Netherlands Cyber Security Roadmap Towards Taiwan

February 2022 (update March '23)

Authors: Security Delta (HSD), Innovation Quarter (IQ),
Netherlands Office Taipei (NLOT),
Rijksdienst voor Ondernemend Nederland (RVO)

Summary

The aim of this roadmap is to provide an integral approach to knowledge exchange, innovation collaboration, and business facilitation between the Netherlands and Taiwan in the field of cyber security. By identifying the areas of synergy between the Netherlands and Taiwan, this roadmap structures the objectives for collaboration and formulates related activities. The roadmap is established through a collaborative effort by the Dutch cyber sector, Security Delta (HSD), Innovation Quarter (IQ), the Netherlands Enterprise Agency (RVO), and the Netherlands Office Taipei (NLOT) and is intended for the Dutch cyber security private sector as well as relevant (research) institutes.

Cyber security is a priority sector in both Taiwan and the Netherlands. Since 2018, Taiwan and the Netherlands have increasingly cooperated on this sector. The potential opportunities for cooperation between the Netherlands and Taiwan generally follow complementary characteristics of the cyber security landscapes. In particular, the combination of Taiwanese network/ICT hardware and Dutch software applications creates an interesting cooperation model. The identified opportunities include academic research collaboration, the integration of ICT hardware and cyber security software, joint business incubation, and joint business development. Based on the analysis of the Dutch and Taiwanese cyber security sectors, these opportunities lay, amongst others, in the fields of ICT, operational security (e.g. IoT, critical infrastructure), and expertise from Dutch niche players on topics as threat intelligence, penetration testing, and data security (privacy). To illustrate, Taiwan is a large-scale manufacturer of network hardware and IoT applications; collaboration with Dutch cyber software companies will enhance the products and widen the market for Dutch cyber solutions. Moreover, the international market for niche solutions such as IoT and critical infrastructure applications is expected to grow and mature in the coming years. Utilizing the complementary characteristics of the Dutch and Taiwanese cyber sectors, joint solutions and services can be developed. Furthermore, for Dutch cyber security companies, the collaboration with Taiwan can be used to access surrounding markets in (South)East Asia and the Pacific region, and vice-versa.

In addition, while the Netherlands has strong niche players and a history of international and cross-sectoral cooperation, Taiwan has a demand for cyber security in its critical infrastructure and key industries, especially in the manufacturing (such as network hardware, IoT applications and semiconductor) and the health care and financial sectors.

The overall goal of the Netherlands Cyber Security Roadmap towards Taiwan is formulated as:

▶ The Netherlands and Taiwan create integrated solutions in ICT hardware and cyber security software via strong academic, innovation, and business collaborations.

Working towards this goal, all events will be aligned via objectives, for which three main focus areas have been chosen:

Knowledge: Facilitate knowledge and information exchange between the Netherlands and Taiwan in the fields of research, business, and policy.

Innovation: Stimulate academic and R&D collaboration between universities, research institutes, and cyber companies from the Netherlands and Taiwan.

Business: Support bilateral/international business development for Dutch and Taiwanese cyber companies.

Contents

Introduction

Digitalization is one of the most important drivers of current economic growth and offers solutions for various societal challenges. At the same time, due to the rapid adoption of digital technologies and increased vulnerability to cyber risks, cyber security has become a significant challenge worldwide. The role of cyber security is therefore becoming increasingly important for protecting information, data, and privacy, as well as securing industry and (critical) infrastructure. Both Taiwan and the Netherlands have frequently suffered cyber incidents in the past.

The Netherlands Cyber Security Roadmap towards Taiwan presents a multi-annual programming, as envisioned by a collaboration of the Dutch cyber sector, Security Delta (HSD), Innovation Quarter (IQ), the Netherlands Enterprise Agency (RVO), and the Netherlands Office Taipei (NLOT). The roadmap is intended for the Dutch cyber security private sector as well as relevant (research) institutes. This roadmap is built around the shared ambition of establishing growth in the Dutch and Taiwanese cyber security sectors through interaction with relevant companies, research organizations, and institutions. By structuring activities along the presented strategy with a common goal, less fragmentation and more focus, we mean to facilitate Dutch parties gaining an understanding of the Taiwanese cyber security landscape and the opportunities that arise from it.

To actualize Dutch-Taiwanese interactions on cyber security topics, coordinated cooperation between public sector and private sector is paramount. Working together towards a shared ambition requires an understanding of the current demand and supply in these markets, and the societal issues these originate from. Hence, this roadmap presents an outline of the cyber security landscapes of Taiwan and the Netherlands in order to identify areas of synergy. The characteristics and qualities of certain (sub)sectors and niches are envisioned to be complementary to one another and therefore could give rise to new R&D and/or business opportunities.

Meanwhile, the COVID-19 pandemic has shown a substantial increase in the use of digital networks, online activities, and cybercrime. Digital networks moved from being important, to being crucial for day-to-day activities. Having security capabilities in place has become a requirement for both businesses and governments in a syn-pandemic economy, presenting new opportunities to cyber security companies. Nonetheless, the pandemic (and the unpredictable nature thereof) can also be a hurdle when trying to establish international collaboration between Dutch and Taiwanese organizations, especially when it comes to physical activities such as business visits and missions.

This roadmap is a living document and will be reviewed annually by Security Delta (HSD), InnovationQuarter (IQ), the Netherlands Enterprise Agency (RVO), and the Netherlands Office Taipei (NLOT). During this review, developments in policies, international investing trends or the pandemic will be accounted for.

Cyber Security in Taiwan and the Netherlands

TAIWAN

Taiwan occupies a unique economic and political position on the world stage. It is a world leader in manufacturing and is especially renowned for its dominant network hardware and semiconductor industry. To illustrate, Taiwan is the number 1 manufacturer of ICT hardware products worldwide and semiconductor giant TSMC alone accounts for 54% of the 2020 global cyber security foundry market as well as 15% of Taiwan's gross domestic product. Needless to say, the semiconductor industry plays a key role in the successes of rapidly emerging digital technologies such as IoT, AI, robotics, electric vehicles and quantum computing.

Taiwan is one of the most digitally attacked economies in the world, both in the private and public sector. This is exemplified by the WannaCry-attack on TSMC in August 2018, resulting in a loss of 2.6 billion NTD (≈81.7 million EUR). Since then, several Taiwanese tech companies like Foxconn, Compal electronics, Asus, Acer, and Quanta also became victims of cyber-attacks. Moreover, the number of cyber-attacks against the Taiwanese Ministry of Foreign Affairs increased 40-fold between 2018 and 2020 and have significantly increased during the COVID-19 pandemic. After the visit of speaker Pelosi to Taiwan, cyber attacks on Taiwan government units on Tuesday surpassed 15,000 gigabits, 23 times higher than the previous daily record. Threats like these have prompted increased awareness of cyber security challenges in public and private sectors in Taiwan.

Following the above-described characteristics, cyber security holds a prominent position in Taiwan's national policy on industrial development. In 2018, President Tsai Ing-Wen introduced the slogan "Cyber Security is National Security" , showing that the government attaches great importance to cyber security. The *Action Plan to develop the Cyber Security Industry*, next to the *National Cyber Security Program of Taiwan (2017-2020)* aimed to lay a foundation for a safe and trustworthy digital society through government investments in cyber security infrastructure and joint defense mechanisms. More recently, with a budget of 113 billion NTD (≈3.55 billion EUR), the program for *Promoting the Six Core Strategic Industries includes* cyber security as one of the core strategic industries. The program is aimed at taking early advantage of global supply chain transformations in the post-pandemic era to position Taiwan as a key power in the world economy. Moreover, the *Taiwan Cyber Security Center of Excellence Program (in Mandarin)* is launched, containing a budget of 818 million NTD (≈25.7 million EUR), focusing on developing core technologies, cultivating cyber security professionals, developing ICS security training sites for critical infrastructure protection, start-up incubation, and international cooperation.

The Taiwanese government is putting forth efforts to increase cyber resilience through regulatory reform, establishing sectoral cyber security standards, stimulating the development of the cyber security sector and technology, and government restructuring. In 2021, Taiwan established a Cyber Security Demonstration Center in Shalun, Tainan, where live exercises are conducted in a variety of industries. The center also plays a role in certification and talent cultivation.

In 2022 the Ministry of Digital Affairs (MODA) was established. The Ministry of Digital Affairs is responsible for promoting Taiwan's overall digital policy innovation and reform. By consolidating the five major fields of telecommunications, information, cyber security, internet, and communications, MODA plans digital development policies and coordinates infrastructure, environment preparation, and resource management to ensure national cyber security, encourage cross-sectoral digital transformation, and enhance digital resilience.

Next to this, the National Institute for Cyber Security has been launched in January 2023. Its goal is to enhance the nation's cyber security technology competence, and promote the research, development, and application of cyber security technology. It does this through its own research, assisting government agencies and critical infrastructure, nurturing talents and promoting awareness, and supporting industry development and regulations.

These efforts aim to strengthen Taiwan's overall cyber security capacity and make it a more secure and digitally resilient economy.

You can find a more extensive overview of the cyber security markets of Taiwan and the Netherlands in the report on *“Research of Cyber Security Industry in Taiwan”* by the Industrial Technology Research Institute (June 2019).

The Taiwanese cyber security sector is mainly focused on the development of cyber security solutions for 5G, IoT, AI and industrial innovations, as well as opportunities ensuing from personal data protection regulations. The commencement of the Cyber Security Management Act (2019) stimulated this domestic demand, by stating that private organizations are obliged to enforce personal data protection while providers of critical infrastructure are obliged to implement a cyber security maintenance plan that complies with the requirements of the assigned cyber security responsibility level.

The aforementioned study on the domestic Taiwanese market, shows that in the three largest industries (manufacturing, banking, and health care), 73% of the enterprises had elementary abilities to prevent cyber attacks, however; only 14% of the enterprises had advanced abilities to prevent cyber attacks. The survey also found that about 40% of the manufacturing companies have to strengthen their security in the areas of identity and access control, data security, and system security.

As a result of the policy priority of cyber security, both government authorities and private companies in Taiwan have increased their investments in cyber security in recent years, resulting in a booming sector. The overall output value of Taiwan's cyber security industry in 2019 increased to NT$49.34 billion (≈1.55 billion EUR) by 12.3% over 2018. Nearly 60% of the domestic cyber security service providers were estimated to grow from the previous year, with the average revenue increasing by 23%. The Taiwanese sector has proved particularly strong in hardware solutions; this growth was mainly driven by a substantial increase in the export of cyber security network hardware.

THE NETHERLANDS

The Netherlands has one of the largest digital infrastructures, making it the digital gateway to Europe. The country is hosting the world's largest Internet Exchange points, over 290 data centers and 11 of 15 transatlantic sea cables come to land in the Netherlands. Today's Dutch economy has become highly dependent on this infrastructure and the foreign investments that result from them. Consequently, the Dutch government recognizes the importance of ICT infrastructure, encourages its domestic development, and has made large investments in the high-tech industry. Hence, cyber security is considered essential.

Yet also, the Netherlands has to deal with economic and market-based threats such as cybercrimes, industrial espionage, and malicious cyberattacks. As a reaction to these threats, the National Cyber Security Centre (NCSC) of the Ministry of Justice and Security was established as National CERT for critical infrastructure. As the protection of ICT infrastructure is mostly decentralized, the Netherlands shows a large number of CERTs that are specialized in different sectors and hosted by multistakeholder initiatives. Furthermore, the Digital Trust Center (DTC) hosted by the Ministry of Economic Affairs plays a role in promoting cyber resilience in the private sector by sharing information, tools, and advice.

Every two years, the Netherlands Ministry of Security and Justice publishes the “National Cyber Security Strategy” (NCSS) following ever-changing threats. In the last years, it emphasized the need for more coordination between the supply and demand of cyber security talents. Furthermore, the government has committed to spend about 400 million euros on cyber security research and development plans led by NWO and TNO, in cooperation with the Dutch academic and business communities.

The Netherlands can be described as an “open and dynamic economy” and is seen as a leader in Europe on cyber security - with a strong research, startup, and practitioner ecosystem. The amount of venture capital invested in Dutch technology startups was nearly 1.7 billion euros, a number that is growing every year. The Netherlands has an international business climate and a multilingual workforce, making the country a strategic location as “the digital gateway to Europe”. Besides, Dutch cyber security products are considered transparent, privacy-and user-friendly. While the Netherlands is large enough to distinguish itself on a global level, it is also small enough to pose no threat to other countries, therefore, perceived as a reliable partner that delivers trustworthy technology. Another supporting factor in this is that the Netherlands has a strong hacking community. This allows for a multidimensional insight into cyber security. In the coming years, this will be further implemented through the new European NIS2 legislation, which means that more sectors will be named ‘critical infrastructures’.

The Netherlands distinguishes itself in the following four key sectors/niches:

1. Operational Technology (OT) / Internet of Things (IoT) Security

   The Netherlands has a strong industrial economy, amongst others in high-tech manufacturing, chemicals, and energy. This has made Operational Technology (OT) and Industrial Control Systems (ICS) security an area of focus for entrepreneurs and researchers.

   Furthermore, the Dutch government, cyber security industry, and universities have recently started a major research program called “INTERSCT”. This program is focused on securing everything related to the Internet of Things (IoT). IoT is likely to remain a priority research area for the Netherlands because emerging technologies such as 5G are expected to catalyze IoT device connectivity.

2. Penetration Testing / Vulnerability Scanning
   The Netherlands has ample experience in the field of hacking and cyber security. The hacking culture in the Netherlands has created a strong talent pool for services firms to find researchers and testers. This has helped differentiate the Netherlands in "offensive" security and responsible disclosure, including penetration testing and vulnerability scanning services and technologies.

3. Threat Intelligence
   The earlier a possible cyber threat is detected, the less damage can be done to potentially critical systems (e.g. financial sector, energy, water, etc). Threat intelligence is about collecting, analyzing and interpreting (large amounts of) cyber threat information. The rapid exchange and sharing of this information with relevant stakeholders are important conditions for improving cyber resilience. In this, the Dutch cyber sector can play an important role because of its strong reputation in threat intelligence and its role as a neutral partner. Indications of cyber threats enable an organization to take proactive measures, both operationally and for the long term. As governments and large enterprises often purchase multiple threat feeds and rely on multiple vendors, this thus makes it an important and profitable sector.

4. Privacy e.g. GDPR
   With the General Data Protection Regulation (GDPR), the EU has become a model for data privacy. While privacy and security have traditionally been separate fields, data security and privacy are converging in both policy and technology. The Dutch laws and regulations are fully aligned with the European standards.

The Dutch market also faces some weaknesses that are encountered more generally across the field of cyber security. The first weakness concerns a lack of awareness about cyber threats amongst the Dutch public. Secondly, while the quality of Dutch cyber security talent and experts are relatively high, there is a shortage in the quantity of sufficiently trained and educated talent at the moment. Especially as the demand for talent is expected to rise, employers are increasingly looking for experienced cyber security professionals and are not always willing to invest in human capital. Thirdly, because the Netherlands is a small country and the service sector has a large share over industry and agriculture, the internal outlet market is relatively small. Therefore, cyber security solutions are less scalable within the Netherlands itself and international cooperation is required to effectively develop and implement solutions.

Additionally, the high costs that are often associated with the implementation of cyber security solutions may form a barrier to their implementation, especially by smaller businesses (SMEs). This leads to a vulnerable domestic market. This market may also be threatened by an increasing number of foreign competition and international acquisitions. Finally, it is important to consider the threat that Covid-19 related travel restrictions (and their economic consequences) may form, especially as international interactions are of crucial importance to the Dutch cyber security market.

Analysis

Based on the development in the cyber security landscapes of the Netherlands and Taiwan, similarities, complementary strengths, and opportunities can be identified. These opportunities form the basis for the objectives and the subsequent activities as identified in this roadmap. Table 1 provides a schematic comparison between the two cyber security sectors.

The governments of Taiwan and the Netherlands have placed cyber security high on the policy agenda and both are stimulating international collaboration. The potential opportunities for collaboration between the Netherlands and Taiwan generally follow complementary characteristics of the cyber security landscapes. In particular, the combination of Taiwanese network hardware and Dutch software applications creates an interesting collaboration model. The identified opportunities include academic research collaboration, the integration of ICT hardware and cyber security software, joint business incubation, and joint business development.

Based on the analysis of the Dutch and Taiwanese cyber security sectors, these opportunities lay, amongst others, in the fields of ICT, operational security (e.g. IoT, critical infrastructure), and expertise from Dutch niche players on topics as threat intelligence, penetration testing, and data security (privacy). To illustrate, Taiwan is a large-scale manufacturer of network hardware and IoT applications; collaboration with Dutch cyber software companies will enhance the products and widen the market for Dutch cyber solutions. Moreover, the international market for cyber solutions such as IoT and critical infrastructure applications is expected to grow and mature in the coming years. Utilizing the complementary characteristics of the Dutch and Taiwanese cyber sectors, joint solutions and services can be developed. Furthermore, for Dutch cyber security companies, the collaboration with Taiwan can be used to access surrounding markets in (South)East Asia and the Pacific region, and vice-versa.

Lastly, while the Netherlands has strong niche players and a history of international and cross-sectoral cooperation, Taiwan has a demand for cyber security in its key industries, especially in the critical infrastructure (particularly state-owned utility companies), manufacturing (such as network hardware, IoT applications, and semiconductor), and the health care and financial sectors. This offers many opportunities for companies from both markets to benefit from each other's technologies and expertise. Although both economies have different characteristics, the Netherlands being a service-based economy and Taiwan being a manufacturing-based economy, both domestic markets for cyber solutions remain relatively small.

Table 1: A schematic comparison between the cyber security sectors in the Netherlands and Taiwan

	The Netherlands	Taiwan
Similarities	Strengths: • Cyber security high on policy agenda and a priority sector for both governments • Active academic and white-hat community and support Challenges: • Small domestic markets • Domestic companies are mostly SME's (incl. start-up's) actively exploring international markets and facing heavy competition from multinationals • Shortage of qualified and experienced cyber security personnel/experts • General lack of cyber security awareness amongst the public • Potential travel limitations due to the Covid-19 pandemic	
Complementary strengths	• History of international collaboration	• Government's support on international expansion
	• Actively promoting PPP for international collaboration	• Actively building a national/international PPP mechanism for cyber security
	• Access/gateway to Europe	• Access/gateway to Asia
	• Access to capital (venture capital investments)	• Demand for capital to support sector development
	• Specialized in software solutions	• Specialized in ICT hardware and IT based cyber security solutions
	• Well established niche players for OT/IoT/offensive security/threat intelligence/privacy legislation	• Strong focus on digitalization of leading manufacturing sectors and new technology development in 5G, IoT, AI with demand for cyber solutions
	• Expertise in Critical Infrastructure Protection	• Demand for Critical Infrastructure Protection (particularly for state owned utility companies)
	• Well established cyber security professional training scheme	• Actively building up cyber security professional training scheme (shortage of certified cyber security professionals)
Opportunities	• Knowledge and information exchange	
	• Joint research collaboration (TW+NL)	
	• Joint international business development and investment (Europe + Asia)	
	• Joint business incubation (soft-landing and access to capital)	
	• Joint cyber solution development (hardware + software, OT + IT)	

Goal and Objectives

Since 2018, Taiwan and the Netherlands have increasingly collaborated on the topic of cyber security. Together, various activities such as missions, webinars, and visits have been organized (see Appendix). Consequently, warm connections have been established between major public and private organizations in the field of cyber security and an overall goal has been identified.

The overall goal of the Netherlands Cyber Security Roadmap towards Taiwan is:

► The Netherlands and Taiwan create integrated solutions in ICT hardware and cyber security software via strong academic, innovation, and business collaborations.

In general, the ambition is to benefit from the complementary nature of both cyber security sectors, and structure the efforts along a comprehensive strategy. Following the opportunities as described in previous chapters, three focus areas are prominent and formulated in objectives, namely:

Knowledge: Facilitate knowledge and information exchange between the Netherlands and Taiwan, in the fields of research, business and policy.

► Cyber security has been assigned a priority sector in both Taiwan and the Netherlands. While research is being conducted and policies and business prospects develop rapidly, it is important to "keep up". The sharing of accumulated knowledge, specialized experiences, and latest insights serves multiple purposes. Identified topics for further knowledge exchange are, for example: Critical Infrastructure Protection, Public Private Partnership, Resilience Centers, and Professional Training Programs.

Innovation: Stimulate academic and R&D collaboration between universities, research institutes and cyber companies from the Netherlands and Taiwan.

► Taiwan and the Netherlands show complementary expertise and technologies in the field of cyber security, whilst its governments are stimulating international collaboration. This provides a perfect base for R&D collaboration through various instruments, as well as the joint development (co-creation) of cyber security solutions by both (academic) institutes and companies.

Business: Support bilateral/international business development for Dutch and Taiwanese cyber companies .

► Taiwan has a maturing cyber security industry, a growing awareness about cyberresilience, and a government which supports international expansion. Here lie opportunities for joint international business incubation and joint business development, such as the integration of ICT hardware and cyber software. Additionally, Taiwan can be used as a gateway to the Asian markets, and similarly the Netherlands as gateway to Europe.
Another opportunity lies in the domestic demand for cyber security solutions in Taiwan from the large manufacturing industry and state-owned utility companies, especially on the topic of critical infrastructure protection.

Activities and Instruments

Working towards the objectives as described above, the following activities are planned to be organized, in relation to (indicated on the right side) knowledge, innovation and/or business:

OBJECTIVE #1 KNOWLEDGE 💬 | OBJECTIVE #2 INNOVATION 💡 | OBJECTIVE #3 BUSINESS 🤝

1. **Knowledge-based events** for research, business and policy such as: **webinars and seminars** and **high level visits** with officials or industry leaders. 💬

   Led/coordinated by: HSD

   Seminars and webinars are one way of facilitating knowledge exchange. This allows the Dutch and Taiwanese cyber security sectors to directly benefit from the respective others' expertise. Appropriate topics can be identified when looking at the complementary nature of the two ecosystems. An example is the NL-TW Cyber Opportunity Webinars (June 2020) which provided Dutch cyber security companies with a chance to learn about the Taiwanese cyber security landscape and related opportunities.

2. Reaping the benefits of the **collaboration between the Dutch Research Council (NWO) and National Science and Technology Council in Taiwan** (to facilitate researcher exchange & joint conferences), and develop or utilize suitable support mechanisms (funding). 💬 💡

   Led/coordinated by: NLOT

3. Promote **business incubation**: supporting GlobalEPIC and other soft-landing programs. 🤝

   Led/coordinated by: HSD

   Business incubation through the promotion of soft-landing programs, such as the Global EPIC soft-landing program, is meant to facilitate the establishment of business-connections between various international cyber security markets.

4. Support joint **cyber security solution development**: by means of matchmaking and exploring suitable funding schemes (such as EUREKA GlobalStars and Horizon Europe). 💡

   Led/coordinated by: NLOT

5. **Cyber security missions**: outbound (to Taiwan) or Inbound (to the Netherlands) with tailor-made itinerary of relevant events and activities. 💬 💡 🤝

   Led/coordinated by: RVO

   Cyber security missions, both inbound and outbound, with focus on innovation and or trade, are a way to facilitate knowledge exchange, enable collaboration and/or stimulate business development.

6. Support **participation in large events:** such as SEMICON Taiwan, HITCON, Explore Next Cyber Taiwan, CYBERSEC and/or the ONE Conference.
Led/coordinated by: NLOT

Participation in large events, such as the abovementioned conferences, provide a good opportunity for companies or research organization to connect with experts in the field, engage in discussions on innovation and state-of-the-art technologies, and/or engage in business or R&D opportunities.

7. Support **demand driven (business) matchmaking:** between Taiwanese and Dutch parties.
Led/coordinated by: NLOT

On-demand matchmaking can be on the level of individual companies (companies requesting to be introduced to potential partners), as well as on the level of specific niches (such as OT applications, electric vehicles, amongst others).

Instrument

A good **propositioning** of the Dutch cyber security sector (focused on the qualities and its unique selling points) is recommended to enter and expand in the Taiwanese cyber security ecosystem. Visibility can be created with the help of a strong **public-private branding**, with good communication tools. Existing branding tools will be integrated, such as the proposition 'The Netherlands: The (Secure) Digital Gateway to Europe' by Security Delta and 'the Dutch customer journey' of InnovationQuarter.
Led/coordinated by: HSD

In order to realize the aforementioned activities, when resources are required, suitable **government funding mechanisms** may be identified, depending on the nature of the activity and its participants. It must be noted that these instruments are demand driven and the actual application for funding should be an initiative of the private sector parties. Examples of funding mechanisms include the public private cooperation (PPS)-mechanism, Starters International Business (SIB) budgets, Partners in International Business (PIB), and a "DHI"-subsidy scheme (meant for demonstration projects, feasibility studies, and investment preparation project).
Led/coordinated by: RVO

Regular coordination between HSD, InnovationQuarter, RVO, and the Netherlands Office Taipei will take place to guide and structure the activities and align them with the defined objectives. This includes an **annual review** of the roadmap.
Led/coordinated by: RVO

Appendix:

Overview of previous activities btween the Netherlands and Taiwan in the field of cyber security

DATE	Activity/ Event
MAR '18	Conference Cyber Security Startup Ecosystem
MAY '18	Conference Critical Infrastructure Protection (CIP), and MoU signed Security Matters, TWISC and III
SEP '18	POC project for CIP in Taiwan Power Company and Chinese Petroleum Corporation (CPC)
OCT '18	Joint GDPR Conference
OCT '18	Taiwan Cyber Security Delegation attending Cyber Security Week 2018 and visit potential partners (including Security Delta, municipality of The Hague, TU/e, TU/Delft and University of Twente)
OCT '18	Global EPIC soft-landing programme. Participating countries: NL, Taiwan, UK, Canada, Poland, USA
'19	Ecorys and Equidam contracted by Taiwanese government
MAR '19	TU/Delft visited Taiwan on the topic of cyber security and signed MoU with TWISC
MAY '19	Fact finding mission, incl NL-TW Cyber security Exchange Forum. Delegation: Compumatica, TU/Delft Safety & Security Institute, ReaQta, EclecticIQ, Bitdefender and Innovation Quarter
OCT '19	Taiwan Cyber Security Delegation (business & academic) visiting ONE Conference, incl Taiwan-Netherlands Cyber Security Roundtable and visits to Municipality of the Hague (Hack the Hague), DITSS and Cyber Resilience Center Brainport
NOV '19	Digital Minister, Audrey Tang visiting HSD on potential collaboration in Digital Democracy, Cyber Security and Critical Infrastructure Protection
NOV '19	Signing of a G2G bilateral MoU during the visit of DG BEB to Taiwan on cyber security and start-ups
JUN '20	Market report Cyber Security in Taiwan performed by ITRI (assigned by Netherlands Office Taipei, in cooperation with RVO)
JUN '20	Webinar about Security Opportunities in the Netherlands and Taiwan
AUG '20 – OCT '20	Digital Cyber Security Innovation Mission Taiwan, incl business webinars, partnership matchmaking and a Call for Solutions. NL companies: Bitdefender, Blue Arca, Compumatica, EclecticIQ, Fox-IT, Guardian360, Reaqta, Secura, TNO and X-Systems.
NOV '21	Taiwan Representative Chen visits HSD campus
MAR '22	Cyber Security discussion about Taiwan @HSD
JULY '22	Cyber Security Information Session online
NOV '22	ASML "Cyber Initiative" platform discussed during formal dinner
FEB '23	Representative Tielman meets Minister Tang from the newly established Ministry of Digital Affairs

Appendix:

Foreward looking agenda

DATE	Activity/ Event
APRIL '23	**RSA Conference in San Francisco (24-27 April '23)** Delegates from the Netherlands and Taiwan are both participating the RSA Conference in USA. We aim to schedule a meeting between the delegates.
MAY '23	**CyberSec Taiwan (9-11 May '23)** CYBERSEC is the largest annual cybersecurity event in Taiwan. With the participation of 300 cybersecurity companies and 250 knowledgeable speeches, CYBERSEC has more than 10,000 registered attendees every year. The theme of CYBERSEC 2023 is "Bring Security to", covering new technologies such as IoT, autonomous vehicles, artificial intelligence, and space satellites, and a wide range of applications such as hospitals and energy facilities. We aim to welcome 2-3 companies and a guest speaker from the Netherlands at CyberSec '23. Personalized programs are created to serve specific interest of the companies. Matchmaking will be supported by Taiwanese partners Ministry of Digital Affairs (MoDA) and the Industrial Technology Research Institute (ITRI).
OCT '23	**ONE Conference (Oct '23?)** The ONE Conference is Europe's prime cybersecurity event. A leading platform for sharing knowledge, best practices and research results. A wide variety of topics will be addressed: from highly technical subjects such as malware detection, incident response, and law enforcement cases to less technical subjects, such as partnerships between the public and the private domain, governance and recent cybersecurity research. A delegation from Taiwan is planning to participate. The mission objective is to introduce Taiwanese experts from the government, private and academic sector to the major developments in the Netherlands in the field of cyber security (i.e., policy, infrastructure, research and development, international cooperation and more). The Taiwanese delegation will also meet with local companies, research institutes and government agencies, to explore future partnerships and share experiences and ambitions on tackling global cybersecurity challenges. Moreover, Taiwanese hackers hope to join the Hack The Hague event.