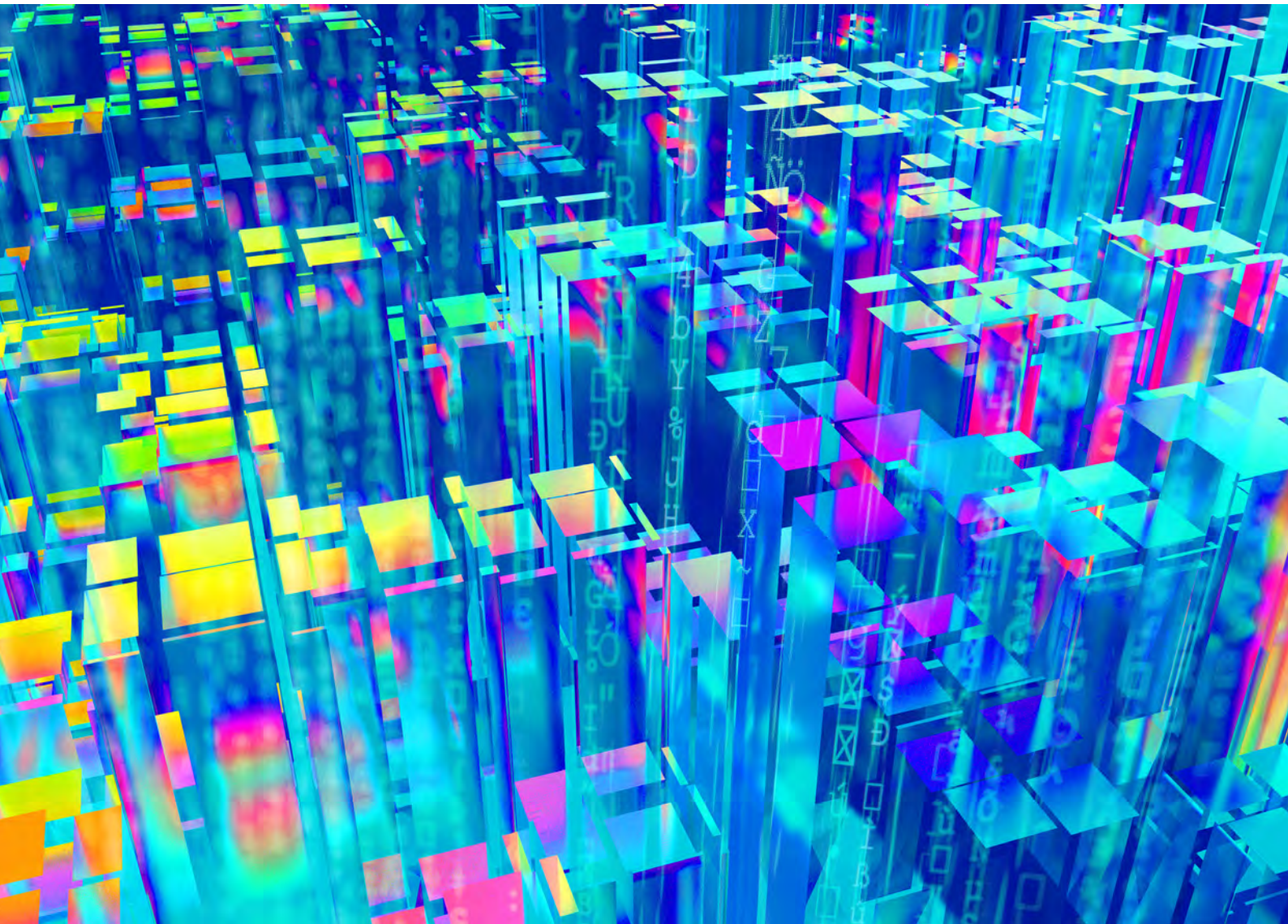
Netherlands Enterprise Agency

Strategic Perspectives on Taiwan–Netherlands Cybersecurity Cooperation: Current Status and Future Directions

April 2026



Preface

Dear reader,

In today's world, safeguarding technological resilience and strategic autonomy is more important than ever. At the same time, strong innovation ecosystems increasingly rely on trusted international partnerships. As cyber threats grow in scale and complexity, particularly in the semiconductor and ICT sectors, identifying and strengthening such partnerships has become a shared priority.

This report, Strategic Perspectives on Taiwan–Netherlands Cybersecurity Cooperation, explores the evolving collaboration between two highly advanced digital economies. Taiwan is the heart of the global IT supply chain and operates at the frontline of emerging cyber threats, while the Netherlands brings strong expertise in security software, industrial systems (OT/ICS), and regulatory frameworks. Together, these complementary strengths provide a strong foundation for deeper cooperation.

This report highlights how strategic priorities align. It traces the development of bilateral engagement, from initial exchanges to more structured collaboration, such as the 2024 Netherlands–Taiwan Cyber Consortium MoU. Our aim is to support policymakers, researchers, and industry leaders in identifying concrete opportunities for cooperation in areas including Post-Quantum Cryptography (PQC), AI security, and semiconductor standards (SEMI E187).

This study was commissioned by the Netherlands Innovation Network of the Netherlands Office Taipei (NLOT) and carried out by the Association of Hackers in Taiwan (HIT). It reflects a shared commitment to the "Triple Helix" model, in which government, industry, and academia work closely together. We also gratefully acknowledge the contributions of Security Delta (HSD), the Ministry of Digital Affairs (MODA), and many other experts in building strong partnerships between the Netherlands and Taiwan.

We hope this report contributes to continued collaboration between the Netherlands and Taiwan, and helps translate shared ambitions into concrete initiatives. We value your feedback and look forward to further exchange.

Kind regards,

Anouk van der Steen - Director for Innovation, Technology and Science in Taiwan
Cathy Soong - Senior Advisor for Innovation, Technology and Science in Taiwan
Ian Chen - Senior Advisor for Innovation, Technology and Science in Taiwan

HIT 社團法人台灣駭客協會
ASSOCIATION OF HACKERS IN TAIWAN

Table of Contents

Executive Summary

Core Findings

Taiwan, a global technology powerhouse with a critical role in the silicon-driven industry, has become the bedrock of the international IT supply chain. Simultaneously, its unique geopolitical status places it at the frontline of democracy. This position makes Taiwan a primary target for state-sponsored threat actors, cementing the island's role as a pivotal player in the global cybersecurity landscape.

Taiwan and the Netherlands have maintained ongoing cybersecurity interactions since 2020 through the HSD cooperation framework. Both sides exhibit highly complementary strengths: Taiwan's ICT hardware and semiconductor supply chain advantages versus the Netherlands' cybersecurity software, OT/IoT security expertise, and EU market access. However, existing cooperation remains predominantly exchange-based and has yet to evolve into large-scale, sustainable, project-based collaboration with measurable outcomes. This report argues that Taiwan–Netherlands cybersecurity cooperation is no longer optional but strategically necessary and outlines a concrete pathway to translate existing exchanges into measurable, sustainable outcomes.

This report presents five core findings:

- **Converging Threat Landscapes and the Imperative for Collaboration**: Taiwan remains a primary target for state-sponsored actors—predominantly from China—due to its sensitive geopolitical status, while its lucrative ICT sector faces relentless attacks from profit-driven cybercriminals originating from Russia. The scale of this pressure is immense, with Taiwan's government networks enduring an average of 2.4 million cyberattacks per day in 2024 (National Security Bureau, 2025). Conversely, the Netherlands confronts its own sophisticated challenges: Russian actors frequently target its Critical Information Infrastructure (CII), and its vital semiconductor industry is a recurring target for industrial espionage linked to China. Compounding this, the Netherlands is currently navigating the massive operational and compliance pressures of NIS2 implementation, which impacts approximately 8,000 organizations across its critical sectors (Dutch CSBN, 2024). Shared Threat Urgency: Taiwan's government networks faced an average of 2.4 million malicious or anomalous cyber intrusions/disturbances per day in 2024, while the Netherlands faced compliance pressure from NIS2 implementation affecting approximately 8,000 organizations as an estimate. Both entities have compelling reasons to deepen cooperation. (Source: National Security Bureau, 2025; Dutch CSBN, 2024)

- **Natural Complementarity and Strategic Synergy**: There is a deep, natural complementarity between the cybersecurity ecosystems from Taiwan and the Netherlands. Taiwan anchors this partnership with its global leadership in ICT hardware (security), real-world threat intelligence, and critical semiconductor cybersecurity standards, such as SEMI E187. In turn, the Netherlands offers advanced proficiency in OT/ICS security, penetration testing, privacy compliance, and navigating complex EU regulatory frameworks. This synergistic combination creates a powerful value proposition, effectively bridging the gap between physical infrastructure and software-driven defense to achieve competitive advantages that neither party could attain in isolation. Natural Complementarity: Taiwan leads globally in semiconductor cybersecurity standards (SEMI E187), real-world threat intelligence, and ICT hardware (security). The Netherlands excels in OT/ICS security, penetration testing, privacy compliance, and EU regulatory frameworks.

- **Transitioning from Fragmented to Structured Strategic Cooperation**: The Netherlands–Taiwan Cyber Consortium MoU, signed at the ONE Conference in October 2024, established a publicly announced industry-led consortium framework, marking a transition from ad hoc exchanges to structured cooperation. However, past bilateral interactions have often been limited to ad-hoc projects. The report emphasizes the need to establish an institutionalized framework—such as annual summits, joint research initiatives, and long-term training programs—to transform episodic collaborations into sustainable strategic assets. 2024 MoU as Institutional Foundation: The Netherlands–Taiwan Cyber Consortium MoU, signed at the ONE Conference in October 2024, established a publicly announced industry-led consortium framework, marking a transition from ad hoc exchanges to structured cooperation.

- **Funding Asymmetry as Key Bottleneck**: Taiwan's direct government funding for international cybersecurity cooperation is limited, relying primarily on MODA programmes (notably the Cybersecurity Industry Promotion Program, ACW) administered by the Administration for Digital Industries (ADI). The Netherlands benefits from funding under the EU Horizon Europe and Digital Europe programs, creating a resource asymmetry that must be addressed structurally.

- **Five Priority Technology Opportunity Areas**: Post-quantum cryptography, supply chain security, AI security, threat intelligence sharing, and OT/ICS resilience all present viable joint research and commercialization opportunities.

Three Priority Actions

- Establish a Bilateral Tech-ISAC for Threat Intelligence Sharing: Create a formal threat intelligence exchange mechanism connecting Taiwan's TWCERT/CC and the Netherlands NCSC, focused on APT groups targeting semiconductor and critical technology sectors. Suggested target: 6 months to launch, 12 months to formalize.

- Form a Joint Post-Quantum Cryptography Research Consortium: Use Horizon Europe Cluster 3 as the funding framework, pairing Taiwan's Post-Quantum Cybersecurity Industry Alliance (established by ADI in 2024) with Dutch academic partners at TU/Eindhoven, TU/Delft and Radboud University. Target: proposal submission within 6-12 months.

- To accelerate the commercialization of cutting-edge technologies and foster mutual market access, we propose the launch of a dedicated Taiwan–Netherlands Cybersecurity Acceleration Platform for scale-ups and SMEs. By integrating strategic resources from SECPAAS, HSD Campus, this platform will establish a robust bilateral soft-landing and Proof of Concept (PoC) testing mechanism. This initiative aims to facilitate the expansion of Taiwanese cybersecurity scaleups and SMEs into the Netherlands—serving as a strategic gateway to the European market—while simultaneously integrating mature Dutch OT/ICS solutions into Taiwan's industrial and manufacturing supply chains. We set a clear target to onboard and support an initial cohort of five companies within 6 to 12 months.

List of Abbreviations and Glossary

Abbreviation	Full Name	Description
HSD	Security Delta	Europe's largest security cluster, headquartered in the Hague
ADI	Administration for Digital Industries	Taiwan's MODA digital industry authority
ACS	Administration for Cyber Security	Taiwan's national cybersecurity administration under MODA
G2G	Government-to-Government	Bilateral cooperation at the governmental level
I2I	Industry-to-Industry	Bilateral cooperation at the industry level
NLOT	Netherlands Office Taipei	Dutch representative office in Taiwan
RVO	Netherlands Enterprise Agency	Dutch government agency for international business
NCSC-NL	National Cyber Security Centre	The Netherlands' national cybersecurity authority and CSIRT for the central government and vital sectors, operating as an agency under the Ministry of Justice and Security; the Ministry of Justice and Security (NCTV) serves as commissioner
CERT	Computer Emergency Response Team	Incident response coordination body
SOC	Security Operations Center	Centralized cybersecurity monitoring and response facility
OT/ICS	Operational Technology / Industrial Control Systems	Technologies managing physical industrial processes
PoC	Proof of Concept	Technical validation of a proposed solution or partnership
NIS2	Network and Information Systems Directive 2	EU directive mandating cybersecurity requirements for ~8,000 Dutch entities
PQC	Post-Quantum Cryptography	Cryptographic algorithms resistant to quantum computing attacks
ISAC	Information Sharing and Analysis Center	Sector-specific threat intelligence sharing organization
CTF	Capture the Flag	Competitive cybersecurity challenge format
SEMI E187	SEMI Cybersecurity of Semiconductor Equipment Standard	World's first international cybersecurity standard for semiconductor fab equipment
SECPAAS	Security Platform as a Service	ITRI-managed platform for Taiwanese cybersecurity firms entering European markets via HSD
HITCON	Hacks in Taiwan Conference	Asia-Pacific's premier hacker conference and CTF community
ZTA	Zero Trust Architecture	"Never trust, always verify" security design principle

Ch 1

Current Status of Taiwan–Netherlands Cybersecurity Collaboration

1.1 Introduction: Background, Cooperation Origins, and Key Issues

Background and Origins of Cooperation

Taiwan, a global technology powerhouse with a critical role in the silicon-driven industry, has become the bedrock of the international IT supply chain. Simultaneously, its unique geopolitical status places it at the frontline of democracy. This position makes Taiwan a primary target for state-sponsored threat actors, cementing the island's role as a pivotal player in the global cybersecurity landscape.

Taiwan–Netherlands cybersecurity cooperation began to take shape in 2018 through initial connections between ITRI and HSD partner organizations. In May 2019, a Dutch delegation visited Taiwan to attend "Explore Next Cyber Taiwan 2019". Around the same period, TU Delft and TWISC signed an MoU to explore further cooperation.

According to the Netherlands Cyber Security Roadmap Towards Taiwan (first published April 2022, updated March 2023, jointly authored by HSD, InnovationQuarter, RVO, and NLOT), the rapid digitalization and surge in cybercrime during the COVID-19 period expanded attack surfaces for both High-tech island industries and critical infrastructure, prompting both governments to prioritize cybersecurity as a key policy area. The roadmap aims to establish a more integrated, multi-year cooperation framework centered on three pillars: knowledge exchange, innovation stimulation, and bilateral business facilitation, reducing fragmentation and enabling Dutch industry and research institutions to better understand Taiwan's cybersecurity ecosystem.

The roadmap explicitly identifies complementary strengths: Taiwan offers ICT hardware, networking equipment, manufacturing scale, and supply chain advantages (including IoT applications); the Netherlands provides cybersecurity software and niche services, including OT/IoT security, critical infrastructure protection, threat intelligence, penetration testing and vulnerability assessment, and data security and privacy compliance.

Analytical Questions (Decision-Oriented for Taiwan and the Netherlands)

The study aims to (1) establish an evidence-based baseline of bilateral interaction; (2) identify structural barriers to deeper cooperation; and (3) propose feasible, sequenced cooperation models.

1.2 Research Objectives, Scope, and Methodology

Research Objectives

- Establish an evidence-based baseline of Taiwan–Netherlands cybersecurity interaction (2020–2025)
- Analyze potential cooperation directions across government, industry, and community/ research levels
- Produce actionable collaboration proposals, including initiative lists, roadmap, resource requirements, and expected benefits.

Scope Definition

Cybersecurity domains covered: governance, critical infrastructure, supply chains, cloud/data security, talent development, exercises, standards/regulation, and scaling-up companies and SMEs ecosystems. Geographic and stakeholder scope: Taiwan and the Netherlands, with NLOT serving as facilitator and coordinator.

Methods and Data Sources

- Document review: roadmaps, meeting records, policy documents, conference agendas (2020–2025)
- Stakeholder covers: G2G, industry, and research community representatives (including HSD, ADI, ITRI, SEMI, etc.)
- Case studies: SEMI E187 semiconductor cybersecurity standard; CyberSec×ONE Conference cooperation; Taiwan–Netherlands Consortium MoU
- Expert workshops and focus groups (selected)

1.3 Overall Cooperation Overview: 2020–2025 Timeline and Collaboration Map

Year-by-Year Timeline of Key Milestones

Year	Format	Key Activities and Outcomes
2018–19	Exploratory	ITRI–HSD initial connections; TU Delft × TWISC MoU signed
2020	Digital Mission	RVO/NLOT Digital Cyber Security Innovation Mission Taiwan ; NL companies: Bitdefender, Blue Arca, Compumatica, EclecticIQ, Fox-IT, Guardian360, Reaqta, Secura, TNO and X-Systems.
2022	Policy Doc.	Netherlands Cyber Security Roadmap Towards Taiwan published (Apr.)
2023	Roadmap Update	Roadmap 2023 updated version published (Mar.); Dutch delegation attends CYBERSEC Taiwan
2024 H1	Recon Mission	HSD's Joris den Bruinen delivers keynote to ~1,000 attendees at CYBERSEC Taiwan 2024; meetings with 15 Taiwanese companies considering European offices in the Netherlands (Source: HSD, 2024)
2024 H2	MoU Signing	Taiwan–Netherlands Cyber Consortium MoU signed at ONE Conference (Oct. 1–2), 8 founding members; witnessed by MODA's Astor Zhuang and Dutch EZ official Jos De Groot (Source: HSD, 2024)
2025	Deepening	Dutch delegation attends CYBERSEC Taiwan 2025 (Apr.), including a keynote by Dimitri van Zantvliet, CISO of Dutch Railways; Dutch participation also extended to HITCON CISO Summit 2025, where Mahdi Abdulrazak, Group Information Security and Risk Officer at SHV Energy delivered keynote; In parallel, ADI Director General Mr. Jiunn-Shiow Lin delivers the first-ever international keynote at The Hague Cyber Security Week; inaugural Taiwan–Netherlands Cybersecurity Roundtable (Sep.) (Sources: CYBERSEC 2025; HITCON CISO Summit 2025; MODA ADI, 2025)

Source: HSD Securitydelta.nl (2020–2025); MODA ADI Press Releases (2025); InnovationQuarter (2022)

Collaboration Map by Level and Theme

Cooperation can be mapped across three levels, G2G, I2I, and Community & Research, and across thematic domains spanning policy/regulation, technology, talent development, exercises, investment matchmaking, and scaling-up companies and SMEs acceleration. The overall assessment indicates that interaction remains predominantly exchange-based, with no large-scale sustained project cooperation yet established.

Preliminary Assessment

Three structural characteristics define current cooperation: first, activities are dominated by conferences and knowledge exchange events, with no continuous project execution mechanism; second, cooperation focuses on business matchmaking and knowledge sharing without joint R&D or PoC testbeds; third, while the 2024 MoU establishes an institutional framework, its implementation mechanisms remain to be built.

1.4 Government-to-Government (G2G) Cooperation: Status and Constraints

Existing Dialogue Frameworks and Contact Points

Taiwan–Netherlands G2G cybersecurity cooperation is currently coordinated primarily through NLOT, with ADI, ACS, etc. serving as the main counterparts on the Taiwanese side. Dutch ministerial coordination involves the Ministry of Economic Affairs, the Ministry of Foreign Affairs, and NCSC, with HSD playing a critical bridging role between knowledge institutions and industry. Cooperation formats include bilateral visits, policy briefings, thematic workshops, and mutual participation at flagship annual events, HITCON (Taiwan), CYBERSEC (Taiwan) and ONE Conference (Netherlands).

ADI Expectations and Cooperation Models

ADI's expectations for G2G cooperation span three levels: policy alignment (harmonization with EU NIS2, CRA, and related regulatory frameworks); technical cooperation (joint R&D, co-development of standards); and market access (leveraging the Netherlands as a European gateway for Taiwanese cybersecurity companies entering the EU market).

Model analysis indicates that the bilateral (Taiwan–Netherlands direct) model offers speed and flexibility but limited funding sources. The multilateral EU program model (joint Horizon Europe applications) offers richer funding but restricts Taiwan's participation to "Associated Partner" status, adding administrative complexity.

Preliminary Topic Pool for Cooperation

Category	Topic Area	Taiwan–Netherlands Complementarity
Software/Services	Threat intelligence, incident response, governance	Netherlands APT analysis capabilities × Taiwan's China threat real-world intelligence
	Cloud security, testing & assessment	Netherlands GDPR/privacy compliance expertise × Taiwan's cloud service providers
Hardware/ Supply Chain	Trusted hardware, equipment security certification	Taiwan SEMI E187 standard × Netherlands ASML supply chain
	Supply chain risk management	TSMC compliance requirements × Netherlands OT assessment methodologies
Hybrid	OT/ICS resilience, cross-domain exercises	Taiwan utility exercise experience × Netherlands port/ energy infrastructure
	Post-quantum cryptography, AI security	Taiwan's industry alliance × Netherlands TU Eindhoven, TU Delft, Radboud research capacity

Funding and Resource Constraints (Taiwan Side)

Taiwan's direct government funding for international cybersecurity cooperation is limited, with funding primarily coming from MODA programs such as the Cybersecurity Industry Promotion Program (ACW). Proposed solutions include: phased PoC designs (reducing single-commitment funding thresholds), blended funding structures (combining government subsidies, industry co-investment, and EU program funding), and platform-based cooperation (sharing infrastructure costs through HSD Campus and SECPAAS).

1.5 Industry-to-Industry (I2I) Cooperation Status

Taiwan–Netherlands industry interactions to date have been predominantly exploratory and exchange-based, comprising corporate site visits, matchmaking sessions at flagship trade events (CYBERSEC Taiwan, ONE Conference), and exploratory bilateral meetings. While supply chain collaboration, distribution partnerships, joint market entry strategies, and technology integration (e.g., embedding Taiwanese cybersecurity hardware into Dutch managed security services) represent the natural maturation paths for I2I cooperation, evidence of these advanced collaboration modes remains limited as of 2025. The most concrete commercial signal observed thus far was at CYBERSEC 2024, when 15 Taiwanese companies expressed interest in opening European offices in the Netherlands (Source: HSD, 2024). So far, a number of Taiwanese cybersecurity companies have established subsidiaries in the Netherlands, including TXOne, Keypasco, Lanner Electronics, and Turing Space, indicating growing commercial momentum that has not yet translated into closed deals or operational joint ventures.

Key bottlenecks include: insufficient use case specificity (lack of joint customers or shared trial environments); absence of PoC testbeds and co-certification mechanisms; regulatory and procurement barriers (unclear compliance pathways for Taiwanese products entering EU public procurement); and language and cultural differences affecting the pace of trust-building.

1.6 Community and Research Cooperation Status

Community and research cooperation offers low barriers and relatively low costs, making it a vital foundation for bilateral relations. Active platforms include ONE Conference (Taiwanese delegates participate annually; 2024 marked Taiwan's higher visibility and a more structured team), CYBERSEC Taiwan, HITCON, and a strengthening research track centered on Academia Sinica's collaboration with Dutch post-quantum cryptography researchers—especially at TU/e and, in relevant areas, Radboud University. Earlier links, such as the TU Delft–TWISC initiative, helped open dialogue, but the stronger ongoing research momentum is now more clearly visible in the Academia Sinica–Netherlands cryptography network. Cooperation formats encompass joint research, workshops, training, and CTF competitions. The primary challenge remains the lack of translation mechanisms to convert research outcomes into policy and industry impact.

Ch 2

Taiwan's Cybersecurity Strengths Relevant to Collaboration with the Netherlands

2.1 Taiwan's Cybersecurity Ecosystem Overview

Taiwan's cybersecurity ecosystem is built on three mutually reinforcing pillars: policy governance, industry supply chains, and research communities, which collectively define Taiwan's unique position in the global cybersecurity landscape. The following table highlights key metrics/projects.

Policy & Governance	Industry & Supply Chain	Research & Community
"Cybersecurity is National Security" (2016, 2021, 2025)	SEMI E187 global semiconductor standard	NSYSU cybersecurity master program (2019, first in Taiwan)
MODA Administration for Cyber Security (2022)	F-ISAC covers all 200+ financial institutions	AIS3/ISIP talent integration platform
FSC mandatory CISO requirement (2023)	TXOne Networks: $145M total funding	HITCON: Asia-Pacific's top hacker conference
Phase VII National Cybersecurity Program (2025–28, NT$8.8B)	Trend Micro: ~USD 1.9B annual revenue	CYBERSEC annual conference: 20,000+ attendees

Sources: MODA ACS (2024); US Trade.gov Taiwan Cybersecurity (2024); FinTech Global (2024); Business Sweden (2023)

2.2 Taiwan's Global Value Proposition in Cybersecurity

Taiwan offers three unique core value propositions in the global cybersecurity landscape that hold strategic appeal for Dutch and EU partners.

First, real-world-scale threat intelligence. Taiwan is among the world's most intensively targeted democracies by state-sponsored cyberattacks. Government networks faced an average of 2.4 million intrusion/disturbance attempts per day in 2024, double the 2023 figure (Source: National Security Bureau, January 2025). Taiwan's NSB reported 906 cyber cases involving government and private sectors in 2024, up from 752 in 2023; the sharpest growth was observed in telecommunications (650%), transportation (70%), and the defense supply chain (57%). (Source: National Security Bureau, January 2025). This threat environment endows Taiwanese institutions with real-world intelligence and response capabilities that no other entity can replicate in simulation.

Second, centrality in the semiconductor supply chain. Taiwan accounts for roughly 20% of global semiconductor production value and over 60% of global foundry revenue, with TSMC alone holding approximately 70% of the pure-play foundry market. In terms of the most advanced logic capacity (typically ≤7nm), Taiwan produces over 90% of the global total, making it the indispensable node for AI, high-performance computing, and advanced mobile chips. The Netherlands' ASML is the world's sole manufacturer of extreme ultraviolet (EUV) lithography machines essential to advanced chipmaking. The two entities share a "common destiny" relationship in semiconductor supply chain security, and the SEMI E187 framework directly addresses the joint security imperative of the TSMC–ASML supply chain.

Third, the integration potential of ICT hardware and cybersecurity software. Taiwan's scale advantage in networking equipment, embedded systems, and IoT device manufacturing complements the Netherlands' technical depth in cybersecurity software, penetration testing, and compliance services. Combined, they can produce "hardware-secured" integrated solutions with strong competitive potential in global OT/IoT markets.

2.3 Policy and Governance Capabilities

Taiwan's cybersecurity regulatory framework has evolved continuously, demonstrating depth of governance. The Cyber Security Management Act, originally enacted in 2018, was amended and promulgated in September 2025, expanding its applicability, raising the maximum penalty to NT$10 million, and strengthening reporting obligations for critical infrastructure providers across nine designated sectors.

Institutionally, the ACS was established in August 2022 under MODA to coordinate national cybersecurity policy; the National Institute of Cyber Security (NICS), launched in January 2023, provides technical support and research capacity; TWCERT/CC serves as the national cybersecurity incident response coordination center with international CERT network connectivity.

The Phase VII National Cybersecurity Development Program (2025–2028) allocates NT$8.8 billion (~USD 300 million) (Source: Invest Taiwan, 2024), with four pillars: national preparedness, infrastructure risk reduction, industry development, and AI application, demonstrating long-term government commitment to cybersecurity.

2.4 Cybersecurity Industry Landscape

Taiwan's cybersecurity industry generated NT$60.37 billion (~USD 1.87 billion) in output value in 2025, with government targets of NT$74.93 billion by 2026(Source: TPEX 2026). The ecosystem comprises approximately 368 cybersecurity companies employing around 9,000 professionals, with a target of 10,000 by 2025. Growth rates consistently outpace global averages: the 2016–2022 CAGR of 9.1% exceeded the global 8.1% (Source: Business Sweden, 2023).

The industry ecosystem can be categorized into six major clusters:

- Global Cybersecurity Service Providers: Trend Micro (annual revenue ~USD 1.9B, 65+ countries, 7,000+ employees) (Source: Trend Micro About, 2024)
- OT Industrial Security: TXOne Networks (total funding USD 145M, Series B+ from Trend Micro and strategic investors) (Source: FinTech Global, 2024)
- APT Threat Intelligence: CyCraft (AI-driven SOC automation)
- Offensive Security Research: DEVCORE (discoverers of ProxyLogon and other critical vulnerabilities)
- Financial Cybersecurity: Operates under FSC and F-ISAC frameworks, covering all 200+ financial institutions (Source: FSC, 2017)
- Semiconductor Cybersecurity: ITRI, NYCU Cybersecurity Institute, and TSMC co-lead the SEMI E187 standard ecosystem

2.5 Scale-ups/SMEs and Innovation

Taiwan's cybersecurity Scale-ups and SMEs ecosystem is growing rapidly. According to Tracxn, Taiwan has approximately 88 cybersecurity Scale-ups and SMEs, of which 24 have completed funding rounds and 12 have reached Series A or above (Source: Tracxn, 2024).

Key accelerator resources include Taiwan Tech Arena (TTA), which provides Scale-ups and SMEs soft-landing services; ITRI's entrepreneurship acceleration program; and CYBERSEC, the largest showcase platform with over 20,000 attendees and 500+ exhibitors in 2025. Innovation themes center on AI-assisted security, post-quantum cryptography applications, IoT security chips, and MSSP (Managed Security Service Provider) models.

The SECPAAS platform (managed by ITRI) has become the primary soft-landing mechanism for Taiwanese cybersecurity companies entering European markets, playing an indispensable bridging role within the Taiwan–Netherlands cooperation framework.

2.6 Case Studies

Case Study 1: SEMI E187 Semiconductor Cybersecurity Standard

Published in January 2022, SEMI E187 is the world's first international cybersecurity standard for semiconductor manufacturing equipment, led by TSMC and co-developed with ITRI, TXOne Networks, and National Yang Ming Chiao Tung University (NYCU). The standard covers 12 core requirements across operating system security, network segmentation, endpoint protection, and security monitoring. TSMC made E187 compliance mandatory in all new procurement contracts from 2023, and the requirement extends to TSMC's overseas fabs in the United States, Japan, and Germany, extending the standard's influence throughout the global supply chain, and continuing to develop new versions.

Implications for the Netherlands: ASML and other Dutch equipment suppliers serving TSMC or TSMC-related fab programmes may increasingly need to meet E187-based customer procurement and verification requirements where applicable. Dutch cybersecurity firms and hardware security specialists, can provide complementary services in E187 compliance verification, security assessment, and equipment certification, creating concrete commercial opportunities.

Sources: TSMC ESG Report (2024); SEMI.org (2022, 2024); PEER Group SEMI Standards (2024)

Case Study 2: Taiwan–Netherlands CyberSecurity Consortium MoU (2024)

The Taiwan–Netherlands Cyber Consortium MoU, signed on October 1–2, 2024, at ONE Conference in The Hague, brings together CFLW Cyber Strategies and Security Delta(HSD) (Dutch side), with Keypasco Europe, Lydsec Digital Technology, Chelpis Quantum, Jmem Technology, PhantomCloud Communication, and Turing Space (Taiwanese side). It operates under ITRI's SECPAAS framework. Witnesses included Taiwan's ADI MODA Assistant Director, Astor Zhuang, and Dutch Ministry of Economic Affairs official, Jos De Groot.

This is the first formal bilateral cybersecurity enterprise framework in the history of Taiwan-Netherlands relations, marking an upgrade from individual company matchmaking to organized consortium cooperation, with HSD Campus designated as the soft-landing base for Taiwanese companies entering European markets.

Sources: HSD Securitydelta.nl (2024); UDN (2024)

Ch 3
Cooperation Gaps and Opportunities

3.1 Gap Analysis

Based on document review and stakeholder consultations, structural cooperation gaps can be grouped into five dimensions:

Gap Type	Manifestation	Root Cause
Misaligned Priorities	Taiwan focuses on Chinese APT defense; Netherlands is stronger in institutionalized critical infrastructure governance, EU compliance and OT/ICS security	Different threat models and regulatory environments
Lack of Projectization	Interactions dominated by seminars; no continuous work packages or milestone management	Absence of shared governance architecture and dedicated resources
Resource Asymmetry	Netherlands can access EU program funding; Taiwan relies on limited MODA/ADI programme budget	Taiwan's non-EU status excludes it from Digital Europe Programme SO_3 calls
Regulatory and Trust Barriers	Unclear compliance pathways for Taiwanese products in EU public procurement	EU adequacy decision for Taiwan data transfers not yet granted
Insufficient Industry Cases	Lack of joint customers and shared PoC testbed environments	Bilateral companies have not yet developed genuine commercial interdependence

3.2Thematic Opportunity Areas

Opportunity Area 1: Supply Chain Security and Trusted Computing

The strategic interdependence of the TSMC–ASML supply chain makes supply chain security the highest-priority cooperation domain. Specific opportunities include joint development of E187 compliance verification tools, semiconductor supply chain risk rating services, and a trusted hardware certification framework extending to TSMC's overseas fabs. Dutch cybersecurity vendors, particularly OT security specialists, can provide complementary security assessment, penetration testing, and equipment certification services within the E187 ecosystem. Beyond the semiconductor sector, the security verification mechanisms and supply-chain risk management methodologies developed under the E187 framework could serve as a reference model for other critical infrastructure domains with strong OT dependencies. This would allow Taiwan–Netherlands cooperation to evolve from semiconductor supply chain security toward broader industrial and critical infrastructure cybersecurity collaboration.

This direction aligns directly with two flagship Dutch policy initiatives that should serve as institutional anchors on the Netherlands side. First, TNO's "Cyber-Secure Systems by Design" programme translates security-by-design principles into engineering processes for embedded systems, IoT, and OT environments — a methodological framework that pairs naturally with Taiwan's hardware and equipment manufacturing strengths. Second, the new House of Cyber initiative (EUR 60 million conditional purchase of the former Aegon headquarters in The Hague's Mariahoeve district, approved by the city council in February 2026) will physically co-locate NCSC, the Ministry of Defence, the National Police, the Netherlands Forensic Institute, HSD, and other partners under one roof. The House of Cyber provides a natural Dutch-side institutional anchor for sustained Taiwan–Netherlands supply chain security collaboration, particularly for activities that benefit from co-located government, industry, and operational expertise. Embedding the bilateral E187 / supply chain workstream into the House of Cyber agenda from inception is a high-leverage early action.

Opportunity Area 2: Critical Infrastructure and OT Security

Taiwan has accumulated extensive real-world experience in cybersecurity drills for power, water, and telecommunications critical infrastructure, particularly in countering targeted Chinese attacks. The Netherlands leads Europe in OT security for ports (Port of Rotterdam), energy, and water utilities. Jointly developing OT/ICS cybersecurity frameworks that combine Taiwan's operational scenarios with Dutch technical methodologies presents high complementarity potential.

Opportunity Area 3: Threat Intelligence and Incident Response

Taiwan's threat intelligence sharing on Chinese state-sponsored APT groups (BlackTech, Flax Typhoon, Mustang Panda, etc.) is highly valuable to Dutch and EU partners. Dutch firms Fox-IT and EclecticIQ are recognized European leaders in APT tracking and threat intelligence platforms. Establishing a formal bilateral threat intelligence sharing and partnership mechanism, a Bilateral Tech-ISAC connecting TWCERT/CC and NCSC, and a cross-entity intelligence partnership, represents the most immediately feasible near-term cooperation direction.

Opportunity Area 4: Post-Quantum Cryptography (PQC)

NIST finalized three PQC standards in August 2024 (FIPS 203, 204, 205), with NSA's CNSA 2.0 mandating compliance for all new national security system acquisitions by January 2027. Taiwan's ADI established the Post-Quantum Cybersecurity Industry Alliance in 2024, with its case study selected from 340+ global submissions for presentation at ONE Conference 2025. Dutch academic institutions TU Eindhoven, TU Delft and Radboud University hold globally recognized expertise in post-quantum cryptography research. The EU's Horizon Europe 2025 program allocated EUR 16 million specifically for PQC research, representing a critical funding window for joint applications. *(Source: MODA ADI, 2025)*

Important structural caveat: Taiwan is neither an EU Member State nor a Horizon Europe Associated Country, and the Digital Europe Programme is at least as closed, and often more restrictive, to direct Taiwanese applicants. Taiwan participates in Horizon Europe only as an Associated Partner under Article 9.1 of the Model Grant Agreement, meaning Taiwanese entities join consortia at their own cost. Taiwan's National Science and Technology Council (NSTC) has operated a Co-Funding Mechanism (CFM) since 2022 — listed in the EU's official CFM document alongside Australia, Brazil, Canada, India, Japan, Mexico, China, Monaco, Republic of Korea, and Switzerland — which provides domestic funding for Taiwanese researchers participating in Horizon Europe projects. The practical implication is that any joint PQC application requires a designated lead coordinator (which could be Dutch-led or from other countries when applicable), with Taiwanese partners bringing their own NSTC funding. This structural constraint also points to a broader strategic objective for the bilateral cooperation: actively advocating for greater EU openness to Taiwan in cybersecurity-relevant Horizon Europe and Digital Europe calls, where Taiwan's technical contribution — in PQC(including design, quantum cryptanalysis, and hardware implementation), semiconductor supply chain security, and real-world APT intelligence — is uniquely valuable and not substitutable from EU/Associated countries alone. The Netherlands is well positioned, both bilaterally with Taiwan and within EU policy fora, to champion this opening.

A new obstacle is that some calls restrict associate partners to OECD countries, thereby excluding Taiwanese partners. Some calls are even limited to entities registered in EU member states. These would appear to be open to Taiwanese companies who have successfully established a branch in the Netherlands; however, such calls recently started to require an "Ownership and Control" clause and are closed to entities that are deemed to be controlled from outside the EU.

This once again excludes Taiwanese companies that the Netherlands has worked hard to attract. For example, a Taiwanese cybersecurity company recently faced eligibility barriers in the Digital Europe Cybersecurity Call. Despite its established Dutch branch, it was blocked by ownership control requirements. While concerns about Chinese and Russian companies receiving EU funding are understandable, and scrutiny of Russia-controlled shadow entities has appropriately increased since the Ukraine war, Taiwanese companies are now unintended collateral damage in these restrictions.

Opportunity Area 5: AI Security, IoT/5G Emerging Domains

Horizon Europe Cluster 3 allocated EUR 40 million for "Generative AI for Cybersecurity" as a single topic in 2025, the largest single funding opportunity for bilateral joint research. Taiwan's AI chip manufacturing capacity (TSMC's manufacturing and CoWoS technology provides the critical advance for the majority of the world's high-end AI chips) complements Dutch AI security research methodologies. For 5G security, Taiwanese vendors possess base station equipment hardening capabilities that can address Dutch telecommunications providers' 5G network protection needs.

3.3 Cooperation Model Design

Joint Initiatives: Shared Democratic Values as Foundation

A defining feature distinguishing the Taiwan–Netherlands cybersecurity partnership from purely transactional technology cooperation is the alignment of democratic values. Both entities face authoritarian state-sponsored cyber threats — the Netherlands from Russia, Taiwan from China — and both explicitly frame cybersecurity as an extension of democratic resilience and rule of law. This shared normative foundation provides a uniquely durable basis for trust that goes beyond commercial interest.

The parallel is instructive: just as the Netherlands has positioned its cybersecurity cooperation with Ukraine as a democratic solidarity commitment during the Russia–Ukraine war — providing a range of assistance including incident response, threat intelligence sharing, and resilience-building — Taiwan's cybersecurity experience under sustained Chinese cyber operations represents a comparable case of democratic resilience under existential pressure. Taiwan can serve as both a reference model and a future cooperation partner in this framing.

A concrete institutional embodiment of this direction is the SeaSEC (Seabed Security Experimentation Center), inaugurated in The Hague, where the Netherlands, Denmark, Germany, Finland, Norway, and Sweden conduct research on protecting undersea infrastructure — submarine cables and energy pipelines — from physical and digital threats. The undersea cable dimension is directly relevant to Taiwan, which depends on a small number of submarine cables for international connectivity and has experienced targeted interference attempts.

Beyond infrastructure security, democratic value alignment opens cooperation channels in the information domain: countering disinformation campaigns, combating cognitive warfare, and strengthening digital civic resilience. Taiwan's experience with large-scale disinformation operations targeting elections and public opinion, and the Netherlands' similar exposure from Russian influence operations, provide shared problem framing for joint research and policy development.

RightsCon 2025, hosted in Taiwan, signals Taiwan's growing role as a convening hub for the global digital rights and internet freedom community — a community that overlaps significantly with technical cybersecurity researchers concerned with surveillance, censorship infrastructure, and privacy-preserving technologies. This creates a natural connection point for Dutch organizations working at the intersection of cybersecurity and human rights, including privacy-enhancing technologies and post-quantum cryptography for rights protection.

Practically, democratic value alignment reinforces cooperation in privacy-enhancing technologies, PQC deployment for protecting sensitive communications, and a secure information infrastructure. It also provides the political legitimacy for deeper intelligence sharing and joint exercises that purely commercial partnerships cannot easily sustain.

Community-Centric Triple Helix Model

The Netherlands' most distinctive and exportable cybersecurity asset is not any single product or company — it is its Triple Helix Model: the tight integration of government (public policy and diplomatic support), private sector (innovative technology and solutions), and knowledge institutions (TNO, TU Eindhoven, TU Delft, Radboud University, providing frontier research and development). This ecosystem architecture generates systemic resilience exceeding what any single participant — public, private, or academic — could achieve independently.

For the Taiwan partnership, this report propose adapting this model by substituting the knowledge institution pillar with the community pillar — replacing formal academic institutions as the third vertex with Taiwan's vibrant hacker and practitioner community (HITCON, CTF teams and security researchers). In this model, academia / research institutes remain essential, but this Community-Centric Triple Helix reflects Taiwan's actual ecosystem dynamics more accurately: much of Taiwan's cutting-edge security research and talent development happens in community settings, not traditional academic structures.

Pillar	Dutch Standard Model	Taiwan-Adapted Model
Public	NCSC, MOEA, Ministry of Foreign Affairs: policy frameworks and diplomatic support	NSC, ACS, ADI, NICS, NLOT: digital resilience policy, regulatory coordination, and diplomatic facilitation
Private	Fox-IT, EclecticIQ, Hadrian, Riscure: innovative technology products and managed services	Trend Micro, TXOne, CyCraft, DEVCORE, ChangingTec, Team T5, Keypasco, WiSECURE Technologies hardware security, OT, APT intelligence, PQC migration
Knowledge / Community	TNO, TU Eindhoven, TU Delft, Radboud, CWI: frontier R&D and standardization contribution	Academia Sinica HITCON community, CTF teams, TWCERT/CC, TWISC: practitioner-led research, talent pipeline, and international trust networks

The community pillar's value lies in speed, trust, and talent pipeline. HITCON CTF consistently maintains a premier position on CTFtime, the globally recognized authority for cybersecurity competitions. Furthermore, its excellence is underscored by its long-standing status as a pre-qualifier for DEF CON CTF, the world's most prestigious cybersecurity challenge, its CISO Summit attracting C-suite decision-makers, and its Cyber Range offering real-world exercise infrastructure make it a unique asset that no institutional equivalent can replicate. Integrating HITCON into the cooperation model — not merely as a conference venue but as an active cooperation pillar — is the single most differentiating strategic choice available for the Taiwan–Netherlands partnership.

Model Type	Applicable Context	Specific Mechanism Design
Joint Initiative (Democratic Values)	Policy-sensitive, trust-building, long-term legitimacy	Bilateral cybersecurity policy roundtable anchored in democratic solidarity; disinformation resilience working group; privacy and PQC cooperation extending digital rights framing
Community-Centric Triple Helix	Talent development, practitioner research, rapid trust formation	HITCON × ONE Conference cross-participation; HITCON Cyber Range open to Dutch teams; bilateral CTF; HITCON CISO Summit as government–community dialogue bridge
PoC Testbed	Technology validation, pre-commercialization	HSD Campus + Taiwan NICS digital lab; joint enterprise testing with SECPAAS framework
Working Group	Standards, regulatory alignment	SEMI Taiwan–NL Working Group; NIS2/Cybersecurity Management Act alignment; SeaSEC undersea infrastructure research collaboration
Multilateral Program	Research-intensive, high funding	Horizon Europe Cluster 3 joint applications; Taiwan as Associated Partner; Eureka/Eurostars cross-border R&D grants

3.4 Funding and Resource Pathways

Taiwan Side

Primary funding sources: MODA's Cybersecurity Industry Promotion Project (ACW) and international cooperation sub-programs within the Phase VII National Cyber Security Development Program (NT$8.8B, 2025–2028). Recommended approach: design phased PoCs meeting MODA application specifications, starting with small-scale pilots below NT$5 million each to minimize administrative barriers.

Netherlands and EU Side

The Netherlands government supports bilateral cooperation activities through RVO's International Business Development (IBD) instruments. At the EU level, Horizon Europe Cluster 3 (EUR 90.55 million total for 2025, including EUR 40 million for "Generative AI for Cybersecurity") is the most important joint research funding source. The Digital Europe Programme allocated EUR 15 million for PQC transition, though Taiwan cannot apply directly, access requires joining as part of a Dutch-led consortium.

Industry Co-Funding

Industry-sourced options include TIIN Capital's cybersecurity-focused venture fund, CYBERSEC Taiwan's corporate sponsorship mechanisms, and HSD Campus's joint PoC co-funding model (50% industry co-investment per party). The "Cybersecurity Made in Europe" quality label, administered by HSD, enhances European market credibility for Taiwanese companies upon certification.

Ch 4
Strategic Recommendations for Future Collaboration

4.1 Strategic Framework

Three-Pillar Structure

The strategic framework is organized around three parallel cooperation pillars: Government, Industry, and Academia/Community, each with a distinct thematic axis, operating simultaneously but at different rhythms. This structure reflects the Community-Centric Triple Helix model proposed in 3.3 Cooperation Model Design and ensures that cooperation is not dependent on any single channel.

Pillar	Thematic Axis	Core Focus
Government	Digital Resilience & Policy Exchange	Policy dialogue, regulatory alignment, critical infrastructure protection, and formal intelligence-sharing mechanisms anchored in democratic values
Industry	Semiconductor Industry → Full Supply Chain	Starting from the TSMC–ASML semiconductor nexus, expanding outward to cover the full hardware and software supply chain security ecosystem
Academia / Community	Democracy, Human Rights, PQC & Research	Joint research cooperation grounded in shared democratic values, including PQC and privacy-enhancing technologies; community-to-community exchanges; talent pipeline and practitioner-driven innovation.

Phase 1 (Year 1): Enter Taiwan's Cybersecurity Ecosystem: Build Trust

The primary objective of the first year is presence and trust-building. The Netherlands should establish visible, authentic participation in Taiwan's cybersecurity ecosystem before expecting deep project commitments. All Year 1 activities are designed to be low-risk, low-cost, and high-relationship-value.

Pillar	Year 1 Actions
Government	• Formally launch a 3-year PIB (Partners for International Business) project, with RVO as the Dutch anchor and Taiwan's MODA (ADI/ACS) as the counterpart • Pilot the inaugural "Taiwan–Netherlands Cybersecurity Strategic Roundtable" as a side event at HITCON or HITCON CISO Summit • Join the National Institute of Cyber Security (NICS) and CODE (Cyber Operations Defense Exercise) program as an international observer/partner • Launch bilateral cybersecurity policy research focusing on mapping regulatory divergences between NIS2 and Taiwan's Cybersecurity Management Act
Industry	• Establish a Dutch Cybersecurity Pavilion at CYBERSEC Taiwan (booth presence and co-organized sessions) • Nominate Dutch teams to participate in HITCON Cyber Range/CTF exercises • Organize a bilateral Taiwan–Netherlands cybersecurity company visit and exchange delegation • Invite Taiwanese and Dutch companies to co-apply for Eureka / Eurostars cross-border R&D grants • Participate in SEMICON Taiwan and add a dedicated cybersecurity zone within the Netherlands National Pavilion
Academia / Community	• Launch a bilateral researcher and talent exchange visit program, connecting Taiwan's academic cybersecurity centers (Academia Sinica IIS, NTU, NYCU Cybersecurity Institute) with Dutch counterparts (TNO, TU Eindhoven, TU Delft, Radboud University) • Facilitate signing of joint training or joint thinktank agreements between Taiwanese and Dutch universities • Co-organize the Annual Taiwan–Netherlands Cybersecurity Summit in partnership with HITCON • Establish cross-participation between HITCON and ONE Conference, Taiwanese community delegates at ONE Conference, Dutch community researchers at HITCON

Phase 2 (Year 3): Explore Cooperation Models: Diverse, Fast, Measurable

By Year 3, the relationship has sufficient trust capital to attempt substantive, project-based cooperation. The emphasis shifts to generating a portfolio of small, measurable cooperation cases across all three pillars, demonstrating viability before committing to large flagship programs.

Pillar	Year 3 Actions
Government	• Advance Regulation and Policy Alignment: complete NIS2 ↔ Taiwan Cybersecurity Management Act mapping document • Establish a regularized intelligence-sharing mechanism between NCSC-NL and Taiwan's NICS • Facilitate mutual recognition of cybersecurity compliance standards between the two sides • Conduct the first Taiwan–Netherlands Joint Critical Infrastructure Cybersecurity Exercise (tabletop format) • Hold the institutionalized Taiwan–Netherlands Cybersecurity Strategic Roundtable (annual)
Industry	• Cyber Range / Joint Exercises: co-organize a live-fire exercise with HITCON Cyber Range, open to both Taiwanese and Dutch enterprise teams • Activate the PIB (Partners for International Business) collective market expansion program, coordinating 5–8 Dutch and Taiwanese companies in joint market entry initiatives • Deepen SEMICON participation to build a sustained Taiwan–Netherlands semiconductor cybersecurity supply chain dialogue
Academia / Community	• Issue a bilateral Call for Research targeting priority topics: APT intelligence, PQC implementation, and submarine cable/undersea infrastructure security; provide research grants to incentivize joint publications • Co-organize a Taiwan–Netherlands Joint CTF competition in partnership with HITCON CTF, with scenarios focused on Industrial Control System (ICS) security • Establish a bilateral mentorship program: cybersecurity mentors from each entity guide counterpart students in cross-border research projects

Phase 3 (Year 5): Taiwan and the Netherlands as a Europe-Asia Democratic Cybersecurity Hub

The five-year horizon envisions Taiwan and the Netherlands as co-anchors of a democratic cybersecurity axis spanning Europe and Asia, not merely bilateral partners, but convening powers that attract other like-minded entities into an expanded cooperation architecture.

Pillar	Year 5 Actions
Government	• Jointly publish a Digital Sovereignty White Paper representing both governments' positions on democratic digital governance • Establish a mutually recognized cybersecurity testing and certification mechanism to ensure bilateral policy compatibility • Expand the Joint Critical Infrastructure Cybersecurity Exercise to include additional Euro-Asian partner nations and entities • Expand the Taiwan–Netherlands Cybersecurity Strategic Roundtable to a multilateral Euro-Asia format, inviting additional democratic partner nations and entities
Industry	• Facilitate commercial alliances and technology cooperation between Taiwanese and Dutch cybersecurity vendors • Establish a joint procurement platform exclusively for trusted companies from both sides • Leverage the Global EPIC platform to enable substantive Scale-ups and SMEs soft-landing, physical presence at HSD The Hague or Taiwan, with real customer pipelines
Academia / Community	• Establish a virtual Taiwan–Netherlands Cybersecurity Research Institute with a rotating directorship • Create a permanent "Taiwan–Netherlands Cybersecurity Talent Pool" with regular bilateral researcher secondments and an alumni network

NLOT's Coordination Role

NLOT plays an indispensable role in cross-domain coordination across all three pillars and all three phases. Functions: governmental dialogue interface between Taiwan's ADI/ACS and Netherlands NCSC/MOEA; institutional brokering between HSD/RVO and Taiwan's ITRI/NICS; PIB program anchor in Taiwan; and convening authority for the Taiwan–Netherlands Cybersecurity Strategic Roundtable. NLOT's unique position as a trusted presence in both ecosystems makes it the central coordinating node in this cooperation architecture.

4.2 Joint Research Initiatives

Post-Quantum Cryptography (PQC)

Post-quantum cryptography represents the single highest-value research collaboration opportunity between Taiwan and the Netherlands, because both sides hold globally recognized and complementary positions in this field — Taiwan in hardware implementation and algorithm development, the Netherlands in foundational algorithm design and migration methodology. Uniquely, key researchers from both sides already have established professional relationships (notably, PQC authority Professor Tanja Lange of Eindhoven University of Technology serves as a visiting scholar at Academia Sinica, Taiwan), making this the lowest-friction flagship research topic to launch.

Taiwan's PQC Research and Industry Strengths

- Algorithm Development: The team led by Distinguished Research Fellow Dr. Bo-Yin Yang at Academia Sinica's Institute of Information Science has been a sustained participant in NIST's PQC standardization competition. Algorithms co-developed by this team — including UOV (Unbalanced Oil and Vinegar), MAYO, and SPHINCS+ — have reached NIST finalist or alternate candidate status.

- PQC Accelerator Chips and Hardware Security Modules: Taiwanese companies including WiSECURE Technologies and Chunghwa Telecom's R&D teams have successfully developed HSMs (Hardware Security Modules) and PQC IC smart cards supporting PQC algorithms. Taiwan's hardware research maturity in side-channel attack resistance (anti-side-channel attack, SCA) is directly critical for ensuring that PQC chips remain secure against physical adversaries in real-world deployment environments.

- Migration-Focused Scale-ups and SMEs: Chelpis Quantum (池安量子) specializes in PQC migration solutions, helping enterprises transition legacy RSA/ECC encryption systems to quantum-resistant specifications — addressing the urgent enterprise need created by NIST's 2024 final standards.

- International PQC Event Hub: Taiwan is increasingly a global convening point for PQC. PQCrypto 2025 was held in Taipei; Taiwan will host Real World Crypto 2026, attracting top global cryptography practitioners. These events create natural intersection opportunities with Dutch researchers.

Netherlands' PQC Research and Industry Strengths

- Foundational Algorithm Leadership: Dutch researchers have made decisive contributions to NIST-selected algorithms. Professor Andreas Hülsing (TU/e) is a core co-designer of SLH-DSA (originally SPHINCS+), now a final NIST standard (FIPS 205). Dutch teams also contributed to ML-KEM (originally Kyber, FIPS 203) and ML-DSA (originally Dilithium, FIPS 204) — the three algorithms now forming the global PQC standard suite.

- PQCrypto Conference: The PQCrypto conference series — the premier international academic forum for post-quantum cryptography — was co-founded by Professor Tanja Lange. Her dual role as a founding figure of global PQC research and a visiting scholar at Academia Sinica Taiwan creates a direct institutional bridge between the two ecosystems.

- National PQC Migration Handbook: The most operationally significant Dutch contribution is the PQC Migration Handbook, jointly published in 2023 (renewed in late 2024) by AIVD (Netherlands Intelligence and Security Service), NCSC-NL, TNO (Netherlands Organisation for Applied Scientific Research), and CWI (Centrum Wiskunde & Informatica). This handbook is the definitive practical reference for organizations transitioning cryptographic systems, and its government-endorsed status gives it regulatory weight.

- Quantum Delta NL: The Dutch government has invested heavily in quantum technologies through the Quantum Delta NL national program, which tightly integrates national research resources with industry supply chains — providing a well-resourced institutional vehicle for joint Taiwan–Netherlands PQC initiatives.

Proposed Joint PQC Research Agenda

- Hardware-Accelerated PQC for Semiconductor Environments: Combine Taiwan's PQC chip design expertise (WiSECURE, Academia Sinica) with Dutch algorithm optimization research (TU/e, CWI) to develop PQC implementations optimized for semiconductor manufacturing equipment — directly extending the SEMI E187 security framework to the post-quantum era.

- Side-Channel Resistant PQC Implementations: Joint research on physical-layer security for PQC chips, combining Dutch hardware security attack expertise (Radboud, TU Delft) with Taiwan's SCA defense hardware maturity.

- Enterprise PQC Migration Toolkits: Translate the Dutch PQC Migration Handbook methodology into practical migration tools and assessment frameworks adapted for Taiwan's financial sector (F-ISAC) and critical infrastructure operators.

Key Reference: PQC Migration Handbook (AIVD, NCSC-NL, TNO, CWI, 2023/2024); NIST FIPS 203/204/205 (2024); Quantum Delta NL Program

Product Security and Bug Bounty

Taiwan and the Netherlands are complementary leaders in offensive security research and hardware-level product security testing — Taiwan through its world-class CTF community and semiconductor industry exposure, the Netherlands through its pioneering hardware security analysis institutions and rigorous product certification ecosystem.

Taiwan's Strengths

- Elite CTF and Vulnerability Research Community: Taiwan's CTF teams consistently rank in the global top tier at international competitions including DEF CON CTF, with multiple top-3 finishes — demonstrating world-class capability in software vulnerability discovery and low-level architecture security analysis. Several prominent international vulnerability disclosures originate from Taiwanese researchers.

- NICS Bug Bounty Program: Taiwan's National Institute of Cyber Security operates a structured Bug Bounty program targeting critical government systems — creating a national model for responsible disclosure that can be compared with and connected to Dutch programs.

- HITCON ZeroDay: HITCON's ZeroDay vulnerability disclosure platform provides a community-driven channel for responsible disclosure of vulnerabilities in products widely used in Taiwan's critical infrastructure — directly relevant to product security cooperation.

- SEMI E187 Security Provisions: Taiwan's leadership in SEMI E187 includes security requirements covering patch management, vulnerability scanning, and software update authentication for semiconductor manufacturing equipment — extending product security norms into industrial hardware contexts.

Netherlands' Strengths

- TNO Cyber-Secure Systems by Design: TNO's program translates complex security requirements into executable engineering processes, helping manufacturers build security into products from the design stage rather than retrofitting it — directly relevant to Taiwan's hardware-dominant industry.

- Hardware Security and Side-Channel Attack Research: Radboud University and TU Delft are globally recognized leaders in side-channel analysis (SCA) and fault injection (FI) research — not only identifying vulnerabilities in chips and embedded systems, but developing low-power, attack-resistant algorithms specifically for IoT products. This is precisely the expertise needed to harden Taiwan's semiconductor and IoT hardware exports.

- Riscure (now part of Keysight): This Dutch-origin company is the global standard-setter for hardware security testing tools and services; its testing frameworks are used by semiconductor companies worldwide to validate product security — creating a direct commercial bridge to Taiwan's semiconductor vendors.

- NCSC-NL Product Testing Standards: NCSC-NL maintains high-specification testing criteria for products used in critical infrastructure, including smart grid equipment — providing a certification pathway relevant to Taiwanese hardware vendors seeking EU market entry.

- NEN Standards Participation: The Netherlands Standardisation Institute (NEN) actively contributes to ISO and IEC international cybersecurity standards, ensuring Dutch technical expertise is embedded in global product security norms that Taiwan's exporters must comply with.

Proposed Joint Product Security Research Agenda

- Cross-border Bug Bounty Coordination: Link Taiwan's NICS Bug Bounty with Dutch coordinated vulnerability disclosure frameworks to create a bilateral responsible disclosure protocol for products with supply chain presence in both jurisdictions.

- Hardware Security Certification for Semiconductor Equipment: Joint development of side-channel attack testing methodologies specifically for semiconductor fab equipment, building on SEMI E187 compliance requirements and Dutch hardware security expertise.

- IoT Security Design Framework: Combine TNO's Secure by Design methodology with HITCON community vulnerability research to produce a practical IoT security design guide applicable to Taiwan's IoT hardware manufacturing ecosystem.

APT Threat Intelligence

Taiwan's exposure to sustained, sophisticated Chinese state-sponsored APT campaigns (BlackTech, Flax Typhoon, Mustang Panda, and others) generates real-world intelligence on adversary TTPs (Tactics, Techniques, and Procedures) that is uniquely valuable to European partners facing the same threat actors. The Netherlands' NCSC and firms like EclecticIQ have established APT tracking and threat intelligence platform capabilities that complement Taiwan's raw intelligence advantage with analytical frameworks and European attribution experience. Formal bilateral APT intelligence sharing — through the Bilateral Tech-ISAC proposed in Section 4.1 — should treat APT research as the primary knowledge exchange content.

Undersea Infrastructure Security (SeaSec)

The opening of the SeaSEC (Seabed Security Experimentation Center) in The Hague — bringing together the Netherlands, Denmark, Germany, Finland, Norway, and Sweden for collaborative research on protecting undersea critical infrastructure — creates a directly relevant cooperation opportunity for Taiwan. Taiwan depends on a small number of submarine cables for international internet connectivity, and these cables have been identified as high-value targets in conflict scenarios. The physical security of undersea infrastructure intersects with cybersecurity in monitoring, intrusion detection, and command integrity of undersea sensor and response systems.

Proposed joint research areas include:

- Submarine Cable and Pipeline Monitoring: Research applying sonar systems, unmanned underwater vehicles (UUVs), and distributed sensor networks for real-time detection of unauthorized approach or sabotage of undersea fiber-optic cables. Taiwan's experience defending against cable interference and the Netherlands' SeaSEC research infrastructure can be directly paired.

- Cyber-Physical Security of Undersea Infrastructure: Developing threat models and defensive architectures for the command and monitoring systems that manage undersea cable landing stations and energy pipeline endpoints — systems that are both physically and digitally vulnerable.

- Legal and Policy Framework for Undersea Infrastructure Protection: Joint research on international law, attribution frameworks, and policy responses for undersea infrastructure attacks — a domain where the Netherlands' legal research institutions (T.M.C. Asser Institute) and Taiwan's experience with grey-zone coercion can produce policy-relevant outputs.

Reference: SeaSEC Center inauguration, The Hague (2024–2025); participating nations: Netherlands, Denmark, Germany, Finland, Norway, Sweden

Collaboration Structure

All four research areas follow the "1+1+1" consortium architecture: one Taiwanese research institution (lead) + one Dutch research institution (co-lead) + one enterprise partner from each side (application validation). For PQC and Product Security, the recommended funding pathway is Horizon Europe Cluster 3 (Taiwan as Associated Partner) or Eureka/Eurostars bilateral R&D grants. For APT and SeaSEC, government-to-government program funding (PIB, RVO IBD instruments, MODA/ACS international cooperation budgets) is the more appropriate channel.

4.3 Talent and Training Exchange

Exchange Formats and Target Groups

- Short-term visits (2–4 weeks): Taiwanese cybersecurity personnel in residence at HSD Campus; Dutch cybersecurity experts attending CYBERSEC or HITCON workshops in Taiwan
- Researcher exchange program: Bilateral graduate student and postdoctoral exchange focused on PQC, OT security, and AI threat detection
- Train-the-Trainer: Each side trains 10 seed instructors who then execute in-island training programs to multiply impact

Train-the-Trainer Design

Training curriculum built around three core modules: (1) Semiconductor supply chain security (SEMI E187 framework); (2) OT/ICS red team penetration testing; (3) APT threat hunting methodology (focused on TTP analysis of China-linked APT groups). First cohort target: complete training in 2026.

4.4 Annual Taiwan–Netherlands Cybersecurity Summit

Institutionalization Design

Recommended scheduling: The Hague Cyber Security Week (September–October) as the primary venue, with a satellite session at CYBERSEC Taiwan (March–April) each year, creating two structured dialogue occasions annually. Rotating host model: odd years hosted by Taiwan (during CyberSec), even years hosted by the Netherlands (during ONE Conference).

Linkage with ONE Conference

Institutionalize Taiwan's ONE Conference delegation (fixed annual composition: government + industry + academia); institutionalize Dutch speaker participation at CYBERSEC with keynote addresses (extending the 2024–2025 model). Summit agenda-setting to be aligned with annual threat assessment reports (Taiwan: NSB Annual Report; Netherlands: CSBN).

Expected Outputs

"Taiwan–Netherlands Cybersecurity Cooperation Annual Statement" published each Summit, tracking objective completion

Summit matchmaking to generate at least 3 new bilateral cooperation initiatives or PoC agreements per edition

"Taiwan–Netherlands Cybersecurity Policy Dialogue Working Group" holding at least 2 formal meetings per year

4.5 Cyber Range / Joint Exercises

Exercise Types and Scenarios

Three exercise types are recommended, progressively building bilateral exercise capacity:

- Tabletop Exercise: Ransomware attack on semiconductor supply chain scenario; conducted during Summit; low cost, high policy dialogue value
- Technical Exercise: OT environment penetration testing and APT attack simulation; conducted at HSD Campus or NICS laboratory environments
- Joint Cyber Exercise (long-term goal): Connecting Taiwan's MODA exercise programs with NCSC's Cyber Storm-type exercises. Reference model: Taiwan's first participation in U.S. CISA Cyber Storm IX in 2024 (2,200 participants, 11 countries, 300 organizations) (Source: The Defense Post, 2024)

Participants and Outputs

ACS (Taiwan) and NCSC (Netherlands) serve as government co-hosts; HSD, ITRI, and NICS as technical implementation bodies; bilateral cybersecurity enterprises as scenario providers and observers. Each exercise produces an After-Action Review (AAR) for bilateral policy reference.

4.6 Regulation and Policy Alignment

Mapping Work

Taiwan's Cybersecurity Management Act and Dutch NIS2 (The Dutch Cyberbeveiligingswet (Cbw), which implements NIS2, had passed the House of Representatives in April 2026, with the Dutch government previously targeting Q2 2026 for entry into force; however, at the time of writing, final enactment should still be presented as pending) share high comparability in critical infrastructure definitions, incident reporting timeframes, and security measure requirements.

Recommendation: Establish a bilateral Regulation Alignment Matrix to clarify compliance pathways for Taiwanese companies entering the Dutch/EU market.

Working Group

Establish a "Taiwan–Netherlands Cybersecurity Regulatory Dialogue Working Group" meeting twice annually, with topics alternating between: (1) cross-border data flows and privacy protection (including GDPR adequacy decision progress); and (2) product cybersecurity (alignment between EU Cyber Resilience Act and Taiwan's corresponding regulations).

Outputs

- Annual Policy Brief summarizing bilateral regulatory divergences and convergence trends
- Cybersecurity compliance guidance handbook (Traditional Chinese) for Taiwanese companies entering Dutch/EU markets
- NIS2-aligned cybersecurity capability maturity assessment tool for Taiwan's critical infrastructure operators

4.7 Scale-ups/SMEs and Innovation Collaboration

Accelerator Exchange

Establish a bilateral scaling-up Companies and SMEs exchange program between HSD Campus and Taiwan Tech Arena (TTA): 5 companies from each side per year in 3-month reciprocal soft-landings. Taiwanese firms using HSD Campus should be positioned to receive market-entry guidance, customer introductions, and support in understanding European qualification pathways; access to the ECSO "Cybersecurity Made in Europe" label would be relevant only if the firm later establishes a qualifying European structure. Dutch scaling-up companies and SMEs at TTA receive ADI priority recommendations for Taiwanese customer matchmaking and government pilot environments.

Joint PoCs and Investment Matchmaking

Design a "Taiwan–Netherlands Cybersecurity PoC Fund" built on the SECPAAS platform: 50% from Taiwan's ACW program, 50% from TIIN Capital or RVO subsidy, with each PoC budgeted at NT$3–5 million over a 6-month execution cycle. Select 5–8 PoC applications annually, prioritizing PQC applications, OT security tools, and AI-driven threat detection.

Ch 5
Conclusion

Taiwan–Netherlands cybersecurity cooperation has evolved from exploratory contacts to a partnership with genuine institutional foundations in less than seven years. The core driver is inescapable strategic interdependence: Taiwan holds over 60% of global foundry revenue and produces over 90% of the world's most advanced logic chips; ASML is the world's sole EUV equipment manufacturer. The cybersecurity resilience of this shared supply chain is a common interest and a lifeline for the global technology ecosystem.

This report's central argument is that Taiwan–Netherlands cybersecurity cooperation is no longer optional; it is strategically necessary. Taiwan's sustained exposure to Chinese intrusions/disturbance attempts (2.4 million daily in 2024; Source: NSB, 2025) has generated real-world threat intelligence that no European partner can replicate in simulation. The Netherlands' NIS2 compliance infrastructure, OT security methodologies, and European market access are indispensable resources for Taiwan's cybersecurity industry internationalization. Their combination creates a strategic multiplier effect far exceeding what either side can achieve independently.

The 2024 MoU and the 2025 Summit activities signal that Taiwan–Netherlands cybersecurity cooperation has entered a "deep phase", the institutional architecture is established, execution capacity is accumulating, and what is now needed is the translation of exchange-based interactions into measurable, sustainable, and scalable concrete cooperation outcomes.

Three Priority Actions

- Launch the Bilateral Tech-ISAC Threat Intelligence Sharing Mechanism: Connect TWCERT/CC and NCSC focused on APT threats to semiconductor and critical technology sectors. Target: 6 months to launch, 12 months to formalize.

- Form the Post-Quantum Cryptography Joint Research Consortium: Use Horizon Europe Cluster 3' s 2026 call as the target window, with ADI' s Post-Quantum Alliance and TU Eindhoven, TU Delft/Radboud as the core research team. Target: proposal submission within 6-12 months.

- Establish the Taiwan–Netherlands Cybersecurity scaling-up companies and SMEs Acceleration Platform by Integrating SECPAAS, HSD Campus, and TTA resources into bilateral soft-landing mechanisms. First cohort of 5 companies to launch in 2026.

Taiwan's global cybersecurity value lies not merely in being a market or a partner, but in being a living laboratory that forges cybersecurity capabilities under the world's most demanding operational conditions. The Netherlands stands to gain a decisive first-mover advantage in Europe by deepening this strategic partnership now.

Appendices

Appendix A List of Bilateral Cooperation Events (2018–2025)

Date	Format	Key Content and Outcomes	Organizer
May 2019	Recon Mission	“Explore Next Cyber Taiwan 2019”; TU Delft × TWISC MoU signed	HSD / NLOT
Jun–Jul 2020	Digital Mission	3-session online matchmaking; 10–15 corporate cybersecurity needs collected	RVO / NLOT
Mar 2022	Business Mission	InnovationQuarter Digital Cyber Security Innovation Mission to Taiwan	InnovationQuarter
Apr 2022	Policy Document	Netherlands Cyber Security Roadmap Towards Taiwan published	HSD/IQ/RVO
Mar 2023	Roadmap Update	Roadmap 2023 updated; Dutch delegate attends CYBERSEC Taiwan	HSD / RVO
May 2024	Recon Mission	HSD keynote to ~1,000 at CYBERSEC 2024; meetings with 15 potential Dutch-office companies	HSD
Oct 2024	MoU Signing	Taiwan–Netherlands Cyber Consortium MoU signed at ONE Conference; 8 founding members	HSD / ADI
Apr 2025	Business Mission	Dutch delegation at CYBERSEC Taiwan 2025; Dutch NS CISO keynote; meetings with NCSC, HITCON board	HSD / NLOT
Sep–Oct 2025	Summit / Keynote	ADI Director General delivers first international keynote at Hague Cyber Security Week; inaugural Taiwan–Netherlands Cybersecurity Roundtable	ADI / NCSC

Sources: HSD Securitydelta.nl; MODA ADI Press Releases; InnovationQuarter; TU Delft

Appendix B Opportunity Matrix

Cooperation Domain	Feasibility	Strategic Importance	Funding Accessibility	Priority
Post-Quantum Cryptography Joint Research	★★★★☆	★★★★★	Horizon Europe	P1 — Immediate
Bilateral Tech-ISAC	★★★★☆	★★★★★	Government core budget	P1 — Immediate
Semiconductor Supply Chain (E187 expansion)	★★★★★	★★★★★	Industry co-funding	P1 — Immediate
Annual Cybersecurity Summit	★★★★★	★★★★☆	Low cost, self-funded	P2 — 6 months
OT/ICS Joint Exercises	★★★☆☆	★★★★★	Government program + NCSC	P3 — 1–3 years
AI Security Joint Research (Horizon Europe)	★★★☆☆	★★★★★	Horizon Europe EUR 40M	P3 — 1–3 years
Regulatory Alignment Working Group	★★★★☆	★★★★☆	Low cost, government-led	P2 — 6 months

Appendix C Key Data Summary

Metric	Taiwan	Netherlands	Source
Cybersecurity market size (2024)	~USD 1.7B (NT$53.78B)	~USD 2.35–3.21B	Trade.gov; Mordor Intelligence
Number of cybersecurity companies	~368 firms	~432 firms (400+ in The Hague)	ACW; HSD
Cybersecurity professionals	~9,000 (target: 10,000)	~15,000 (estimated)	MODA; Trade.gov
Government cybersecurity budget	NT$8.8B (2025–28)	EUR 111M (2022–28 strategy)	MODA; Dutch Government
Daily cyberattacks on government intrusions/ disturbance attempts	2.4 million (2024, doubled)	“Significant and diverse” (CSBN 2024)	NSB 2025
Annual confirmed cybersecurity incidents	906 cases (2024, +20%)	At least 121 ransomware incidents (2024)	Taipei Times; CSBN 2025
Market CAGR	9.1% (2016–22), vs. 8.1% global	~10.8% (2024–29 forecast)	Business Sweden; Mordor Intelligence
Flagship annual conference	CyberSec: 20,000+ attendees, 500+ exhibitors	ONE Conference global top-tier)	iThome; ECCC
Scaling-up company/ SME/ Startup ecosystem	88 firms, 24 funded, 12 at Series A+	Hadrian valuation $1.6B (Jan. 2026)	Tracxn; PitchBook
Landmark semiconductor/OT standard	SEMI E187/E188 (TSMC-led)	N/A	SEMI.org; CISA
Key international exercise participation	CISA Cyber Storm IX (2024, first-ever)	NATO Locked Shields; Cyber Storm (12-nation partner)	The Defense Post (2024); NATO CCDCOE

Disclaimer: Market size figures are drawn from cited external sources; variations across reports reflect different research methodologies. Original source reports should be consulted for definitive figures.

Appendix D Glossary of Key Terms

- Cyber Range: A simulated network environment platform used for attack/defense exercises, penetration testing, and incident response training, replicating real-world infrastructure without operational risk.
- Tabletop Exercise: A discussion-based exercise format involving scenario simulation without live technical system operations; suitable for policy decision-makers and senior executives.
- Advanced Persistent Threat (APT): Highly technical, long-duration cyberattack campaigns conducted by state-sponsored or organized criminal groups, characterized by sustained infiltration and data exfiltration.
- Zero Trust Architecture (ZTA): A security design principle of “never trust, always verify”, no user, device, or network segment is assumed trustworthy without continuous verification.
- Soft Landing: A market-entry model where foreign companies receive local support (office space, regulatory guidance, customer matchmaking) through an in-market partner such as HSD Campus, reducing the cost and risk of market entry.
- CNSA 2.0 (Commercial National Security Algorithm Suite 2.0): NSA’ s post-quantum cryptographic algorithm specifications for national security systems, mandating compliance for all new acquisitions by January 2027.
- NIS2 Directive: EU Directive 2022/2555 mandating enhanced cybersecurity requirements for operators of essential and important entities. The Netherlands is transposing NIS2 through the Cyberbeveiligingswet (Cbw), expected to enter into force Q2 2026, affecting approximately 8,000 organizations.
- Cyber Resilience Act (CRA): EU regulation establishing cybersecurity requirements for products with digital elements, affecting hardware and software manufacturers, directly relevant to Taiwanese ICT vendors selling into EU markets.
- SECPAAS (Security Platform as a Service): An ITRI-managed platform connecting Taiwanese cybersecurity companies with European markets through HSD Campus, including soft-landing services, partner matchmaking, and market intelligence.
- F-ISAC (Financial-Information Sharing and Analysis Center): Taiwan’ s financial sector threat intelligence sharing center, established in 2017 and achieving 100% coverage of all 200+ financial institutions by May 2019 (Source: FSC, 2017).

This is a publication of
Netherlands Enterprise Agency
Prinses Beatrixlaan 2 | 2595 AL Den Haag
Postbus 93144 | 2509 AC Den Haag
T +31 (0) 88 042 42 42
Contact us
www.rvo.nl

Netherlands Enterprise Agency | July 2026
Publication number: RVO-139-2026/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.