CSR Recommendation ‘Digital Autonomy and Cybersecurity in the Netherlands'

How do we reduce our digital dependencies while maintaining an open economy?

CSR

Cyber Security Council

Cyber Security Raad

CSR Recommendation Digital Autonomy and Cybersecurity in the Netherlands

How do we reduce our digital dependencies while maintaining an open economy?

CSR
Cyber Cyber
Security Security
Council Raad

May 6, 2021

CSR Recommendation 2021, No 3

Excellencies,

You hereby receive the Recommendation ‘Digital Autonomy and Cybersecurity in the Netherlands’ from the Cyber Security Council (hereinafter: the Council).

Introduction

Digital autonomy is at the heart of our rule of law and thus the foundation of our society. Digital autonomy is a complex and urgent issue which is an important part of an integrated approach to cyber resilience, including the necessary investments in line with the Council's previous Recommendation on this matter.[1] The present recommendation specifically addresses digital autonomy in relation to cybersecurity. This is necessary in view of the huge urgency of the subject and the need to draw attention to it at the appropriate levels.

The ultimate challenge is: *how can we as the Netherlands retain control over our democracy, the rule of law and our economic innovation system in the digital world.* Our ability to take decisions autonomously is under pressure from three angles:

- ***Cyber threats continue to increase***, with smaller countries and non-state actors also entering the global arena.[2] These concern direct threats to our vital infrastructure (sabotage), systematic theft by state actors of intellectual property from our knowledge-intensive businesses (*economic espionage*), digital extortion (*ransomware*) and targeted misinformation and systematic infiltration of social media to influence, for example, our elections and democratic processes.
- ***The geopolitical tensions between the US and China are increasing,*** with digital technologies now the battleground for the competition for global leadership (also called: the *tech cold war*).[3] The main focus of the battle is on 5G/6G leadership, quantum computers, computer chip technology and *artificial intelligence (AI).* Both the US and China regularly draw the *sovereignty card* in this context. For example, the US’s ban on Huawei as a supplier of US telecommunications infrastructure. In addition, Huawei is now also restricted in its ability to purchase computer chips produced with US technology outside the US. Not surprisingly, China is retaliating with export restrictions on technology.[4]
- ***As a society, we are becoming increasingly dependent on digital infrastructures that are in the hands of a limited number of dominant foreign market players.*** The data of virtually all European companies and citizens now reside in the cloud of US technology companies in particular, and are therefore not available for European innovation. [5] Social media platforms are increasingly defining the rules of the game of our democracy, due to their lack of measures to combat misinformation, *fake news* and political influence on their platforms.[6] The strong dependence on non-European companies also entails control by other countries, which have different rules when it comes to espionage, privacy and the release of data.

[1] CSR Opinion ‘Integral approach to cyber resilience’, CSR Opinion 2021, No. 2

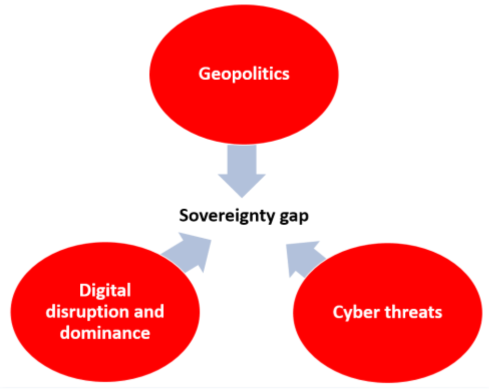
[2] Sanger, D.A. (2018), *The perfect weapon. War sabotage and fear in the cyber age*, New York; Crown. Corien Prins also points out that the new digital weapon changes the (geopolitical) order: "The balance of power is shifting as smaller countries can also enter the global arena. Without having to engage in a large-scale military confrontation or actually enter the territory of another State. In short, it is relatively easy to develop a great deal of strength’, https://www.njb.nl/blogs/consequenties-van-een-nieuw-type-oorlogsvoering/

[3] https://usinnovation.org/news/whos-winning-tech-cold-war-china-vs-us-scoreCouncil

[4] For a summary article, see: https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html

[5] Digital Services Act package, Inception Impact Assessment, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital services

[6] European Commission, ‘Tackling online disinformation’, https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation



Europe, too, feels the threat of what is sometimes called the *techcolonialism* of the US and China. Where in 2017 it was *not done* to mention European sovereignty and Europe was in favor of the open liberal market economy and, for example, European research programmes had to be *open to the world*[7], the restoration of the EU's *technological sovereignty* (in addition to the recovery from the corona crisis and the fight against climate change) has now become the core ambition of the European Commission and the European Council for the next five years.[8] Digital sovereignty has become *Chefsache* at European level and in several Member States. At the beginning of March 2021, 11 EU countries called in public letters to the European Commission for an even stronger commitment to measures to strengthen European digital sovereignty [9] In the Netherlands, however, it is not yet sufficiently present on the political agenda and considerations of digital autonomy are not systematically taken into account in the drafting of policies and legislation. The Council observes that cybersecurity has so far mainly been addressed in a technical and reactive manner, and hardly from the broader perspective of strategic autonomy. As a result, we usually lag behind events and we have to respond to incidents in crisis mode. However, challenges and threats to strategic autonomy in cybersecurity are too important not to be considered from a broad perspective.

The Council has commissioned researchers Freddy Dezeure and Paul Timmers to conduct a study[10] into 'Strategic Autonomy and Cybersecurity in the Netherlands' (hereinafter: *the study*). This study provides an in-depth analysis of the whole spectrum of threats to our control of strategic cyber-security knowledge, technologies, innovations and skills and their impact on our strategic autonomy. The Recommendation of the Council is be based on the results of this study. *The Council recommends that those in positions of responsibility and interested parties read the recommendation and the report.*

In view of the urgency and importance of the subject, the Council will actively promote a broad dissemination of this recommendation and the study and will also organize a number of workshops. In addition, the Council, in cooperation with the researchers, will provide a practical assessment framework to develop proactive, coherent and integral policy in order to strengthen digital autonomy.

The Council believes that action must and can be taken now to ensure strategic autonomy with regard to cyber security.

[7] 'Horizon 2020 is open to the world', https://ec.europa.eu/programmes/horizon2020/en/area/international-cooperation.

[8] See also Ursula Von der Leyen's inaugural speech as President of the Commission: "We must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies, https://ec.europa.eu/info/sites/info/files/president-elect-speech-original_en.pdf

[9] 'Digital sovereignty letter European Commission from Germany, Denmark, Estonia and Finland', d.d. March 1, 2021, https://www.valitsus.ee/en/news/heads-government-germany-denmark-estonia-and-finland-europes-digital-sovereignty-gives-us and 'Letter on digital sovereignty by 8 EU countries', d.o.b. March 8, 2021, https://edri.org/wp- content/uploads/2021/03/POLITICO_Letter-on-digital-sovereignty-by-8-EU-countries.pdf

[10] Dutch strategic autonomy and cybersecurity, Paul Timmers and Freddy Dezeure, January 2021, https://www.cybersecurityraad.nl/documenten/rapporten/2021/02/18/onderzoeksrapport-digitale-autonomie

Sovereignty is generally associated with territoriality, jurisdiction, a population, authority with internal recognition (*internal legitimacy*) and external recognition (*external legitimacy*). ***Strategic autonomy*** is a *means* of gaining and maintaining sovereignty and consists of the capabilities and capacities to take and implement decisions on key aspects of the long-term future in the economy, society and democracy. ***Digital autonomy*** is strategic autonomy in the digital domain.

What is digital autonomy?

Digital autonomy is not limited to our state's control over the use and deployment of critical digital systems and the data generated and stored by them. It should also be translated into the broader public interest of **economy** (control over essential economic ecosystems), **society** and **democracy** (trust in the legal system and quality of democratic decision-making).[11] An important dimension of digital autonomy is the cybersecurity of our critical sectors, processes, and data. The ever-increasing cyber threats are undermining our digital autonomy. These concern the whole spectrum of a direct threat to our vital infrastructure, systematic theft of intellectual property of our knowledge-intensive companies that are global leaders, digital extortion, targeted misinformation and systematic infiltration of social media to influence elections and democratic processes. [12]

If our government and critical sectors do not have control over important processes and data, this will primarily affect the *internal legitimacy* of the state. Cyber threats can also put pressure on the *external legitimacy* of the Netherlands. For example, it appears that the Dutch digital infrastructure is regularly abused by state actors in cyber attacks against other countries.[13] The Netherlands is attractive for this because the digital infrastructure is of high quality and digital capacity can be leased relatively easily. This form of abuse can damage the international image of the Netherlands and be detrimental to interests with its allies. It thus undermines our external legitimacy in international relations.[14]

Digital sovereignty cannot be separated from the three basic principles of information security: *confidentiality, integrity and availability*.[15] In these three areas autonomy should be guaranteed, not only at the level of a *specific system* in a given sector (such as an ICT system in the criminal justice chain), but also in the wider context of the economy, society and democracy.

Weakening control over *economic ecosystems and knowledge* can jeopardize sovereignty - thinking of lack of control over critical technology, such as AI and cryptography and other forms of information security. If there is not enough innovation in our country, there will potentially be new dependencies. For example, new technologies play an increasingly crucial role in cyber resilience.[16]

[11] For definitions see: Timmers, P., Strategic Autonomy and Cybersecurity, European Institute of Security Studies, May 2019.

[12] See the Netherlands 2020 Cyber Security Assessment (CSBN 2020) for an up-to-date overview of all types of cyber threats, https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020.

[13] Cybersecurity assessment Netherlands 2020 (CSBN 2020), National Coordinator of Counter-Terrorism and Security (NCTV), June 2020

[14] Cybersecurity assessment Netherlands 2020 (CSBN 2020), National Coordinator of Counter-Terrorism and Security (NCTV), June 2020, p. 18, with reference to the AIVD Annual Report 2019, April 2020.

[15] Also known as the CIA for cybersecurity: *Confidentiality, Integrity, Availability*.

[16] Knowledge and Innovation Agenda Security, Ministry of Economic Affairs & Climate, 2019; See also Van Boheemen, G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos (2019). Cyberable with new technology - Opportunity and need for digital innovation. The Hague: Rathenau Instituut. See also CSR Recommendation 'Towards structural deployment of innovative applications of new technologies for cyber resilience in the Netherlands', CSR Opinion 2020, No. 5, September 2020, p. 3.

As an example, Al facilitates the execution of cyber attacks because existing vulnerabilities can be automatically discovered and exploited on a large scale.[17] AI is also expected to enable automatic detection and recovery of software vulnerabilities. With post-quantum cryptography, we should eventually enable data encryption that can withstand attacks using the computing power of a quantum computer.[18]

With regard to *societal and democratic interests*, these mainly concern the functioning of and trust in the rule of law. In terms of sovereignty, this mainly concerns the *internal* legitimacy of the state. When internal legitimacy is in question (for example, when the state has no control over the election process because it has been infiltrated and manipulated by foreign powers), external legitimacy may also be at risk (the Netherlands as a reliable international partner).

Approaching cybersecurity from a sovereignty perspective

Due to the multifaceted nature of the causes of the pressure on our digital sovereignty and rapid geopolitical developments, there is no one-size-fits-all solution. Our sovereignty will have to be supported by a 'smart' combination of measures. A 'smart' approach also means weighing costs against benefits. Digital autonomy does not mean self-reliance or self-sufficiency. That is not possible for the Netherlands and often not for Europe either. Let alone that it would be desirable. Globalisation has brought enormous benefits, certainly for the Netherlands. Balkanization of technology and protectionism can hinder global trade and therefore also cost prosperity and jobs in the Netherlands. The Netherlands would therefore do well to take stock of its dependencies and reduce unilateral dependencies, also outside the well-known EU and NATO alliances.[19]

1. Strong at home, strong in Europe, strong in the world

The Netherlands and the EU will only have a voice on the international digital arena, and therefore in geopolitics, if we are strong in our own right. That means more control over own data, more grip on critical digital processes, and more innovation and knowledge under our own control. This must go hand in hand with our traditional strength, the internal market and European values.

The European Commission's ambition to promote technological sovereignty has meanwhile led to a series of European policy proposals.[20] The Netherlands can play a driving role in EU policy by ensuring that its own vision of digital autonomy is made explicit in Dutch policy and by making this vision and approach a contribution to EU policy. The Netherlands, like the frontrunners Germany and France, would thus create clarity and strengthen itselve as discussion partner.

[17] Cybersecurity assessment Netherlands 2020 (CSBN 2020), National Coordinator of Counter-Terrorism and Security (NCTV), June 2020, p. 15 - 26.

[18] CSR Recommendation 'Towards structural deployment of innovative applications of new technologies for the cyber resilience of the Netherlands', CSR Opinion 2020, No. 5, September 2020, p. 4.

[19] The WRR cites as examples countries such as South Korea, Chile, Canada and New Zealand, Holland's Spoor, Country wide & WRR strategy discussions, Report on Future Multilateral Order, p. 3. The EU is also committed to active cyber dialogs in this sense, including with Japan and South Korea.

[20] One of the first policy papers was from the European Commission/High Representative for Foreign Affairs and Security Policy, 'Reproducibility, deterrence and defense: building strong cyber security for the EU', 13 September 2017. See below: European Commission, 'A European Data Strategy', COM(2020)66, 19 February 2020; European Commission, White Paper 'On Artificial Intelligence - A European approach to excellence and trust', 19 February 2020; 'A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem', the GAIA-X project initiated by the German and French Governments, October 2019, based on principles of *sovereignty-by-design*.

This is topical, given the considerable number of EU policy proposals that have a relationship with digital autonomy.[21] This also puts the Netherlands in a better position to steer the hundreds of billions that the EU has allocated for digital investments, such as the European funding programmes for research & development (Horizon), digital innovation (Digital Europe), rollout of European digital infrastructure (Connecting Europe Facility), core projects where cooperation can take place without violating competition law (Important Projects of Common European Interest (IPCEI)), and recovery from the crisis (Resilience and Recovery Fund).[22] This also puts the Netherlands in a better position to realise its own agenda with European co-financing.

The ambition to play a leading role in Europe and to be a partner in this dialogue requires a number of fundamental steps to be taken at national level.

2. Approach to cybersecurity is insufficient from the perspective of strategic autonomy

The Council observes that cybersecurity has so far been addressed mainly in a technical and reactive manner, and hardly at all from the broader perspective of strategic autonomy. In the Netherlands, digital autonomy is not yet sufficiently on the political agenda and considerations of digital autonomy are not structurally included in the drafting of policies and legislation. Legislation is now mainly used to compensate for loss of digital autonomy rather than to prevent loss of digital autonomy. One example of the latter is the Commission's recent proposal for a Digital Markets Act[23] , which is a step in the direction of curbing the digital platforms that are operating as a gatekeeper of the digital world.

In a previous recommendation, the Council noted that, as the Netherlands, we do not currently have sufficient insight into our new dependencies[24] and are therefore unable to pursue sufficiently proactively coordinated technology policies in the field of research, valorization and industrial capacities.[25] This also requires that companies in the Netherlands operate in a thriving ecosystem; an ecosystem in which they have the ability to grow through adequate access to, inter alia, talent, data and funding. As the question of sovereignty affects more and more areas of the economy, society and democracy, control must be exercised centrally. To this end, the council believes that the necessary integration of policy and the associated accountability is lacking. Acting reactively should be combined with proactive monitoring and anticipation, also on the basis of structural reports to the House of Representatives. This requires that different policy areas and interests are closely linked, with *top-level* steering (*'Whole-of-Government'*).

Countries such as the US, the United Kingdom and China link their strategic autonomy to their ambitions to remain militarily autonomous and dominant. To this end, they have created processes and resources that continuously link the objectives with the necessary means to achieve them in a coordinated way.

[21] Relevant in this context is the proposed 2020 review of the Network & Information Security Directive ('NIS2') which concerns cyber-resilience; as well as the Digital Markets Act and Digital Services Act proposed in 2020 which regulate large digital platforms and the proposed Data Governance Act on access to and sharing of European data. Relevant legislation expected in 2021 is the review of the EU Regulation on electronic identity/electronic signature and other 'trust services' ('eIDAS2') and new legislation on high-risk applications of artificial intelligence, as well as legislation on specific EU data spaces ('data spaces') as for health data.

[22] The volume of digital investments as specifically committed is at least €134.5 billion in the Resilience & Recovery Fund, €7.5 billion in the Digital Europe program, around €3 billion in Connecting Europe Facility and a significant proportion of the €83.9 billion in Horizon Europe (in the past around 15%)

[23] The Digital Services Act package: https://ec.europa.eu/digital-single-market/en/digital-services-act-package

[24] Meanwhile, there has been a gradual increase in attention to this issue in various departments and an initiative is under way to identify the (geopolitical) economic dependencies that make our country vulnerable. The Cabinet is currently working on a methodology to systematically capture geopolitical vulnerable dependencies: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/02/10/tk-nationale-veiligheid- strategische-afhankelijkheden-en-planbureau/tk-nationale-veiligheid-strategische-afhankelijkheden-en-planbureau.pdf

[25] Reflections on digital sovereignty, Moerel and Timmers, 2020.

In addition, these countries, as well as France, use a strategic approach to stimulate their technological lead and continue to support this with financial, regulatory and procurement instruments. For example, the US uses a list of 'foundational and emerging technologies'. In an earlier recommendation[26] the Council insisted on the need to establish such a list of key technologies.

3. There is an important difference in the innovation environment between Europe and the US

The Netherlands had historically a strong position in key areas of cybersecurity such as cryptography. The Netherlands is still strong in terms of knowledge, including in emerging areas such as quantum technology and AI. But the transformation of that knowledge into products and services is often taking place elsewhere, even though they are essential for the digital autonomy in cybersecurity in the Netherlands. In particular, the US and China are more efficient in transforming science into markets and ultimately into dominance. They also do not hesitate to influence international standards to their advantage.[27]

Factors that hinder healthy Dutch (and European) cybersecurity business are the low willingness to invest compared to the US and China, the colonization of the innovation ecosystem by the large digital platforms and the lack of proactive analysis from the strategic autonomy perspective. The US, for example, has a more favorable ecosystem for startups, tapping into the network of entrepreneurs and risk investors and which is reflected in the investment climate. Startups are launching more easily and grow faster. As a startup in Europe, it is difficult to attract risk capital when it has no meaningful annual recurring revenue in the books yet. And if a European startup is successful and needs further funding, it usually goes the US to raise it. The reason for this is that investment tickets of more than EUR 100 million are very rare in Europe.

The risk of takeovers of successful European high-tech companies by parties outside Europe is therefore very high. US companies are constantly monitoring new innovations and start-ups, which they then take over at an early stage and integrate into their own offerings.[28] This means that there is no longer a *level playing field,* but serious market distortion. As part of an integrated approach, mitigating measures can here too be taken in a proactive way, for example by tightening export and acquisition restrictions, combined with active public participation in key companies, including the selective use of resources from the National Growth Fund.

The Council also refers to examples of mechanisms and processes that lead to a better innovation environment, such as in the UK (*Defense S&T Strategy, Govern Smarter*), Finland (*Business Finland*), Switzerland (*Innovation climate*) and Italy (*National Cybersecurity Perimeter*).

4. Three core facilities

The Council recommends that the following three core facilities be addressed as a matter of priority in order to strengthen our position both at home and in Europe. These facilities should be integrated into, or at least contribute to, European policies. The implementation of these core facilities requires close cooperation and coordination between the public authorities and the technological industry. A key factor for the success of this policy will be transparency and predictability in which the government intends to invest and innovate, as well as a clear framework for how parties can cooperate within the competition rules.

[26] CSR Recommendation 'Towards structural deployment of innovative applications of new technologies for the cyber resilience of the Netherlands', CSR Opinion 2020, No. 5, September 2020

[27] Paul Timmers, Geopolitics of Standardization, April 9, 2020, https://directionsblog.eu/the-geopolitics-of-standardisation/

[28] The US FTC is currently examining the strategy of major technology companies to stifle competition by systematically purchasing innovative startups.

This also requires that the public authorities actively use their procurement power for the purpose of digital sovereignty and make full use of the possibilities to include other factors than the lowest cost.

- **Sovereignty-respecting cloud:**
  The cloud is becoming the central infrastructure for business and public services. This also applies to our sensitive applications, ranging from the COVID-19 approach, the detection of criminals to the management of the Rotterdam port. In order to make large-scale use of AI data analysis, huge computing power is required. The cloud infrastructure needed for this will soon become the foundation for the Dutch and European innovation and knowledge infrastructure. Maintaining control over this is an essential part of the Dutch strategic autonomy.[29] Current market dynamics are characterized by a few dominant foreign tech companies. The dependence on non-European providers involves control by countries, which apply different rules in terms of, for example, espionage, privacy and the release of data. The government should develop a vision of an integrated and binding cloud outsourcing framework and actively deploy its procurement power to stimulate national cloud initiatives that contribute to the European cloud initiatives, some of which are already under way.[30]

- **Secure digital communications networks for the whole of the Netherlands**:
  We are increasingly dependent on digital communications for the well-being of citizens and a strong economy. Think of video meetings, and *smart homes*, but also new security-critical services such as *smart energy grids*, intelligent mobility systems and remotely controlled care robots. The development and management of the underlying technical systems and networks (such as routers, switches, DNS servers) are increasingly dominated by foreign parties. As a result, organizations and individuals have only a limited understanding of their dependencies on these parties and their systems, let alone control over them. This restricts our ability to decide autonomously and to act on how we set up our digital infrastructure and to which parties we want to entrust the transportation of our data. In a number of countries *quantum key distribution* is going to be used for essential communications from government, defense and finance. The Netherlands must take part in this and aspire to become one of the leaders. The Netherlands should also promote and contribute to a *responsible internet* at world level. An action plan should be drawn up to enable users to understand the network infrastructure that transports their data and communications (such as power concentrations and *single-point-of-failure*). It should also provide them with additional security-related options, including authentication and digital signatures. This will give them more control over their dependencies on the Internet and thus increase their trust in and control over Internet communications.[31]

- **Post-quantum cryptography**:
  Without cryptography, there is no protection of the most sensitive public information, industrial secrets of companies and personal information of citizens. The encryption as we know it is hacked by state actors, controlled by dominant non-EU market players, and will be cracked by quantum computing in a few years.

[29] Reflections on digital sovereignty, Moerel and Timmers, 2020. See also the German Industrial Strategy 2030. Guidelines for a German and European industrial policy', in which it is recognized that insufficient understanding of new technologies poses a direct risk to maintaining the technological sovereignty of the German economy.

[30] Meanwhile, Dutch cloud, hosting and infrastructure companies have entered into a coalition to contribute to GAIA-X: http://www.tno.nl/nl/over-tno/nieuws/2020/11/nederlandse-cloud-infrastructuur-coalitie-cic-eerste-stap-naar-capable digital-digital-netherlands

[31] For a first start, see: A Responsible Internet to Increase Trust in the Digital World, https://www.sidnlabs.nl/downloads/2v6sEqlLniFGTWbbKqTvhx/ee9f96134c0607c67efe40940039cd76/Hesselman_et_al-2020-Journal_of_Network_and_Systems_Management.pdf

> The government needs to invest in post-quantum cryptography, which means digital security services and solutions that can ensure long-term protection of sensitive information, including as new technologies emerge, applications emerge and cyber attacks evolve.

The three above-mentioned core facilities are a *conditio sine qua non* for safeguarding our digital sovereignty. At the same time, investment in these core facilities and the associated knowledge is a huge opportunity for the Dutch ICT and Internet industries, which are traditionally strong in these areas. The Netherlands has a leading position in quantum technology. In addition, AMS-IX is one of the world's largest Internet hubs, .nl is one of the largest and safest country top-level domains in the world, and we have a large hosting industry. With the basics in order and our internationally recognized qualities in governance, democracy and diplomacy, it is a realistic ambition for the Netherlands to offer the best digital gateway to Europe; the country with the best digital protection of knowledge and sensitive information and with the greatest confidence of citizens and businesses to participate in the digital society. The core facilities will only contribute to our sovereignty if we combine the interventions. The study and its assessment framework show how to address this.

Recommendations

Digital autonomy touches the heart of our society. We must therefore be resilient and be able to anticipate our (digital) future proactively and in a coordinated manner. The Council recommends that a number of specific issues be initiated without delay *in anticipation* of the elaboration and implementation of its previous recommendations, as the Council considers that these cannot wait for the development of such policies. The following actions are needed in the short term to strengthen our position:

1. **Implement a digital autonomy cybersecurity assessment framework.**
2. **Ensure three core facilities in anticipation of national strategy and policy making.**
3. **Raise awareness of the importance of strategic autonomy in cybersecurity.**
4. **Improve the valorization and innovation climate in the Netherlands.**
5. **Actively pursue alignment with EU policies and EU funding.**

Re 1. Implement a digital autonomy cybersecurity assessment framework.

The Council will make available a proposal for a ‘Manual for the application of the *digital autonomy and cybersecurity Assessment Framework’*. A number of Council members will organize interdepartmental workshops support this. This manual with the assessment framework should be made available urgently for policy development and legislative preparation. Only in this way can we prevent that sovereignty remains an *after-thought*. The Council recommends that this assessment framework be used and that its use be gradually extended over time. Such a framework can make a major contribution to (anticipating) the potential risks to digital sovereignty and create the opportunity to anticipate them in a timely and consistent manner.

Re 2. Ensure three core facilities in anticipation of national strategy and policy making.

The following three core facilities should be addressed as a matter of priority in order to achieve strategic autonomy in the basic infrastructure for the economy, society and democracy:

- Sovereignty-respecting cloud for secure data storage and data analysis
- Secure digital communications networks
- Post-quantum cryptography

In the annexes to this recommendation, the Council has made a start on this.

Re 3. Raise awareness of the importance of strategic autonomy in cybersecurity.

The importance of strategic autonomy in cybersecurity has so far not been sufficiently recognized at all relevant levels of the Dutch government, politics, business and science, but also among our main partners in the EU. Digital autonomy begins with knowledge and understanding so that all parties can take action to eliminate or minimize digital threats. We need to be aware of the developments, challenges and needs with respect to digital autonomy. In view of the urgency and importance of the subject, the Council will actively promote the dissemination of this recommendation and the study and organize a number of workshops.

Re 4. Improve the valorization and innovation climate in the Netherlands.

Our valorization and innovation climate needs to be greatly improved. This requires a different organization and steering. Examples of mechanisms and processes from other countries can be inspiring, such as in the US (*Darpa, In-Q-Tel*), the UK (*Defense S&T Strategy, Govern Smarter*), Finland (*Business Finland*), Switzerland (*Innovation climate*) and Italy (*National Cybersecurity Perimeter).*

Another recommendation is to provide structural support to the provision of academic expertise required to independently validate claims of key technology providers (*trust validators*). Support measures for new businesses through 'smart' procurement procedures, public authorities like *launching customer* and targeted innovation support are tools to improve opportunities for valorization. The introduction of protective measures, such as the strengthening of internal market conditions and export and takeover restrictions combined with active public participation in key companies, including the selective use of resources from the National Growth Fund, could also be envisaged.

Re 5. Actively pursue alignment with EU policies and funding.

The Netherlands can play a driving role in EU policy by ensuring that its own vision of digital autonomy is made explicit in Dutch policy and that this vision and approach is a contribution to EU policy. The Netherlands, like the frontrunners Germany and France, would thus create clarity and strengthen itself as interlocutor. This is topical in view of the significant number of EU policy proposals related to digital autonomy.[32] This also gives the Netherlands a better starting position to steer the hundreds of billions allocated by the EU to digital investments, such as the European funding programs for research and development (*Horizon Europe*), digital innovation (*Digital Europe*), the roll-out of European digital infrastructures (*Connecting Europe Facility*). We should also consider the key projects which can cooperate without infringing competition law (*Important Projects of Common European Interest (IPCEI)),* and the recovery of the crisis (*Resilience and Recovery Fund*).[33] This also puts the Netherlands in a better position to achieve its own agenda *with European co-financing.*

[32] Relevant in this context is the proposed 2020 review of the Network & Information Security Directive ('NIS2') which concerns cyber-resilience; as well as the Digital Markets Act and Digital Services Act proposed in 2020 which regulate large digital platforms and the proposed Data Governance Act on access to and sharing of European data. Relevant legislation expected in 2021 is the review of the EU Regulation on Electronic Identity/Electronic Signature and other 'trust services' ('eIDAS2'), the new legislation on high-risk applications of artificial intelligence, as well as legislation on specific EU data spaces ('data aspaces') as for health data.

[33] The volume of digital investments as specifically committed is at least €134.5 billion in the Resilience & Recovery Fund, €7.5 billion in the Digital Europe program, around €3 billion in Connecting Europe Facility and a significant proportion of the €83.9 billion in Horizon Europe (around 15% in the past).

Digital Autonomy and Cybersecurity in The Netherlands| CSR

TARGETED RECOMMENDATIONS

The recommendations of the Council are addressed to the public authorities and, through public authorities, also to the business community. Only by improving cooperation between the public sector, the private sector and knowledge institutions can digital autonomy with regard to cybersecurity be guaranteed in the future and can Dutch society continue to rely on the security and continuity of our digital society.

Recommendation of the Council to the outgoing Prime Minister:

1. Still this year assume responsibility for our digital autonomy at the highest possible level[34] and take into account digital autonomy in a structured way in the preparations for Ministerial Council meetings.
2. Organize strategic autonomy in cyber security as a continuous, proactive, and integrated activity at political and policy implementation level.
3. Hand over this recommendation to the incoming Cabinet in order to ensure continuity of the targeted advice.
4. Introduce an annual digital autonomy overview report by 2022, preferably as an integrated part of an existing report.

The Council recommends the outgoing Minister for Justice and Security, the outgoing State Secretary for Economic Affairs and Climate and the outgoing State Secretary for Home Affairs and Kingdom Relations jointly to initiate, in cooperation with the main stakeholders (public, private and science)[35]:

5. Implement before the end of 2021 the ‘Digital Autonomy and Cybersecurity Assessment Framework’ for policies and legislation and support implementation with workshops.
6. Identify (digital) dependencies in 2021 and define concrete targets for strategic control in cyber security. Use the proposed assessment framework.
7. Take a leading position within the EU on the basis of its own vision of digital autonomy, which also allows for targeted use of European co-financing.
8. Focus directly on raising awareness of the usefulness and necessity for digital autonomy among both public and private parties.
9. Coordinate the implementation of the three core components mentioned above, for a start see Annex 1 of this recommendation.

[34] CSR Advisory Report ‘Integral approach to cyber resilience’, CSR Opinion 2021, No. 2

[35] As also mentioned in the letter from State Secretary Keijzer of the Ministry of Economic Affairs and Climate Change addressed to the President of the Second Chamber of States General on 'Exploration Results and Follow-up to Cybersecurity Knowledge Development and Innovation', d.d. April 9, 2020.

10. Encourage the further development of knowledge and innovation in the area of digital autonomy, and align with European developments. Start these actions in 2021 on the basis of a comprehensive approach.
11. Focus actively on valorization and the creation of a favorable innovation climate with a focus on digital autonomy and cybersecurity.

The Council recommends that the outgoing Minister for Education, Culture and Science,
in cooperation with key stakeholders, initiate the following action:

12. This year actively engage in knowledge development and knowledge retention in the cyber domain. Encourage high-quality education and research so that our country has a strong knowledge base and a sufficient number of qualified staff.

The Council recommends the outgoing Secretary of State for Home Affairs and Kingdom Relations to initiate the following actions in cooperation with key stakeholders:

13. Align the central government procurement policy with the need for digital autonomy.
14. Encourage such an approach also for decentralized authorities.

The Hague,
On behalf of the Cyber Security Council,

Hans de Jong
Co-Chairman CSR

Pieter-Jaap Aalbersberg
Co-Chairman CSR

ANNEXES

These annexes provide a starting point for the delivery of the three core facilities. Further (policy) development is required for further detail and validation.

ANNEX 1: CORE FACILITIES

Objective 1: Sovereignty-respecting cloud

With sovereignty-respecting cloud, we mean a cloud infrastructure and service that protects cloud data and processes from access by unauthorized third parties and maintains control over the future value added from data analysis (AI) and trust services.

Current triggers related to strategic autonomy and cybersecurity:

- Increasing dominance and *lock-in* ambitions of the large *hyperscalers*.
- Threat of unauthorized third-party data access in cloud projects with an impact on the functioning of and trust in the state.
- Legal developments (Cloud Act and Cloud providers report US, Schrems II) and cloud policy developments in EU (GAIA-X, data spaces, AI).
- Technical developments in privacy protecting data processing.

Cloud is becoming the central infrastructure for most companies and public services. The current market dynamics are characterized by a number of parties (Microsoft, Amazon, Google, Alibaba), which also have a large grip on the knowledge ecosystem. Moreover, data is recognized as a ‘raw material’ and is essential for a country's future prosperity and well-being. Here, too, we are witnessing the emergence of a battleground where the major players (Google, Apple, Facebook, and the Chinese parties, such as Alibaba and ByteDance) are fighting it out between themselves. Counterplay can come from government, as customer and regulator and emerging related industry (AI, eID, edge computing, new forms of encryption).

Data and processes in the cloud should be protected from unauthorized or undetected access by third parties, such as the infrastructure provider, government, marketeers or criminals. Legislation, such as *General Data Protection Regulation (GDPR)*, already provides a certain level of protection but it relies on respectful implementation and enforcement. It would be better to embed the protection in a reliable and controllable way in the technology that holds the data and processes.

Objective:
Gain adequate control over cloud providers and their controlling governments in terms of value-added services and data and the next cloud generation, such as industrial cloud, by 2025. It is not at this stage the intention -and even an illusion - to regain control over the large cloud platforms.

Examples of possible measures, including at EU level:

Politics, policy and organization:

- An unambiguous and coherent and binding cloud policy for the government that is also extended to (coordinated) procurement policies, possibly operating conditions, by 2022 at the latest.
- Participation in European cloud projects that are promising for our country, from the end of 2021.
- Active contribution to EU policies and legislation (NIS2, eIDAS2, DMA, DSA, AI, cloud, data spaces), including strategic autonomy perspective, immediately.
- Government as *launching customer* of new privacy protection cloud solutions in areas such as justice/police and health.[36]

Knowledge, R&D, Industry:

- Prioritization and coherence of Dutch support for research and innovation in relevant areas, deciding this in 2022. The Netherlands shall include this priority in the European programs Horizon Europe, Digital Europe, CEF and EU4Health.
- Active and targeted support for innovation, monitoring growth investments in relevant startups, interaction with users in industrial sectors, such as logistics, defense and health, to raise awareness and free up resources.
- Long-term financial support of academic expertise that can validate and ensure trust in cloud technology. Promote the use of privacy-protective cloud solutions in business in areas such as logistics.

[36] Where no delivery date is mentioned, the measure is intended to apply from 2022 (or asap).

Objective 2: Secure digital communications networks for the whole of the Netherlands

With secure nationwide communications, we mean providing Internet connectivity and services with built-in cybersecurity for the whole country.

Current triggers related to strategic autonomy and cybersecurity:

- Broadening of the digital threat across the country to organizations that are less cyber-resilient but therefore no less important (e.g. health sector).
- Introducing new technology (5G and IoT), increasing the surface attack.
- For essential data, nationwide secure communications are a *conditio sine qua non*.
- Competition on price from network operators, which facilitates the purchase of less reliable network equipment and security shortfalls.
- Possible foreign acquisitions of critical network infrastructure.
- Emergence of new technologies (OpenRAN, quantum key distribution).

Cyber threats are now hitting virtually all economic and social players via the digital communications networks. COVID-19 shows that we need to protect new critical data and applications across the country. The digital communications infrastructure is fundamentally changing with 5G and Internet of Things and is distributed more, is becoming more distributed, dynamic and flexible. EU legislation already foresees a significant extension of cyber security obligations, but this is not sufficient to compensate for the lack of maturity and resilience of most companies and organizations. Incorporating greater security into the network with which these companies and organizations communicate with the outside world can reduce cyber risks. The EU is also strongly committed to quantum communications and future network generations (6G).

The need for cybersecurity, general market legislation and targeted government cooperation with providers of secure communications may mean that the authorities intervene more strongly in the market. If this were to distort competition, it would clearly have to be in the national interest.

Objective:
Foresee nationwide, built-in secure and stable *end-to-end* digital communications latest by 2025 as the backbone of economy, society and democracy. Accompany this with targeted awareness raising and support for the broad population and all segments of the economy.

Examples of possible measures:

Politics, policy and organization:

- Integrated plan for nationwide, secure and stable *end-to-end* digital communications in 2022.
- Extending the functionality and coverage of the National Detection Network (by 2025).
- National awareness raising campaigns.
- Selectively share threat information with the telecom operators.
- Impose security requirements on telecom at national level, based on EU legislation (NIS, Telecom Act, certification as in EU Cyber Act), extended to include built-in security requirements.
- Deploy secure *end-to-end* networks in all government activities, with *backbone* protection based on Quantum Key Distribution (by 2025).
- Actively monitor M&A/FDI in telecom providers.
- Make investment in cybersecurity attractive to businesses and citizens, for example in fiscal matters.

Knowledge, R&D, Industry:

- Prioritizing Dutch support for research and innovation in relevant domains (network security, optical and quantum communications, Quantum Key Distribution, 6G) by 2022.
- Active and targeted support for innovation, monitoring growth investments in relevant startups, interaction with users of telecoms operators to raise awareness and free up resources.
- Setting up 5G flagships in the Netherlands (e.g. logistics, health, industry).
- Active participation in 5G/6G standardization.

Objective 3: Post-quantum cryptography

'Post-quantum cryptography' refers to digital security services and solutions that can guarantee long-term protection of sensitive information, even if new technologies and applications emerge and cyber attacks evolve. The target users of post-quantum encryption are government and high-tech industry (protection of intellectual property).

Current triggers related to strategic autonomy and cybersecurity:

- Emerging technologies that make current encryption unsafe (quantum computing).
- Growing threat of espionage by states (incidentally, from enemies and friends).
- The disappearance of relevant industry in the Netherlands.
- New techniques (homomorphic, post-quantum) that provide longer, or even unlimited, assurance.

Post-quantum encryption solutions are strongly linked to strategic autonomy. The Netherlands has systematically lost control due to the disappearance of manufacturing industry and a market-oriented approach. Recovery of full control is unrealistic. Cooperation with *like-minded* partner countries will be necessary. Cooperation in the EU or globally is only useful in this case in terms of influencing reliable standards and the associated certifications. It is not feasible to have sufficient confidence in the manufacturing and supply chain on a broad geographical basis in this matter.

Objective:
Make a selection of operational and validated post-quantum solutions (products, services and expertise) available to the Dutch government and selected private parties (high-tech industry and science) from 2022.

Examples of possible measures:

Politics, policy and organization:

- A unambiguous, coherent and long-term government encryption policy, extended to (coordinated) public procurement policies and exemption clauses for security reasons (Art. 346 TFEU) to promote a stable market for manufacturing industry as of 2023.
- Government as *launching customer* of new encryption solutions.
- Active monitor M&A/FDI at encryption vendors.
- Strong and reliable partnerships with partner countries, such as France, Germany and Switzerland, which still have a relevant manufacturing industry, from 2023 onwards.

Knowledge, R&D, Industry:

- Long-term financial support for academic expertise for trust validation. Develop and implement a solution testing/validation program by 2023.
- Encourage expertise and entrepreneurial appetite for new manufacturing industry if there is a sufficient market, combined with processes and tools that can be used to strengthen autonomy (Defense Industry Strategy, National Growth Fund).
- Targeted financial support for R&D with the conscious objective of deliberately building innovation and manufacturing in the Netherlands, if necessary by selecting a few well-chosen areas.
- Active participation or at least close monitoring of standardization of post-quantum encryption algorithms (NIST etc.).

ANNEX 2: EXAMPLE ELABORATION OF RESPONSIBILITIES

The CSR Advisory Report 'Integral approach to cyber resilience' indicates that responsibilities should be placed with the Ministerial Commission chaired by the Ministry of General Affairs (AZ) for the integration of digital autonomy for cyber security, on the basis of a centralised national cyberresilience strategy. For specific tasks, the obvious approach is to build on existing strengths and tasks. Examples of such tasks, building on the three core facilities in the previous annex, are, in a broad sense, the development of industrial policy in sub-areas. In addition, government should act as a launching customer where possible.

A general task is to finance major interventions, for example from the National Growth Fund.

More specific tasks:

- New privacy protection cloud solutions in areas such as justice/police and health.
- Integrated plan for nationwide, secure and stable *end-to-end* digital communications in 2022.
- Extending the functionality and coverage of the National Detection Network, fully in 2025.
- Further development of selective threat information sharing with the telecoms operators.

Also:

- An unambiguous and coherent and binding cloud policy of the government that is also being extended to (coordinated) procurement policies, possibly operating framework conditions, by 2022 at the latest.
- Deploy secure *end-to-end* networks in all government activities, with *backbone* protection based on Quantum Key Distribution 2025.
- A unambiguous, coherent and long-term public encryption policy, followed by (coordinated) procurement policies and exemption clauses for security reasons in public procurement (Art. 346 TFEU) to promote a stable manufacturing market as of 2023.

Example tasks within the EU and international framework are:

- Participation in GAIA-X from end-2021 onwards;
- Strong and reliable partnerships with partner countries such as France, Germany and Switzerland which still have a relevant manufacturing industry from 2023 onwards.