

Akcan, Melis; Groep, David; Ritzen, Jozef M. M.; Rounding, Nicholas

Working Paper

A strategy for cybersecurity and digital sovereignty for the Netherlands (2025-2035) contribution to a coalition agreement

UNU-MERIT Working Papers, No. 2025-029

Provided in Cooperation with:

Maastricht Economic and Social Research Institute on Innovation and Technology (UNU-MERIT),
United Nations University (UNU)

Suggested Citation: Akcan, Melis; Groep, David; Ritzen, Jozef M. M.; Rounding, Nicholas (2025) : A strategy for cybersecurity and digital sovereignty for the Netherlands (2025-2035) contribution to a coalition agreement, UNU-MERIT Working Papers, No. 2025-029, United Nations University (UNU), Maastricht Economic and Social Research Institute on Innovation and Technology (UNU-MERIT), Maastricht,
<https://doi.org/10.53330/ZMFF2486>

This Version is available at:

<https://hdl.handle.net/10419/339049>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<https://creativecommons.org/licenses/by-nc-sa/4.0/>



Working Paper Series

#2025-029

A Strategy for Cybersecurity and Digital Sovereignty for the Netherlands (2025–2035) Contribution to a Coalition Agreement

Melis Akcan, David Groep, Jo Ritzen and Nicholas Rounding

Published 4 December 2025

DOI: <https://www.doi.org/10.53330/ZMFF2486>

Maastricht Economic and social Research institute on Innovation and Technology (UNU-MERIT)
email: info@merit.unu.edu | website: <http://www.merit.unu.edu>

Boschstraat 24, 6211 AX Maastricht, The Netherlands
Tel: (31) (43) 388 44 00

UNU-MERIT Working Papers

ISSN 1871-9872

**Maastricht Economic and social Research Institute on Innovation and Technology
UNU-MERIT**

UNU-MERIT Working Papers intend to disseminate preliminary results of research carried out at UNU-MERIT to stimulate discussion on the issues raised.



<https://creativecommons.org/licenses/by-nc-sa/4.0/>

A Strategy for Cybersecurity and Digital Sovereignty for the Netherlands (2025–2035)¹

Contribution to a Coalition Agreement

December 2025

by

Akcan, Melis, Forips BV

Groep, David, Maastricht University (Technical Engineering, DACS)

Ritzen, Jo, Maastricht University (UNU-Merit)

Rounding, Nicholas, Maastricht University (ROA, SBE)

with advice from Schoenmaekers, Sarah, Maastricht University (Law)

JEL Classifications, H56, O38, L86, F52

Keywords

Cybersecurity; Digital Sovereignty; Public Procurement; Innovation Policy

Abstract

This paper proposes a mission-oriented national strategy for strengthening cybersecurity and achieving digital sovereignty in the Netherlands for 2025–2035. It outlines an integrated framework across four pillars: national cyber resilience, sovereign digital procurement, innovation and ecosystem development, and societal capacity-building. Emphasizing European cooperation, secure-by-design principles, and strategic public investment, the strategy aims to reduce dependence on non-EU technologies, enhance

¹) With thanks for comments to Cody Barrow (EclecticIQ), Marjolijn Bonthuis (ECPD), Joris den Bruinen and Lieve Lubbe (Security Delta), Hans Franken (Leiden University), and Frank van Heemskerk (ASML).

deterrence capabilities, and support talent development. A phased implementation roadmap highlights concrete actions for government, industry, and academia to ensure long-term national security, economic resilience, and democratic integrity in an increasingly contested digital landscape

1. Vision and Strategic Imperative

In the 21st century, cybersecurity and digital sovereignty are fundamental requirements for our national security, economic resilience, democratic integrity, and social well-being. As one of the most digitized countries in the world, the Netherlands faces a dual challenge: defending against increasingly sophisticated cyber threats, while ending its strategic dependence on non-EU technology suppliers who cannot guarantee the digital rights of Dutch citizens nor the digital sovereignty of the Dutch government.

Our vision for 2035 is a resilient, innovative, and sovereign digital Netherlands—a nation that safely harnesses the opportunities of digitalization, protects the fundamental rights of its citizens, and upholds its democratic autonomy through technological freedom. This requires a paradigm shift: from fragmented, reactive policy toward a bold, mission-oriented national strategy that integrates cybersecurity, digital sovereignty, and European cooperation at its core.

2. Foundations for Integrated Action

To realize this vision, the next government must act decisively across four interconnected pillars:

Pillar 1: Strengthen National Cyber Resilience

- **Mandatory Security Standards:** Legally require all operators of critical infrastructure (energy, defense, finance, health, transport, IT) to meet minimum security standards and certifications in line with the EU Cybersecurity Act (CSA) and the NIS2 Directive.

- **Active Defense & Deterrence:** Develop robust technical and diplomatic capabilities to deter and respond to state-sponsored cyber aggression, thereby strengthening our national and NATO cyber defense posture.

Modernized Legal Framework: Introduce a new, comprehensive Cybersecurity Act in 2026 to consolidate obligations, streamline incident reporting, and ensure full alignment with NIS2 (Network and Information Security Directive 2, The European Union's updated directive on cybersecurity for essential and important entities.) and GDPR (General Data Protection Regulation, The EU regulation governing the protection of personal data and privacy.).

Pillar 2: Achieve Digital Sovereignty through Strategic Procurement

- **Leverage Public Procurement Power:** Use the considerable purchasing power of the Dutch public sector (around 20% of GDP) to build a sovereign European digital ecosystem. Launch coordinated, mission-driven tenders for critical digital services (e.g., cloud, productivity software, identity management), ensuring sufficient growth capital to prevent strategic companies from seeking futures outside Europe.
- **Enforce Sovereignty Criteria:** Mandate that all publicly procured digital services meet non-negotiable criteria: 1) All data must be stored and processed exclusively within jurisdictions guaranteeing long-term compliance with European privacy standards; 2) Guaranteed service continuity immune to foreign political interference; 3) Contractual protection against unilateral changes or termination of service.
- **Build European Alliances:** Lead the formation of European coalitions and IT supplier consortia to develop competitive, sovereign alternatives—transforming the Netherlands from a passive consumer into an active architect of Europe's digital future.

Pillar 3: Stimulate Innovation and a Sovereign Ecosystem

- **Invest in Domestic Knowledge:** Provide R&D funding, innovation-driven procurement guarantees, and risk capital to boost the development and adoption of Dutch and European cybersecurity products.

- **Focus on Future-Proof Technologies:** Prioritize investment in strategic domains such as post-quantum cryptography, AI-driven security, and secured IoT via public-private partnerships.
- **Embed the Secure-by-Design Principle:** Integrate cybersecurity from the design stage into emerging technologies (e.g., AI, quantum computing) in critical sectors.
- **Support SMEs:** Create targeted incentive and guidance programs to help small and medium-sized enterprises overcome the cost and complexity of certification and compliance.

Pillar 4: Build a Digitally Resilient and Skilled Society

- **Education Reform:** Integrate digital literacy into the national curriculum starting from secondary education. Expand university quotas and specialized programs to train 20,000 new cybersecurity experts by 2035.
- **National Awareness Campaigns:** Launch permanent, year-round public campaigns to promote cyber hygiene across all layers of society.
- **Cyber Reserve Force:** Strengthen the national cyber reserve corps of volunteer experts from industry and academia to enhance response capacity during major crises.

3. Governance and Cooperation: The Dutch Model

The unique Dutch model of public-private cooperation is our greatest strength and must be further reinforced.

- **Empower the Cyber Security Council (CSR):** Formalize its role as an independent advisory body ensuring continuous strategic dialogue among government, business, and academia.
- **Strengthen the NCSC:** Continue supporting the National Cyber Security Center as the central hub for national threat intelligence, incident coordination, and guidance.
- **Develop a National Cyber Campus:** Build upon the NCSC and the Dutch PPP model (Security Delta/HSD) to establish a federated network of regional and sectoral hubs and labs, linked to a central physical location

for the Dutch Cyber Resilience & Response Center—focusing on innovation, funding, talent development, and resilience networking.

- Expand the National Cyber Resilience Network: Strengthen the roles of Information Sharing and Analysis Centers (ISACs), sectoral CSIRTs, crisis simulations, and innovation platforms to accelerate threat information sharing and joint innovation.
- Contribute to a Solid European Legal Framework: Ensure the legality of data storage within the EU/EEA and that public tenders can be reserved for EU/EEA participants, in line with the EU/EEA Government Procurement Agreement under the WTO and Article 25 of Directive 2014/24/EU.

4. Phased Implementation Roadmap (2025–2035)

Phase	Key Actions
Phase 1: Foundation (2025–2026)	Conduct comprehensive security audits in all critical sectors. Introduce the new Cybersecurity Act. Establish the framework for pooled sovereign procurement and begin building European consortia.
Phase 2: Acceleration (2027–2029)	Launch the first major sovereign IT tenders for 2030–2034 procurements. Establish a national Cyber Resilience & Response Center for real-time public-private data exchange. Integrate cybersecurity into education curricula.

Start pilot projects for post-quantum cryptography.

Phase 3: Consolidation (2030–2032) Sustainably scale the deployment of domestic cybersecurity products. Expand joint cyber defense exercises with EU and NATO partners. Formally establish the Cyber Reserve Force.

Phase 4: Sovereignty & Leadership (2033–2035) Publish and implement a national strategy for cloud and data sovereignty. Evaluate strategic outcomes, update the national strategy, and position the Netherlands as a world leader in secure and sovereign digital innovation.

5. Conclusion: A Call for Digital Leadership

The convergence of geopolitical instability, rapid technological change, and persistent cyber threats demands a response equal to the scale of the challenge. Incremental improvement alone will not suffice.

Is digital sovereignty in Europe an illusion, knowing that in the first quarter of 2025 about 98% of ASML's customers were outside the EMEA region? It will be—unless strong leadership is shown.

This integrated strategy provides a roadmap to secure our digital future, protect our democracy, and create economic opportunity. By combining our globally admired collaborative model with a determined shift toward technological sovereignty, the Netherlands can and must lead Europe in building a digital space that is secure, resilient, and fundamentally free.

We call on the next coalition government to embrace this mission-oriented approach and commit the necessary political will and resources to make this vision a reality.

The UNU-MERIT WORKING Paper Series

- 2025-01 *Development strategies for the green hydrogen economy in emerging economies* by Fabianna Bacil, Anthony Black, Marina Domingues, Jun Jin, Rasmus Lema, Glen Robbins and Sören Scholvin
- 2025-02 *Do global value chains and local capabilities matter for economic complexity in EU regions?* by R. Boschma, E. Hernández-Rodríguez, A. Morrison and C. Pietrobelli
- 2025-03 *Innovation and productivity: the recent empirical literature and the state of the art* by Jacques Mairesse, Pierre Mohnen and Ad Notten
- 2025-04 *Digital Technologies, Hiring, Training, and Firm Outcomes: Evidence from AI and ICT Adoption in Indian firms* by Sneha Marydas, Nanditha Mathew, Giordano De Marzo and Carlo Pietrobelli
- 2025-05 *New technologies and employment: the state of the art* by Marco Vivarelli and Guillermo Arenas Díaz
- 2025-06 *Formal-Informal Supply Chain Linkages and Firm Productivity in Sub-Saharan Africa: The Role of Human Capital* by Gbenoukpo Robert Djidonou, Neil Foster-McGregor and Nanditha Mathew
- 2025-07 *Internet Access and Youth's Mental Health and Well-being: Evidence from Ethiopia* by Trang Thi Pham and Pui-Hang Wong
- 2025-08 *A Twin Transition or a policy flagship? Emergent constellations and dominant blocks in green and digital technologies* by Linnea Nelli, Maria Enrica Virgillito and Marco Vivarelli
- 2025-09 *Good for business, not so much for the environment? Entry into importing and the energy intensity of Indian plants* by Michele Delera, Nanditha Mathew and Tania Treibich
- 2025-10 *The role of business visits in fostering R&D investment* by Marco Vivarelli, Mariacristina Piva and Massimiliano Tani
- 2025-11 *Not as innocent as it seems? The effects of "neutral" messaging on refugee attitudes* by Tobias Hillenbrand, Bruno Martorano and Melissa Siegel
- 2025-12 *Europeanizing Universities: A Catalyst for Social Cohesion and Sustainable Economic Development* by Jo Ritzen
- 2025-13 *Robots & AI Exposure and Wage Inequality: A Within Occupation Approach* by Florencia Jaccoud
- 2025-14 *Social Protection and Climate Disasters: Brazil's Responses to the 2024 Rio Grande do Sul Floods* by Raquel Tebaldi
- 2025-15 *A New Perspective on European Labour Migration: A Case Study of the Opportunity Cost for Greece and Poland* by Katrin Marchand, Pavlos Liagkas, Dani Smith and Aleksandra Wojnar
- 2025-16 *Does Training in AI Affect PhD Students' Careers? Evidence from France* by Pierre Boutros, Eliana Diodati, Michele Pezzoni and Fabiana Visentin
- 2025-17 *Endogenous R&D elasticities of productivity functions and BERD bias: Explorations of functional coefficient regressions* by Thomas Ziesemer
- 2025-18 *A data set for domestic and foreign private and public R&D stocks and labour-augmenting technical change for 44 rich or emerging economies with explorations on panel unit roots, cointegration, growth rate slowdown, and con- or divergence* by Thomas Ziesemer

- 2025-19 *Avenues to Maximizing Value Added from Critical Minerals* by Carlo Pietrobelli and Jorge Valverde
- 2025-20 *Corruption as a Gendered Barrier: Informal Institutions and the Limits of Democratization in North Macedonia* by Milka Muratovska, Ina Kubbe and Ortrun Merkle
- 2025-21 *Generative AI: A Double-Edged Sword for Western Democracy* by Jo Ritzen
- 2025-22 *Artificial intelligence as a complement to other innovation activities and as a method of invention* by Guillermo Arenas Díaz, Mariacristina Piva and Marco Vivarelli
- 2025-23 *Social Media and Son Preference: Evidence from India* by Praachi Kumar and Bruno Martorano
- 2025-24 *Human Capital and Occupational Mobility: The Case of Brazil* by Renata Mayer Gukovas
- 2025-25 *Local Gains from Global Minds: The Impact of Collaborating with Foreign-Educated Researchers on Non-Mobile Researchers' Performance* by Rodrigo Ito, Fabiana Visentin, Robin Cowan, Diego Chavarro and Tommaso Ciarli
- 2025-26 *Reforms welcome? Evidence on the nature of asylum backlash and orderly admissions as a remedy* by Tobias Hillenbrand
- 2025-27 *Social movements' impact on inequality beliefs, preferences for redistribution, and political participation* by Bruno Martorano, Laura Metzger, Patricia Justino and Francesco Iacoella
- 2025-28 *Automation and the Margins of Export Performance: Evidence from French Firms* by Thao Trang Nguyen, Giacomo Domini, Marco Grazzi, Daniele Moschella and Tania Treibich
- 2025-29 *A Strategy for Cybersecurity and Digital Sovereignty for the Netherlands (2025–2035) Contribution to a Coalition Agreement* by Melis Akcan, David Groep, Jo Ritzen and Nicholas Rounding