



Whitepaper

Cybersecurity and Digital sovereignty - Bridging the gaps

Authors

Paul Timmers, Matthijs Punter, Claire Stolwijk

TNO innovation
for life

Contents

Chapter 1 [p.3](#)[Executive summary](#)**Chapter 2** [p.4](#)[Analysing cybersecurity sovereignty](#)**Chapter 3** [p.6](#)[From analysis to action](#)**Chapter 4** [p.18](#)[Increasing impact of actions](#)**Chapter 5** [p.25](#)[Conclusions, main recommendations and actions](#)**Annex I** [p.27](#)[Interviewed experts](#)**Annex II** [p.28](#)[Cybersecurity sovereignty Indicator](#)**Annex III** [p.29](#)[Questionnaire](#)**References** [p.30](#)

Chapter 1

Executive summary

This study provides recommendations how to bridge the digital sovereignty gap in cybersecurity, in the Netherlands, domestically, in the EU and beyond. The study is based on an extensive set of interviews, literature reviews and the expertise of the authors.

This study builds on the technology stack model for digital sovereignty presented in ‘Towards a sovereign digital future – the Netherlands in Europe’.¹ It also makes explicit geopolitical forces and the cybersecurity ecosystem. It identifies priorities for cybersecurity strategic autonomy or cybersecurity digital sovereignty, which is defined as the necessary capabilities, capacities and control (in cybersecurity) in order to be able to decide and act on the own future in economy, society and democracy. Gaps in strategic autonomy in cybersecurity can pose a direct risk for sovereignty. Cybersecurity strategic autonomy is also a condition for digital sovereignty in general.

The actions that are recommended in this study address what the necessary cybersecurity knowledge is to possess and how much in terms of solutions the Netherlands and the EU, possibly in partnership with trusted third countries, must be able to produce. Actions must take into account real-world dynamics such as barriers to act, synergies between actions, time- and path-dependencies.

The main recommendations are:

- Agree on cybersecurity digital sovereignty as a **top political priority** in the Netherlands and EU.
- Adopt the **political objective** of **full cybersecurity sovereignty** (that is, cybersecurity strategic autonomy) in politically-accepted international partnerships, within a 10-year horizon.
- **Join-up policy actions** as cybersecurity sovereignty can only be effectively

deliver through combining policy actions, e.g., investment and public procurement, regulation and innovation.

- Adopt the proposed **prioritized action plan for cybersecurity sovereignty**, with phases according to the severity of cybersecurity risks for sovereignty.
- Implement **focused actions** that exploit strengths in cybersecurity technologies and business or tackle acute sovereignty gaps, e.g., in cloud, 6G, cryptography, AI, and quantum tech.
- Accompany the general and specific actions with ‘**action for better action**’ such as strengthening evidence, deepening synergies, political and operational accountability.

Knowledge institutes can play a significant role in strengthening strategic autonomy in cybersecurity for the benefit of the

Netherlands and its partners in the EU and internationally. Governments, nationally and in the EU, must take **political leadership** in strengthening cybersecurity sovereignty.

This report does not aim to provide a complete overview of the state of play of cybersecurity in relation to digital sovereignty, but rather focuses on the most important issues raised by experts and expert analysis and corresponding action-oriented recommendations.

¹ Claire Stolwijk et al., ‘Towards a Sovereign Digital Future – the Netherlands in Europe’ (TNO, February 2024).

Chapter 2

Analysing cybersecurity sovereignty

2.1 Introduction

the overall rationale to increase digital sovereignty can be extended à fortiori to cybersecurity. Cyber-incidents strike at the heart of sovereignty. A cyber-attack can put at risk the very basic functioning of society and economy when disrupting critical infrastructures such as electricity or telecommunications. Cyber-theft of intellectual property and state secrets, disinformation and dominance by foreign ICT suppliers undermine in the long-run our companies, jobs, democracy and the legitimacy of government. These risks are real today.

Cybersecurity is influenced by the forces of geopolitics, new technologies, and global economics. The EU, let alone the Netherlands (NL), has limited influence on these forces but is not powerless either, that is, the Netherlands and the EU do

have options to increase the 3C's of their strategic autonomy: **capabilities** – what is known –, **capacities** – the resources to act or to produce, and **control** – how much say it has over capabilities and capacities. This report focuses on cybersecurity strategic autonomy or, in the terminology of the overall TNO report,² cybersecurity digital sovereignty or for brevity **cybersecurity sovereignty**.

2.2 Analytic approach

this study is based on an extensive set of interviews, literature review and expertise of the authors. A growing literature addresses digital sovereignty and within this cybersecurity.³ Yet, there is still a paucity of literature that is fully dedicated to cybersecurity sovereignty.⁴ This study aims in that sense to make a contribution.

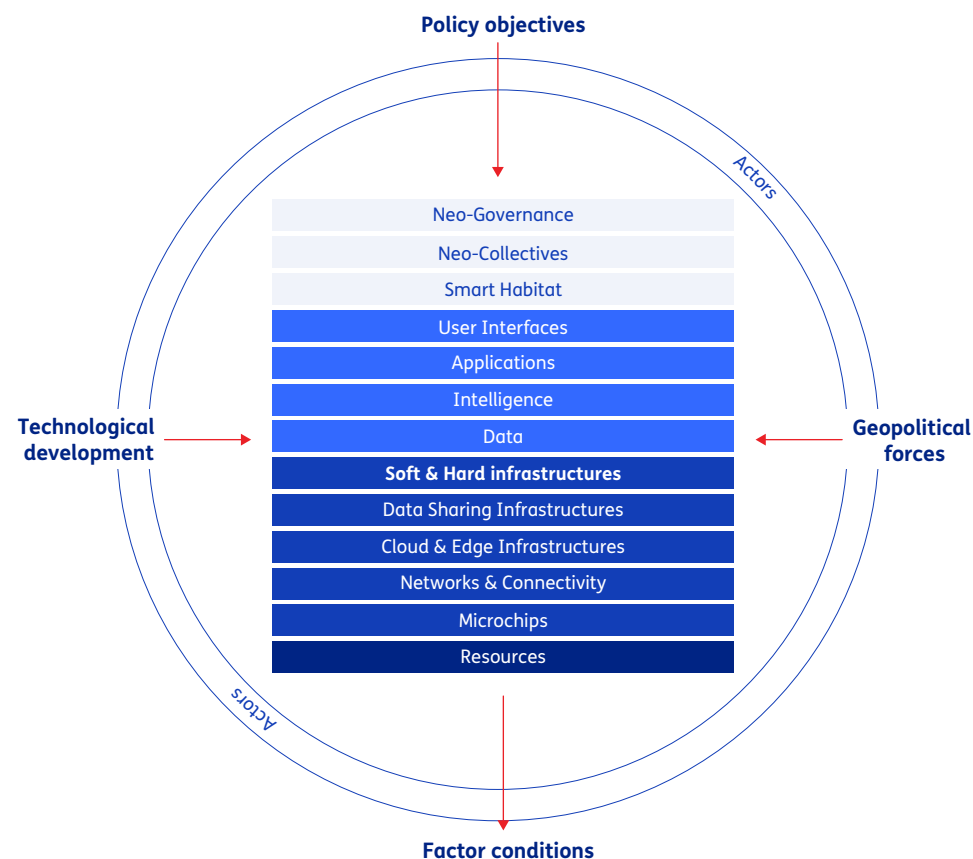


Figure 1 Extended TNO stack model

² Claire Stolk et al.

³ Some recent literature includes Maaike Okano-Heijmans, 'Open Strategic Autonomy: The Digital Dimension', Clingendael, 23 January 2023, <https://www.clingendael.org/publication/open-strategic-autonomy-digital-dimension>. and Gijzen, B.M.M. et al., 'Digitale Infrastructuur en Digitale Open Strategische Autonomie: Methodiek voor identificatie afhankelijkheden, kwetsbaarheden en maatregelen | TNO', 2023, <https://www.tno.nl/nl/zoeken/>. and Juurd Eijssvoegel et al., 'Is Europa gedoemd tot afhankelijkheid?' | NRC Serie, NRC, 2024, <https://www.nrc.nl/serie/is-europa-gedoemd-tot-afhankelijkheid/>.

⁴ Early examples are Paul Timmers and Freddy Dezeure, 'Strategic Autonomy and Cybersecurity in the Netherlands | Cyber Security Council' (Cyber Security Council, 2021), <https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands>; Lakke Moerel and Paul Timmers, 'Reflections on Digital Sovereignty - EU Cyber Direct', Research in Focus, 21 January 2021, <https://eucyberdirect.eu/research/reflections-on-digital-sovereignty>. and (in Dutch) M.A. Veenendaal et al., 'Whitepaper Strategische Autonomie Op Cybersecurity | TNO-HCSS', accessed 1 July 2024, <https://publications.tno.nl/publication/34637841/3Cb4mi/TNO-2020-R11599.pdf>.

We analyse the inputs within an extension of the technology stack model for digital sovereignty.⁵ The extension helps is to focus attention on geopolitical forces, political objectives, and actors of the cybersecurity ecosystem (see Figure 1 and identify factors of concern and actors in the ecosystem. It also draws attention to context-dependencies. Based on further analysis of the dynamics of the interplay between ecosystem and context, it allows to take account of path- and time-dependencies.

In order to arrive within such an overall framing at action-oriented recommendations, we prioritize potential **cybersecurity** areas of concern according to their **risks for sovereignty** in the usual harms-probability model, which is elaborated in the next chapter.

Then, we formulate actions to address the concerns about capabilities, capacities and control (3C) model, or in other words, increasing cybersecurity sovereignty in terms of knowledge and skills, how much can be done, and how much there is of a say. We focus on sets of actions that – collectively - increase all 3C's, while prioritizing actions in three phases as explained in with the help of Figure 2 in the next two chapters. We then provide a framework for action and in finally summarize the main recommendations.

⁵ Claire Stolk et al., 'Towards a Sovereign Digital Future - the Netherlands in Europe'.

Chapter 3

From analysis to action

This chapter analyses the critical importance of cybersecurity for sovereignty, the state of play in cybersecurity strategic autonomy in the Netherlands and Europe, and actions to bridge gaps and overcome barriers to strengthening cybersecurity strategic autonomy.

The sections below conclude with recommendations and related actions, numbered resp. **Rn** and **Am**.

3.1 Cybersecurity sovereignty as a top-priority

weak cybersecurity sovereignty is an important and rising concern.⁶ The Netherlands and EU have a significant dependency on a limited number of foreign ICT providers. For instance, digital infrastructures are increasingly controlled by non-European tech companies. Non-European cloud providers now have 75% of the market up from 65% in 2019. Notably, the market is dominated by

three large USA cloud providers (Amazon AWS, Microsoft Azure, Google Cloud).⁷ The market of secure hardware modules is dominated by providers from the USA and Israel. There are few large Dutch cybersecurity companies (though some technology companies such as NXP have a very large security activity). The cybersecurity market leaders in Europe are all foreign. Promising European cybersecurity companies with their talented staff are bought up by foreign investors with deep pockets. More evidence of the dominant presence of non-European actors in digital technologies and markets is provided in chapter 2 of 'Towards a sovereign digital future – the Netherlands

in Europe'.⁸ The resilience and economic security risks of critical (digital) supply chain dependencies have been pointed out by the European Commission⁹ and by several recent studies.¹⁰

Experts that we interviewed unanimously agree that the Netherlands and the EU must increase its cybersecurity sovereignty. However, suggestions how to increase cybersecurity sovereignty differ among experts as regards priorities, ambition, feasibility and international partners. A number of the experts believe that total cybersecurity sovereignty should be the ultimate aim for the EU (no one claims this as an ambition for the Netherlands on its own). They consider half-way control over cybersecurity as a continued and unacceptable risk for sovereignty, especially for values and democracy that the EU subscribes to. This opinion fits

with a realist perspective on international relations, a view that has gained ground with the war against Ukraine and may get further reinforced in case of a re-election of Trump. Several experts also point to the need to control digital technologies in general given their impact on sovereignty.

Other experts either do not see full cybersecurity sovereignty at EU-level as desirable or feasible given the context. For the 'not-desirable camp' the context is the international world order, adhering to a liberalist perspective on international relations namely that absolute cybersecurity sovereignty is not necessary because external threats can be managed and remaining damages to sovereignty are less than the wider benefits from open trade, free flow of innovation, or global common goods like fighting. For the 'not-feasible camp' the context is contingent in the temporal (historic, present, future) sense. In such a contingency perspective

⁶ Although not discussed here, cybersecurity sovereignty is intertwined with physical security, for instance, to protect mobile stations, ensure electricity supply for data centres or hospital systems, or avoid damage to undersea cables, etc. Combining digital and physical security is increasingly addressed by public policy.

⁷ Rathenau Instituut, 'Digitale Afhankelijkheid Zet Onze Autonomie Onder Druk', April 2024, https://www.rathenau.nl/sites/default/files/2024-04/Bericht_aan_het_parlement_Digitale_afhankelijkheid_en_autonomie_Rathenau_Instituut.pdf.

⁸ Claire Stolk et al., 'Towards a Sovereign Digital Future - the Netherlands in Europe', chap. 2.

⁹ European Commission, 'An EU Approach to Enhance Economic Security', Text, European Commission - European Commission, 20 June 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358.

¹⁰ For instance, Joris Teer, Abe de Ruijter, Michel Rademaker, 'Navigating the Great Game of Chokepoints: Assessing Geopolitical Risks and Advancing Dutch and European Strategic Indispensability in Digital Value Chains', March 2024, <https://hcscs.nl/report/navigating-the-great-game-of-chokepoints/>.

priorities have time and path dependency.¹¹ That is, in some areas cybersecurity sovereignty has irrevocably been lost and in others, especially greenfield, areas much is still possible. In this perspective priorities also depend on historic, current and future geopolitical and technological developments¹² and may have to be adjusted when the context changes (think of China's stance on Taiwan, USA elections, or the rise of generative AI and the related emerging industry structure which appears to show a high concentration of power).

Care has to be taken that these views may be rather NL- or EU-centric. For instance, historic materialism as espoused by China, says – simplified – that geopolitical power originates in production factors, notably new technologies and related technological security. When aspiring geopolitical power these production factors need to fully be brought under control.

Such geopolitical control ambitions are far from the thinking in the Netherlands or the EU.

These two perspectives can be reconciled, however. First, both groups of experts agree that cybersecurity sovereignty is still not a top political priority, a **Chefsache**, even if much has progressed at lower levels in government, amongst business, and in interest organizations. This is remarkable as underestimating cybersecurity sovereignty is the proverbial iceberg that can sink the state. Both perspectives also agree that full cybersecurity sovereignty is the direction to go. They also agree that this cannot be done by the Netherlands on its own but must be realized in politically trusted alliance with other countries. They also agree that cybersecurity sovereignty is both eminently geopolitical and a key factor determining qualities of the industrial-technological ecosystem such as

resilience, reliability and trustworthiness. Where they differ is that the first view says that this alliance comprises the EU and the second view says that this alliance also comprises other trusted, likeminded countries than EU Member States only. That would notably also include the USA though generally there are both significant concerns are expressed about a possible Trump-minded outcome of the 2024

USA elections and the continued rise of dominant USA platforms in cloud, AI and cybersecurity. Both also agree that critical dependencies on not-likeminded countries like China need to be reduced. In other words, both advocate de-risking from China where the first group also extends de-risking to the USA. This leads to the following recommendations and actions:

Recommendations	Actions
R1. Make cybersecurity sovereignty a top-level political concern in the Netherlands ¹³ and EU	A1. Dutch research and technology organisations to stimulate enhanced understanding of cybersecurity sovereignty as a top priority for the new Dutch government in 2024. A2. The Dutch government and partners to promote cybersecurity sovereignty as political top priority to the new European Commission and European Parliament in 2024
R2. Define as objective to achieve full cybersecurity sovereignty in a politically trusted partnership of countries	A3. Make an EU and corresponding Dutch plan to realise full cybersecurity sovereignty with EU and politically-acceptable international partnerships.
R3. Prioritize de-risking with respect to non-likeminded countries, in particular China	A4. Perform an EU cybersecurity chokepoints study as part of the EU economic security strategy. ¹⁴

11 For a broader framing of (digital) sovereignty and international relations see André Barrinha and G. Christou, 'Speaking Sovereignty: The EU in the Cyber Domain', *European Security* 31, no. 3 (3 July 2022): 356–76; Paul Timmers, 'Sovereignty in the Digital Age', in *Introduction to Digital Humanism* (Springer, 2023), 571–92, http://dx.doi.org/10.1007/978-3-031-45304-5_36, to which the EU has sought to elicit a more comprehensive approach underpinned by a move to become more "technologically sovereign". We seek in this article to critically unpack what such claims to technological sovereignty mean for the EU in the cyber domain and what the practical implications are of the EU taking ownership of and performing sovereignty. More specifically, in seeking to conceptually unpack technological sovereignty in its internal and external manifestations, we show how its articulation, legitimisation and operationalisation has implications and consequences for the EU's identity and action in the cyber domain.", "container-title": "European Security", "ISSN": "0966-2839", "issue": "3", "note": "publisher: RoutledgeIn eprint: <https://doi.org/10.1080/09662839.2022.2102895>", "page": "356-376", "source": "Taylor and Francis+NEJM", "title": "Speaking sovereignty: the EU in the cyber domain", "title-short": "Speaking sovereignty", "volume": "31", "author": [{"family": "Barrinha", "given": "André"}, {"family": "Christou", "given": "G."}], "issued": [{"date-parts": [{"2022", "7", "3"}]}, {"id": "10201", "uris": [{"http://zotero.org/users/9234048/items/L6XBM552"}], "itemData": [{"id": "10201", "type": "chapter", "container-title": "Introduction to Digital Humanism", "page": "571-592", "publisher": "Springer", "title": "Sovereignty in the Digital Age", "URL": "http://dx.doi.org/10.1007/978-3-031-45304-5_36", "author": [{"family": "Timmers", "given": "Paul"}], "issued": [{"date-parts": [{"2023", "12", "21"}]}, {"schema": "https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}]}

12 An example of a contingent approach is to now prioritize cyber-protection, recognizing the dominance of the three USA cloud/platform companies (Microsoft, Amazon, Google) and call upon these to now provide high-security-by-default, without dropping the importance of cybersecurity sovereignty, as done by Freddy Dezeure, Lokke Moerel, George Webster, 'Digital Sovereignty Is Impossible Without Big Tech: A Call to Action', *Atlantische Commissie* (blog), 19 December 2023, <https://www.atlcom.nl/artikel-atlantisch-perspectief/digital-sovereignty-is-impossible-without-big-tech-a-call-to-action/>.

13 "Gezien de toename in afhankelijkheden, ook ten opzichte van grote technologiebedrijven, moet het nemen van maatregelen voor het behoud van onze digitale autonomie centraal op het hoogste politieke en ambtelijke niveau worden belegd CSR, 'CSR Urgentieverklaring 2023 - Advies - Cyber Security Raad', Beleidsnota (Ministerie van Justitie en Veiligheid, 7 August 2023), <https://www.cybersecurityraad.nl/documenten/adviezen/2023/08/07/csr-urgentieverklaring-2023>.

14 European Commission, 'An EU Approach to Enhance Economic Security'.

Joining-up for effective policy
Cybersecurity sovereignty is par excellence a geopolitical, industrial/economic, and societal challenge. Consequently, a synergistic set of policies must be pursued. This is surely easier said than done. Despite serious efforts over the past years, the Dutch cybersecurity and strategic autonomy policies of the Ministry of Economic Affairs and of the Ministry of Foreign Affairs are still perceived by most experts as being disjointed. The Netherlands is not alone in this respect. At EU level and in several EU Member States and in the USA¹⁵ the same can be observed.

China appears to be an exception in this respect, apparently integrating its policies. For instance, its Belt-and-Road Initiative (foreign investment) with standardisation (in ITU) and prioritizing Chinese companies, underpinned by the international economic policy of dual circulation that is clearly focused on building domestic strength (i.e., autarkic strategic autonomy).¹⁶

Even within a policy domain such as economic/industrial policies it is not self-evident that all possible instruments reinforce each other, such as R&D support, standardisation, education, public procurement, and defence industrial policy. At EU-level there is some progress in this respect, as demonstrated by the semiconductor industrial policy (EU Chips Act), but much more can and must be achieved in several digital areas including in cybersecurity.¹⁷

The Netherlands has much potential and credibility to pursue synergistic cybersecurity sovereignty policy. A targeted effort must be pursued to realise this potential and fully mobilise the Netherlands as a driver in this respect in the EU.

Recommendations

R4. Cybersecurity sovereignty policy must be a synergistic combination of policies (industrial, defence, trade, foreign,) and policy instruments (regulation, guidance, promotion, investment, ...)

Actions

A5. The Dutch government and socio/economic partners to develop joined-up cybersecurity sovereignty policy based on integrated interdepartmental policymaking with policy synergies preferably anchored to existing forms of cooperation

An **illustration** of integrating policy domains in some cybersecurity areas is given in Table 1. The table lists individual actions in policy domains (such as market regulation or investment funding) but cannot display that these actions are **above all** to be designed and implemented in a joined-up or synergistic way, that is, such that they are reinforcing each other. In the first column some important cybersecurity areas are given, resulting from expert interviews. This is not, however, an exhaustive list. Three such areas are shown here, as examples, but the list can be extended to comprise all relevant cybersecurity sovereignty priorities. On the basis of the examples in the first column, the next chapter will provide a general framework for action to strengthen capacities, capabilities and control, i.e., strategic autonomy.

15 Henry Farrell and Abraham Newman, 'The New Economic Security State', Foreign Affairs, 19 October 2023, <https://www.foreignaffairs.com/united-states/economic-security-state-farrell-newman>. U.S. National Security Adviser Jake Sullivan begged his listeners' indulgence for straying out of his lane by delivering a major address about economics. But his actual argument—that decades of free-market zealotry had weakened the country's national security—was anything but apologetic. "Ignoring economic dependencies that had built up over the decades of liberalization had become really perilous—from energy uncertainty in Europe to supply-chain vulnerabilities in medical equipment, semiconductors, and critical minerals," Sullivan said. "container-title": "Foreign Affairs", "ISSN": "0015-7120", "issue": "6", "language": "en-US", "note": "Volume Title: November/December 2023", "source": "Foreign Affairs", "title": "The New Economic Security State", "URL": "https://www.foreignaffairs.com/united-states/economic-security-state-farrell-newman", "volume": "102", "author": [{"family": "Farrell", "given": "Henry"}, {"family": "Newman", "given": "Abraham"}], "accessed": [{"date-parts": [{"2023", 12, 2}]}], "issued": [{"date-parts": [{"2023", 10, 19}]}], "schema": "https://github.com/citation-style-language/schema/raw/master/csl-citation.json")

16 PRC State Council, 'China's New "dual Circulation" Development Paradigm', 21 March 2021, https://english.www.gov.cn/news/topnews/202103/28/content_WS60604adbc6d0719374afb4a.html.

17 Detailed examples for cloud, digital identity in addition to semiconductors are in Paul Timmers, 'Digital Industrial Policy for Europe | CERRE Report' (CERRE, 12 December 2022), <https://cerre.eu/publications/digital-industrial-policy-for-europe/>. These cases equally take into account geopolitical, industrial ecosystem, and firm-level interests. For an analysis of 5G/6G see Paul Timmers, 'Strategic Autonomy Tech Alliances', FEPS Strategic Autonomy Series, 30 March 2022, https://www.feps-europe.eu/attachments/publications/220331%20final_strategic%20autonomy%20tech%20alliances-3a.pdf.

Table 1 Integrating policy domains (PQC = Post Quantum Cryptography; CRA = (EU) Cyber Resilience Act; CA = (EU) Cyber Act ; FDI = Foreign Direct Investment (inbound); OIS = Outbound Investment Screening; DMA = (EU) Digital Markets Act; EDIW = European Digital Identity and Wallet Act; IAM = Identity and Access Management; EUCS = EU Cloud Certification Scheme; CI = Critical Infrastructure)

Policy Domain / Cybersecurity Area	Public Procurement . Civil . Military	Standards & Certification	Market Regulation	R&D	Capital / Investment	Talent & Skills	Trade In/out-bound	International Cooperation Bilateral, Global
Cryptography	Govt as smart specifier / developer	Open PQC	Certification in CRA/ CA	Quantum R&D as priority	Deep Tech fund ¹⁸	PQC training for SMEs	EU/NL FDI Screening EU/NL OIS ¹⁹	Invest in int'l PQC standards
Cloud as critical infrastructure	Govt as smart buyer	ENISA GAIA-X CISPE	DMA EDIW	Edge, AI, IAM R&D as priority		Public sector training	Inbound: regulaion (cf. EUCS)	Establish data flow adequacy
Threat Intelli-gence	Govt as smart buyer	EU Cyber Shield		Advanced AI research as priority	Deep Tech fund	Talent scouting, favorable work conditions	Inbound: constraints on FDI	Public interest pilots like humani-tarian CI's; GFCE capacity building

3.1.1 A phased approach: setting priorities according to risks

most experts agree that building cybersecurity sovereignty must be done in a phased way, by setting priorities according to risks. Aspiring everything at once is unrealistic. The priorities that are most often named are critical infrastructures (physical and digital critical infrastructures) and the core of government (state secrets, government decision-making, diplomacy, defence). Generally, when queried about prioritization, experts suggest a risk-

based approach. A well-known approach is to define risk as the product of incident probability and incident harm (in this context, harm for sovereignty).

Incident probability and incident harms can be depicted as in Figure 2 in a qualitative way, based on ENISA Threat Landscape and assessments by the experts.²⁰

¹⁸ Deep Tech Fund, see Ministerie van Algemene Zaken, 'Kabinet richt ambitieus start-up en scale-upbeleid op deep tech en marktkapitaal - Nieuwsbericht - Rijksoverheid.nl', nieuwsbericht (Ministerie van Algemene Zaken, 26 May 2023), <https://www.rijksoverheid.nl/actueel/nieuws/2023/05/26/kabinet-richt-ambitieuus-startup-en-scale-upbeleid-op-deep-tech-en-marktkapitaal>.

¹⁹ Outbound=Outbound Investment Screening (OIS), see European Parliament, 'Outbound Investment Screening', 20 August 2023, <https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-outbound-investment-screening>. At EU level this includes the EU FDI Regulation; in The Netherlands the VIFO Act (Wet Veiligheidstoets investeringen, fusies en overnames).

²⁰ ENISA, 'ENISA Threat Landscape 2023', Report/Study, ENISA, 19 October 2023, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

The approach to prioritize according to risk suggests tackling cybersecurity sovereignty in phases, for instance, as suggested in Figure 2:²¹

- Phase 1 is addressing core of government and a limited set of highest-risk critical infrastructures,
- Phase 2 leverages the work of phase 1 for a wider set of critical infrastructures and ultimately, leveraging both phase 1 and phase 2
- Phase 3 addresses other areas where cybersecurity sovereignty is at risk. Determining the classification into phases is not an exact science nor does it need to be, and moreover, needs to have a degree of flexibility as the reality of cyber-threats develops.

Core of government

In the extended stack model even ‘core of government’ runs all the way from the lower stack layers up to applications and user interfaces, classified by Ministries as secret or state secret information. Indeed, the security classification of government and related guidance on information security (cf. Baseline Information security or BIO in the Netherlands)²² appears to be a useful stepping stone to identify priorities, starting from the highest classification. Moreover, comparable security classification is used in EU and

NATO context and therefore may lend itself for a common and standardized approach with certification similar to Common Criteria that has been used for over 30 years (see Table 2). Such certification must be still further developed and aligned with EU legislation such as the Cyber Security Act and the announced national cybersecurity label²³ as well as the scrutiny done by government for its own systems.

Core of government and generally cloud infrastructures comprise a huge range of ICTs. In nearly all of those there is a large foreign dependency. Experts advise to consider in an integrated way the steps related to the development, go-to-market and use of the related ICTs and increase 3Cs in a coherent way in these steps. That is, generally, to strengthen secure development and deployment, be the best in class in security monitoring supported by the best tools such as for monitoring of endpoint security and build a scale-up investment narrative and bring investors together. And, of course, have extremely well-functioning cyber-incident response and cyber exercises.

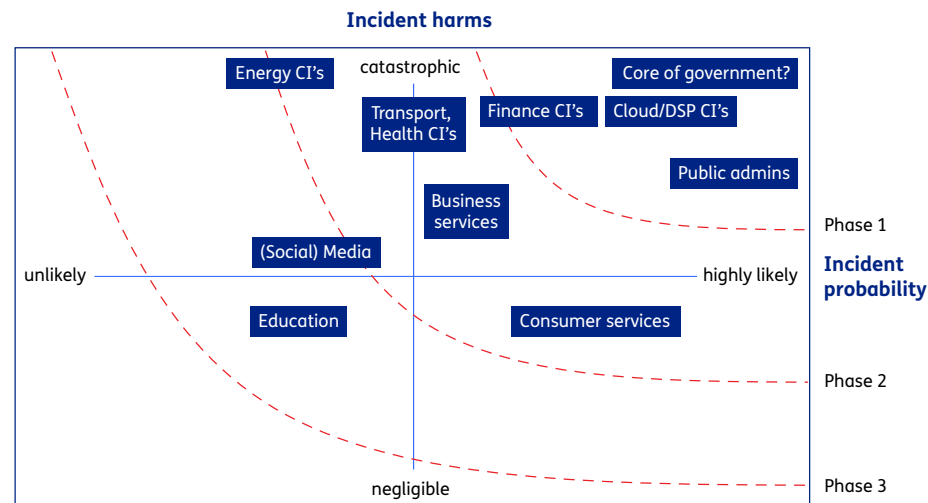


Figure 2 Prioritizing cybersecurity risk impact as harms x risk probability

Table 2 Security classifications

Region	Level 1	Level 2	Level 3	Level 4
EU	EU Top Secret	EU Secret	EU Confidential	EU Restricted
Netherlands	STG. Zeer geheim (STG=staatsgeheim)	STG. Geheim	STG. Confidentieel, Vertrouwelijk	Departementaal vertrouwelijk, Dienstgeheim
NATO	Cosmic Top Secret (CTS)	Focal Top Secret (FTS) NATO Secret (NS) NATO Confidential (NC)	Focal Top Secret (FTS) NATO Secret (NS) NATO Confidential (NC)	NATO Restricted (NR)

²¹ See also Fig 10 in Claire Stolwijk et al., ‘Towards a Sovereign Digital Future - the Netherlands in Europe’.

²² NL Government, ‘Baseline Informatiebeveiliging Overheid - BIO’, accessed 17 December 2023, <https://www.bio-overheid.nl/>.

²³ iBestuur, ‘Kabinet wil cyberkeurmerk voor ICT-leveranciers’, iBestuur, 20 September 2023, <https://ibestuur.nl/artikel/kabinet-wil-cyberkeurmerk-voor-ict-leveranciers/>.

Moreover, for any priority area, many experts stress that there is not a one-size-fits-all action to take. Rather, they raise suggestions for tuned interventions, whether public procurement, R&D, or scale-up investment. A narrative per area, such as cryptography or sovereign cloud, about tuned intervention can avoid

unrealistic ambition. The challenge is to keep multiple narratives coherent. This is in terms of public policy a natural task in the Netherlands for Min-EZK.

The next sections come back to both integrated as well as selective approaches.

Recommendations	Actions
R5. Prioritize cybersecurity sovereignty in a phased approach starting with core of government, cloud/DSP and financial critical infrastructures, and public administrations	A6. Develop a cybersecurity sovereignty plan with ecosystem actors for high assurance crypto A7. Develop a cybersecurity sovereignty plan for cloud/digital identity based on current initiatives (GAIA-X, EUID Digital Wallet) A8. Assess state of cybersecurity sovereignty in financial critical infrastructures and issue guidance if needed A9. Develop smart buyership-based plan for cybersecurity sovereignty in public administrations
R6. Expand from phases with highest priority into others a phased approach to other areas of ICT such as business and consumer systems	A10. Adapt guidance on whole-of-ecosystem cybersecurity sovereignty solutions for highest priority areas
R7. Address cybersecurity sovereignty in a whole-of-ecosystem approach with case-dependent priorities	A11. Increase cybersecurity skills, see Netherlands Cybersecurity Strategy (NLCS) ²⁴

²⁴ 'Nederlandse Cybersecuritystrategie 2022-2028 - Nationaal Cyber Security Centrum', onderwerp (Nationaal Cyber Security Centrum, 10 October 2022), <https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie>.

3.2 Undertaking targeted policy actions

the previous sections gave a general approach to strengthen cybersecurity sovereignty. Within this general approach targeted actions should address some of the most serious sovereignty gaps as identified by experts and our analysis. These actions should also exploit strengths of the Netherlands and the EU. They enable a pro-active forward-looking action to pre-empt the opening up of new sovereignty gaps. These actions are discussed in the next sections.

Targeted policy action to address weaknesses

3.2.1 Cloud, AI, Cybersecurity

There are important differences as regards capabilities-capacities-control in between the many ICT components that go into any of the digital areas of Figure 2. For instance, for the core of government needs encryption, cloud services and AI. On the one hand, the general perception is that the Netherlands has an opportunity given its strength in high-end cryptography,²⁵ although Dutch companies seem to be rather confined to a limited (national) market. On the other hand, as regards cloud services, there is today much reliance on USA cloud providers. Moreover, these are expanding rapidly into key value-added AI services, and have already captured and

tightly integrated cybersecurity services.

Today there are still alternatives (from EU as well as elsewhere) even if these are less known. Experts stated that in such a comparison these alternatives could stand their ground but that the information on costs, functionality and security need to be better made available for fair comparison with the dominant providers. This would be one action to increase cybersecurity sovereignty.

The EU and several Member States push hard for more EU cloud autonomy: ENISA has put forward concrete and security requirements providing greater control; the GAIA-X initiative and CISPE seek to increase choice in cloud and data sovereignty with standards for data infrastructures that allows to combine offers of several providers,²⁶ but has a substantial non-EU membership including of Chinese providers; the EU has expressed the ambition but not yet come forward with an action plan for edge cloud as a paradigm shift that can bypass the dominant providers providing an alternative to centralised cloud; and the EU and Member States have committed to invest into an IPCEI on cloud and edge in

²⁵ dcypher, 'Netherlands Cryptoland', 2023, <https://dcypher.nl/cms/view/a9e8bb3c-8c4f-4869-87f1-f45b9a536850/cryptography>

²⁶ TNO, 'Gaia-X: A European Initiative for Increased Digital Sovereignty', tno.nl/en, 2024, <https://www.tno.nl/en/digital/digital-innovations/data-sharing/gaia-digital-sovereignty/>.

which also the Netherlands takes part.²⁷ This range of initiatives, is however, not yet a fully joined-up, consistent and complete cloud strategy with the aim to increase digital and cybersecurity sovereignty. The EU and the Netherlands can therefore be said, as regards cloud, to be weak in control and capacity but reasonably strong in capability. The current actions in cloud are also not enough. Control continues to erode (market share of big providers continues to grow from 65% in 2019 to over 75% today).

As regards AI, both control and capacities are very weak, even if there is great capability in the EU (and several of the best AI researchers in the USA actually come from the EU). There is little sign that the EU is catching up. In fact, the lack of 3C in AI, today's most important technology development, provides a very worrying telltale of what happens when there is no pro-active approach to digital sovereignty and control is lost. None of the big AI companies is in Europe. Nearly all jobs in AI are created in the USA and China. USA and Chinese investment dwarfs Europe's. 60% of AI technology leaders in the USA are from abroad, of which one-third from Europe. The EU may be a leader in regulating AI – and cybersecurity – and there may be a Brussels effect but 'referees

do not win games'. The EU is losing AI sovereignty while the AI transformation has just started.

Therefore, urgently a much firmer Cloud + AI + Cybersecurity strategy is needed, to start with for the case of core of government. The advantage of this approach is that public procurement restrictions and preferential treatment as well as public procurement of innovation – smart buyership can all legitimately be mobilized²⁸ (which, by the way, is what the USA and China also do).

Investment and scaling-up

Recommended actions have to be consistent within the techno-industrial ecosystem approach of the extended stack model of Figure 1. Creating maximum synergy in that ecosystem means, for instance, to link up relevant demand-side sectors and the supply-side that provides technology. In the case of The Netherlands this would include such as logistics (ports, multimodal transport), semiconductor equipment, and defence.

There is a need to build the case for scale-up investment from Europe. Experts signal that there may be a great cybersecurity capability in the Netherlands and in the EU but that promising companies are often acquired by foreign capital and then

grow in terms of capacity under new and foreign ownership into global markets. Alternatively, they stay small and confined to national markets. The recommended action is to produce investor briefs for selected areas of cybersecurity and meet with private and public investors who are interested to make scale-up capital, e.g., over 50-100 M€, available. They would be motivated both by financial return and by contributing to the common cause of safeguarding sovereignty of the Netherlands and the EU. This action is relevant for selected areas in phase 1, such as high assurance cryptography, with a perspective on Post Quantum Cryptography (PQC), and AI-enabled threat intelligence. This action may also be relevant for phase 2 and 3 such as for scaling up European secure identity and secure wallet providers.

Such risk capital/investment action must be combined with favourable market proscribing and market facilitating actions, such as respectively Internal Market-based cybersecurity certification (as in the EU Cyber Security Act and Cyber Resilience Act) and public procurement.²⁹ The Netherlands can promote specifications for high assurance cryptography and threat intelligence solutions in EU legislation (through implementing Acts) and European

or, better, international standards. It can also develop guidance or rules for public procurement and to share these with likeminded other countries. This set of actions around risk capital is an example of targeted and synergistic policy.

No people, no play

The greatest challenge to cybersecurity sovereignty, signalled by all experts involved in this study, is next to lack of top-level leadership, the very significant lack of skilled people – and this especially for SMEs – and, to some extent, lack of talent. This is rather a capacity than a capability problem: the EU and the Netherlands do have the knowledge but not enough skilled people. Some believe that already today there is a war for talent in the Netherlands which is being won by massive USA capital. This demonstrates an issue of lack of control in the sense of strategic autonomy.

Skills, talent, labour market are Pillar IV of the Netherlands Cyber Security Strategy³⁰ which says "The government is working with educational institutions to roll out upskilling and reskilling programmes to enhance employees' cybersecurity expertise. They are also working alongside the business community and other relevant parties. Any obstacles and

²⁷ European Commission, 'IPCEI Next Generation Cloud Infrastructure and Services', 5 December 2023, https://competition-policy.ec.europa.eu/state-aid/ipcei/approved-ipceis/cloud_en.

²⁸ NATO now also strengthens its involvement in innovation through the DIANA fund (for R&D&I) and the NIF fund (for risk investment).

²⁹ Market intervention actions can be market-creating, market-facilitating, market-modifying, market-proscribing (i.e. regulating), and market-substituting, see Vinod K. Aggarwal and Andrew W. Reddie, 'Comparative Industrial Policy and Cybersecurity - a Framework for Analysis' 3, no. 3 (2 September 2018): 291–305.

³⁰ Ministerie van Justitie en Veiligheid, 'The Netherlands Cybersecurity Strategy 2022-2028 - Publication - National Coordinator for Security and Counterterrorism', publicatie, 6 December 2022, <https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028>.

limitations in that collaboration that stem from legislation will be identified and examined to see how they can be resolved. And “The government is investing in higher professional education in the sciences, which includes cybersecurity. Resources are being allocated to (1) higher intake, (2) lower drop-out and switch rates, (3) higher lateral intake, and (4) induction/ hot transfer to the labour market.” A problem here is that it is hard to see how the Strategy is operationalized, while it mentions hardly any parties explicitly, except for Min-J&V and the Cyber Security Council (CSR).³¹ Experts come with more concrete ideas such as to prioritize cyber security labour in the interest of vital sectors or to scout-in from or outsource to East Europe.

Role of government

Government is widely expected to step up its activities in cybersecurity sovereignty, both in the Netherlands and in the EU. Already measures for market regulation for phase 1 priorities were presented. Government is also best placed to give the urgently needed authoritative guidance on cybersecurity rules and regulations. Earlier it was argued that this can only happen with national and EU-level political leadership.

Moreover, several experts have suggested that current government public procurement policy in particular for cloud services offers already today good possibilities to increase cybersecurity sovereignty, but that this is still little known or understood. If this is the case, guidance could be tremendously helpful.

However, there is more government can do such as funding to financially supporting large scale pilots in public-private cooperation. In the Netherlands this should build on the above-mentioned strengths in certain economic sectors (such as logistics) and in cooperation platforms. The Netherlands can stimulate that this also happens at European level, for instance, by proposing an IPCEI on cybersecurity digital sovereignty, and by its vote on workprogrammes of European investment schemes, from Horizon Europe to Next-Generation Europe. Furthermore, and importantly, government can pre-emptively protect strategic autonomy cybersecurity technologies and knowledge by foreign investment control. In the Netherlands this can be by taking a golden share in critical companies through its recent Deep Tech fund. An equivalent at European level does not yet exist but should be tabled by the Netherlands as an option.

The Netherlands can also be a pioneer by bringing a cybersecurity sovereignty focus in European awareness, skills and talent initiatives, such as ENISA’s Cyber Awareness Month and ERA research excellence. A good example, located in phase 1 and phase 2 (see Figure 2) would be to build a European pool of expertise to cyber-protect offshore internet and energy critical infrastructures, that are threatened in the North Sea but also in the Baltic Sea and in the Mediterranean.

A still underused opportunity is civil-military cooperation on cybersecurity. Protecting sovereignty is the supreme task of the defence arm of government. Several roles in the Netherlands Defence Industrial Strategy have been mentioned (as smart buyer, smart co-developer, smart specifier, etc). These actions fit in phase 1. Can these also have leverage to build capabilities and capacities more widely, outside the military domain, and be more relevant for civil use in phase 1, 2 and 3 areas? The Netherlands and the EU could for instance learn on job mobility schemes from Israel, Finland, the USA and the UK. The reverse should also be pursued, namely job mobility from civil to military, and is possibly even more relevant given that the private sector is often leading in innovation (rather than for instance NATO).

As indicated, actions should ‘live’ in the techno-industrial ecosystem and therefore always involve partners. While hopes are high about the stimulating role of the public sector and in particular of defence, and concrete action is being taken such as the NATO’s defence innovation accelerator (DIANA)³² and €1 billion innovation fund (NIF),³³ the reality in Europe is that such collaboration with defence in the field of fast-developing emerging technologies is fairly recent and still has to prove that it can be fast and result in significant dual use spillovers. The USA (and possibly China

Recommendations

R8. A more forceful skills and talent strategy must be put in place with concrete obligations.

Actions

A12. Adopt ideas such as from employment prioritization measures during COVID crisis
A13. In implementing Pillar IV of the Netherlands Cyber Security Strategy, assign clear responsibilities

³¹ Tweede Kamer memorie van toelichting van 19 sept 2023: “Monitoring en evaluatie van de Nederlandse Cybersecurity Strategie (NLCS) zal ex-durante en ex-post plaatsvinden. Dit betreft een nulmeting door de WODC (in uitvoering), jaarlijkse rapportage aan de Tweede Kamer (#1 is najaar 2023), en een tussenevaluatie van de voortgang van de strategie in 2025.”

³² <https://www.diana.nato.int/>.

³³ <https://www.nif.fund/>.

too) has a significant advantage in the civil-military closeness over many years. For instance, Palantir, an AI/data analytics/cyber company, greatly benefits for its data platform from its support to military data fusion in the war in Ukraine which it then can exploit for its civil use such as for the health data of the UK's National Health Service. A data/cyber/cloud company such as Oracle benefits from its support to the USA military for software and assets tracking which is the basis to support secure ICT supply chain such as with Software Bill of Materials (SBOM).

ICT supply chain security has become a very important topic for both EU and USA and is supported by a combination of economic security and cybersecurity policy. For instance, in the EU this is a priority in the economic security package³⁴ as well as supported by the Cyber Resilience Act³⁵ and the USA and EU collaborate in the trans-Atlantic Trade and Technology Council (TTC) on common SBOM specifications.

Finally, important strengthening can happen in government as a bridge-builder. Civil-military cooperation is one example, but, as mentioned, bridging external and internal policies could be stronger,

ensuring that they align and mutually reinforcing each other, in the Netherlands and in the EU. In fact, this is no longer an option, and not doing so would be irresponsible given that countries such as China and Russia actively undermine the Netherlands and EU sovereignty by aligning their own external (foreign affairs and external security) and internal (i.e. industrial and internal security) policies.

The Netherlands is in an excellent position to show the way, benefiting from strong interest in cybersecurity and strategic autonomy in the Ministry of Foreign Affairs as well as in the Ministries of Economics, Justice and Security, and Home Affairs. Such synergy would strengthen cybersecurity sovereignty actions that need international standards for cybersecurity and cybersecurity in international supply chains (of ICT and others). In phase 1 this is in digital service critical infrastructures such as for Access and Identity Management ('digital ID'), encryption and confidential computing. In phase 2 this is in transport/logistics, health and energy critical infrastructures. This gives a clear focus to this external-internal alignment as there are international forums for all these topics.

Government, as orchestrator of many digital initiatives and related initiatives, is par excellence the bridge builder of the private and public sector with cybersecurity sovereignty initiatives that comprise both. An example is cybersecurity in the energy sector, a 'topsector' in the Netherlands, with a strong activity in cybersecurity (e.g., ENCS). Cybersecurity sovereignty in energy obviously has to be pursued building on,

and driven by, the ongoing initiatives in that topsector. Similarly, this holds at EU level, for energy, but also for other sectors such as the financial sector. The focus on sovereignty in EU legislation and initiatives in these sectors still leaves much to be desired. The Netherlands can champion this agenda at EU-level, as a concrete example of bridging internationally.

Recommendations

R9. Define targeted policy actions to fill sovereignty gaps

Actions

A14. Concrete targeted policy actions indicated by experts are:

- a. build in public-private cooperation the case for scale-up investment in cybersecurity sovereignty in the Netherlands and the EU
- b. legitimize sovereign-by-default in government procurement of cybersecurity and require 'comply-and-explain'
- c. specification and procurement of cybersecurity sovereign innovation in civil-military partnerships
- d. skills and talent mobility support notably towards East European and likeminded countries
- e. join-up economic affairs and foreign policies (NL) and likewise internal and external policies (EU)³⁶

³⁴ European Commission, 'An EU Approach to Enhance Economic Security'; European Commission, 'New Tools to Reinforce the EU's Economic Security - European Commission', 26 January 2024, https://commission.europa.eu/news/new-tools-reinforce-eus-economic-security-2024-01-24_en

³⁵ Council of the European Union, 'Cyber Resilience Act - Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020', 20 December 2023, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_17000_2023_INIT_7_1JJJ&issued={"date-parts":\[\["2023",12,20\]\]}&schema={"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_17000_2023_INIT_7_1JJJ&issued={"date-parts":[[)

³⁶ Even within a policy domain such as economic affairs or foreign affairs the notions of (open) strategic autonomy, digital sovereignty or cybersecurity sovereignty sometimes could be shared more consistently.

3.2.2 Building on strengths

The Netherlands cannot and should not seek to pursue each and every aspects of cybersecurity sovereignty – as argued, cybersecurity sovereignty is to be achieved in trusted partnerships. The Netherlands would do best to build on its strengths such as:

- **Strong academic, innovation, and industrial actors** in areas such as cryptography, semiconductors, 6G, AI, threat intelligence, defence; a strong set of user industries such as logistics & transport, financial, manufacturing;³⁷
- **Strong cooperation platforms** and set of cooperation initiatives including Hague Security Delta, dcypher, Topsectoren/CS4NL, CyberVeiligNederland, DIVD, QuantumDelta, InnovationQuarter, InvestNL, TechLeap, Dutch Data Centers, Online Trust Coalition, ECP.NL, ENCS, De Waag, FERM, and others;
- **Strong policy interest** and commitment by several ministries including EZK, BuZa, BZK, J&V, and related organisations/agencies such as CSR, NCSC, National Coordinator for Security and Counterterrorism (NCTV), Digital

Trust Center, Rijksdienst Digitale Infrastructuur, AIVD, MIVD, and hosting of international cybersecurity initiatives such as GFCE with an articulated set of cybersecurity policies including cybersecurity R&D&I funding.³⁸ The Netherlands has also an extensive agenda for open digital strategic autonomy which includes cybersecurity as one of 10 policy priorities.³⁹

A similar argument to build on strengths can be made for the EU, which has strong capabilities and capacities – though not always control – in areas such as digital networks (mobile, fixed, satellite), edge cloud, IoT, secure hardware (semiconductors), quantum technologies, and increasingly also in supercomputing. The EU has over the past 10 years build up an extensive set of cooperation platforms – often related to legislation – for cyber-protection. Finally, there is no other area in the EU Internal Market where as much has been put in place as regulatory and other initiatives as cybersecurity, which is clear evidence of the strong policy interest.

It could be argued to first focus on a limited number of ICTs where there is such knowledge, industrial, cooperation and policy strengths. such as cryptographic software and hardware. Experts, however, express no common view on this.

As an example, for the Netherlands, this could include high assurance encryption. On the one hand, there is a domestic cryptography industry, so apparently there are few concerns about the 3Cs at national level. However, long-term viability of industry and solutions is an issue as the case of Fox-IT shows, and more generally as argued by the Nederland Cryptoland paper.⁴⁰ Moreover, in the near-future (by 2025) the cryptography industry and users need to deal with PQC amidst rising espionage threats and IP (intellectual property) theft by unfriendly third states which undermines long-term competitiveness.

Assuming that it is not desirable for the current captive market to persist as it is costly and possibly not viable once quantum computing – expected to be very expensive – becomes a reality, a forward-looking cryptography industrial policy motivated by cybersecurity sovereignty

and aiming to at least serve the EU and be suitable to be taken to the European level is needed. Within this policy plan, the public sector as the key client can still be in the role of smart developership.

Another example is open source. The Netherlands and Europe have a long tradition and presence in the open-source community and **open source**, also in cybersecurity, is a policy actively supported by the Dutch government,⁴¹ while the recent EU Cyber Resilience Act takes an encouraging approach to open source.⁴² In addition, the Netherlands is **strong in the EU and has internationally** presence and credibility in cybersecurity policy. If the Netherlands and the EU would choose to promote open source, they would provide one natural pathway to the alignment and bridging of internal and external policies, that was mentioned above.

These are just two examples. While it would take too far to analyse all potentials of strengths and related policy action similar to what we just did for cryptography, interestingly, generally experts urge to anticipate technological changes. They believe that the Netherlands and the EU should have plans to claim new

³⁷ See also Ministerie van Economische Zaken en Klimaat, 'De Economische Kansen van de Cybersecuritysector', 6 April 2023, <https://open.overheid.nl/documenten/ronl-028a9c2f629a0c1558c0dc078e81fbc2f4f0074e/pdf>; Partner Navigator, and Rabobank en Dutch Data Center Association, 'IT & Digitale Infrastructuur in Nederland', Dutch Data Center Association, September 2023, <https://www.dutchdatacenters.nl/publicaties/it-digitale-infrastructuur-in-nederland/>

³⁸ Though such funding, both at EU and at NL level (e.g., a recent NWO Call) could be more strongly linked to strengthening strategic autonomy and the defence of sovereignty, see e.g., 'Call open: 15 miljoen euro voor cybersecurity voor digitale weerbaarheid | NWO', 4 October 2023, <https://www.nwo.nl/nieuws/call-open-15-miljoen-euro-voor-cybersecurity-voor-digitale-weerbaarheid>.

³⁹ Minister van Economische Zaken en Klimaat, 'Kamerbrief over aanbidding Agenda Digitale Open Strategische Autonomie - Kamerstuk - Rijksoverheid.nl', kamerstuk (Ministerie van Algemene Zaken, 17 October 2023), <https://doi.org/10.17/kamerbrief-aanbieden-agenda-digitale-open-strategische-autonomie-coco-5-oktober>.

⁴⁰ dcypher, 'Netherlands Cryptoland'.

⁴¹ Minister A. van Huffelen, 'Kamerbrief Digitale Gemeenschapsgoederen', 7 June 2023, <https://open.overheid.nl/documenten/0871a588-06c0-45e5-883a-89d4b22403a5/file>. See also Nationaal Cyber Security Centrum, 'Factsheet Open Source Security - Factsheet - Nationaal Cyber Security Centrum' (Nationaal Cyber Security Centrum, 24 May 2023), <https://www.ncsc.nl/documenten/factsheets/2022/december/12/factsheet-open-source-security>; Bart Jacobs, 'Open source als strategisch instrument', iBestuur, 21 November 2021, <https://ibestuur.nl/artikel/open-source-als-strategisch-instrument/>.

⁴² 'EU CRA: What Does It Mean for Open Source?', 30 December 2023, <https://berthub.eu/articles/posts/eu-cra-what-does-it-mean-for-open-source/>.

technology ground and thus get ahead in cybersecurity sovereignty-of-the-future. Areas that are mentioned by the experts include post-quantum cryptography, AI for cybersecurity, cybersecurity in 6G combined with dense IoT, and secure edge cloud.

Yet, though the intentions are good, a thorough X-ray **from a sovereignty perspective** of technology developments in the EU and the Netherlands is missing. The risk is – as for AI – that the EU and the Netherlands again set themselves up for loss of digital sovereignty in new technology areas. Yet, they would want to avoid having to embark on another exercise to rescue sovereignty as had to be done for 5G security.⁴³

Recommendations	Actions
R10. Define targeted policy actions to build on national and EU in terms of technological and business (' verdienmodel ') strengths; in particular building on strong actors, cooperation, policy interest of the Netherlands	A15. Develop targeted integrated and synergistic cybersecurity sovereignty plans for each emerging critical ICT such as AI and quantum ⁴⁴ as well as for existing areas of strength such as cryptography, 5G, and others.
R11. Prioritize cybersecurity sovereignty in emerging critical ICTs notably in quantum technologies, AI (notably AI-enabled threat intelligence), 6G/IoT, edge cloud	A16. take as the Netherlands the lead to define an open-source cybersecurity initiative.

⁴³ Unfortunately, signs are not always promising. For instance, a 6G architecture by the authoritative 5G PPP takes a lightweight approach to sovereignty concerns Massod Khorsandi Bahare et al., 'The 6G Architecture Landscape - European Perspective' (Zenodo, 6 February 2023), <https://zenodo.org/record/7313232>. within the 5G Public Private-Partnership (5G PPP)

⁴⁴ For quantum commendable preparatory work is being done e.g., 'White Paper: Mapping the Supply Chains for Quantum Communication', Quantum Delta NL, 15 March 2023, <https://quantumdelta.nl/news/white-paper-mapping-the-supply-chains-for-quantum-communication>.

3.3 Navigating the complex regulatory landscape

A consistent comment of the experts is that the landscape of EU cybersecurity rules and regulations is very complex⁴⁵ even if the laws themselves are not contested.⁴⁶

This will get in the way of concrete action. Unfortunately, the cyber-related laws do not foresee escape clauses or regulatory sandboxes in order to accelerate actions.

Yet, there is a concrete way forward, namely, to provide strong and authoritative guidance for instance in the form of European Commission (EC) Recommendations. This is not a plea for additional regulation but rather that such guidance should help in many instances to navigate the cybersecurity regulatory landscape, that is, help to cut through the maze of rules and regulations and thereby make regulation more understood,

effective and thereby accepted.⁴⁷ The first EC Recommendation could be delivered within one year. Political theory suggests that in a politically and technically complex landscape, such recommendations need political leadership.

One could argue that the market can take care of providing such guidance, but a lesson from the GDPR is that the market does not do so in a timely fashion nor in a way that as a matter of priority benefits European companies.

One could also argue that this is not a core action but rather an enabling or accompanying action (see next chapter). However, signals are that the complexity of the cybersecurity regulatory landscape takes away precious management time and technical resources which is putting at risk attention to sovereignty concerns.

⁴⁵ Some of the most important laws are the Network and Information Security Directive (NIS2) which is currently in transposition. The Cyber Security Act (addressing ENISA and certification, soon to be reviewed) and the Cyber Resilience Act (certified ICT security of products with digital elements and connection to a device or network). For an extensive overview of EU cybersecurity legislation see Christina Rupp, 'Navigating the EU Cybersecurity Policy Ecosystem', 27 June 2024, <https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem>.

⁴⁶ This is not only emerging from the expert interviews but also raised by other experts and organisations in cybersecurity and related fields such as privacy, see e.g., Michiel Steltman, 'Jaarlijkse Rapportage Privacy En Gegevensbescherming', 6 December 2023, and <https://onlinetrustcoalitie.nl/>.

Recommendations

R12. Promote EU-level authoritative and simplifying guidance on cybersecurity legislation

Actions

A17. As the Netherlands, request EC Recommendations for cybersecurity in the EU Single Market (with a workplan based on public consultation) and an expert group reporting to European Commission and NIS Coordination Group.

⁴⁷ This would also fit well with an extensive agenda of reporting simplifications related to EU legislation that the European Commission has embarked upon, see Annex II of European Commission, 'Commission Work Programme 2024 Delivering Today and Preparing for Tomorrow' (202310-17), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A638%3AFIN>.

Chapter 4

Increasing impact of actions

This chapter focuses on how to improve actions, based on insights from the practice of cybersecurity initiatives and actions that have been undertaken so far at national and European level.

Practice shows that at the same time it would not be wise waiting to undertake the most urgent actions. In parallel, the need must be met to have better data and information such as domestic vs foreign purchasing. While acting, it also necessary to continue to improve our understanding of barriers such as regulatory complexity, cybersecurity action dynamics, and the interplay of technological and geopolitical developments with international economy such as the rise of AI or ICT supply chain dependencies. Furthermore, it is imperative to be sensitive to path- and time-dependencies of actions in terms of urgency and prioritization. Although there is no ready-made and comprehensive model, this can still be tackled systemically with accompanying actions based on the recommendations in the diagram below and by applying expert assessment.

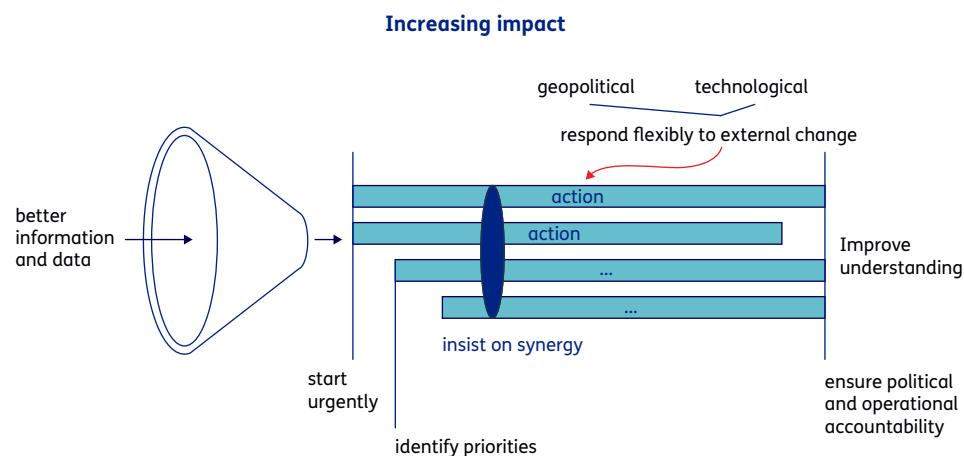


Figure 3 Recommendations for better, more impactful actions

4.1 Improving data, monitoring, and agility

Many experts believe that the Netherlands is in a relatively good position to undertake actions for cybersecurity sovereignty. This view is to some extent underpinned by the Netherlands Cybersecurity Strategy reporting.⁴⁸ However, a profound full analysis, based on product/services, is lacking. This is a risk, even more so as there is virtually no data about the actual current cybersecurity sovereignty position of the Netherlands. The situation is equally troublesome for the EU. The risk is that, under pressure to step up cyber-defences in order to ward off rampant cybercrime, cyber-attacks by Russia and cyber-espionage by China, the EU and the Netherlands trade-off short-term improvement of resilience against long-term and systematic improvement of autonomy.^{49,50}

Towards a market-watch for cybersecurity sovereignty

To improve insight in the state-of-cybersecurity sovereignty in the

Netherlands and in the EU, a cybersecurity sovereignty market-watch should be established to track:

- origin of supply of cybersecurity-related products
- important developments for cybersecurity in emerging technologies and own involvement
- domestic and foreign investment and mergers & acquisitions (M&A) in cybersecurity companies
- state of play of domestic cybersecurity talent and skills
- involvement in cybersecurity-related standards development.

While there is also no systematic tracking of the more general notion of digital dependency, the current situation has been analysed to some extent. This shows that most European countries have a large digital dependency in particular on the USA and to some extent also on China. The analysis also shows that the dependency on the USA has increased over the years, mainly due to the rise of platform companies.⁵¹

There is also a softer variant of digital sovereignty (i.e., softer than the Unilateral Approach scenario of the full TNO report or the autarky and strategic partnership approaches),⁵² namely one that advocates mutual interdependency. This assumes that a strategic equilibrium can be achieved, also with adversaries, if both sides are vitally dependent on each other (by analogy, think of the approach to contain the nuclear arms race though the concept of mutually assured destruction). These days, an example might become the domain of chips between China and the USA, Europe, and its allies. The pawns of mutual interdependency include rare earths from China and top-of-the-range lithographic equipment. However, this might also be a balancing between trade interests in different domains, such as the Chinese car market vs German industrial machinery.

Importantly, however, the assumption that mutual interdependency is feasible and sustainable is not solidly supported by evidence and has been researched to a limited extent only.⁵³ It has also not been developed with respect to cybersecurity. This must be further investigated and verified or falsified.

Action to increase cybersecurity sovereignty should run in parallel to increasing evidence and understanding. Indeed, ahead of a full overview of vulnerabilities that endanger resilience and – potentially – also sovereignty, the Dutch National Cybersecurity Centre (NCSC) has issued guidance to deal with risks in ICT supply chains.⁵⁴ Provided that this guidance gets operationalised (for instance, how to perform solid and comparable assessment of the relevance of digital sovereignty for a specific company?) and remains updated in terms of geopolitical risk assessment, it can play an important role for digital and cybersecurity sovereignty in the Netherlands. The Dutch NCSC is developing in this way a toolset that lends itself to be ‘Europeanised’. The political priority and operational priority recommendations of the present report (R1, R2, R3, R5) will help to strengthen the political and operational framework supporting such NCSC work.

Related is the need to create clarity as regards cybersecurity sovereignty-compatible solutions. For instance, with increased use and complexity of cloud, most cyber-incidents now happen in public cloud solutions. A perceived narrative is

48 Ministerie van Justitie en Veiligheid, ‘The Netherlands Cybersecurity Strategy 2022-2028 - Publication - National Coordinator for Security and Counterterrorism’.

49 A similar problem is occurring in solar panels, where climate policy targets risk increasing (the already huge) dependence on China. The response is a call for diversification and build-up of domestic capacity, see Graham Allison, ‘China’s Dominance of Solar Poses Difficult Choices for the West’, Financial Times, 22 June 2023, sec. Solar power

50 We can take here a leaf from the book by China on increasing autonomy, decoupling and derisking, a policy followed since several years to reduce ‘chokepoints’. An analysis of over 30 cases with a variety of strategies, such as diversification, building domestic capacity, IP copying, is provided by Ben Murphy, ‘Chokepoints - China’s Self-Identified Strategic Technology Import Dependencies’, Center for Security and Emerging Technology (blog), May 2022, <https://cset.georgetown.edu/publication/chokepoints/>

51 Maximilian Mayer and Yen-Chi Liu, ‘Digital Autonomy? Measuring the Global Digital Dependence Structure’, Konrad Adenauer Stiftung (Konrad Adenauer Stiftung KAS, 3 May 2022). See also research into digital dependencies by Bernardus Jansen et al., ‘Pushing Boundaries: An Empirical View on the Digital Sovereignty of Six Governments in the Midst of Geopolitical Tensions’, Government Information Quarterly 40, no. 4 (1 October 2023): 101862, <https://doi.org/10.1016/j.giq.2023.101862>.

52 Timmers, ‘Sovereignty in the Digital Age’.

53 See Henrique Choer Moraes and Mikael Wigell, ‘Balancing Dependence: The Quest for Autonomy and the Rise of Corporate Geoeconomics’, in The Political Economy of Geoeconomics: Europe in a Changing World, ed. Milan Babić, Adam D. Dixon, and Imogen T. Liu, International Political Economy Series (Cham: Springer International Publishing, 2022), 29–55, https://link.springer.com/chapter/10.1007/978-3-031-01968-5_2. These authors define ‘balancing dependence’ (states intervene in order to reduce economic dependencies on foreign actors, i.e. close to the notion of economic security, as well as ‘corporate geoeconomics’, where companies try to preserve autonomy from (such) state intervention.

54 Nationaal Cyber Security Centrum, ‘Omgaan met risico’s in de toeleveringsketen - Publicatie - Nationaal Cyber Security Centrum’, publicatie (Nationaal Cyber Security Centrum, 15 August 2023), <https://www.ncsc.nl/documenten/publicaties/2023/augustus/15/risico's-in-de-toeleveringsketen>.

that only the dominant cloud providers can deliver functionality and performance with the highest levels of security and resilience. Some experts (and competitors) contest this narrative. It is also not known to what extent current purchasing of cybersecurity solutions, driven by urgent needs for more resilience, could be eroding long-term autonomy by increasing foreign dependencies (cf. the growing market share of non-EU cloud providers).⁵⁵ The EU, driven by concerns about the risks of abuse of dominant position, introduced the Digital Markets Act but this law is not addressing cybersecurity.

A reliable and credible narrative about cybersecurity solutions (such as cloud) should come from a combination of impartial assessment and shared insights of users. This should also take into account long-term **non-financial** costs to sovereignty, to enable political decisions, that is, answering the question ‘what is the cost of cybersecurity sovereignty’ in a complete and nuanced way.

Towards an indicator for cybersecurity sovereignty

It is self-evident that cybersecurity sovereignty actions need to be monitored. Not only on deliverables vs milestones but also on their ultimate achievement which is to improve capabilities, capacities, and control. It is therefore useful and important for political and public communication to have a single **cybersecurity sovereignty indicator** and to define milestones on the way to realising more cybersecurity sovereignty (c.f., Recommendation R2). Therefore, an action is to develop such an indicator, which is suggested to be the product of degree of capability, capacity, and control. Annex II gives some suggestions to develop this indicator. Individual actions should come with their cybersecurity sovereignty impact assessment (a proper impact assessment addresses both financial and non-financial impact, both in terms of costs and benefits).⁵⁶ Such impact assessment is also necessary to realistically assess ‘residual risks’ in areas where the desired level of cybersecurity sovereignty may not be achieved (some experts mention cloud and cybersecurity as an example).

⁵⁵ Foreign cloud providers increasingly offer ‘sovereign cloud’. Such offerings are being analysed whether they really provide full sovereignty guarantees. The Dutch NCSC concluded that risks of intrusion by the USA is low (NCSC-NL, “‘Kleine kans’ dat Amerikaanse overheid toegang krijgt tot Europese gegevens op basis van de CLOUD-Act - Expertblogs - Nationaal Cyber Security Centrum”, webpagina (Nationaal Cyber Security Centrum, 23 November 2022), <https://www.ncsc.nl/actueel/weblog/weblog/2022/kleine-kans-dat-amerikaanse-overheid-toegang-krijgt-tot-europese-gegevens-op-basis-van-de-cloud-act>). Others analysts continue to raise concerns on the USA Cloud Act, e.g., Erik van Klinken, ‘Microsoft Cloud for Sovereignty Isn’t All It’s Cracked up to Be’, Techzine Europe, 16 December 2023, <https://www.techzine.eu/blogs/privacy-compliance/114459/microsoft-cloud-for-sovereignty-isnt-all-its-cracked-up-to-be/>.

⁵⁶ This is still rare, though, in the field of digital sovereignty, let alone in cybersecurity sovereignty. A case study on digital sovereignty Common European Data Spaces providing such financial and non-financial impacts, both in terms of costs and benefits, is Carine van Oosteren, Claire Stalwijk, and Fokel Ellen, Daan Pisa, Matthijs Punter, ‘Inzicht in de Kosten En Baten van Digitale Strategische Autonomie’, 2024.

Recommendations	Actions
R13. Address urgent need for more extensive market monitoring and increased visibility of foreign dependencies (that pose a risk in the sense of R3)	A18. Define actions in national and Digital Europe programmes to aggregate and validate cybersecurity market surveys (for dependencies see A4) A19. Develop a cybersecurity indicator and continuously monitor progress in capabilities, capacities and control
R14. Have solid understanding of current and future strategic behaviour in international political-economic relations	A20. Undertake research into the question whether mutual interdependency enhances strategic stability. Similarly for other assumptions on digital dependencies.
R15. Choice of solutions must be based on hard and comparable evidence of current strengths of cybersecurity and long-term risks for sovereignty	A21. Perform a critical assessment of cybersecure solutions, starting with cloud services

Importantly, the recommendation above address both the supply-side and the buy-side in terms of cybersecurity sovereignty. Namely, the cybersecurity sovereignty indicator would assess the supply side in terms of capabilities and capacities that are under own control. The market monitoring assesses the buy-side namely what is being purchased and dependencies with a risk for sovereignty. Where the objective is to increase cybersecurity sovereignty, this objective should obviously also be reflected in the market, that is, cybersecurity-sovereign solutions have an increasing market share.

4.2 Timing and time are of the essence

The technological and geopolitical reality evolves fast, which huge implications for cybersecurity (cf. the rise of AI, the war against Ukraine, USA elections). Better data, understanding, indicator, and monitoring should be combined with pro-active monitoring and adaptive response to deal with geopolitical and technological changes.

The time dimension of actions is not only about resilience versus autonomy, but also about building cybersecurity sovereignty versus the speed of technology development. The emergence of AI, 6G, edge cloud, and quantum technologies and their application for cybersecurity are

a double sword: on the one hand they risk creating ever more dependency on a few ever more powerful suppliers with deep pockets. Today several experts report a worrying wave of foreign (especially USA) takeovers of small companies in these fields where the main objective seems to be to buy talent. On the other hand, there is now a window of opportunity to develop autonomy, as these technologies will become foundational for the near-future cybersecurity. How near is this, how long will the window be open? This must be assessed on a technology-by-technology basis but likely for AI and edge cloud there is no more than a few years, for 6G perhaps 5 years, and for quantum it may be 10 years.

Recommendations

R16. Recognize the critical need for a practice of systematic monitoring and for flexible response to address cybersecurity sovereignty

Actions

A22. Institutionalize at the Netherlands and EU-level pro-active monitoring of and adaptive response to cybersecurity-related geopolitical and technological changes.

4.3 Leading in trust through cooperation

Above it was suggested that a gradual expansion of cybersecurity sovereignty should be pursued, going from areas with the highest expected damages to the less critical areas. This is a rather technocratic and rational perspective. Soft factors must also be taken into account, such as building trust amongst the actors concerned. Such trust may be self-evident for protecting the core of government but is far less evident when, for instance, protecting IP of the manufacturing and knowledge industries. Expanding circles of trust is a social construction process. Probably it is fair to assume that the Netherlands has shown to be good at this (see also the NLCS), but as actions aim at EU scale this should not be taken for granted. Nevertheless, the past has shown that it is not an impossible task either as has been demonstrated for instance in the energy sector or with cooperation under the NIS Directive. Trust mechanisms are a capacity and control over these is part of cybersecurity sovereignty. Likely new trust mechanisms are warranted, for instance, to ensure that quantum solutions for cybersecurity get European scale, **even if they are deployed in the core of another European government.**

It may take a lot of time to get all ducks on a row at EU-level, even if – importantly – joint EU decision-making has significantly

accelerated in cybersecurity during the present European Commission. The Netherlands should therefore explore all mechanisms, including intergovernmental cooperation, as permitted by the Treaties. An intergovernmental funding mechanism compatible with state aid is the Important Project of Common European Interest (IPCEI). In addition, there are further for enhanced cooperation possibilities under the EU Treaties,⁵⁷ next to intergovernmental conventions outside the Treaties (cf. in the past the Prüm Convention).

Recommendations

R17. The Netherlands should champion trust-building and scale-enhancing measures at EU-level and across the EU, also in emerging areas

4.4 Political and operational accountability

Government has many roles in facilitating and accelerating the improvement of cybersecurity sovereignty such as political leadership and providing the policy framework, proposing and implementing coherent, synergistic policy measures from market regulation and industrial policy including funding and talent/skills policy, to trade, export and foreign investment controls and international engagement. Government has a bridge building role, for civil-military cooperation, for public-

Actions

- A23. As part of a quantum industrial policy, proactively propose to the EU-level quantum cybersecurity requirements that combine the free flow of solutions in the internal market with respect for national and EU security
- A24. Explore as the Netherlands an Important Project of Common European Interest (IPCEI) in cybersecurity

private cooperation, and for international cooperation and multilateralism.

Above all, government must ensure political and operational accountability. Currently, cybersecurity may have a high profile in policy agendas at EU and national level but is rarely being accounted for in terms of impact on sovereignty. The actions proposed here must be accompanied by including delivery of cybersecurity sovereignty top political and operational dialogues and regular democratic reporting.

⁵⁷ Title IV, Art. 20 of the Treaty on the European Union and related articles 326-334 of the Treaty on the Functioning of the European Union.

4.5 Framework for action

A framework for cybersecurity sovereignty action should show all relevant policy domains and specific instruments, assess to what extent capabilities-capacities-control get improved, possibly with specific targets. This should be linked to evidence-gathering actions and monitoring and foresee flexibility to react not only to

progress in the plan but also to external events, notably of geopolitical and technological nature.

The approach of risk-harm times risk-probability suggests that the framework for action should run in phases: a first phase 1 focused on the high-risk, high-impact areas of core of government and cloud/digital

service providers critical infrastructures (CI's) as well as public administrations. This will address necessarily facilities such as basic cloud that are also used in other parts of economy and society. Phase 2 builds on phase 1 for areas with lower but still substantial risk and impact of cyber-incidents. This includes other critical infrastructures as well as business and

consumer services. Phase 3 can address remaining and specific cybersecurity sovereignty issues such as in (social) media and education.

The advantage of this approach is that the most urgent and important matters are addressed first and that phases build on each other as generic ICT (such as generic

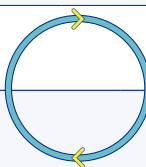
Example actions	Public Procurement . Civil . Military	Standards & Certification	Market Reg'n	R&D	Capital	Talent & Skills	Trade . Inbound . Outbound	International Cooperation . Bilateral . Global	Cybersecurity sovereignty goal In 5 /10 years
Crypto-graphy	Smart specifier, developer, buyer of PQC	Open PQC		Quantum as priority	Deep Tech fund	PQC training for SMEs	EU/NL FDI EU/NL OIS	Invest in international PQC standards	++ 0 / +++
Cloud as critical infrastructure	Smart buyer	ENISA GAIA-X	DMA EDIW	Edge AI IAM		Public sector training	Inbound controls	Establish data flow adequacy	+ 0 0 / +++
AI for threat Intelligence	Private-Public initiative		EU AI Act	Nationaal Groeifonds	NL Deep Tech Fund	AI+cyber +CI in higher educat'n	Inbound controls	AI Safety, UN AI	+ 0 0 / +++
<div> <div>Accompanying actions</div> <div> Evidence Monitoring (supply and buy-side of market) Timing Synergies Accountability </div> </div> 									

Table 3 Action Framework (with example actions and linking to accompanying actions for more impact)

cloud, IoT, AI or telecommunications) is used everywhere. From the inputs to this study there is a wide range of potential actions, can be fitted into this framework. Some actions are tuned to specific cybersecurity solutions, others are less specific, as detailed in the previous chapter. Accompanying actions are also needed in order to get more impact, as identified above.

Figure 4, building on Table 1, gives three examples of applying the framework for action. The ultimate outcome must be increased cybersecurity sovereignty. Supply-side and buy-side should match, that is, the market should work such that what **can be supplied** as sovereign solutions in the EU also **actually gets bought** in the EU. The actions therefore have both supply-side and buy-side policy measures. For instance, in cryptography, sovereign post-quantum crypto solutions are enabled by initiatives such Horizon Europe funding and a deep tech funding while at the same time governments engage in buying these solutions as their role as smart specifier, developer and buyer.

Chapter 5

Conclusions, main recommendations and actions

5.1 Conclusions

Strengthening digital sovereignty with respect to cybersecurity, or cybersecurity sovereignty, is a significant challenge for the Netherlands and the EU, but a challenge that must be addressed as it concerns the very legitimacy and future of economy, society and democracy in the Netherlands and the European Union.

This report, based on expert interviews and our own expert analysis, gives a set of recommendations and concrete actions, admittedly a high level of ambition, to strengthen cybersecurity sovereignty.

Taking up these actions is the responsibility of all actors in the cybersecurity ecosystem. Knowledge institutes and industry can play an important role in stimulating cybersecurity sovereignty and supporting implementation. A specifically strong leadership role must be played by government, at national level in the Netherlands, and as national governments jointly with EU institutions at the European level, in partnership with industry and knowledge institutes, while being open to strategic partnerships with trusted third countries.

5.2 Main recommendations and actions

Most recommended actions can be implemented by presently active actors and organisations. However, change gear of gear is a must, in order to not lose ever more ground as Europe. Therefore, what is often mentioned by experts is the need for **political leadership** to make cybersecurity sovereignty a top priority, to provide for authoritative navigation of cybersecurity regulations, to accelerate collaboration and delivery across the EU and internationally.

Summarizing the main recommendations and associated actions:

1. **Cybersecurity sovereignty (that is, cybersecurity strategic autonomy) must become a top political priority** in the Netherlands and EU. Research and technology organisations in the Netherlands should seek to enhance understanding of cybersecurity sovereignty as a top priority for the new Dutch government in 2024. The government in turn should promote this to the new European Parliament and Commission in 2024–2025. Cyber-

resilience should get strengthened and increasingly be based on cyber-sovereign solutions. Otherwise long-run autonomy gets weakened, home-grown cyber-security industry would get marginalized, talent moves away, knowledge disappears, and foreign dependency would grow ever more.

2. **Realise full cybersecurity sovereignty with EU and politically-accepted international partnerships.** Most interlocutors recommend: within 10 years. Cybersecurity sovereignty cannot be realised by the Netherlands and not even by the EU on their own. Partnering with politically-accepted likeminded countries, with long-term stability, will be necessary and may be even desirable for global stability. This is neither autarky nor protectionism (like in the Unilateral Approach scenario of the full TNO report), but balanced economic and societal self-interest. China is a significant risk, therefore, prioritize de-risking from China where cybersecurity is concerned; by EU with support by the Netherlands (based on recent EU Economic Security policy).

Pursue joined-up, synergistic policy actions as the only road to cybersecurity sovereignty. The Dutch government and her economic/societal partners should develop joined-up policy in existing cooperation and investment platforms and, as trailblazer, demand the EU to do likewise. One cannot legislate oneself into sovereignty. Rather, joining up means being comprehensive, combining regulation with industrial, R&D, standardisation, investment, public procurement, education, trade, and international relations policies, all to build up and strengthening own capacity and capability, under own control.

3. **Make the regulatory landscape for cybersecurity easier to navigate**, in order to not lose time and effort with the risk that long-term autonomy erodes. All experts consulted for this report are worried that the many cybersecurity regulations and initiatives are highly confusing leading to uncertainty, investment fear and huge workload. One action can be to provide European Commission Recommendations for cybersecurity in the EU Single Market based on an expert group reporting

to European Commission and NIS Coordination Group and a workplan based on public consultation. The first Recommendation could be delivered within one year. Also to be explored is a program of AI for the Cybersecurity Single Market.

4. **Prioritize in relation to the severity of cybersecurity risks for sovereignty.**

The cybersecurity ‘risk-space’ is vast. Some risks are more severe and/or likely than others. Not everything can be tackled at once. The first priority is cybersecurity for the most critical risks, in the upper-right corner in Figure 2 (sovereignty for core of government, public administrations, cloud). Doing so cuts across the stack and delivers reusable solutions that can be leveraged to address the lower risk levels (for other critical infrastructures, business services, consumer services). Action plans should build on ongoing initiatives (cf., Kamerbrief on open strategic autonomy). Ministry/EU to lead and cooperate with knowledge institute and industry.

5. **Define targeted policy actions and priority technological areas** to tackle lacuna and build on national/EU strengths in technology and business models (‘**verdienmodel**’) such as in cryptography, threat intelligence, or services. Market regulation is largely in place, but significant gaps persist in risk

capital, talent, demand-supply linkage (including for public procurement), and international industrial engagement.

Fast wins include:

- building a private-public partnership for scale-up investment in cybersecurity sovereignty
- sovereign-by-default government procurement of cybersecurity with ‘comply-and-explain’
- specification/procurement of cybersecurity sovereign innovation in military-civil partnerships
- skills and talent mobility support notably towards East European and likeminded countries
- join-up economic affairs and foreign policies (NL) and internal and external policies (EU).

Open-source cybersecurity is promising, given domestic strengths and international reputation. Priority technology areas for the Netherlands include AI-enabled threat intelligence, cloud, 6G, cryptography, quantum cybersecurity, given national strengths, pressing needs for more autonomy and business opportunity.

In addition, experience of over ten years of cybersecurity initiatives shows that accompanying actions are also needed in order to ensure flexibility, relevance, and impact. These accompanying actions are:

A. **Continuously improve evidence base:** cybersecurity market surveys and impact assessments; further research

on de-risking, economic security, and mutual interdependency.

- B. **Adapt to the evolving reality:** institutionalize pro-active monitoring and adaptive response to deal with geopolitical and technological changes.
- C. **Deepen synergies:** design packages of actions such that they have mutual leverage, given limited resources and in order to respond to the similar strategy of geopolitical competitors.
- D. **Political and operational accountability:** include delivery of cybersecurity sovereignty in dialogues between top political and operational level, commit to regular democratic reporting.
- E. **Improve understanding:** pro-active and planned learning, since cybersecurity sovereignty is vulnerable to unintended consequences, e.g. in resilience vs autonomy, convenience vs security.

Annex I

Interviewed experts

Opinions expressed in this report should not be attributed to any of the interviewees.

Person (*)	Company, role
Eddy Boot	dcypher, Director
Patrick de Graaf	TNO
Hans de Jong	Former NXP, Lead PSIRT, Fellow, Competence Centre Crypto & Security
Timon Domela Nieuwenhuis Nyegaard	Cybersecurity Policy Advisor
Hans Folmer	Dutch Army, Major General
Stijn Grove	Dutch Data Centers, Managing Director
Liesbeth Holterman	Cyberveilig Nederland, Strategic Advisor
Bert Hubert	Expert
Nathalie Jaarsma	Former NL Ambassador at-Large for Security Affairs & Cyber
Bart Jacobs	Professor Security, Privacy & Identity Radboud Universiteit, Nijmegen
Oscar Koeroo	Ministerie van Volksgezondheid, Welzijn, CISO Concern
Bernold Nieuwesteeg	Entrepreneur and founder of Centre for the Law and Economics of Cyber Security at Erasmus University Rotterdam
Anjos Nijk	European Network for Cyber Security (ENCS), Managing Director
Ronald Prins	Hunt & Hackett, Founder
Peter van Burgel	AMS-IX, CEO
Constantijn van Oranje	TechLeap, Special Envoy
Kees Verhoeven	Bureau Digitale Zaken, CEO

(*) In addition, one anonymous expert.

Annex II

Cybersecurity sovereignty Indicator

Here we provide suggestions for developing a cybersecurity sovereignty indicator, without claiming that this is the ultimate answer. Ideally, this is an outcome indicator: how much does strengthening cybersecurity strategic autonomy contribute to improving sovereignty, i.e., reducing harm to sovereignty. The difficulty is, however, that sovereignty cannot be measured, as this notion has no unique definition. Even if a definition could be proposed, it is unlikely that this will be measurable as there are incomparable qualities involved (e.g., foundational, territorial, and institutional sovereignty).⁵⁸

One could also consider measuring inputs, that is anything that is related to cybersecurity and is relevant for sovereignty, i.e. to have control, capabilities, and capacities (3C) in order to avoid putting sovereignty at risk through breaches of confidentiality, integrity, and availability (the C-I-A of cybersecurity). There would still be the difficulty to weigh the degree of risk, that is, the likelihood of a breach times the harm to sovereignty. If, however, this

aspect of identifying harms and weighing is replaced by expert assessment of relevant harms to sovereignty, we can proceed by drawing up a list of cybersecurity inputs and assessing to the extent of 3C for each.

Inputs are about more than hardware and software. They also include people, procedures, rules and regulations. In other words, it is necessary to draw up a Cybersecurity Bill of Resources (CyBOR) and identify for each element on this list the degree of control, capabilities, and capacities (Figure 5). Although this would be a large list and may point to other large lists of inputs to each of these elements in turn, drawing up such a list is a manageable endeavour.

This approach to a cybersecurity sovereignty indicator is complementary to work done by the European Commission's Joint Research Centre on measuring open strategic autonomy.⁵⁹ The proposed approach takes a more general approach to capabilities and capacities, where the JRC approach zooms in on innovation autonomy and economic

autonomy. In addition, and importantly, the proposed approach makes the dimension of 'control' more explicit in both capabilities (cf. in innovation) and in capacities (cf. economic production). This approach is also complementary, as mentioned before, to work on costs/benefits of digital sovereignty actions.⁶⁰ It allows to include in benefits the change in cybersecurity sovereignty indicator.

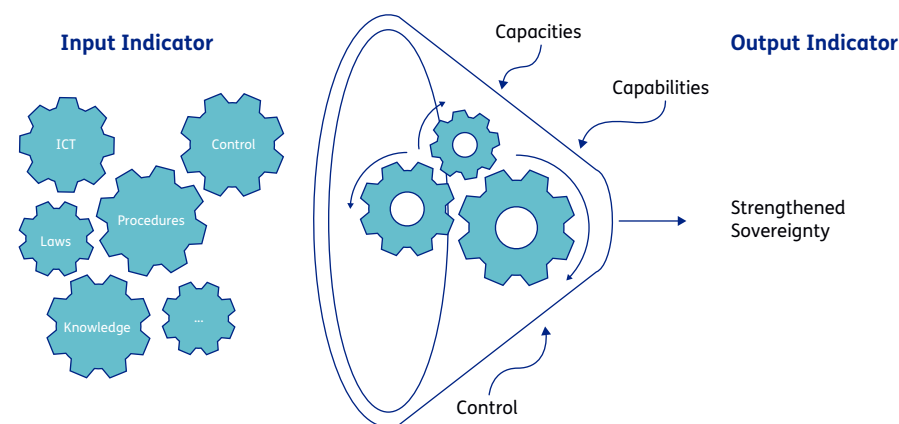


Figure 4 Towards a cybersecurity digital sovereignty indicator.

⁵⁸ Christopher Bickerton et al., 'Conflicts of Sovereignty in Contemporary Europe: A Framework of Analysis', *Comparative European Politics* 20, no. 3 (1 June 2022): 257–74.

⁵⁹ Henning Kroll, 'Assessing Open Strategic Autonomy | JRC', JRC Publications Repository, 4 January 2024, <https://doi.org/10.2760/767279>

⁶⁰ Gijzen, B.M.M. et al., 'Digitale Infrastructuur en Digitale Open Strategische Autonomie: Methodiek voor identificatie afhankelijkheden, kwetsbaarheden en maatregelen | TNO'.

Annex III

Questionnaire

Questions

1. General comments/observations
 2. Should NL have more strategic autonomy in cybersecurity? What about the EU?
 3. Most important areas for strategic autonomy in cybersecurity for NL: e.g., core of govt such as defence & diplomacy, critical infrastructures, intellection property (which?), data (which)..? (considering risk x damage)
 4. Extent of dependency, now, dependent on whom
 5. What is acceptable level of dependency, now, in future?
 6. Feasibility of strategic autonomy in cybersecurity, now, in 5 years, in 10 years
 7. Where can we be in the balance of resilience vs autonomy, now, in 5 years, in 10 years
 8. Which cybersecurity technologies / solutions
 9. Recommendations for action?
 10. What to do as NL within EU?
 11. What to do as NL, internationally?
- Your area of expertise / background
 - Who has market data on companies, markets, products/services (in NL)?
 - Who else to interview?
 - What did we forget or needs special attention?

References

Aggarwal, Vinod K., and Andrew W. Reddie. 'Comparative Industrial Policy and Cybersecurity - a Framework for Analysis' 3, no. 3 (2 September 2018): 291–305.

Allison, Graham. 'China's Dominance of Solar Poses Difficult Choices for the West'. **Financial Times**, 22 June 2023, sec. Solar power.

Bahare, Massod Khorsandi, Anastasius Gavras, Marco Gramaglia, John Cosmas, Xi Li, Ömer Bulakci, Arifur Rahman, et al. 'The 6G Architecture Landscape - European Perspective'. Zenodo, 6 February 2023. <https://zenodo.org/record/7313232>.

Barrinha, André, and G. Christou. 'Speaking Sovereignty: The EU in the Cyber Domain'. **European Security** 31, no. 3 (3 July 2022): 356–76.

Bart Jacobs. 'Open source als strategisch instrument'. iBestuur, 21 November 2021. <https://ibestuur.nl/artikel/open-source-als-strategisch-instrument/>.

Bickerton, Christopher, Nathalie Brack, Ramona Coman, and Amandine Crespy. 'Conflicts of Sovereignty in Contemporary Europe: A Framework of Analysis'. **Comparative European Politics** 20, no. 3 (1 June 2022): 257–74.

Carine van Oosteren, Claire Stolwijk, and Fokel Ellen, Daan Pisa, Matthijs Punter. 'Inzicht in de Kosten En Baten van Digitale Strategische Autonomie', 2024.

Choer Moraes, Henrique, and Mikael Wigell. 'Balancing Dependence: The Quest for Autonomy and the Rise of Corporate Geoeconomics'. In **The Political Economy of Geoeconomics: Europe in a Changing World**, edited by Milan Babić, Adam D. Dixon, and Imogen T. Liu, 29–55. International Political Economy Series. Cham: Springer International Publishing, 2022. https://link.springer.com/chapter/10.1007/978-3-031-01968-5_2.

Christina Rupp. 'Navigating the EU Cybersecurity Policy Ecosystem', 27 June 2024. <https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem>.

Claire Stolwijk, Matthijs Punter, Paul Timmers, Julian Rabbie, and David Regeczi. 'Towards a Sovereign Digital Future - the Netherlands in Europe'. TNO, February 2024.

Council of the European Union. 'Cyber Resilience Act - Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020', 20 December 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_17000_2023_INIT.

CSR. 'CSR Urgentieverklaring 2023 - Advies - Cyber Security Raad'. Beleidsnota. Ministerie van Justitie en Veiligheid, 7 August 2023. <https://www.cybersecurityraad.nl/documenten/adviezen/2023/08/07/csr-urgentieverklaring-2023>.

dcypher. 'Netherlands Cryptoland', 2023. <https://dcypher.nl/cms/view/a9e8bb3c-8c4f-4869-87f1-f45b9a536850/cryptography>.

ENISA. 'ENISA Threat Landscape 2023'. Report/Study. ENISA, 19 October 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

Erik van Klinken. 'Microsoft Cloud for Sovereignty Isn't All It's Cracked up to Be'. Techzine Europe, 16 December 2023. <https://www.techzine.eu/blogs/privacy-compliance/114459/microsoft-cloud-for-sovereignty-isnt-all-its-cracked-up-to-be/>.

'EU CRA: What Does It Mean for Open Source?', 30 December 2023. <https://berthub.eu/articles/posts/eu-cra-what-does-it-mean-for-open-source/>.

European Commission. 'An EU Approach to Enhance Economic Security'. Text. European Commission - European Commission, 20 June 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358.

- Commission work programme 2024 Delivering today and preparing for tomorrow (202310-17). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A638%3AFIN>.
- 'IPCEI Next Generation Cloud Infrastructure and Services', 5 December 2023. https://competition-policy.ec.europa.eu/state-aid/ipcei/approved-ipceis/cloud_en.
- 'New Tools to Reinforce the EU's Economic Security - European Commission', 26 January 2024. https://commission.europa.eu/news/new-tools-reinforce-eus-economic-security-2024-01-24_en.

European Parliament. 'Outbound Investment Screening', 20 August 2023. <https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-outbound-investment-screening>.

Farrell, Henry, and Abraham Newman. 'The New Economic Security State'. **Foreign Affairs**, 19 October 2023. <https://www.foreignaffairs.com/united-states/economic-security-state-farrell-newman>.

Freddy Dezeure, Lokke Moerel, George Webster. 'Digital Sovereignty Is Impossible Without Big Tech: A Call to Action'. **Atlantische Commissie** (blog), 19 December 2023. <https://www.atlcom.nl/artikel-atlantisch-perspectief/digital-sovereignty-is-impossible-without-big-tech-a-call-to-action/>.

Gijsen, B.M.M., Nooren, P., Sambeek, M. van, Stokking, H., and Vries, A. de. 'Digitale Infrastructuur en Digitale Open Strategische Autonomie : Methodiek voor identificatie afhankelijkheden, kwetsbaarheden en maatregelen | TNO', 2023. <https://www.tno.nl/nl/zoeken/>.

iBestuur. 'Kabinet wil cyberkeurmerk voor ICT-leveranciers'. iBestuur, 20 September 2023. <https://ibestuur.nl/artikel/kabinet-wil-cyberkeurmerk-voor-ict-leveranciers/>.

Jansen, Bernardus, Natalia Kadenko, Dennis Broeders, Michel van Eeten, Kevin Borgolte, and Tobias Fiebig. 'Pushing Boundaries: An Empirical View on the Digital Sovereignty of Six Governments in the Midst of Geopolitical Tensions'. **Government Information Quarterly** 40, no. 4 (1 October 2023): 101862. <https://doi.org/10.1016/j.giq.2023.101862>.

Joris Teer, Abe de Ruijter, Michel Rademaker. 'Navigating the Great Game of Chokepoints: Assessing Geopolitical Risks and Advancing Dutch and European Strategic Indispensability in Digital Value Chains', March 2024. <https://hcss.nl/report/navigating-the-great-game-of-chokepoints/>.

Juurd Eijssvoogel, Clara van de Wiel, Jan Benjamin, Floor Bouma, Marc Hijink, and Milo van Bokkum. 'Is Europa gedoemd tot afhankelijkheid? | NRC Serie'. NRC, 2024. <https://www.nrc.nl/serie/is-europa-gedoemd-tot-afhankelijkheid/>.

Kroll, Henning. 'Assessing Open Strategic Autonomy | JRC'. JRC Publications Repository, 4 January 2024. <https://doi.org/10.2760/767279>.

M.A. Veenendaal, T.C.C. van Schie, M. Rademaker, and L. Faesen. 'Whitepaper Strategische Autonomie Op Cybersecurity | TNO-HCSS'. Accessed 1 July 2024. <https://publications.tno.nl/publication/34637841/3Cb4mi/TNO-2020-R11599.pdf>.

Maaïke Okano-Heijmans. 'Open Strategic Autonomy: The Digital Dimension'. Clingendael, 23 January 2023. <https://www.clingendael.org/publication/open-strategic-autonomy-digital-dimension>.

Mayer, Maximilian, and Yen-Chi Liu. 'Digital Autonomy? Measuring the Global Digital Dependence Structure, Konrad Adenauer Stiftung'. Konrad Adenauer Stiftung KAS, 3 May 2022.

Minister A. van Huffelen. 'Kamerbrief Digitale Gemeenschapsgoederen', 7 June 2023. <https://open.overheid.nl/documenten/0871a588-06c0-45e5-883a-89d4b22403a5/file>.

Minister van Economische Zaken en Klimaat. 'Kamerbrief over aanbidding Agenda Digitale Open Strategische Autonomie - Kamerstuk - Rijksoverheid.nl'. Kamerstuk. Ministerie van Algemene Zaken, 17 October 2023. <https://doi.org/10.17/kamerbrief-aanbieden-agenda-digitale-open-strategische-autonomie-coco-5-oktober>.

Ministerie van Algemene Zaken. ‘Kabinet richt ambitieus start-up en scale-upbeleid op deep tech en marktkapitaal - Nieuwsbericht - Rijksoverheid.nl’. Nieuwsbericht. Ministerie van Algemene Zaken, 26 May 2023. <https://www.rijksoverheid.nl/actueel/nieuws/2023/05/26/kabinet-richt-ambitieuw-startup-en-scale-upbeleid-op-deep-tech-en-marktkapitaal>.

Ministerie van Economische Zaken en Klimaat. ‘De Economische Kansen van de Cybersecuritysector’, 6 April 2023. <https://open.overheid.nl/documenten/ronl-028a9c2f629a0c1558c0dc078e81f8e2f4f0074e/pdf>.

Ministerie van Justitie en Veiligheid. ‘The Netherlands Cybersecurity Strategy 2022-2028 - Publication - National Coordinator for Security and Counterterrorism’. Publicatie, 6 December 2022. <https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028>.

Moerel, Lokke, and Paul Timmers. ‘Reflections on Digital Sovereignty - EU Cyber Direct’. **Research in Focus**, 21 January 2021. <https://eucyberdirect.eu/research/reflections-on-digital-sovereignty>.

Murphy, Ben. ‘Chokepoints - China’s Self-Identified Strategic Technology Import Dependencies’. **Center for Security and Emerging Technology** (blog), May 2022. <https://cset.georgetown.edu/publication/chokepoints/>.

Nationaal Cyber Security Centrum. ‘Factsheet Open Source Security - Factsheet - Nationaal Cyber Security Centrum’. Nationaal Cyber Security Centrum, 24 May 2023. <https://www.ncsc.nl/documenten/factsheets/2022/december/12/factsheet-open-source-security>.

- ‘Omgaan met risico’s in de toeleveringsketen - Publicatie - Nationaal Cyber Security Centrum’. Publicatie. Nationaal Cyber Security Centrum, 15 August 2023. <https://www.ncsc.nl/documenten/publicaties/2023/augustus/15/risico's-in-de-toeleveringsketen>.

NCSC-NL. “‘Kleine kans’ dat Amerikaanse overheid toegang krijgt tot Europese gegevens op basis van de CLOUD-Act - Expertblogs - Nationaal Cyber Security Centrum’. Webpagina. Nationaal Cyber Security Centrum, 23 November 2022. <https://www.ncsc.nl/actueel/weblog/weblog/2022/kleine-kans-dat-amerikaanse-overheid-toegang-krijgt-tot-europese-gegevens-op-basis-van-de-cloud-act>.

‘Nederlandse Cybersecuritystrategie 2022-2028 - Nationaal Cyber Security Centrum’. Onderwerp. Nationaal Cyber Security Centrum, 10 October 2022. <https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie>.

NL Government. ‘Baseline Informatiebeveiliging Overheid - BIO’. Accessed 17 December 2023. <https://www.bio-overheid.nl/>.

NWO. ‘Call open: 15 miljoen euro voor cybersecurity voor digitale weerbaarheid | NWO’, 4 October 2023. <https://www.nwo.nl/nieuws/call-open-15-miljoen-euro-voor-cybersecurity-voor-digitale-weerbaarheid>.

Partner Navigator, and Rabobank en Dutch Data Center Association. ‘IT & Digitale Infrastructuur in Nederland’. Dutch Data Center Association, September 2023. <https://www.dutchdatacenters.nl/publicaties/it-digitale-infrastructuur-in-nederland/>.

PRC State Council. ‘China’s New “dual Circulation” Development Paradigm’, 21 March 2021. https://english.www.gov.cn/news/topnews/202103/28/content_WS60604adbc6d0719374afba4a.html.

Quantum Delta NL. ‘White Paper: Mapping the Supply Chains for Quantum Communication’, 15 March 2023. <https://quantumdelta.nl/news/white-paper-mapping-the-supply-chains-for-quantum-communication>.

Rathenau Instituut. ‘Digitale Afhankelijkheid Zet Onze Autonomie Onder Druk’, April 2024. https://www.rathenau.nl/sites/default/files/2024-04/Bericht_aan_het_parlement_Digitale_afhankelijkheid_en_autonomie_Rathenau_Instituut.pdf.

Steltman, Michiel. ‘Jaarlijkse Rapportage Privacy En Gegevensbescherming’, 6 December 2023. https://www.linkedin.com/posts/michielsteltman_de-autoriteit-persoonsgegevens-adviseert-activity-7138101518892716032-lmWA/?utm_source=share&utm_medium=member_ios.

Timmers, Paul. 'Digital Industrial Policy for Europe | CERRE Report'. CERRE, 12 December 2022. <https://cerre.eu/publications/digital-industrial-policy-for-europe/>.

- 'Sovereignty in the Digital Age'. In **Introduction to Digital Humanism**, 571–92. Springer, 2023. http://dx.doi.org/10.1007/978-3-031-45304-5_36.
- 'Strategic Autonomy Tech Alliances'. FEPS **Strategic Autonomy Series**, 30 March 2022. https://www.feps-europe.eu/attachments/publications/220331%20final_strategic%20autonomy%20tech%20alliances-3a.pdf.

Timmers, Paul, and Freddy Dezeure. 'Strategic Autonomy and Cybersecurity in the Netherlands | Cyber Security Council'. Cyber Security Council, 2021. <https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands>.

TNO. 'Gaia-X: A European Initiative for Increased Digital Sovereignty'. tno.nl/en, 2024. <https://www.tno.nl/en/digital/digital-innovations/data-sharing/gaia-digital-sovereignty/>.

Authors

Paul Timmers, Matthijs Punter,
Claire Stolwijk



Contact

Matthijs Punter

Senior Researcher
Data Ecosystems TNO ISP

✉ matthijs.punter@tno.nl

☎ +31 6 2246 0065

TNO is an independent public research organisation. With over 4,000 specialists, we work together with entrepreneurs, scientists, policymakers, individuals, and society as a whole to create a safe, healthy, sustainable, and digitally connected society. Technological innovation can bring health and happiness to people and the planet. That is what drives us every day.