *Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures, NATO Science for Peace and Security Series D: Information and Communication Security*, Vol. 51, pp. 99–109, 2018.
6. National Information and Communication Security Taskforce, Executive Yuan, *National Cyber Security Program of Taiwan (2021 to 2024) Republic of China (Taiwan)*, 2021.
7. *National Cyber Security Program of Taiwan (2017 to 2020)*, 2016.
8. Strong M., 2021, *Taiwan government departments targeted by hackers 5 million times per day*, https://www.taiwannews.com.tw/en/news/4340699.

9. The Executive Yuan, *The Executive Yuan. Structure and Functions*. https://english.ey.gov.tw/Page/E43650B2CB14861B.
10. Wang M.-H., Nguyen N.-L., Dai S.-c., Chi P.-W., Dow C.-R., *Understanding Potential Cyber-Armies in Elections: A Study of Taiwan*, "Sustainability" 2020, 12, 2248. https://doi.org/10.3390/su12062248
11. Yau Hon-min, *A Critical Strategy for Taiwan's Cybersecurity: A Perspective from Critical Security Studies*, "Journal of Cyber Policy" 2019, 1–21.
12. Yau Hon-min, *Explaining Taiwan's Cybersecurity Policy Prior to 2016: Effects of Norms and Identities*, "Issues & Studies" 2018, 54, no. 02, 1–30.

WERONIKA JAKUBCZAK – holds PhD in war studies from the Polish National Defence Academy and post-doctoral degree in security studies (Polish Naval Academy). She has been researching globalisation, cybersecurity, international and national security as well as territorial defence since 2004. She is a member of the Institute of Internal Security at the Main School of Fire Service, Warsaw, Poland.

WERONIKA JAKUBCZAK – jest doktorem nauk wojskowych (Akademia Obrony Narodowej) oraz doktorem habilitowanym nauk o bezpieczeństwie (Akademia Marynarki Wojennej). Od 2004 roku zajmuje się badaniami nad globalizacją, cyberbezpieczeństwem, bezpieczeństwem międzynarodowym i narodowym oraz obroną terytorialną. Jest pracownikiem Instytutu Bezpieczeństwa Wewnętrznego Szkoły Głównej Służby Pożarniczej.

HON-MIN YAU – received his PhD from the Department of International Politics, Aberystwyth University. His research interests focus on global security, technology and national security policy. He holds position of Hon-min Yau – Assistant Professor at National Defense University, Republic of China.

HON-MIN YAU – uzyskał tytuł doktora na Wydziale Polityki Międzynarodowej Uniwersytetu w Aberystwyth. Jego zainteresowania badawcze koncentrują się na bezpieczeństwie globalnym, technologii i polityce bezpieczeństwa narodowego. Pracuje jako adiunkt na Uniwersytecie Obrony Narodowej, Republika Chińska.