Ministry of Foreign Affairs

Research of Cyber Security Industry in Taiwan

Commissioned by the Netherlands Enterprise Agency

>> *Sustainable. Agricultural. Innovative. International.*

ITRI
Industrial Technology
Research Institute

Research of Cyber Security Industry in Taiwan

Industrial Technology Research Institute (ITRI)
Industry, Science and Technology International Strategy Center (ISTI)

June 2020

ITRI
Industrial Technology
Research Institute

Table of Contents

List of Contents

List of Tables

List of Figures

Executive Summary

Taiwan and the Netherlands have been cooperating on cybersecurity issues more and more frequently. To create concrete and mutually beneficial opportunities for both parties, it is necessary to better understand the current cybersecurity developments in Taiwan and the Netherlands. Commissioned by the Netherlands Office Taipei, this research explores the cybersecurity developments in Taiwan and the Netherlands and opportunities for future cooperation. This research consists of three parts: cybersecurity developments in Taiwan and the Netherlands; opportunities, constraints, obstacles, and benefits for bilateral cooperation in cybersecurity; and recommended strategies and action plans for bilateral cooperation in cybersecurity.

I. Cybersecurity developments in Taiwan and the Netherlands

(I) Cybersecurity development in Taiwan

1. Cybersecurity policy

In recent years, the cybersecurity industry has been the focus of industrial development policy in Taiwan. The units in charge are the Department of Cyber Security, Executive Yuan and the Industrial Development Bureau, Ministry of Economic Affairs. The Department of Cyber Security, Executive Yuan proposed the "Action Plan for Cybersecurity Industry Development (Draft)" based on the conclusions of the Strategy Review Board Meeting (SRB) and the "National Cyber Security Program of Taiwan (2017-2020)" promulgated in November 2017. As of today, the said program, which includes "promoting the cybersecurity industry's capacity" in the key tasks of promoting the medium-term/long-term development of national cybersecurity infrastructure, has been implemented for three consecutive years.

The said action plan aims to build an innovative ecosystem for Taiwan's cybersecurity industry in hopes of "building a global cybersecurity start-up hub and promoting Taiwanese security brands." It expects to gradually increase the overall national defense through forward-looking policy guidance and national investment. The four major strategies are described as follows: establishing a demand-oriented training system for cybersecurity talents; consolidating the niche market and forming international partnerships; establishing product testing sites to deliver results required to enter the international market; and fueling cybersecurity investment to establish global presence.

2. Results of the cybersecurity development promoted by the Ministry of Economic Affairs

In line with the above-mentioned "Action Plan for Cybersecurity Industry Development," the Ministry of Economic Affairs has systematically promoted the development of Taiwan's cybersecurity industry from the aspects of talent, market, technology, standards and environment. The results over the past three years have started to roll in as follows: Between 2017 and 2018, there were a total of 1,313 trainees, and 52 of them were employed by cybersecurity companies such as SYSTEX Corporation and HwaCom Systems Inc., with a 80% employment rate; a cybersecurity service team was set up to build a supply and demand matchmaking system for diagnosing and matching small and medium enterprises; with the 5+2 innovative industries (i.e. IoT) being priorities, critical infrastructure sites (i.e. oil, water, and electricity) were opened up to help cybersecurity start-ups accumulate their experience in product development and technological research and development; between 2016 and 2019, a total of 11 qualified APP testing labs were established, with 1,941 APPs certified; as of 2019, a total of 7 IoT security product testing standards were developed, including 3 for video surveillance, 2 for smart buses, and 2 for smart street lights, and 5 products from 3 cybersecurity companies passed the IP Camara certification; in 2017, Taiwan and Israel worked together to develop I.X/Vision IT; a cybersecurity solution alliance was also formed to secure orders in cooperation with nForce SECURE (Thailand).

3. Cybersecurity needs

Based on the cybersecurity framework proposed by the National Cyber Security Centre (NCSC), this research adopted the questionnaires and interviews targeting Taiwan's top three industries in output value, namely manufacturing, banking, and health care, to analyze these industries' cybersecurity needs and gaps. In terms of the three industries' overall defense against cyberattacks, 73% of the Taiwanese enterprises had elementary abilities to prevent cyberattacks; that is, they could guard against sufficient cyberattacks; however, only 14% of the enterprises had advanced abilities to prevent cyberattacks. For manufacturing companies, financial institutions, and health care companies, there are needs for cybersecurity in aspects of system protection policies and procedures, identity and access control, data security, system security, system and cyber resilience, and cybersecurity awareness and training.

According to the results of analysis, about 40% of the manufacturing

companies on average have to strengthen identity and access control, data security, and system security and are in need of cybersecurity solutions such as authentication, control and recording of access and authorization processes, data access control, key data access software/hardware protection, security and vulnerability scanning, application whitelisting and OT vulnerability management; about 45% of the health care companies have to strengthen identity and access control, data security, and system security and are in need of cybersecurity solutions such as authentication for data access or service, control and recording of access and authorization processes, data confidentiality protection, software/hardware security and vulnerability scanning, OT vulnerability management and application whitelisting; as to financial institutions, given that all business-related data are sensitive due to the special nature of the industry, they have been more alert to cybersecurity for a long time compared with companies in other industries, so the security gap is relatively small. Only 8% of the financial institutions are in need of cybersecurity solutions such as identity management and privileged access management, data confidentiality protection, key data access software/hardware protection, software/hardware security and vulnerability scanning.

4. Taiwan's cybersecurity ecosystem

Since the government of Taiwan has invested in resources to support the cybersecurity industry in recent years, some unprecedented changes have taken place. The most obvious difference is the emergence of cybersecurity start-ups. In the past three years, driven by the government's efforts to promote the cybersecurity development, a total of 22 cybersecurity start-ups have been established, 12 of which are founded by white hat hacker communities. The establishment of cybersecurity start-ups helps promote the industrial development in terms of talents and funds; the most significant significance is to inject innovation into technological research and development in Taiwan's cybersecurity industry.

The output value of Taiwan's cybersecurity industry in 2019 increased to NT$49.34 billion by 12.3% over 2018; there were a total of 324 cybersecurity companies and 8,800 cybersecurity professionals in the industry. Growth in 2019 was mainly driven by the substantial growth in the export of cybersecurity network hardware and the domestic demand for cybersecurity services. Taiwan's cybersecurity industry consists of 8 sub-industries, namely endpoint and mobile device security, network security, data and cloud application

security, IoT security, cybersecurity operations management services, cybersecurity testing, identification, and consulting services, system integration services, and cybersecurity support services.

Among these sub-industries, endpoint and mobile device security and network security are relatively large in Taiwan's cybersecurity industry in terms of the number of manufacturers and output value, with the most capacity of cybersecurity technology. Driven by the government policy and increasing security awareness, the prospects of Taiwan's cybersecurity have been brightening in recent years. In 2019, revenue of nearly 60% (59%) of the domestic cybersecurity service providers was estimated to grow from the previous year, with the average revenue increasing by 23% (mainly due to an increased domestic demand for cybersecurity services); in addition, driven by the government's policy that "cybersecurity is national security," 56% of the domestic cybersecurity companies also expected that revenue in 2019 and 2020 would grow for two consecutive years.

5. Strengths and opportunities of Taiwan's cybersecurity industry

The greatest strengths and opportunities in the development of Taiwan's cybersecurity industry rest on the existing technology industry and government support. The world's leading chip, semiconductor, and ICT manufacturers in Taiwan provide the foundation and edges for the cybersecurity industry to develop chip security solutions and ICT supply chain security solutions. Upholding the policy that "Cybersecurity is National Security," the government has invested resources in cybersecurity infrastructure and joint defense mechanisms in recent years, and set up a dedicated cybersecurity unit and the information and communications technology branch under the Ministry of National Defense. More importantly, the Cyber Security Management Act took effect in 2019, driving the overall cybersecurity industry's need for compliance.

With increasing cybersecurity threats and damage caused in recent years, governments around the world have gradually paid attention to cybersecurity issues. The government of Taiwan has also attached importance to critical information infrastructure protection (CIIP) and cybersecurity challenges in various fields such as finance, transportation, energy, and health care, and has opened up related sites for cybersecurity companies to cultivate their hands-on experience. The establishment of IoT security criteria and industry standards will also help build local IoT security brands; in addition, the application of artificial intelligence (AI) to cybersecurity is one of the domains of Taiwanese

cybersecurity startups. The integration of AI and cybersecurity technology will be conducive to the development of edge computing-type endpoint security solutions in the future.

(II) Cybersecurity development in the Netherlands

The government of the Netherlands promulgated the first "National Cyber Security Strategy: Success Through Cooperation" in February 2011. The second version was published two years later in 2013. In response to this strategy, the government of the Netherlands established the National Cyber Security Centrum (NCSC) to oversee the coordination of national security initiatives and set up the Nederlandse Cyber Security Raad (CSR) as a national strategic consulting agency.

The unit in charge of cybersecurity in the Netherlands is National Cyber Security Center (NCSC), a division of Cyber Security Directorate (DCS) and managed by the National Coordinator for Security and Counterterrorism (NCTV) under the Ministry of Security and Justice.

In 2013, the government of the Netherlands established the Hague Security Delta (HSD), which is now the paramount counseling agency for the cybersecurity ecosystem. Currently, the HSD has nearly 300 partners, making it the largest cybersecurity industry cluster in Europe.

Attaching great importance to talent cultivation, the government of the Netherlands established the Dutch Cyber Security Platform for Higher Education and Research (DCYPHER) in 2016, with special emphasis on higher education in the field of cybersecurity; in addition, the government of the Netherlands pays much attention to the research and development of cybersecurity technology. Each year, the government of the Netherlands will spend about 400 million euros (about 436 million US dollars) on the cybersecurity research and development plans led by the Netherlands Organization For Applied Scientific Research (TNO) and the Netherlands Organization for Scientific Research (NWO) in cooperation with the Dutch academic and business communities.

The Netherlands has a higher cybersecurity capacity than the European or even global average. According to the scope of the Dutch cybersecurity industry published by Cybersecurity Observatory (https://cyberstartupobservatory.com), there are about 60 cybersecurity companies in the Netherlands. In addition to cybersecurity products such as endpoint security, network security, and cloud security, more cybersecurity companies specialize in fields of cyberattack

detection, cybersecurity services, and cybersecurity operations management services, and cybersecurity intelligence.

II. Opportunities, constraints, obstacles, and benefits for bilateral cooperation in cybersecurity

Over the past two years, Taiwan and the Netherlands have been cooperating on cybersecurity issues more and more frequently and have held seminars or visits of significance, laying a solid foundation for bilateral cooperation. In 2018, the Industrial Development Bureau, Ministry of Economic Affairs secured cooperation with the HSD and became a member of the Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC). Taiwan was the first country in Asia to join the Global EPIC, building a channel of cooperation between the cybersecurity industry and the academia in Taiwan and the Netherlands and benefiting some cybersecurity companies.

At present, Taiwan remains a special political entity for the international community, which may be a potential obstacle to bilateral cooperation between Taiwan and the Netherlands. The government of Taiwan calls on the government of the Netherlands to take an open attitude toward trade and business cooperation. To eliminate potential obstacles to bilateral cooperation arising from sensitive political issues, Taiwan will maintain informal contact and communication with international organizations through semi-official organizations.

Taiwan-Netherlands cooperation focuses on market expansion, technological cooperation, and policy exchange, which will help cybersecurity companies expand bilateral markets and develop new technologies and solutions. Both Taiwan and the Netherlands may exchange opinions on common cybersecurity policies and issues such as standardization processes, intelligence, and pilot cases.

III. Recommended strategies and action plans for bilateral cooperation in cybersecurity

Based on the conditions of cooperation between Taiwan and Netherlands and strengths and weaknesses in the respective cybersecurity developments, it is recommended that Taiwan and the Netherlands discuss cooperation strategies and models in three aspects: government cooperation, information sharing, and business matchmaking.

In terms of government cooperation, Taiwan has very successful

experience in promoting the cybersecurity standards and certification/ verification systems and has promulgated English versions of relevant documents. Many foreign organizations have expressed willingness to cooperate with Taiwan. Taiwan and the Netherlands may cooperate to set up the interoperable and mutually recognized IoT security standards and certification mechanism to strengthen the cybersecurity capabilities of smart cities and IoT devices.

In terms of information sharing, Taiwan and the Netherlands may, based on the existing cooperation, strengthen information/intelligence sharing and regular visits and exchanges, which help cybersecurity companies adapt to and expand in each other's market.

In terms of business matchmaking, it is advised that Taiwan and the Netherlands develop cybersecurity solutions together and strengthen the capacity of cybersecurity start-ups. According to the research, at least 7 Dutch cybersecurity companies have sufficient capabilities of ICS/SCADA, which are exactly what Taiwan's three major industries need. This is an opportunity worth exploring for future supply and demand matching. With sufficient capabilities of cybersecurity hardware, cyberattack detection, and threat intelligence, Taiwanese cybersecurity start-ups may work with Dutch cybersecurity companies to expand surrounding markets.

Part 1. Analysis of Strengths and Weaknesses

1. Overview of the Cybersecurity Development in Taiwan

(1) Status of national cybersecurity, such as major cybersecurity incidents and sources of cybersecurity threats

Taiwan has a special position of political and economic in the international society. Both public and private sectors in Taiwan face the biggest cybersecurity threats from China. When the United States and Taiwan jointly held the “Large-scale Cyber Defense Exercise” in November 2019, the director of the American Institute in Taiwan indicated that the number of China’s cyberattacks on Taiwan’s technology industry increased by 7 times in 2018 and by 20 times in 2019. The Vice Premier of the Executive Yuan, Taiwan also pointed out that, according to the statistics, 60% of the 30 million cyberattacks on Taiwan per month came from China. According to the statistics released by Check Point in June 2019, malware attacks in Taiwan were four to dozens of times those worldwide. According to research by the National Taipei University, in the US-China trade war, the Chinese cyber warriors spread Taiwan cannot rely on the US message to create internal conflicts between Taiwan ’s pro-China and pro-American factions.

Taiwan has been attacked by ransomware and advanced persistent threats (APT) in recent years. Recently, several data breaches have resulted in the theft and improper sales of hundreds of thousands of personal data. Although it is impossible to guard against various ways of cyberattacks, a threat to a significant loss of profits has aroused the awareness of cybersecurity protection in major public and private sectors such as government agencies, medical institutions, and service providers in Taiwan. Cybersecurity has been incorporated into an integral part of the national policy; industries have also increased investment in cybersecurity and talent recruitment; in addition, the cybersecurity industry and protection technologies have received more attention from all circles.

Table 1 Major Cybersecurity Incidents in Taiwan

Date	Way of Attack	Major Incident
2019/08	Ransomware	Hosts in the Ministry of Health and Welfare, large hospitals, and medical clinics were hacked. Important data such as patient profiles, staff rosters, medical images, and medical records were locked by encryption viruses. More than 55 medical institutions were the victims of the incident.
2019/07	Taking control of the server by malware upload	The database of 1111 Job Bank was hacked, resulting in the leak of 200,000 job seekers' personal data such as ID number, name, birthday, e-mail, phone number, address, and company.
2019/06	Taking control of the server by malware upload	590,000 personal data such as ID number, name, agency, job number, and job title were leaked from the Ministry of Civil Service and exposed on the foreign websites, affecting 243,376 people.
2019/04	APT	ASUS's automatic software update tool server was hacked, and the number of affected users worldwide may exceed 1 million.
2018/08	Malware	TSMC was attacked by the wannacry virus, which caused the production line to shut down and lost TWD 2.6 billion.
2018/08	Creating accounts with administrative rights after implanting backdoors	More than 2.98 million personal data of the citizens in Taipei were leaked and sold on a foreign forum.
2017/05	Exploiting website vulnerabilities	About 360,000 client data of Lion Travel, including name, phone number, and products purchased, were hacked. Lion Travel faced a claim of NT$3.63 million in a class action and is currently appealing to a higher court.

Source: Websites

(2) Development of national cybersecurity policy and organizational structure

With the development of innovative technologies such as mobile devices and the Internet of things (IoT), cyber security has become a key issue in the emerging digital economy. To facilitate industry transformation in the face of the digital economy, the Executive Yuan has proposed the policy called "Digital Nation & Innovative Economy Development Program (2017-2025)." As cyber security is the foundation for the

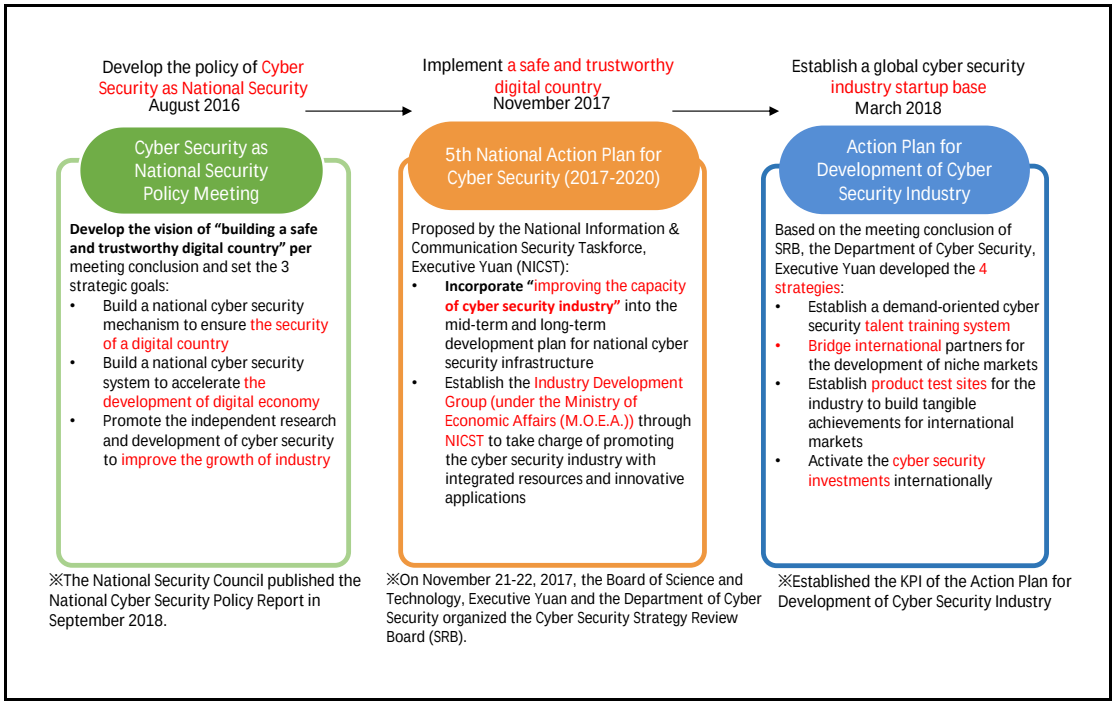
development and popularization of digital technologies applications, the National Security Council, Office of the President proposed the cybersecurity strategy report, “Cybersecurity Is National Security,” in August 2016, demonstrating its determination to defend the digital nation.

In June 2017, the Board of Science and Technology, Executive Yuan (BOST) convened the “Conference on Cybersecurity Flagship Program & Industrial Development” to discuss expand or upgrade the strategies and specific action plans for the cybersecurity industry. According to the conclusions of the conference, BOST and the Department of Cyber Security (DSC), Executive Yuan organized the “Strategy Review Board Meeting (SRB)” between November 21 and November 22, 2017 to discuss the development in Taiwan’s cybersecurity industry from three aspects, namely international linkage, local linkage, and industrial linkage.

After the SRB, DSC proposed the “Action Plan for Cybersecurity Industry Development (Draft)” based on the conclusions of the SRB and the “National Cyber Security Program of Taiwan (2017-2020)” promulgated in November 2017. With the vision of “building a safe and trustworthy digital nation,” the action plan aims to gradually increase the overall national defense through forward-looking policy guidance and national investment and includes “promoting the cybersecurity industry’s capacity” in the key tasks of promoting the medium-term/long-term development of national cybersecurity infrastructure.

The National Information & Communication Security Taskforce has the Industry Development Group (IDB) (by the Ministry of Economic Affairs) in place to be in charge of promoting the cybersecurity industry, integrating industry, government, academic and research resources, and developing innovative applications. To achieve the vision of “building a safe and trustworthy digital nation” and the goal of “promoting the cybersecurity industry’s capacity” effectively, the 3593rd session of the Executive Yuan resolved in March 2018 that “according to the four development strategies proposed in the “Action Plan for Cybersecurity Industry Development,” the Ministry of Economic Affairs is in charge of industrial development, the Ministry of Education is in charge of talent cultivation, the Ministry of Science and Technology is in charge

of technological research and development, the Board of Science and Technology is in charge of the 5+2 Industrial Innovation Program Promotion Office, the Department of Cyber Security is in charge of performance management and inter-ministerial coordination." In line with the action plan, the Art of Cyber War (ACW) project under the Ministry of Economic Affairs creates an innovative ecosystem for Taiwan's cybersecurity industry in hopes of "building a global cybersecurity start-up hub and increase brand awareness of Taiwan's cybersecurity industry."



Source: Compiled by Industry, Science and Technology International Strategy Center, ITRI

Figure 1 Course of Cybersecurity Industry Development Policy Implementation

(3) Current status and development trend of the Taiwanese cybersecurity market

To understand whether Taiwanese companies have sufficient abilities to take appropriate steps to identify, assess and understand the security risks of all information and communications technology (ICT) systems and to organize risk management methods, the Industry, Science and Technology International Strategy Center, ITRI surveyed the current status and development trend of the Taiwanese cybersecurity

market based on the six defense-in-depth tactics proposed by the National Cyber Security Centre (NCSC) (UK) and analyzed the cybersecurity capacities and gaps of the manufacturing, healthcare, and financial industries in Taiwan.

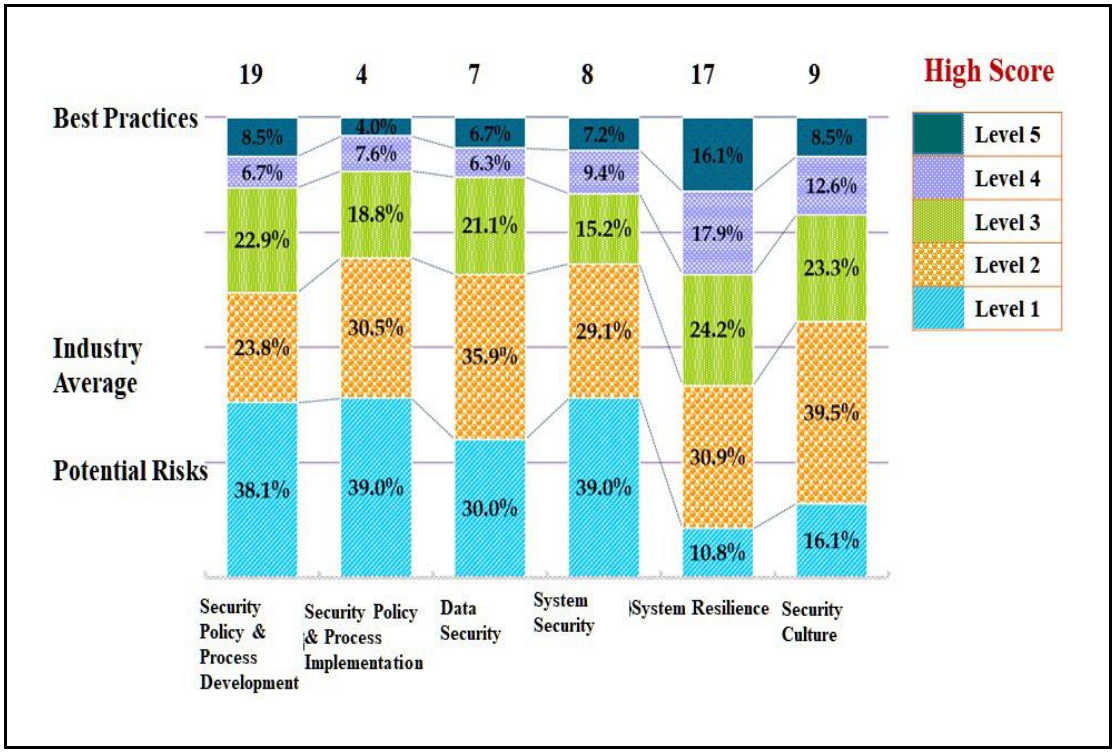
A. Current status of the Taiwanese cybersecurity market

Collectively referred to as enterprises' basic abilities to prevent cyberattacks, NCSC's six defense-in-depth tactics are as follows: System protection policies and procedures, identity and access control, data security, system security, system and cyber resilience, and cybersecurity awareness and training. If the defenses are weak, it indicates that enterprises will have to strengthen investment in a specific project or change their protection strategies, which reflects the enterprises' potential needs of defenses in the future.

Based on the NCSC's six defense-in-depth tactics, the Industry, Science and Technology International Strategy Center, ITRI surveyed the basic abilities of large enterprises/TWSE/TPEx listed companies in Taiwan to prevent cyberattacks in 2019 and retrieved 1,068 questionnaires from 733 manufacturing companies, 302 health care companies, and 33 financial institutions.

After the cross-reference to the 223 samples, the results showed that a total of 162 companies (73%) could got a cyber security protection rating ranging from level 2 to level 5, which means they have a certain level of protect capability against cyberattacks; however, there are only 32 companies can reach level 4 to level 5 that means only 14% enterprises had really advanced abilities to prevent cyberattacks.

If a systematic overall improvement is required, it is necessary to further examine the cybersecurity gaps individually in the six defense-in-depth tactics, as shown in the figure below.



Source: Industry, Science and Technology International Strategy Center, ITRI

Note: (1) System protection policies and procedures: The industry defines the properly communicable business strategies and procedures for protecting the systems and data required to operate the business.

(2) Identity and access control: The industry grasps, records and controls all access data of the ICT systems required for operations.

(3) Data security: The industry protects the data stored or transmitted electronically from having an adverse impact on business operations.

(4) System security: The industry protects critical networks or information systems from others' attacks.

(5) System and cyber resilience: The industry strengthens its ability to guard against cyberattacks.

(6) Cybersecurity awareness and training: The industry properly trains or raises the employees' awareness of security to ensure that employees can make a positive contribution to cybersecurity.

Figure 2 Current Cyber Security Level of Taiwan Businesses

In terms of system protection policies and procedures, 62% of the companies in Taiwan operated in accordance with the ISO/IEC 27001, and about 15% of them adopted better approaches, including conducting some personal interviews or involving employees in the design of processes and policies to make the systems coincide more with the actual practices; they also implemented new or improved policies and processes on a regular basis, allowing people concerned to communicate and evaluate the effect of the strategies.

In terms of identity and access control, more than 61% of Taiwan's enterprises had the ability to control and record the authentication, verification, and authorization

of data or service access; however, nearly 39% of the companies did not clearly define who had access to important ICT systems or sensitive information.

In terms of data security, 70% of Taiwan's enterprises introduced different levels of data protection mechanisms and programs while 30% have not introduced adequate protection mechanisms. At present, Taiwanese enterprises usually protect electronically stored or transmitted data to at least prevent unauthorized access to sensitive data, thereby maintaining data confidentiality. For example, enterprises can prevent the loss or theft of data stored on mobile devices, or they can filter data storage devices and/or transmission media before sending data.

In terms of system security, which is key to guarding against hackers or malware, the results of the survey showed that 61% of Taiwan's enterprises have introduced system protection programs to varying degrees, but 39% have not introduced sufficient system protection mechanisms. At present, the most common practice among the Taiwanese enterprises is to adopt a physical isolation system that disables unnecessary services, software, data flow across a network, and system access in a "least and necessary" manner to reduce the chance of being attacked.

In terms of system and cyber resilience, the results of the survey showed that 89% of Taiwan's enterprises have introduced system and cyber resilience programs to varying degrees, and only 11% have not yet introduced sufficient protection mechanisms for system and cyber resilience, indicating that Taiwan's enterprises have been quite mature in ensuring system availability.

In terms of cybersecurity awareness and training, the results of the survey showed 84% of Taiwan's enterprises have introduced various levels of cybersecurity awareness and training programs; that is, about 16% of Taiwan's enterprises have not yet established these concepts; however, the cybersecurity awareness of Taiwan's enterprises as a whole has increased to a certain extent. Basically, Taiwan's enterprises have been able to provide training on knowledge and skills required for employees to perform their basic functions.

B. Development trend of the Taiwanese cybersecurity market

According to the results of the survey, the Taiwanese cybersecurity market has to fill the gaps in the NCSC's six defense-in-depth tactics, we suggest the following improvements:

a. System protection policies and procedures

Before granting access to the specific personnel, enterprises should introduce the proper authentication, verification, and authorization mechanisms or solutions to users, devices, and systems, which is to be continuously enhanced by Taiwan's enterprises. Granting access to related solutions should be strictly controlled; especially for the personnel of great influence, the access process should be recorded and monitored. If someone changes his/her position or leaves the company, his/her authority should be revoked. In addition to regularly reviewing the access granted, enterprises should revoke inappropriate identity and authorization mechanisms through authentication.

b. Identity and access control

At present, the solutions that have been deployed by about 90% of Taiwan's enterprises neither use two-factor authentication or hardware authentication for high-privileged access nor prevent unauthorized employees from accessing data or service in the systems (i.e. unauthorized use of any online services, access by unauthorized individuals and devices, and loss or theft of user devices).

c. Data security

Taiwan's enterprises have to increase the use of solutions with the following three functions: (1) Maintain data backup, adopt physical isolation, and detect data integrity while protecting software and hardware that access critical data from vulnerabilities; (2) ensure the use of encryption (i.e. VPN) to protect data from unauthorized access or interference during transmission, including Transport Layer Security (TLS) that

protects external data connections, such as Web browsers, and the use of encryption (IPSec) between communication points to protect encryption elements (i.e. digital signatures and keys) from external or unauthorized access; and (3) use multiple network paths and tested automatic backup systems to ensure the availability of basic data (i.e. network topology mapper required to restore the network, safety-critical information, or basic forecast data) in case of cybersecurity incidents.

d. System security

System security is the most important part that Taiwan's enterprises lack at present. Required solutions include penetration testing and vulnerability scanning, which can help enterprises protect their ICT systems from attacks that exploit software vulnerabilities. Most of the Taiwanese enterprises have not yet conducted regular vulnerability and security assessments of their systems and have not been aware that the latest version or patch of support software and applications should be adopted, which requires assistance from cybersecurity service providers.

e. System and cyber resilience

The main need of the Taiwanese enterprises is to be able to ensure the operation of basic functions in the event of failure or damage to ICT systems. Cybersecurity services providers and consultants can assist the enterprises in building resilience in addition to technology. For example, enterprises should ensure that processes can be continued with manual steps or that the ICT systems are well maintained and managed throughout their lifecycles, and that privileged accounts are not used for daily IT activities such as e-mail and web browsing. These practices all help diminish hackers' ability to invade.

f. Security awareness and training

There is still room for improvement in cybersecurity awareness and training. Many

Taiwanese enterprises lack the idea of shaping a positive security culture and fight against cyberattacks only in written instructions and training. According to the results of the survey, nearly 80% of Taiwan's enterprises required professional cybersecurity consulting services to integrate cybersecurity awareness into training programs with the times and regularly make adjustments to coincide with the most secure work pattern within the organization, further shaping a corporate culture reflected in the daily operations.

C. Cybersecurity need of Taiwan's key industries

Based on the survey of the cybersecurity need of Taiwan's three key industries, namely manufacturing, healthcare, and financial, the degree of need by each industry for the aforesaid six defense-in-depth tactics is described below:

Table 2 Cybersecurity Need of Taiwan's Manufacturing, Healthcare, and Financial Industries

Industry / Need	Manufacturing	Healthcare	Financial
System protection policies and procedures	● 36% of the companies should strengthen ● focus on designing security procedures and policies based on ISO/IEC standards	● 49% of the companies should strengthen ● focus on developing ISO/IEC protection policies for the cybersecurity management required in the work environment of the healthcare industry	● 15% of the companies should strengthen ● focus on designing the standard procedures for cybersecurity that are more in line with working conditions, risk management, and business strategies
Identity and access control	● 41% of the companies should strengthen ● focus on building the capacity to control ad record the authentication, access, and authorization process	● 46% of the companies should strengthen ● focus on building the capacity to control ad record the authentication, access, and authorization process for data or service access	● 8% of the companies should strengthen ● focus on identity management and privileged access management
Data security	● 38% of the companies should strengthen ● focus on data access control, key data access software/hardware protection, and security and vulnerability detection	● 37% of the companies should strengthen ● focus on data confidentiality and software/hardware security and vulnerability detection	● 8% of the companies should strengthen ● focus on data integrity and confidentiality, key data access software/hardware protection, and software/hardware security and vulnerability detection
System security	● 45% of the companies should strengthen ● focus on application whitelisting and OT vulnerability management	● 52% of the companies should strengthen ● focus on OT vulnerability management and application whitelisting	● 8% of the companies should strengthen ● focus on preventing flaws in internal operation management
System and cyber resilience	● 12% of the companies should strengthen ● focus on system resilience capacity building and system life cycle maintenance and management	● 17% of the companies should strengthen ● focus on ensuring the operation of basic functions in case of ICT system failure or damage	None
Security awareness and training	● 20% of the companies should strengthen ● focus on promoting different levels of cybersecurity awareness and training programs	● 17% of the companies should strengthen ● focus on establishing a cybersecurity culture	None

Source: Industry, Science and Technology International Strategy Center, ITRI

(4) Strengths and weaknesses in cybersecurity

This section will briefly explain the strengths and weaknesses of Taiwan's cybersecurity industry. For more information, see (7) SWOT analysis of Taiwan's cybersecurity industry.

A. Weaknesses of Taiwan's cybersecurity industry

a. The scale and the output value are small; a good cybersecurity ecosystem is required

The scale and output value of Taiwan's cybersecurity industry are still small. Most of the cybersecurity companies with the capacity of research and development are small and medium enterprises. It is difficult to compete with major international companies, causing the key components of the domestic market such as financial institutions, high-tech companies, and large organizations to import cybersecurity products. This hinders the long-term development of Taiwan's cybersecurity industry. In terms of market, technology, and talent, the government has to assist in building a sound environment for the development of Taiwan's cybersecurity industry.

b. Enterprises lack cybersecurity awareness

When developing products and services, Taiwan's ICT industry considers costs and is lack of "Security Inside", hindering the sales of Taiwanese ICT products worldwide due to privacy risks. For example, the Federal Trade Commission of the U.S. accused HTC, Asus, and D-Link of lacking privacy protection and cybersecurity for their products; in addition, enterprises lack cybersecurity awareness and have no incentive to introduce cybersecurity products. Most of the Taiwanese enterprises still take a "Nice to Have" attitude towards cybersecurity products. It is necessary for cybersecurity companies to make a lot of efforts to promote cybersecurity products and raise the cybersecurity awareness within the organization.

c. Most of the Taiwanese cyber security companies are small and medium enterprises deficient in international marketing resources

Most of the Taiwanese cyber security companies are small and medium enterprises. In 2016, nearly 60% of the Taiwanese cyber security companies had annual revenue below NT$100 million and were deficient in international marketing resources. Most of their products were exported to Asian countries; however, only 35% of the companies exported to China, Malaysia, the U.S., Japan, and Singapore. Start-ups are a force behind technological innovation in Taiwan's cybersecurity industry; however, the venture capital market in Taiwan pays little attention to cybersecurity start-ups, and these start-ups are struggling to expand customers and make ends meet. Overall, the marketing resources of Taiwan's cybersecurity industry are relatively insufficient. How to assist cybersecurity companies in developing export strategies and strengthening connections with international markets is a major issue for the development of Taiwan's cybersecurity industry.

d. The cybersecurity ecosystem lacks sites and standards

The lack of domestic large-scale cyberattack defense test sites results in the insufficient capability and maturity of Taiwanese cybersecurity products, making it impossible to effectively evaluate the cybersecurity level and compete with international competitors; moreover, Taiwan's cybersecurity industry lacks standards, test specifications, and complete cybersecurity inspection and certification systems, making the cybersecurity products vulnerable to privacy breaches and foreign penalties.

e. There are gaps in key technologies and professionals

A large amount of human resources and time are required for the research and development of key cybersecurity technologies; at present, domestic cybersecurity companies are small and lack sufficient funds, making it is difficult to invest in the research and development of key cybersecurity technologies. There is also a lack of integrated system solutions in the cybersecurity protection system; in addition, system solutions such as IoT security and critical information infrastructure are still in the nascent stages of development. Testing sites are required to help achieve their results.

According to the results of the survey, there was a serious shortage of cybersecurity professionals in the government, industry and academia. The main reason was the lack of a systematic talent cultivation system. School education did not meet industrial needs, making it difficult to promote the research and development of key technologies in Taiwan's cybersecurity industry; generally, Taiwan's enterprises lacked the cybersecurity awareness and had their network management personnel who lacked practical experience in cybersecurity work as the cybersecurity personnel concurrently. In summary, there was a serious shortage of cybersecurity professionals in Taiwan and lack of practical experience in cybersecurity. As talent cultivation is the key to the sustainable development of the industry, how to strengthen the quality and quantity of domestic talents and improve the cybersecurity capabilities of government agencies, enterprises and critical infrastructure has become the focus of the development of Taiwan's cybersecurity industry.

B. Strengths of Taiwan's cybersecurity industry

a. Increased demand for defense critical infrastructure creates a new opportunity for the cybersecurity industry

As a new area of the future development of Taiwan's cybersecurity industry, critical infrastructure protection is the focus of recent policy reforms in countries. In recent years, APT attacks against critical infrastructure have occurred one after another, causing serious harm to countries and the public. In addition to developing national policies to strengthen the defense of critical infrastructure, countries around the world are dedicated in improving their protection capabilities through practical exercises.

The government of Taiwan is following the cybersecurity practices in the developed countries and regularly reviewing the scope of defense critical infrastructure. In addition to ensuring effective, real-time information sharing, Taiwan is building sites to develop autonomous detection and monitoring capabilities while strengthening industrial control systems (ICS) such as smart meters, industrial automation, and oil refinery.

b. The increased awareness of IoT security creates an opportunity to expand cybersecurity needs

With the rapid development of IoT, how to provide a safe, secure, and reliable network environment with innovative cybersecurity services is an important issue for Taiwan's cybersecurity policy. The IoT device industry is one of the key industries for Taiwan 's cybersecurity development. With reference to the innovative cybersecurity concepts adopted in developed countries and international cybersecurity companies, Taiwan's cybersecurity enterprises expect to work with foreign cybersecurity enterprises to integrate the concept of "Security by Design" into the product development process and promote cross-domain cybersecurity development.

(5) National program to enhance national cyber resilience and to stimulate development of cybersecurity industry

As mentioned in (2) above, the development of Taiwan's cybersecurity industry promoted by each ministry/department is based on the "Action Plan for Cybersecurity Industry Development" proposed by the Department of Cyber Security. The overall structure and strategies of the said action plan proposed by the Department of Cyber Security and the current status and results of the cybersecurity development promoted by the Ministry of Economic Affairs are described below.

A. Action Plan for Cybersecurity Industry Development

Aiming at building a global cybersecurity start-up hub and promoting Taiwanese security brands, the "Action Plan for Cybersecurity Industry Development" is designed to expand cybersecurity talents, improve competitiveness of domestic cybersecurity products, increase the output value of Taiwan's cybersecurity industry, and drive the development of 5+2 industries. The four major strategies are described as follows:

a. Strategy 1: Establishing a demand-oriented training system for cybersecurity talents

Strategy 1 includes five specific measures: (1) Cultivating enterprise-specific cybersecurity talents; (2) establishing a cross-disciplinary talent cultivation system; (3) matching talents for employment; (4) recruiting international talents; and (5) setting up cybersecurity training institutions. The initial goal is to set up cybersecurity colleges and distinctive cybersecurity departments/institutes with the existing training resources; the ultimate goal is to create a world-class cybersecurity research institution.

b. Strategy 2: Consolidating the niche market and forming international partnerships

Strategy 2 includes three specific measures: (1) Consolidating the niche market; (2) creating demand and developing key technologies; and (3) forming international partnerships. By matching supply with demand in the cybersecurity industry, the strategy aims to increase the independence of local cybersecurity products; in addition, cross-domain cooperation is promoted to develop total cybersecurity solutions that can build the reputation of Taiwanese cybersecurity brands.

c. Strategy 3: Establishing product testing sites to deliver results required to enter the international market

Strategy 3 includes four specific measures: (1) Developing industry standards; (2) implementing product certification; (3) establishing testing sites; and (4) promoting domestic and international business matchmaking through industry promotion project. The initial goal is to identity quality Taiwanese cybersecurity products through certification and testing on-site and recommend them to enterprises, followed by cybersecurity certification for key connected devices in people’s livelihood.

d. Strategy 4: Fueling cybersecurity investment to establish global presence

Strategy 4 includes three specific measures: (1) Studying global cybersecurity needs; (2) raising funds for the cybersecurity industry; and (3) helping establish global

presence with integrated resources. The strategy aims to fund cybersecurity start-ups and provide them with the channels of marketing through overseas representative offices related to government diplomacy and economic trade departments in order to help them establish global presence.

B. Results of the cybersecurity development promoted by the Ministry of Economic Affairs

In line with the above-mentioned "Action Plan for Cybersecurity Industry Development," the Ministry of Economic Affairs has systematically promoted the development of Taiwan's cybersecurity industry from the aspects of talent, market, technology, standards and environment, and the results over the past three years are described below.

a. Talent: Meeting the needs of talent through on-the-job training

i. In line with Strategy 1 (cultivating enterprise-specific cybersecurity talents and establishing a cross-disciplinary talent cultivation system), the Ministry of Economic Affairs aimed to cultivate talent for key communities and industries.

ii. In terms of communities, the Ministry of Economic Affairs worked with the Hacks in Taiwan Association to organize international cybersecurity contests in hopes of enhancing local cybersecurity talents' international competitiveness; in terms of industries, the Ministry of Economic Affairs worked with domestic enterprises and industry associations to establish an independent on-the-job training system for cybersecurity professionals.

C. Between 2017 and 2018, there were a total of 1,313 trainees, and 52 of them were employed by cybersecurity companies such as SYSTEX Corporation and HwaCom Systems Inc., with an 80% employment rate.

a. Market: Setting up a cybersecurity service team to build a supply and demand matchmaking system

i. In line with Strategy 2 (consolidating the niche market), the Ministry of Economic Affairs has set up a cybersecurity service team to build a supply and demand matchmaking system for small and medium enterprises.

ii. Enterprises in need of cybersecurity were guided to query cybersecurity companies registered with the Industrial Development Bureau on the "Industry Counselling 1999" website for reference.

iii. In response to the implementation of the GDPR, the Ministry of Economic Affairs consulted with KPMG and Deloitte about related measures and worked with the cybersecurity service team to diagnose small and medium enterprises and match suitable solutions.

b. Technology: Consolidating key technologies and building cybersecurity solutions through testing sites

i. In line with Strategy 3 (implementing product certification and establishing testing sites), the Ministry of Economic Affairs has selected niche sites to test cybersecurity products, with the 5+2 innovative industries (i.e. IoT) being priorities, and opened up critical infrastructure sites (i.e. oil, water, and electricity) to help cybersecurity start-ups accumulate their experience in product development and technological research and development.

ii. In 2018, the petroleum, water, and electricity threat intelligence database was available in critical infrastructure sites for the cybersecurity service team, white hackers, and the information and communications technology branch of the Ministry of National Defense to share and analyze information.

iii. Since 2018, the Ministry of Economic Affairs has applied cybersecurity products and technologies to IoT security testing sites in other fields (i.e. smart cities and smart townships) and organized cybersecurity contests to encourage cybersecurity enterprises and research institutions (i.e. National Chiao Tung University and Hacks in Taiwan Association) to identify potential security breaches and match them with local cybersecurity products, further developing total cybersecurity solutions.

c. Standards: Developing industry standards to improve local cybersecurity products and service quality

   i. In line with Strategy 3 (developing industry standards), the Ministry of Economic Affairs has introduced international standards to Taiwan's cybersecurity industry and developed the cybersecurity testing and certification system.

   ii. Between 2016 and 2019, a total of 11 qualified APP testing labs were established, with 1,941 APPs certified.

   iii. As of 2019, a total of 7 IoT security product testing standards were developed, including 3 for video surveillance, 2 for smart buses, and 2 for smart streetlights, and 5 products from 3 cybersecurity companies passed the IP Camara certification.

d. Environment: Establishing international marketing channels to support cybersecurity start-ups

   i. In line with Strategy 4 (fueling cybersecurity investment to establish global presence), the Ministry of Economic Affairs integrated marketing channels and resources to help local cybersecurity companies establish global presence.

   ii. In 2017, Taiwan and Israel worked together to develop I.X/Vision IT; a cybersecurity solution alliance was also formed to secure orders in cooperation with nForce SECURE (Thailand).

(6) Cybersecurity ecosystem and the key players

Overall, Taiwan's cybersecurity ecosystem consists of four players, namely the senior (non start-ups) cybersecurity companies, cybersecurity start-ups, international cybersecurity companies, and academic and research institutions. With the active support of the government in recent years, hacker communities and start-ups in Taiwan's cybersecurity industry have begun to boom and inject new cybersecurity products and technologies into the industry, gradually equipping local cybersecurity companies with confidence and strength to enter the international market. The role and

influence of each player in Taiwan's cybersecurity ecosystem are described below, along with a detailed analysis of Taiwan's cybersecurity development in 2019.

A. Taiwan's cybersecurity ecosystem

Since the government of Taiwan has invested in resources to support the cybersecurity industry in recent years, some unprecedented changes have taken place. The most obvious difference is the emergence of cybersecurity start-ups. In the past three years, driven by the government's efforts to promote the cybersecurity development, a total of 22 cybersecurity start-ups have been established, 12 of which are founded by white hat hacker communities. The establishment of cybersecurity start-ups helps promote the industrial development in terms of talents and funds; the most significant significance is to inject innovation into technological research and development in Taiwan's cybersecurity industry.

The senior (non start-ups) cybersecurity companies remain the cornerstone of Taiwan's cybersecurity ecosystem and have become mature over the years. In recent years, the emergence of cybersecurity start-ups has encouraged these companies to accelerate their transformation and upgrades and investment in research and development. The senior (non start-ups) cybersecurity companies are also an important source of talent for cybersecurity start-ups. The movement of talents and technologies between the senior (non start-ups) cybersecurity companies and cybersecurity start-ups is one of the driving forces for the cycle of Taiwan's overall cybersecurity ecosystem.

In addition, research institutions are responsible for training talents and developing forward-looking technologies in the ecosystem. For example, Chunghwa Telecom, Hacker College of National Chiao Tung University, and Information Service Industry Association have worked together to establish a talent training platform. As a measure under the recently implemented policy, it is also a significant demonstration of a future training model for cybersecurity talents.

International cybersecurity companies such as IBM, Cisco, Palo Alto Networks, Checkpoint, Symantec etc., are large in scale and have reputations worldwide, majority

of them were come from US. There are hardly any Taiwanese cybersecurity companies that can compete with them; despite this, international cybersecurity companies can play a role of accelerators in the ecosystem. For example, they can open up API and build a development platform for local cybersecurity start-ups or cooperate with local cybersecurity start-ups to develop new products. Therefore, coopetition exists between international cybersecurity companies and Taiwanese cybersecurity companies.

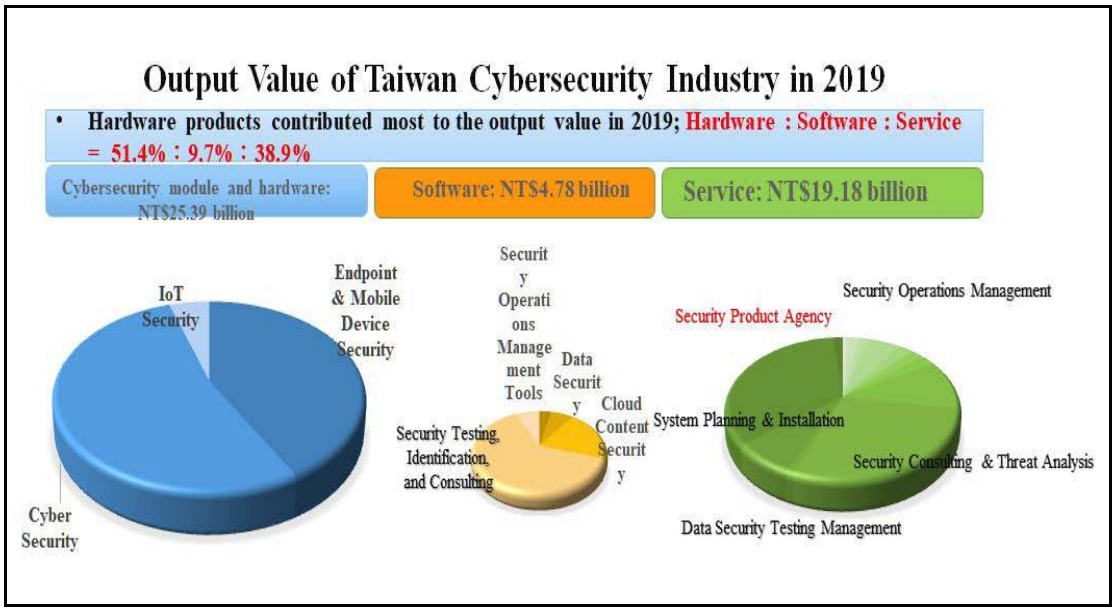
B. Taiwan's cybersecurity development in 2019

The following further analyzes the current development of Taiwan's cybersecurity industry from a supply-side perspective. The overall development will be briefly described, followed by the output value of the sub-industry.

a. Taiwan's cybersecurity development as a whole

According to the research conducted by the Industry, Science and Technology International Strategy Center, ITRI, the output value of Taiwan's cybersecurity industry in 2019 increased to NT$49.34 billion by 12.3% over 2018; there were a total of 324 cybersecurity companies and 8,800 cybersecurity professionals in the industry. Growth in 2019 was mainly driven by the substantial growth in the export of cybersecurity network hardware and the domestic demand for cybersecurity services.

In terms of the increased output value of cybersecurity services, according to the Cyber Security Management Act officially taking effect in early 2019, organs at all levels are under obligation to conduct regular cybersecurity inspections, carry out regular penetration tests, and report cybersecurity incidents. In 2019, the cybersecurity incidents occurred in domestic leading companies, which raised local business owners' awareness of cybersecurity and drove the demand for enterprise cybersecurity systems this year.



Source: Industry, Science and Technology International Strategy Center, ITRI

Figure 3 Output Value Structure of Taiwan Cybersecurity Industry in 2019

In summary, Taiwan's cybersecurity industry experienced larger growth of cybersecurity services. The proportion of cybersecurity services (professional cybersecurity services + cybersecurity agency services) to the output value of Taiwan's cybersecurity industry increased from 31% (NT$ 8 billion) in 2016 to 38.8% in 2019 (NT$ 19.9 billion) , which is close to the proportion of cybersecurity products/services in developed countries. This shows that the domestic needs of cybersecurity have clearly increased.

b. Output value of the sub-industry

Taiwan's cybersecurity industry consists of 8 types of companies, namely endpoint and mobile device security, network security, data and cloud application security, IoT security, cybersecurity operations management services, cybersecurity testing, identification, and consulting services, system integration services, and cybersecurity support services.

In 2019, revenue of nearly 60% (59%) of the domestic cybersecurity service providers was estimated to grow from the previous year, with the average revenue

increasing by 23% (mainly due to an increased domestic demand for cybersecurity services); in addition, driven by the government's policy that "cybersecurity is national security," 56% of the domestic cybersecurity companies also expected that revenue in 2019 and 2020 would grow for two consecutive years.

Source: Industry, Science and Technology International Strategy Center, ITRI

Figure 4 Output Value Distribution of Taiwan Cybersecurity Industry in 2019

The output value of endpoint and mobile device security in 2018 was NT$9.59 billion and was expected to reach NT$10.83 billion in 2019, with an annual growth rate of 12.8%. The main reasons for such growth were that shipments of mobile phone fingerprint recognition modules and server security and trusted modules were smoother than expected in 2019 and that a small quantity of emerging products such as personal security keys were delivered.

The output value of network security in 2018 was NT$12.45 billion and was expected to reach NT$13.95 billion in 2019, with an annual growth rate of 12.1%. The main reasons for such growth were that network security platforms manufactured by network IPC manufacturers for foreign cybersecurity companies grew and that the demand for cybersecurity testing and cybersecurity services in the domestic market increased.

As domestic data and cloud application security companies mainly focus on customized projects, demand for cybersecurity and software manpower is large. The market scale has grown slowly as it is difficult to cultivate domestic cybersecurity professionals. The output value of data and cloud application security in 2018 was NT$2.46 billion and was expected to reach NT$2.65 billion in 2019, with an annual growth rate of 7.8%. In terms of IoT security, the overall sub-industry is still in the testing and IT/OT integration stages, and most of the products are under discussion, experiment, or POC. The output value of IoT security in 2019 was about NT$2 billion, with an annual growth rate of 10.5%.

On the part of cybersecurity operations management services and cybersecurity testing, identification, and consulting services. Due to domestic cybersecurity policies and cyberattacks on domestic leading companies, domestic demand for cybersecurity services increased, including cybersecurity incident notifications and the establishment of cybersecurity monitoring centers. This resulted in an increase in the output value of cybersecurity operations management consulting services by 11.8% in 2019 to NT$5.03 billion and an increase in the output value of cybersecurity testing, identification, and consulting services by 12.3% in 2019 to NT$6.17 billion.

On the part of cybersecurity support services like cybersecurity system integration and cybersecurity agency services, domestic enterprises purchase local and foreign cybersecurity products and services mostly through system integrators or agents, so growth of domestic demand drives the growth of agency services. The output value of cybersecurity support services in 2019 reached NT$8.38 billion.

(7) SWOT analysis of Taiwan cybersecurity industry

A. Strength in cybersecurity

a. Semiconductor and ICT industries are Taiwan's existing strong suppliers

In Taiwan, a complete semiconductor supply chain gathers in areas such as Hsinchu Science Park, including materials, design, and wafer manufacturing, packaging and testing. With a complete semiconductor supply chain and a well-established ICT supply chain, formed a well prepared environment for cyber security companies and chipset companies cooperate to develop security function chips and support cyber security companies to develop ICT supply chain security solutions or get chance to directly practice ICT supply chain protection capability.

b. IoT security and AI integration emerge

With the continuous expansion of IOT applications, IoT security has been increasingly valued, and the diversity of IoT applications has caused more cybersecurity issues. The establishment of IoT security criteria and industry standards will help build local IoT security brands; in addition, the application of artificial intelligence (AI) to cybersecurity is one of the domains of Taiwanese cybersecurity startups. Many proactive threat detection solutions with analytical capabilities have been rolled out, which are very different from passive antivirus software products. In the future, the integration of AI and cybersecurity technology, coupled with Taiwan's ICT and semiconductor manufacturers, will be conducive to the development of edge computing-type endpoint security solutions.

B. Weaknesses in cybersecurity

a. The existing cybersecurity ecosystem lacks testing sites, standards, and resources

At present, Taiwan's cybersecurity industry lacks large-scale testing sites, which makes local cybersecurity products insufficient in depth and maturity and difficult to compete with major international manufacturers; moreover, the existing cybersecurity ecosystem lacks industry standards, testing regulations, and a complete cybersecurity testing and certification system, making products liable to foreign sanctions due to privacy breaches.

b. Connections to international markets are insufficient

At present, Taiwan's cybersecurity industry mostly exports to Asian countries, but the percentage of export is low; only 35% of the companies export to China, Malaysia, the U.S., Japan, and Singapore. Since the industry is mostly made up of small and medium enterprises and lacks international marketing resources, how to assist cybersecurity companies in developing international export strategies has become a major issue; how to assist cybersecurity start-ups in entering the international market and expanding their global presence is also a big challenge.

C. Opportunities for cybersecurity development

a. Demand for critical infrastructure (CI) protection increases

With increased cybersecurity threats and developments in recent years, governments around the world have gradually paid attention to critical information infrastructure protection (CIIP) and cybersecurity challenges in various fields such as finance, transportation, energy, and health care. These cybersecurity challenges need different solutions and dedicated talents, which creates an opportunity for Taiwanese cybersecurity companies to participate and address these cybersecurity issues. Related sites can also be opened up to develop total cybersecurity solutions through cross-domain cooperation.

b. The government poured resources to actively support

When taking office in 2016, President Tsai Ing-Wen stated that “Cybersecurity is National Security,” showing that the government attached great importance to cybersecurity. In addition to a dedicated cybersecurity unit, Department of Cyber Security, Executive Yuan, the Ministry of National Defense established the information and communications technology branch. The government has begun to invest in cybersecurity resources, improve the cybersecurity infrastructure, and strengthen the joint defense mechanism; more importantly, the Cyber Security Management Act that took effect on January 1, 2019 binds government agencies and specific non-government agencies, which is expected to drive overall cybersecurity needs.

c. GDPR’s extended scope of personal privacy protection creates business opportunities for enterprise data protection

Driven by the General Data Protection Regulation (GDPR) proposed by the EU, the protection of personally identifiable information (PII) is more stringent, and GDPR has become a new standard for global privacy protection. Such regulatory requirements create a larger cybersecurity market in Taiwan. Enterprises may expand their investment in data protection solutions in the future to ensure greater security in the application of big data. Some Taiwanese companies specializing in data protection have also continued to advance in anonymization and encryption of personal data to secure their market share with robust data protection products.

D. Threats in cybersecurity

a. International cybersecurity companies’ launch of integrated platform solutions (cloud + network + endpoint) poses a great threat to Taiwanese cybersecurity companies

As cyberattacks become more complex and diversified, threat management solutions are developed towards full protection with integrated SOC platforms that

connect endpoints, networks, and cloud services and the provision of threat intelligence, incident handling and post-disaster identification services. Traditional single-point niche solutions are no longer able to compete with major international manufacturers. Taiwanese cybersecurity companies must work together to develop integrated cybersecurity solutions and sell them in global markets.

b. International cybersecurity companies quickly occupy a dominant position in technology research and development and market competition

The number of international cybersecurity start-ups has increased significantly, leading to technology breakthroughs and innovative business models in the cybersecurity industry. This has attracted market attention and fueled merger and acquisition activities, and the introduction of new cybersecurity products and technologies has been multiplied. International cybersecurity companies continue to consolidate and expand and strike the domestic market, which poses a greater threat to Taiwanese players. After acquiring start-ups' technologies, major international companies upgrade their products and services to further secure their edges, squeezing the market share of Taiwanese cybersecurity products.

2. Overview of the Cybersecurity Development in the Netherlands

The Netherlands is one of the most competitive countries in the world in terms of the popularity of the Internet, the ICT industry, and E-commerce. The government of the Netherlands has invested a lot in the high-tech industry in Eindhoven and set up the Brainport Eindhoven Region, alongside Amsterdam's airport and Rotterdam's seaport, the three main economic pillars of the Netherlands. After Brexit, the Netherlands has become a bridge between UK and Europe and a "digital bridge" between the world and Europe.

According to the Global Competitiveness Report 2019 published by the World Economic Forum (WEF), the Netherlands is the most competitive economy in Europe

Table 3 Taiwan Cybersecurity Industry SWOT Analysis

Strengths (S)	Weaknesses (W)
1. The government policy "Cybersecurity is National Security" is a priority. 2. ICT and semiconductor supply chains are strong. 3. There is a wealth of hacker communities. 4. The Cyber Security Management Act binding government agencies and specific non-government agencies drives cybersecurity needs.	1. The scale and output value are small. 2. Small and medium cybersecurity companies have insufficient international marketing resources 3. The cybersecurity ecosystem lacks testing sites, industry standards, and resources 4. The industry lacks key technologies and professionals 5. It is difficult to retain and recruit local cybersecurity talents.
Opportunities (O)	**Threats (T)**
1. Demand for CI increases. 2. There is an increased awareness of IoT security around the world. 3. AI helps enhance the cybersecurity capacity. 4. Extension of personal data protection regulations creates business opportunities for enterprise data protection	1. International cybersecurity companies' launch of integrated platform solutions (cloud + network + endpoint) poses a great threat to Taiwanese cybersecurity companies. 2. International cybersecurity companies quickly occupy a dominant position in technology research and development and market competition.

Source: Industry, Science and Technology International Strategy Center, ITRI

mainly because of its open and dynamic economy, good physical and digital infrastructure, stable economic policy, well-educated people, effective government and well-functioning institutions.

(1) National regulatory/policy development, including government structure and functions of the departs/agencies involved

A. National cybersecurity laws and regulations

While promoting digital transformation, the Netherlands is facing many threats such as cybercrimes, industrial espionage, and malicious cyberattacks. In 2010, the Dutch Parliament called for drafting of the "National Cyber (Defense) Strategy", known as "Amendment Knops to Create a National Cyber Strategy." Accordingly, the

Ministry of Security and Justice coordinated an overall government measure and promulgated the first "National Cyber Security Strategy: Success Through Cooperation" in February 2011. In response to this strategy, the government of the Netherlands established the National Cyber Security Centre (NCSC) to oversee the coordination of national security initiatives and set up the Nederland Cyber Security Council (CSR) as a national strategic consulting agency.

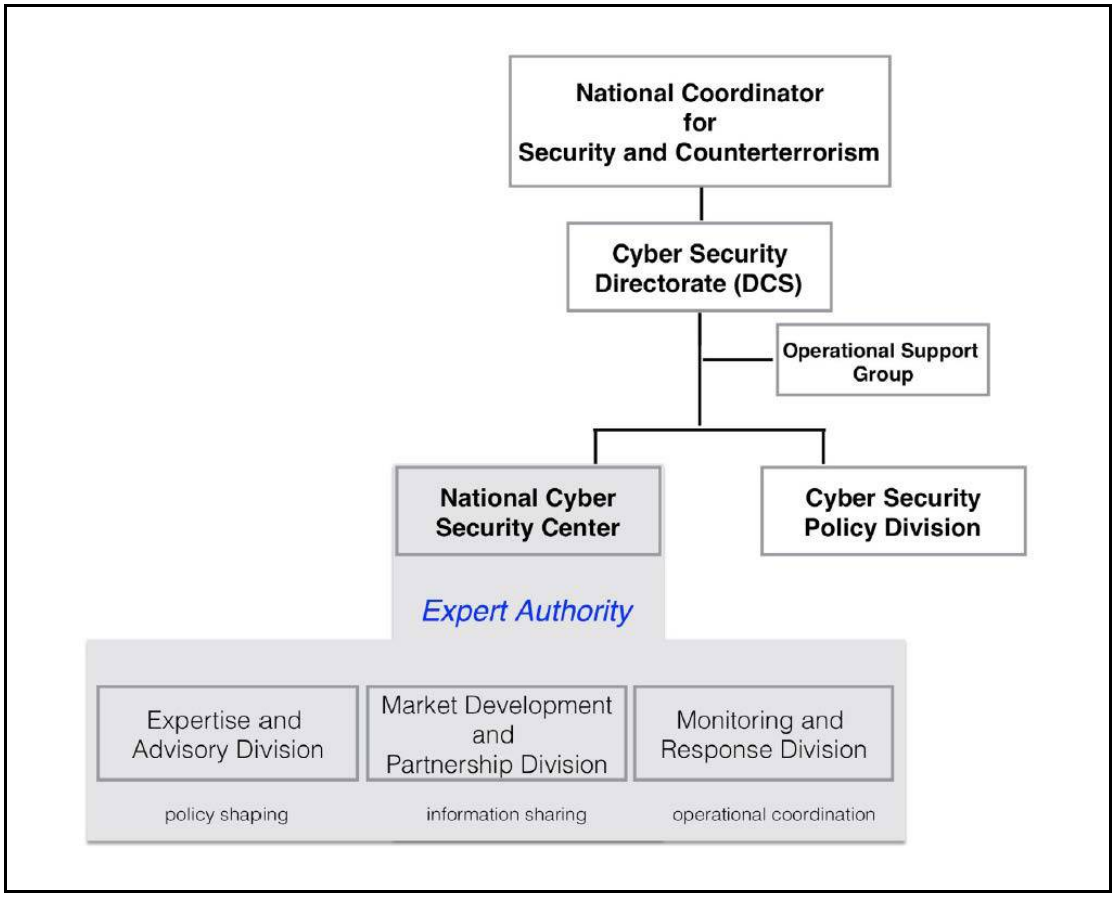
The action plan for this strategy outlines a series of priorities, including strengthening resilience to ICT disruptions and cyberattacks; cultivating rapid response capabilities; strengthening law enforcement; increasing the awareness of social network security; and promoting research, development and education.

In the face of ever-changing threats, the government of the Netherlands updates its cybersecurity framework every two years. In 2013, the Ministry of Security and Justice announced the "National Cyber Security Strategy 2: from Awareness to Capability (NCSS 2)," which clearly defines the relationships between different stakeholders, encourages private participation in international cooperation, and identifies the role of the government in establishing necessary cybersecurity requirements, regulations and standards to protect and improve the security of ICT products and services, as well as adopts a risk-based approach to strike a balance between the protection of Dutch interests and threats to Dutch interests and acceptable social risks. NCSS 2 once again promotes NCSC to a "cybersecurity expert authority" in charge of the country's digital security and cyber resilience and focuses on the cybersecurity of the central government and critical infrastructure, with its core mission expanded to build "secure, open, and stable digital information society."

In August 2017, the government of the Netherlands also published the "Cyber Security Assessment Netherlands 2017: Digital resilience is lagging behind the increasing threat." This report highlights the need for more action given the ever-changing threats, including IoT-related new vulnerabilities; more government investment is needed to enhance knowledge and expertise, strengthen collaboration between the industry, academia, and critical infrastructure, and form more effective public-private partnerships, so as to detect digital threats and fight against cybercrimes.

B. Unit in charge of cybersecurity in the Netherlands

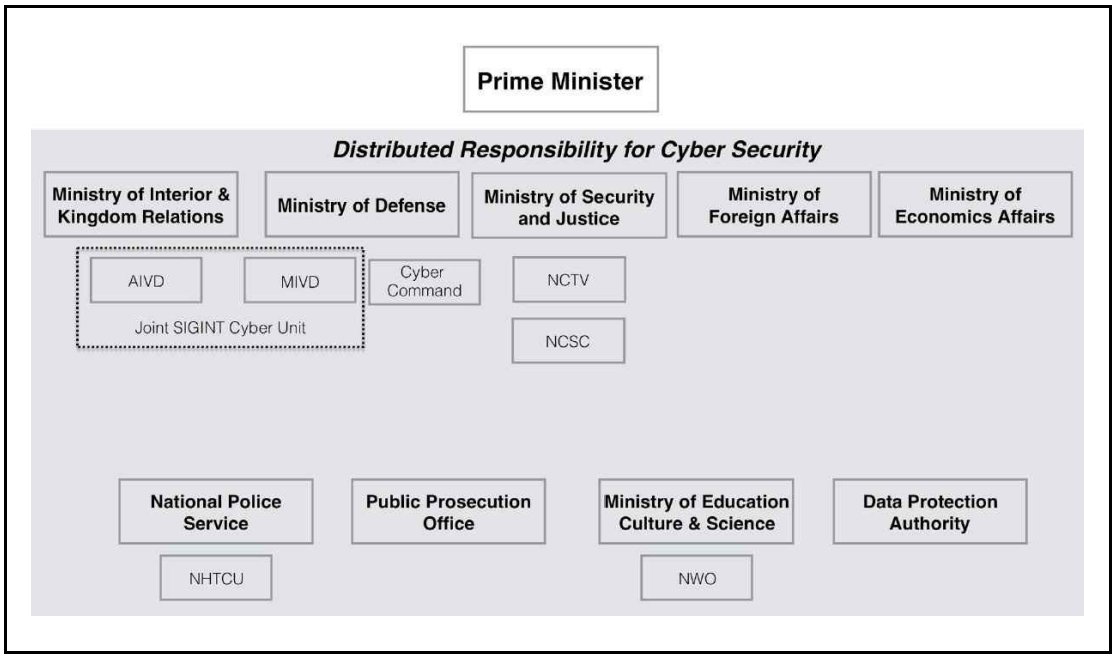
The unit in charge of cybersecurity in the Netherlands is NCSC, a division of Cyber Security Directorate (DCS). Managed by the National Coordinator for Security and Counterterrorism (NCTV) under the Ministry of Security and Justice, NCSC has jurisdiction over the Expertise and Advisory Division, specializing in cybersecurity policy recommendations, the Market Development and Partnership Division, responsible for cybersecurity information sharing and international cooperation, and the Monitoring and Response Division, responsible for cybersecurity incident monitoring and responses.



Source: The Netherlands Cyber readiness at a Glance (2017), Potomac Institute for Policy Studies

Figure 5 Organizational Structure of NCSC

However, NCSC has no responsibility or authority to direct the protective activities of other government agencies such as Ministry of Economic Affairs or Ministry of Foreign Affairs. But, NCSS 2 clearly identifies individual cybersecurity goals and collective responsibilities of at least 20 government agencies. In terms of private companies, most of the responsibilities defined in NCSS 2 fall on financial service providers, telecommunications companies, and other critical facility service providers.



Source: The Global Competitiveness Report (2019), WEF

Figure 6 National Cyber Security Organization in the Netherlands

(2) Cybersecurity ecosystem and the key players

A. Cybersecurity ecosystem counseling organizations

The Netherlands considers research and development, innovation and cooperation among companies, research institutions, and government agencies as the key to its future competition and economic strength. In 2013, the government of the Netherlands established the Hague Security Delta (HSD), a network of businesses, governments and knowledge institutions, that work together on knowledge development and innovation in security". The HSD aims to cooperate with Dutch enterprises, government agencies,

and academic institutions to jointly tackle cybersecurity and ICT innovations, thereby driving economic development with innovations. At the end of 2016, the Netherlands Organization for Applied Scientific Research (TNO) officially opened the Cyber Threat Intelligence lab to try new technologies to improve early cyber threat detection, intelligence gathering, and confidential information exchange. Recently another lab opened at the HSD campus, namely the IoT Forensics Lab by the University of Applied Sciences Leiden.

Currently, the Dutch Security cluster HSD has nearly 300 partners. In this network, security issues are discussed and knowledge is shared on cyber security, national and urban security, protection of critical infrastructures, and forensics. The HSD partners have a common goal: a more secure world, more business activity and more jobs. The HSD partners include 26 government agencies such as Ministry of Security and Justice, Ministry of Defense, Ministry of Economic Affairs, and The Hague City Hall; 19 research institutions such as The Hague Centre for Strategic Studies and TNO; and 10 academic institutions such as TU Delft and Leiden University; as well as large multinational corporations such as AIG, Cisco, and Deloitte, which account for the most, and more than 100 start-ups like Compumatica, Cyberspint, and EclecticIQ.

B. Key players

According to the landscape of the Dutch cybersecurity industry published by Cybersecurity Observatory (https://cyberstartupobservatory.com).

There are about 60 cybersecurity companies in the Netherlands. In addition to cybersecurity products such as endpoint security, network security, and cloud security, more cybersecurity companies specialize in fields of cyberattack detection, cybersecurity services, and cybersecurity operations management services, and cybersecurity intelligence. Many companies also provide services with respect to cybersecurity awareness promotion, cybersecurity training, cybersecurity compliance, and privacy compliance. Some companies have even tapped into emerging block-chain security, medical device security, and industrial control security solutions.

Source: Cybersecurity Observatory

Figure 7 Snapshot of Dutch Cyber Security Companies

(3) Strength in cybersecurity

The key advantages of the Dutch cybersecurity industry are the cultivation of cybersecurity talents and the government's investment in cybersecurity technology research and development.

A. Cultivation of cybersecurity talents

NCSS 2 particularly emphasizes the need for more coordination between the supply and demand of cybersecurity talents in order to gather innovative talents and experts. NCSS 2 also encourages the complete increase in the number of cybersecurity experts and general users' cybersecurity capabilities, "from primary education to higher education, from on-the-job training to vocational training, from the board of directors to production line workers." With this goal set, the Ministry of Security and Justice, Ministry of Economic Affairs, Ministry of Education, Culture & Science, and Netherlands Organization for Scientific Research (NWO) established the Dutch Cyber Security Platform for Higher Education and Research (dcypher) in 2016. Dcypher aims to support the national research and education agenda, with special emphasis on higher education in the field of cybersecurity, to build sufficient cybersecurity knowledge and skills and encourage innovation.

On 22 May, 2019, the 'Human Capital Agenda Security 2019-2022' (HCA Security) was published by HSD Office. The goal of the agenda is to tackle the discrepancies in the labour market by improving the qualitative and quantitative match between demand and supply of security personnel. Access to talent is a crucial prerequisite for the creation of innovative security solutions and the growth of the security sector. Due to the high demand for skilled personnel in the cyber security labor market, HSD has set up an exclusive recruitment website in the field of cyber security. The website provides students and professionals with multiple possibilities and opportunities to gain a deeper understanding of the career and long-term development of the cybersecurity industry.

The Netherlands also has an International Cyber Security Summer School (ICSS) which is an annual summer school, originally organised by NATO C&I Agency, Europol, the Netherlands Ministry of Defence Cyber Command, Leiden University and The Hague Security Delta. The first edition took place in 2015, starting with 40 students. Given the success, further editions of the Summer School have been hosted, allowing up to 60 students to participate in the program. The 2018 edition of the Summer School was also organized by EY. The International Cyber Security Summer School allows students and young professionals to gain deeper knowledge and understanding of cyber security concepts, as they will learn about the latest developments and the cutting-edge cyber security technologies that exist today. In previous editions, students received lectures and insiders' perspectives from a variety of industry experts, working for, inter alios, Europol, NATO, the Dutch Department of Security and Justice, The Dutch General Intelligence and Security Service, and the Amsterdam Internet Exchange (AMS-IX).

B. Investment in cybersecurity technology research and development

In 2012, the government of the Netherlands particularly stressed the importance of Small Business Innovation Research (SBIR). In the first phase, the government funded projects such as cybersecurity data acquisition, real-time network monitoring, and smart grid security, and BYOD security (Bring Your Own Device security), eID identification and authentication, privacy and trust management, and cyberattack detection, at a total amount of more than US$6.5 million.

In the Netherlands, investment in cybersecurity research and development is overseen by multiple government agencies such as the Ministry of Defense, Ministry of Economic Affairs, Ministry of Security and Justice, and Ministry of Infrastructure and the Environment and other independent entities like the CSR. Each year, the government of the Netherlands will spend about 400 million euros (about 436 million US dollars) on the cybersecurity research and development plans led by TNO and NWO in cooperation with the Dutch academic and business communities.

(4) International cooperation in cybersecurity

A. International cooperation in cybersecurity

The government of the Netherlands makes cybersecurity a priority in its foreign policy. In addition to cooperation with EU countries in data protection and privacy protection, the government of the Netherlands has entered into bilateral agreements with many countries. For example, the US-Netherlands Agreement on Cooperation in Science and Technology Concerning Homeland and Civil Security Matters has promoted bilateral cooperation in areas that have a direct impact on national security. Since 2012, the Netherlands and the U.S. has cooperated on the management and responses of cybersecurity incidents, control over system security, and cybersecurity exercises. Strong international cooperation and experience sharing have promoted cost and knowledge sharing and fueled the development of innovative and effective cybersecurity capabilities. The Netherlands has also cooperated with multinational organizations such as the United Nations (UN), Council of Europe, North Atlantic Treaty Organization (NATO), Organization for Economic Cooperation and Development (OECD), and European Union Agency for Law Enforcement Cooperation (Europol).

B. Netherlands-Taiwan cooperation in cybersecurity

In recent years, Taiwan and the Netherlands have also cooperated in many aspects. Since March 2018, the Ministry of Economic Affairs has commissioned the ITRI to organize the “Taiwan-Israel-The Netherlands Forum of Cyber Security in Smart Cities,” where Eindhoven University of Technology (TU/e), Security Matter, and TU/Delft from the Netherlands and the ITRI, Institute for Information Industry, and Taiwan Cyber security Center (TWISC) from Taiwan participated to discuss cooperation on cybersecurity technologies. Since 2018, the Explore Next Cyber Taiwan has been organized in Taiwan in May for two consecutive years. The HSD and Netherlands Office Taipei invited Dutch cybersecurity companies to visit Taiwan. In October 2019, the Ministry of Economic Affairs and ITRI formed a delegation

consisting of select Taiwanese cybersecurity start-ups to attend the “One Conference,” the largest international cybersecurity conference in the Netherlands, in The Hague, and also worked with the HSD to hold a roundtable forum for Taiwanese and Dutch cybersecurity companies.

Part 2. Analysis of International Collaboration Opportunities/ Constraints on Cyber Security Collaboration

1. Overview of the current status, interests in cybersecurity collaboration, and key stakeholders of bilateral cybersecurity field.

(1) Taiwan-Netherlands bilateral exchanges

Cybersecurity as sector for collaboration between the Netherlands and Taiwan started in 2018. Due to a strong interest from both sides, an extensive network with the government, academic/knowledge institutes and the private sector evolved - already showing some interesting results.

Warm connections have been established with some major organizations in the field of cybersecurity in Taiwan. An overview of activities between Dutch and Taiwanese players in the field of cybersecurity:

Table 4 Taiwan-Netherlands Bilateral Exchanges in Recent Years

Date	What	Content	Involvement
03 '18	Conference	Cybersecurity Startup Ecosystem	
05 '18	Conference	Critical Infrastructure Protection	
05 '18	MoU	Critical Infrastructure Protection	Security Matters, Taiwan Cyber security Center (TWISC) and Institute of Information Industry (III)
09 '18	Project	POC project for Critical Infrastructure Protection in Taiwan Power company and Chinese Petroleum Corporation (CPC)	Security Matters (in collaboration with local company team T5, which was introduced in May)
10 '18	Conference	GDPR	
10 '18	TW visit to the NL	Taiwan Cyber Security Delegation visiting the Cyber Security Week 2018 and visit potential partners (including the Hague Security Delta, municipality of the Hague, TU/e, TU/Delft, and University of Twente)	12 people, including participants from TWISC, III and ITRI
10 '18	Program	Collaboration with HSD in the Global EPIC soft-landing program,	

Date	What	Content	Involvement
		which will offer companies and entrepreneurs a unique opportunity to 'soft land' for a trial period in the market of one of the Global EPIC ecosystems. Participating countries including NL, Taiwan, UK, Canada, Poland and USA	
	Contract	Contracted by Taiwanese government	Ecorys and Equidam
03 '19	MoU	TU/Delft visited Taiwan on the topic of Cyber Security and signed an MoU with TWISC	TU/Delft and TWISC
05 '19	Innovation Mission & Joint Symposium	Fact finding mission in cooperation with team IRIS, including TW-NL Cybersecurity Exchange Forum	Companies joining from the NL
10 '19	Mission	Taiwanese delegation joining the One Conference in the Netherlands. Highlight: NL-TW Round Table Discussions, one for business and one for academics	Companies joining from TW

Source: Netherlands Office Taipei

(2) Cooperation with the HSD

In 2018, the Industrial Development Bureau, Ministry of Economic Affairs secured cooperation with the HSD, the Dutch Security cluster and became a member of the Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC). By establishing a global innovation ecosystem, the Global EPIC advocates realizing cybersecurity and economic benefits, developing global initiatives, and sharing expertise within a diversified network. Taiwan was the first country in Asia to join the Global EPIC. In the future, Taiwanese cybersecurity companies can connect with international cybersecurity industry clusters and obtain supports to enter local markets. Through the Global EPIC, ECOLUX, a firmware protection start-up in Taiwan, has been referred by the HSD to a German system integrator to discuss future cooperation on product development.

At the One Conference round table held in the Netherlands in October 2019, bilateral representatives from Taiwan and the Netherlands exchanged opinions on how cybersecurity start-ups should obtain assistance from local cooperation resources when entering the local market. Many Taiwanese and Dutch vendors expressed high interest in expanding into the other market through the Soft Landing project. In addition, in the "New Venture Floor" exhibition area specially set up by One Conference, it can be found that the organizer specifically targets students and research institutions, and retains several booths, so that startups from academic research units have the opportunity to practice business management and let them understand that technology is as important as marketing

Source: Industry, Science and Technology International Strategy Center, ITRI

Figure 8 ITRI and HSD Collaboration

2. Potential obstacles and constraints for collaboration, such as cultural, regulatory and diplomatic

The cooperation between Taiwan and the Netherlands in the field of cybersecurity is in the nascent stages, where both parties are trying and exploring suitable cooperation models. At present, cybersecurity companies in Taiwan and the Netherlands are active in communicating with each other about possible cooperation. The government of Taiwan is optimistic about and open to international cooperation or connection, and has been supportive for local industries in terms of legislation with respect to economy and trade and business cooperation; however, there are differences between Eastern and Western cultures; in addition, Taiwan remains a special political entity for the international community. These factors will more or less affect the establishment of bilateral cooperation between Taiwan and the Netherlands.

The potential cultural obstacles may come from the different business habits in Eastern and Western countries, especially the establishment of cooperation models. In early days, business people attached great importance to interpersonal relationships and took trust and commitment seriously; they often entered into verbal agreements more than written contracts. This is quite difficult for Western companies to adapt and accept and is liable to increase the cost of communication and confirmation. Thanks to globalization, most Taiwanese companies have tended to adopt or follow Western business culture and paid attention to the formulation and signing of contracts.

In terms of potential diplomatic obstacles, Taiwan has a special position in the international community and is not a member of the United Nations. It has been relatively difficult to establish diplomatic relations for a long time; in addition, China has repeatedly imposed pressure on countries around the world, including Taiwan's diplomatic ties, to intensify the restrictions on Taiwan's diplomatic development. Even applications to join non-political or economic related international non-profit organizations such as WHO are rejected. Countries are also very conservative and cautious when encountering issues of cooperation with Taiwan, making it difficult to achieve their ideal goals. At present, informal contact and communication with

international organizations through semi-official organizations is the main way to eliminate potential external obstacles.

The Taiwanese government takes a positive and open attitude towards the development of the cyber security industry, and is optimistic about any kind of domestic and foreign cooperation opportunities that Taiwanese cyber security companies could grasp, whether it is cooperative R&D of technology and products or cooperative market expansion. However, in practice, there are still many difficulties for Taiwan and Netherlands bilateral cyber security vendors to overcome in cooperation. In terms of cooperation to expand the market, since the domestic market size of both parties is quite limited, it is not proper to see occupy each other's market as the ultimate cooperation goal, so as not to fall into the zero-sum deadlock. In terms of R&D cooperation, there are also various risky factors such as confidential protection, homogeneous competition, trust, patents, and ownership of achievements. If it is not from a complementary perspective, there will be hard to find a chance for cooperation.

3. Focus areas for cybersecurity cooperation and the expected benefits, including B2B market

At present, Taiwan-Netherlands cooperation focuses on market expansion, technological cooperation, and policy exchange. The expected benefits are described below.

(1) Market expansion

In terms of market expansion, Taiwan and the Netherlands should be able to take the regional marketing as the main direction and enter the bilateral domestic market as a supplement. Since both parties are members of Global EPIC, it should be possible to discuss the development of advantageous products and services through this platform and jointly strive for opportunities in the EU market. In addition, Taiwan-Netherlands can introduce each other's products and provide more choices based on bilateral market demand gaps.

(2) Technological cooperation

The Netherlands is one of the world's leading countries in cybersecurity technology. Taiwan and the Netherlands may evaluate their respective cybersecurity technologies and work together to develop total solutions based on a complementary model while guiding the development of next generation technologies.

(3) Policy exchange

Both Taiwan and the Netherlands share common cybersecurity policy issues such as IoT security, 5G security, and supply chain security and establish common product or technology security standards. After entering into partnership, both parties may share more information on their standardization processes, key policies, and leading pilot cases as a reference for future administration.

Part 3. Conclusions and Recommendations

1. Synergies and benefits of bilateral cooperation in cybersecurity

(1) Both Taiwan and Netherlands are gateways to economic and trade activities and can assist each other in entering surrounding markets

Both Taiwan and the Netherlands are major gateways to economic and trade activities in each geographic area. By assisting cybersecurity start-ups in landing in each other's region, both parties may work together to enter the surrounding markets. For example, Taiwan is a key hub for the cybersecurity industry in the Asia-Pacific region. After Dutch cybersecurity companies land in Taiwan, they can use Taiwan as the center to expand the Asia-Pacific market; similarly, the Netherlands is a gateway to the European market. After Taiwanese cybersecurity companies land in the Netherlands, they can use the Dutch experience to advance into the European market.

(2) Taiwanese and Dutch cybersecurity industries are similar and complementary

The similarities between Taiwanese and Dutch cybersecurity industries are that domestic demand is relatively small and that cybersecurity companies are mostly small and medium-sized; in addition, both Taiwan and the Netherlands are located at the intersection of regional cyberattacks. With the emergence of digital economy, well-established ICT infrastructure is conducive to the development of cybersecurity start-ups. For Taiwan and the Netherlands, a potential opportunity for cooperation comes from their complementary cybersecurity products and technologies. Taiwanese companies have the advantages of Hardware cybersecurity platforms and threat intelligence while Dutch companies have the advantages of cybersecurity intelligence and infrastructure management and monitoring.

(3) Cooperation opportunities on IoT security testing mechanisms

In October 2019, the Ministry of Economic Affairs of the Netherlands and the Cyber Security Agency of Singapore published the "Internet of Things Security

Landscape Study," which is a referable policy guide. Although Taiwan does not have a sound IoT security regulation, it has very successful experience in promoting individual IoT products such as the "video surveillance system cybersecurity standards and certification/verification system." An English version of the "IoT Security Industry Standards" has been promulgated to promote international exchange. Taiwan and the Netherlands may cooperate to set up the interoperable and mutually recognized IoT security standards and certification mechanism to strengthen the cybersecurity capabilities of smart cities and IoT devices.

2. Vision and goals of the bilateral cooperation in cybersecurity

(1) Strengthening the development of Taiwanese and Dutch cybersecurity start-ups in regional markets

The results of exchanges between the Art of Cyber War (ACW) under the Industrial Development Bureau, Ministry of Economic Affairs and the NTIO, HSD, and Netherlands Enterprise Agency (RVO) over the past two years have started to roll in. In the future, Taiwan and the Netherlands will expand cooperation with the Global EPIC such as Soft Landing to provide more institutional supports, including legal affairs regarding company setup, accounting and tax affairs, business matchmaking, and local recruitment, for cybersecurity start-ups which are ready to land in Taiwanese and Dutch markets.

(2) Cooperating to advance into international markets

By sharing threat intelligence, Taiwanese and Dutch cybersecurity companies may work together to enter the surrounding markets. For example, cybersecurity threats sometimes vary across regions. Through bilateral cooperation, Taiwan and the Netherlands can fully share intelligence and control cyberattack patterns more completely to achieve real-time protection. The combination of Taiwanese network hardware and Dutch software applications may also be a potential cooperation model.

3. Short, medium- and long-term strategies and action plans

Taiwan-Netherlands cooperation strategies and models are proposed below from three aspects: government cooperation, information sharing, and business matchmaking.

(1) Government cooperation: Loosen restrictions for release testing site to facilitate industrial development

A. Taiwan's IoT security standards and certification experience can be the center of cooperation between Taiwan and the Netherlands

Taiwan has very successful experience in promoting the "video surveillance system cybersecurity standards and certification/verification system" and has promulgated an English version of the "IoT Security Industry Standards." Many organizations, including, the European Telecommunications Standards Institute, Cyber Strategy and Cybersecurity Science Research Center (Singapore), National Institute of Information and Communications Technology (Japan), and Malaysian Technical Standards Forum Bhd, have expressed willingness to cooperate with Taiwan. If Taiwan and the Netherlands can work together to establish the interoperable and mutually recognized IoT security standards and certification mechanism, it will help strengthen both parties' cybersecurity capabilities of smart cities and IoT devices.

B. Both parties open up testing sites

Taiwan and the Netherlands can open up testing sites for cybersecurity companies to develop multinational cybersecurity solution. For example, the Hague City Hall has organized the "Hack the Hague" for three consecutive years. In the future, the Hague City Hall may organize the "Hack the Hague" in cooperation with a city in Taiwan to test both parties' cybersecurity capabilities or to test Dutch industrial control cybersecurity solutions in smart manufacturing sites in Taiwan.

(2) Information sharing: Strengthen information sharing and bilateral business cooperation

A. Information/intelligence sharing

TWISC has been working with the Eindhoven University of Technology and TU/Delft for a long time. In the future, both parties may work further to share cybersecurity information/intelligence collected in Asia and Europe.

B. Regular visits and exchanges

In addition to organizing international conferences and exchanges for cybersecurity companies, Taiwan and the Netherlands may consider leveraging the Soft Landing project to provide more institutional supports, including legal affairs regarding company setup, accounting and tax affairs, business matchmaking, and local recruitment, for cybersecurity start-ups which are ready to land in Taiwanese and Dutch markets.

(3) Business matchmaking: Strengthen supply chain security and the development of cybersecurity start-ups

A. Learning from the Cyber Resilience Centre in Brainport Eindhoven

In September 2019, the Cyber Resilience Centre in Brainport Eindhoven was established in the High Tech Campus Eindhoven to improve the overall cybersecurity and network recovery capabilities of the Dutch high-tech industry and its supply chain. Taiwan's electronics industry and ICT industry are also active in building industry-specific cybersecurity mechanisms. Taiwan may refer to the model of the Cyber Resilience Centre in Brainport Eindhoven and have discussions or share information on a regular basis to establish a cyber resilience center for the local high-tech industry. Currently, Taiwan Semiconductor Manufacturing Company (Taiwan) and ASML (Netherlands), the world's largest manufacturer of lithography machines, are the upstream and downstream suppliers, respectively, in the semiconductor industry, and

their respective suppliers work together as well. Taiwan and the Netherlands may build on this to become a globally trusted, secure manufacturing supply chain.

B. Dutch cybersecurity companies can provide more options for Taiwan's three key industries

According to the results of the survey conducted by the ISTI, among Taiwan's three key industries, the manufacturing industry has the most urgent needs for IT/OT system security, data access control, and data leakage protection. The healthcare industry focuses on system compliance, IT/OT security, and data access control. Although the Financial industry has invested greatly in cybersecurity, there is still room for improvement in system compliance.

After mapping the cybersecurity need of Taiwan's three key industries to the landscape of the Dutch cybersecurity industry published by Cybersecurity Observatory, we have found that there are at least 7 major Dutch cybersecurity companies (SECURITY MATTERS, True-xs, Secura, GUARDIAN 360, Secure Link, ThreadStone, Hudson Cybertec) in the field of ICS/SCADA, showing a sufficient technological capacity. This is a great opportunity for business matchmaking for the cybersecurity industry in Taiwan and the Netherlands; in addition, cybersecurity protection policies and procedures and data loss prevention (DLP) are fields where Taiwan's three key industries put more emphasis and have urgent needs. More than 12 Dutch cybersecurity companies invest in compliance & DLP, which is another direction of cooperation in the future.

C. Cooperating to advance into global markets

Dutch cybersecurity companies have sufficient capabilities of cybersecurity testing services, cybersecurity operations management services, and cybersecurity intelligence while Taiwanese cybersecurity start-ups have sufficient capabilities of cybersecurity hardware, cyberattack detection, and threat intelligence. As both cybersecurity markets are composed of small and medium enterprises, Taiwanese and

Dutch cybersecurity companies must find the right partners to expand the respective markets. For example, the short-term plan is to find suitable partners (i.e. system integrators in similar application fields and cooperative cybersecurity companies) to conduct the proof of concept for solutions in specific fields of application; the medium-term plan is to promote sales in related fields; and the long-term plan is to expand surrounding markets based on Taiwan and the Netherlands.

Acronyms

ACW	Art of Cyber War
AI	Artificial Intelligence
APT	Advanced Persistent Threats
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CPC	Chinese Petroleum Corporation
CSR	Cyber Security Raad (Cyber Security Council)
DCS	Cyber Security Directorate
DCSPHER	Dutch Cyber Security Platform for Higher Education and Research
GDPR	General Data Protection Regulation
Global EPIC	Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity
HSD	The Hague Security Delta
ICS	Industrial Control Systems
ICT	Information and Communications Technology
III	Institute of Information Industry
IoT	Internet of Things
ITRI	Industrial Technology Research Institute
MOEA	Ministry of Economic Affairs
NCSC(Netherland)	National Cyber Security Centrum
NCSC(UK)	National Cyber Security Centre
NCSS 2	National Cyber Security Strategy 2
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid (National Coordinator for Security and Counterterrorism)
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek (Netherlands Organization for Scientific Research)
PII	Personally Identifiable Information
POC	Proof of Concept
RVO	Rijksdienst voor Ondernemend Netherland (Netherlands Enterprise Agency)
SBIR	Small Business Innovation Research
SOC	Security Operation Center
SRB	Strategy Review Board Meeting
TLS	Transport Layer Security
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (Netherlands Organization for Applied Scientific Research)

TPEx	Taipei Exchange
TWISC	TAIWAN INFORMATION SECURITY CENTER
TWSE	TAIWAN STOCK EXCHANGE
VPN	Virtual Private Network
WEF	World Economic Forum

Appendix

Table 5　Recommended list of matchmakers

Category	Vendor's English Name	Vendor's Chinese Name
Manufacturing	AAEON TECHNOLOGY INC.	研揚科技股份有限公司
Manufacturing	ACCTON TECHNOLOGY CORPORATION	智邦科技股份有限公司
Manufacturing	ADVANTECH CO., LTD.	研華股份有限公司
Manufacturing	ARCADYAN TECHNOLOGY CORPORATION	智易科技股份有限公司
Manufacturing	ARDOMUS NETWORKS CORPORATION	宇曜智能股份有限公司
Manufacturing	ASKEY COMPUTER CORP.	亞旭電腦股份有限公司
Manufacturing	ASUSTEK COMPUTER INCORPORATION	華碩電腦股份有限公司
Manufacturing	COMPAL ELECTRONICS, INC.	仁寶電腦工業股份有限公司
Manufacturing	DELTA ELECTRONICS, INC.	台達電子工業股份有限公司
Manufacturing	HITRON TECHNOLOGIES INC.	仲琦科技股份有限公司
Manufacturing	MOXA INC.	四零四科技股份有限公司
Manufacturing	NANYA TECHNOLOGY CORPORATION	南亞科技股份有限公司
Manufacturing	QUANTA COMPUTER INC.	廣達電腦股份有限公司
Manufacturing	SERCOMM CORPORATION	中磊電子股份有限公司
Manufacturing	ZYXEL COMMUNICATIONS CORPORATION	合勤科技股份有限公司

Healthcare Industry	National Taiwan University Hospital Zhudong Branch	國立臺灣大學醫學院附設醫院竹東分院
Healthcare Industry	National Cheng Kung University Hospital	國立成功大學醫學院附設醫院
Healthcare Industry	Taiwan Blood Services Foundation	台灣血液基金會
Healthcare Industry	Tung's Taichung MetroHarbor Hospital	童綜合醫療社團法人童綜合醫院
Healthcare Industry	Cheng Ching Rehabilitation Hospital	澄清復健醫院
Financial Industry	FINANCIAL INFORATION SERVICE CO., LTD	財金資訊股份有限公司
Financial Industry	FUBON FINANCIAL HOLDING VENTURE CAPITAL CORPORATION	富邦創業投資股份有限公司
Financial Industry	TAIWAN STOCK EXCHANGE	台灣證券交易所股份有限公司
Financial Industry	China Development Financial Holding Corporation	中華開發金融控股股份有限公司
Financial Industry	EnTie Commercial Bank	安泰商業銀行股份有限公司

This is a publication of
Netherlands Enterprise Agency
Prinses Beatrixlaan 2
PO Box 93144 | 2509 AC The Hague
T +31 (0) 88 042 42 42
E klantcontact@rvo.nl
www.rvo.nl

This publication was commissioned by the ministry of Foreign Affairs.

Publication number: RVO-109-2020/RP-INT

NL Enterprise Agency is a department of the Dutch ministry of Economic Affairs and Climate Policy that implements government policy for Agricultural, sustainability, innovation, and international business and cooperation. NL Enterprise Agency is the contact point for businesses, educational institutions and government bodies for information and advice, financing, networking and regulatory matters.

Netherlands Enterprise Agency is part of the ministry of Economic Affairs and Climate Policy.