RESEARCH IN FOCUS

Reflections on Digital Sovereignty

Prof. Dr. Lokke Moerel,
Tilburg University

Prof. Dr. Paul Timmers,
Oxford University and European University Cyprus

January 2021

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Contents

Abstract

The term digital sovereignty is becoming more and more common in the media and has a variety of meanings. In this public advice, the authors take a closer look at the concept of digital sovereignty. They conclude that digital sovereignty is not limited to the control of a state over the use and design of critical digital systems and the data generated and stored therein, but also concerns the broader scope of **economy** (control over essential economic ecosystems) and **society** and **democracy** (trust in the rule of law and quality of democratic decision-making). The authors provide a concrete overview with examples of the reasons why digital sovereignty of the Dutch State is under pressure, including (i) the increasing dependence of government bodies and critical digital infrastructure providers on a limited number of dominant foreign market players; (ii) the increasing cyber threats to our critical infrastructures, including systematic theft of intellectual property from our knowledge intensive industry sectors, digital extortion, targeted misinformation, and systematic infiltration of social media to influence elections and democratic processes; and (iii) the increasing geopolitical tensions leading to extraterritorial claims by foreign powers, such as export control restrictions on technology imposed by foreign powers and access by foreign powers to data of European citizens and businesses.

The authors analyze the policy and constitutional implications of the identified bottlenecks at the global, EU and Dutch levels. Three case studies are discussed where European legislation insufficiently addresses European (and therefore Dutch) digital sovereignty: (i) the European proposals for a European cloud infrastructure; (ii) the EU Network and Information Security Directive; and (iii) the EU Regulation on electronic identification and trust services for electronic transactions, which includes the recognition of electronic means of authentication of citizens (such as the Dutch DigiD). The authors propose solutions that fit within the current framework of international, European and national law. An important observation is that the EU's mandate to safeguard the necessary form of sovereignty is limited. Digital sovereignty soon touches on the national security of Member States, which under the EU Treaties is the prerogative of the Member States. Where the Member States each can no longer protect their sovereignty, the limited **European** mandate to safeguard **national sovereignty** actually undermines **national security**. Proposals are being made as to how the European legal basis for EU sovereignty can be strengthened. Because the question of sovereignty is affecting more and more areas of the Dutch economy, society and democracy, governance must be centralized. However, the ministries' departments mainly operate in silos, which entails that the necessary integration of policy is lacking. At present, there is even insufficient insight into the new digital dependencies to be able to conduct an integrated and proactive policy in the areas of research, valorization and industry at all. An obvious first step would be to appoint at least a digital affairs coordinator under the direct management of the office of the prime minister, with its own budget and implementing power. Without central direction and control, our country will find itself on an irreversible path of gradual erosion of our national technological and industrial capacities.

This paper was written in assignment of the University of Utrecht 2020 Annual Constitutional Law Conference: *Constitutional Law in the Data Society*. See the Dutch version at: https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf. This is an updated version.

1 Introduction

The term *digital sovereignty* is becoming more and more common in the media and has a variety of meanings.[1] One interpretation is the ability of nation states to control the digital infrastructure on their territory and the data of their citizens. We see, however, that the term is increasingly being used in a broader context. Digital technologies have become the battleground for the competition for global leadership and are leading to ever-increasing geopolitical tensions between the United States and China (also known as the *tech cold war*).[2] The battle is mainly about leadership in the field of 5G, computer chip technology, and *artificial intelligence* (**AI**). Both the United States and China regularly draw the *sovereignty card* in this context. President Trump recently banned popular Chinese apps – such as TikTok and WeChat – because they would undermine the "*national security, foreign policy and economy*" of the United States.[3] Such measures are being framed as the necessary protection of U.S. citizens from the unbridled collection of their data by the Chinese government.[4] The United States is not alone; the Indian government has also announced a ban on large numbers of Chinese consumer apps, including TikTok, because they are a "*threat to sovereignty and integrity*" and undermine "*national security.*"[5]

> **Digital technologies have become the battleground for the competition for global leadership and are leading to ever-increasing geopolitical tensions.**

Another example is the American ban of Huawei as a supplier of American telecom infrastructure. In addition, Huawei is now limited in its ability to purchase computer chips produced outside the United States with American technology. Not surprisingly, China is retaliating.[6]

In the EU, we currently see the concept of digital sovereignty in the media mainly in relation to the dominant position of American (and now also Chinese) tech companies in the field of cloud computing and social media. The data of virtually all European citizens and companies are by now in the cloud of these non-European companies and are therefore not available for European innovation.[7] As far as social media platforms are concerned, their lack of measures to combat misinformation and *fake news* on their

[1] See, for a good overview, Stephane Couture, The Diverse Meanings of Digital Sovereignty, August 5, 2020, http://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/
See also Eanne Kelly, Decoding Europe's new fascination with 'tech sovereignty', Science-Business, September 3, 2020, https://sciencebusiness.net/news/decoding-europes-new-fascination-tech-sovereignty

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

[3] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ ; https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html

[4] In a press statement of Mike Pompeo, secretary of state, on August 5, 2020, the United States announced a Clean Network Program, with five measures to prevent the interception and misuse of U.S. citizens' data: "Working to keep Chinese phone carriers (presumably compromised by Beijing) out of U.S. markets, to have privacy-violating Chinese apps kicked off American app stores, to remove U.S. apps from app stores run by Chinese companies, to keep U.S. citizens' data off of Chinese cloud servers "accessible to our foreign adversaries," and to ensure that the undersea cables that ferry internet signals between continents aren't secretly tapped by eavesdropping Chinese intelligence services," https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/ The U.S. government's accusations against China have a large element of the pot calling the kettle black, given the data practices of U.S. tech companies and the systematic tapping of undersea cables by U.S. intelligence services themselves; see https://theintercept.com/2020/08/06/the-filthy-hypocrisy-of-americas-clean-china-free-internet/

[5] https://timesofindia.indiatimes.com/business/india-business/government-bans-118-mobile-apps-including-pubg/articleshow/77890898.cms

[6] For an overview article: https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html.

[7] Digital Services Act package, Inception Impact Assessment, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers

platforms is particularly criticized.[8] Worrying examples of misinformation are the conspiracy theories of the anti-vax and anti-5G movements, stimulated by Russian infiltration.[9]

Specific friction arose around COVID-19 *contact tracing* apps. Criticism came, in particular, from the French and British governments that Google and Apple, through the technical design of their joint COVID-19 tracing platform, in fact determined for governments how they can collect data from their citizens in the fight against COVID-19.[10] The accusation that Google and Apple exercise power here as a *private government* also appeared in the American press: "[They] are exercising sovereign power (...) You have a private government that is making choices over your society instead of democratic governments being able to make those choices."[11]

"

The restoration of the EU's technological sovereignty is now the core ambition of the European Commission for the next five years.

Not surprisingly, the aforementioned dependencies on foreign parties have led to a series of European policy proposals.[12] Whereas in 2017, talking about European sovereignty was very much *not done* and Europe was in favor of the open liberal market economy, and European research programs, for example, had to be 'open to the world',[13] the restoration of the EU's technological sovereignty (in addition to recovery from the COVID-19 crisis and the fight against climate change) is now the core ambition of the European Commission for the next five years. In her inaugural speech as President of the Commission, Ursula Von der Leyen said: "We must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies. (...) [W]e need infrastructure fit for the future, with common standards, gigabit networks, and secure clouds of both current and next generations."[14] This strategy is also vocally supported by the member states. In the words of French President Emmanuel Macron: "If we don't build our own champions in all areas – digital, artificial intelligence, our choices will be dictated by others." [15] Angela Merkel also announced at the start of the German Presidency of the EU, that the focus will be on: "...technological sovereignty, particularly in key areas such as artificial intelligence and quantum computing, also in securing a secure, trustworthy data infrastructure."

As far as the latter is concerned, an important European project is the so-called *GAIA-X initiative*.[16] This project, initiated by Germany with the support of France, aims to create its own European offering of cloud infrastructure, services, and data and is explicitly based on principles of *sovereignty-by-design*, where the customer has full control over the storage and processing of the data and access thereto.

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

[9] https://allianceforscience.cornell.edu/blog/2020/04/anti-vaxxers-and-russia-behind-viral-5g-covid-conspiracy-theory/

[10] Apt quote of the French minister of digital affairs: "We're asking Apple to lift the technical hurdle to allow us to develop a sovereign European health solution that will be tied our health system" https://www.bloomberg.com/news/articles/2020-04-20/france-says-apple-s-bluetooth-policy-is-blocking-virus-tracker?srnd=progno

[11] Reed Albergotti and Drew Harwell, "Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless." Washington Post, May 15, 2020, https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/

[12] One of the first policy documents was from the European Commission/High Representative for Foreign Affairs and Security Policy, 'Resilience, deterrence and defense: building strong cybersecurity for the EU,' September 13, 2017. See also: European Commission, 'A European data strategy', COM(2020)66, February 19, 2020; European Commission, White Paper 'On Artificial Intelligence - A European approach to excellence and trust,' February 19, 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.

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

[14] https://ec.europa.eu/info/sites/info/files/president-elect-speech-original_en.pdf.

[15] https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/.

[16] Project GAIA-X, A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem, German Federal Ministry for Economic Affairs, October 2019, https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/project-gaia-x.pdf?__blob=publicationFile&v=5; see further Franco-German Position on GAIA-X, February 18, 2020, p. 1 - 2.

Incidentally, the GAIA-X documents themselves indicate that there is still a long way to go: "Europe's digital infrastructure currently lies in the hands of a small number of major non-European corporations: Europe has no notable operating system developers, no relevant search engines, no global social network and no competitive cloud infrastructure."

"

This new European sovereignty thinking is not limited to digital policy, and now encompasses an almost kaleidoscopic range of initiatives and measures.

This new European sovereignty thinking is not limited to digital policy, and now encompasses an almost kaleidoscopic range of initiatives and measures. Work is currently underway on *materials autonomy* for the European Green Deal (securing scarce raw materials needed for batteries for electric cars – such as lithium[17] – and storage of clean energy – such as magnesium),[18] *financial sovereignty* triggered by Iranian sanctions,[19] and *energy autonomy vis-à-vis* Russia.[20] The COVID-19 crisis also exposed Europe's dependency on global *supply chains* of critical raw materials and products, making it painfully clear that we are dependent on China for virtually all of the chemical components needed to produce generic medicines,[21] leading to all sorts of reports on *health sovereignty*.[22] Finally, there is talk of excluding the UK from the secure zone of the Galileo satellite system,[23] combating *fake news*,[24] and restrictions on so-called *Foreign Direct Investment*.[25]

With this range of measures, one cannot escape the question of what exactly the connection is between them and whether these measures indeed can lead to a relevant degree of digital sovereignty for the Netherlands and for the EU as a whole. Therefore, there is all the more reason to take a closer look at the concept of *digital sovereignty* and to analyze its policy and constitutional implications.[26] In this contribution, we will provide an overview of what we understand by digital sovereignty, how the digital sovereignty of the Dutch state is currently under threat, and which measures – at which level – can be considered to improve it. Upfront we here state that for us digital sovereignty does not mean complete self-reliance or self-sufficiency. In general, this is not possible for the Netherlands and often not for Europe, nor is it necessary.

---

[17] Under the flag of the European Battery Alliance, also an IPCEI project, https://ec.europa.eu/growth/industry/policy/european-battery-alliance.

[18] Under the flag of the European Raw Materials Alliance, see, for press release on the European Action Plan on Critical Raw Materials, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1542. For an overview of critical raw materials, Critical Raw Materials for Strategic Technologies and Sectors in the EU, A Foresight Study, 2020, file:///C:/Users/lxm16/Downloads/Critical%20Raw%20Materials%20in%20Technologies%20and%20Sectors_foresight.pdf.

[19] The related financial instrument is INSTEX, https://instex-europe.com/about-us.

[20] Ursula von der Leyen State of the Union September 2020, https://ec.europa.eu/info/sites/info/files/soteu_2020_en.pdf; see also SWP Paper 2019/RP 04, March 2019, European Strategic Autonomy, https://www.swp-berlin.org/10.18449/2019RP04/#hd-d14204e721.

[21] https://www.politico.eu/article/europe-braces-for-coronavirus-induced-drug-shortages/.

[22] See, for example: https://www.ecfr.eu/publications/summary/health_sovereignty_how_to_build_a_resilient_european_response_to_pandemics.

[23] Financial Times, June 13, 2018, "Brussels spurns UK demand for unrestricted access to Galileo satellite" https://www.ft.com/content/332e1a94-6f00-11e8-92d3-6c13e5c92914.

[24] See previously mentioned reference, "Tackling online disinformation."

[25] EU Foreign Direct Investment Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020R1182

[26] There is not yet much academic literature on this subject. For an Essay Collection of the European Denktank: *European Council on Foreign Relations*, Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-Chana Rivalry, July 2020, https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf; see further EOS Position Paper, EU Digital Autonomy: Challenges & Recommendations for the Future of European Digital Transformation, November 2019, http://www.eos-eu.com/Files/EOSEUDigitalAutonomyPositionPaper.pdf. For a broader development in this respect – namely, an explicit link with economic thinking in geo-politics – see Haroon Sheikh's column: https://www.nrc.nl/nieuws/2020/08/07/leer-geo-economisch-denken-ook-in-de-eu-a4008101

2 What is digital sovereignty?

2.1 Sovereignty and strategic autonomy

Sovereignty is a political concept for which there is no unambiguous, generally accepted definition. Sovereignty is generally associated with territoriality, territory (including natural resources), jurisdiction, a population, and authority with both internal and external recognition (legitimacy). *Internal legitimacy* refers to the effectiveness of the state as an executor of governmental tasks (e.g., being in control of the electoral process and the criminal justice chain) and also the recognition by citizens of the government (having confidence in the rule of law). *External legitimacy* primarily concerns the recognition by foreign states and the autonomy of action of a state towards foreign states.

If sovereignty is the *goal*, strategic autonomy is the *means*. Sovereignty must be made operational: what are the means to achieve sovereignty? This is called *strategic autonomy*, a concept that originated in military/defense thinking but is now seen as "the capabilities and capacities to decide and act autonomously on essential aspects of the longer-term future in the economy, society and democracy."[27]

In today's information society, the term *digital sovereignty* is often used as well. It almost always refers to the digital dimension of strategic autonomy, i.e., the ability to decide and act autonomously on the essential digital aspects of our longer-term future in the economy, society, and democracy. This concerns the use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result.[28] A better term than digital sovereignty, therefore, is digital strategic autonomy. In this article, however, we will continue to use the term digital sovereignty, as this is currently the common terminology.

Within digital sovereignty, data sovereignty is also used. This is having control over the storage and processing of data and having control over who has access thereto. European data sovereignty is promoted by the aforementioned GAIA-X cloud initiative and the recent European Cloud Federation Initiative, where standards are set for interoperability between providers and portability of data and where cloud providers will be expected to offer a choice as to where (personal) data are stored and processed, without otherwise requiring storage in Europe.

> ***Portability*** is the ability of applications and to be transferred – with reasonable effort – from one IT environment to another (the process of transfer, we call *migration*).
>
> ***Interoperability*** is the ability of IT systems to work together with other IT systems, allowing data to be exchanged and the use of the data that has been exchanged.

There is even a discussion as to whether certain categories of data (e.g., patient data and industrial data) should be regarded as *sovereign property* in their own right, comparable to natural resources such as gas or oil under our territory. In such a view, territorial rights can then be claimed on European data, as is the case with natural resources. Commissioner Thierry Breton, for example, recently said that "European data should be stored and processed in Europe because they belong in Europe."[29]

---

[27] "The capabilities and capacities to decide and act upon essential aspects of the longer-term future in the economy, society, and democracy," Timmers, P., Strategic Autonomy and Cybersecurity, European Institute of Security Studies, May 2019).

[28] A similar definition is: 'digital sovereignty is the possibility of independent self-determination by the state and by organisations with regard to the use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result,' Digital Summit Focus Group, referred to in the above-mentioned GAIA-X document, October 2019.

[29] According to a POLITICO interview on September 1, 2020, https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe/.

“

In short, the developments of the digital world force us to ask probing questions about sovereignty and autonomy.

It will require little explanation that where governments and providers of critical infrastructure increasingly outsource their ICT systems and data storage and processing to suppliers, new dependencies arise, especially if those suppliers are dominant market players (see section below on hyperscalers). The concept of digital sovereignty then also extends to the autonomy of our government and providers of critical infrastructure vis-à-vis *these commercial parties*, and where these are foreign parties, *to their respective governments*. In short, the developments of the digital world force us to ask probing questions about sovereignty and autonomy. The transition to the digital society and the technologically constructed society[30] has direct consequences for geopolitical relations.

As *food for thought* of how far the questions reach: countries consider the DNA of native flora and fauna as belonging to their natural resources; it falls under their sovereignty. They restrict or at least demand *Fair and Equitable Sharing of Benefits*, as signatories of the Nagoya Protocol.[31] But with digitization and *gene sequencing*, DNA becomes a series of digital data. These data are easy to transfer outside the country and can then be converted back into physical DNA using genetic technologies of digital sequencing. In this case, is the digital representation of DNA part of sovereignty?

2.2 The dimensions of digital sovereignty

2.2.1 Cyber resilience of critical systems, processes and data

An important dimension of digital sovereignty is the *cyber resilience* of our critical sectors, processes, and data. The ever-increasing cybersecurity threats undermine sovereignty. We are talking about the entire spectrum of direct threats to our vital infrastructure, systematic theft of intellectual property from our knowledge-intensive world leading industries that are world leaders, digital extortion, targeted misinformation, and systematic infiltration of social media to influence elections and democratic processes.[32] When our government and critical sectors are not in control of important processes and data, it mainly affects the *internal legitimacy* of the state. Cyber threats can also put pressure on the *external legitimacy* of the Netherlands. For example, it is reported that the Dutch digital infrastructure is regularly abused by foreign state actors in cyber-attacks on yet other countries.[33] 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 reputation of the Netherlands and deteriorate our allied interests, thus undermining our *external legitimacy* in international relations.

As far as cyber threats are concerned, digital sovereignty cannot be separated from the three basic principles of information security, also known as the CIA of cyber security: Confidentiality, Integrity, Availability. In these three domains, autonomy must be safeguarded, not only at the level of a specific system in a specific sector (such as an ICT system in the criminal justice chain), but also in the larger framework of the *economy*, *society*, *and democracy*.

[30] On the relationship between technology and society, see, for example, Jean Baudrillard, Simulacra et Simulation, 1981, and Paul Timmers, “Challenged by “Digital Sovereignty”” in Journal of Internet Law, December 2019.
[31] Nagoya Protocol on biodiversity, https://www.iucn.org/theme/global-policy/our-work/convention-biological-diversity-cbd/nagoya-protocol.
[32] See the 2020 Cyber Security Assessment Netherlands (CSAN 2020) for an up-to-date insight in the digital threats and the interests that could be affected by these. The CNAS is established annually by the Dutch National Coordinator for Counterterrorism and Security. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020.
[33] CSAN 2020, p. 18, with reference to the 2019 Annual Report 2019 of the Dutch General Intelligence and Security Services (AIVD), April 2020.

> ***IACS*** are the systems (consisting of software and hardware elements) that allow industrial organizations to control industrial processes locally or at remote locations and to monitor and process real-time data. These are the systems that control our locks and bridges and ensure that energy and gas are distributed, drinking water is cleaned, and nuclear material is processed.

Through a specific government ICT system, sovereignty can be undermined – think of stealing information from government officials for espionage purposes[34] (*confidentiality*) and cyber-attacks on so-called *Industrial Automation & Control Systems (IACS)* in our[35] critical infrastructure (*availability)*.[36] These systems are the specific target of foreign state actors in order to make sabotage possible in the future as a means of pressure to achieve geopolitical objectives.[37]

> **Digital sovereignty must also be translated into the broader state interest of *economy, society, and democracy*.**

In these cases, we can translate digital sovereignty into *direct requirements* for ICT systems. These include requirements for security, threat detection, continuity (backup, disaster recovery), *vendor lock-in* (preventing dependence on a specific supplier), and access to data by foreign powers (see section on access to data by foreign powers below for an overview of specific dependencies in cloud computing). Digital sovereignty, however, as mentioned above, must also be translated into the broader state interest of *economy, society, and democracy*. This concerns, for example, the degree of control over essential economic ecosystems, knowledge and data, trust in the rule of law, and the quality of democratic decision-making.[38] We give a number of examples below.

> ***Vendor lock-in*** is caused by the fact that a supplier uses its own proprietary standards, which means that software and applications only work on its own platform, making a switch from one customer to another supplier costly or even impossible.

[34] The Dutch General Intelligence and Security Service reports that ministries, intelligence and security services, political parties, and cultural and social organizations, among others, were targeted by political espionage, CSAN 2020, p.19. For example, intelligence is collected to play countries against each other in order to undermine unity and international cooperation within the North Atlantic Treaty Organization and the European Union, CSAN 2020, p. 15. See, for a recent example: Bloomberg, Chinese Hackers Targeted European Officials in Phishing Campaign, September 2, 2020, https://news.bloomberglaw.com/privacy-and-data-security/chinese-hackers-targeted-european-officials-in-phishing-campaign

[35] Also called SCADA systems: Supervisory Control and Data Acquisition. Some cyber attacks are known as SCADA-attacks, like Stuxnet, which disabled Iranian nuclear centrifuges in 2010.

[36] For an overview of vulnerabilities in IACS, see CSAN 2020, pp. 16 and 19. For enemy cyber attacks on IACS in critical infrastructures, see: Gartner, A report for the Dutch Ministry of Justice and Security, Cyber Security Research for Industrial Automation and Control Systems, August 21, 2019, https://www.cybersecurityraad.nl/binaries/CSR_Advies_IACS_Onderzoeksrapport_Gartner_DEF_tcm107-442489.pdf, and the advice of the Dutch Cyber Security Council: "Advice on the digital security of Industrial Automation & Control Systems (IACS) in the critical infrastructure of the Netherlands," April 24, 2020 (CSC Advice on Cyber Security IACS), https://www.cybersecurityraad.nl/binaries/CSR_Advies_IACS_NED_DEF_tcm107-444304.pdf

[37] CSAN 2020, pp. 8 and 16.

[38] For some of these aspects, see also the Unsolicited Opinion of the Dutch Council of State, August 31, 2018, https://www.raadvanstate.nl/@112661/w04-18-0230/

2.2.2 Control of economic ecosystems

In terms of *economic interest*, we have to examine the extent to which we, as the Netherlands, have control over our economic ecosystem, economic value creation, and know how. To this end, there is now a national digital policy,[39] not only for the government as a user of ICT, but also for Dutch companies as suppliers and as a knowledge country.[40] Weakened control over *economic ecosystems and knowledge* can jeopardize sovereignty – think of lack of control over critical technology, such as AI and encryption. If insufficient innovation takes place in these areas, potentially new dependencies arise. For example, new technologies play an increasingly crucial role in cyber resilience.[41] AI may facilitate cyber-attacks by allowing existing vulnerabilities to be detected and exploited automatically and on a large scale.[42] However, AI is also expected to make it possible to automatically detect and restore vulnerabilities in software. Post-quantum cryptography should ultimately enable data encryption that can withstand attacks using the computing power of a quantum computer. Although the quantum computer will not be sufficiently developed to become widely accessible in the coming years, we will urgently need to focus on research and innovation to protect IT systems against the risk of an attack using a quantum computer. As soon as the quantum computer makes it possible to break existing forms of encryption, post-quantum cryptography will be a necessary condition to guarantee the security of data of our government, organizations and citizens.[43] Intelligence services already now work on the premise that foreign states currently systematically intercept and preserve encrypted communications and other information in anticipation that these may be decrypted at a later stage. We therefore have to invest in post-quantum encryption now in order to be able to protect strategic information that requires long term protection.

Within the vast domain of quantum computing research we need to ensure that those topics are under our domestic or EU control that are essential for safeguarding national and EU sovereignty.

Though The Netherlands has a leading quantum computing research platform,[44] our investments (and even the investments by EU programs) are dwarfed by the billions currently invested by Chinese and U.S. governments[45] combined with the investments by large U.S. and Chinese tech companies such as Google[46] and Tencent.[47] Within the vast domain of quantum computing research we need to ensure that those topics are under our domestic or EU control that are essential for safeguarding national and EU sovereignty (such as quantum communications and post-quantum crypto). Where foreign

[39] "ICT and Economy," https://www.rijksoverheid.nl/onderwerpen/ict/ict-en-economie

[40] With specific attention to the cybersecurity sector, https://www.rijksoverheid.nl/onderwerpen/ict/veilige-infrastructuur, http://www.seo.nl/uploads/media/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf.

[41] 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). Cyber resilience with new technology - Opportunity and necessity of digital innovation. The Hague: Rathenau Institute. See also CSR Advice 'Towards the structural deployment of innovative applications of new technologies for the cyber resilience of the Netherlands,' September 18, 2020, https://www.cybersecurityraad.nl/binaries/CSR_Advies_NT_NED_DEF_tcm107-466703.pdf (CSR Advice New Technologies), p. 3.

[42] CSAN 2020, pp. 15 - 26.

[43] CSC Advice New Technologies, p. 4.

[44] In April 2020, Europe's first quantum computer in the cloud was launched by the Technical University of Delft and the Dutch Institute for Applied Science (TNO), https://www.tudelft.nl/en/2020/tu-delft/minister-ingrid-van-engelshoven-and-european-commissioner-mariya-gabriel-launch-europes-first-quantum-computer-in-the-cloud-quantum-inspire/.

[45] See for an overview of U.S. and Chines research investments https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=40db612972de

[46] Google claimed to have reached quantum supremacy with its Google quantum computer called Sycamore, FT September 2019, https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17. On 3 December 2020, Chinese quantum computing researchers also claimed quantum supremacy, https://www.wired.com/story/china-stakes-claim-quantum-supremacy/.

[47] Keen not to become laggards as to quantum computing compared to US big tech, the Chinese company Tencent has announced to invest USD 70 billion in infrastructure and quantum computing, https://quantumzeitgeist.com/tencent-to-invest-70-billion-in-infrastructure-including-quantum-computing/.

companies are at the forefront of the (further) development and implementation of new technologies, such as AI and quantum computing and quantum communications, but also satellite and 5G networks, potentially new dependencies arise. These dependencies go beyond the specific technological applications themselves. To be able to make large-scale use of data analysis by means of AI, enormous computing power is required. It is expected that the cloud infrastructure required for this will become the foundation for the Dutch and European innovation and knowledge infrastructure. Maintaining control over this is an essential part of Dutch strategic autonomy.[48]

2.2.3 Trust in the rules of law and democratic processes

“

Every digitization of government processes creates new vulnerabilities in society, in this case new possibilities of potential influence and disruption of a vital function of our rule of law.

As far as the *social and democratic interests are* concerned, it is mainly about the functioning of the constitutional state and the trust in the rule of law. In terms of sovereignty, this mainly concerns the *internal* legitimacy of the state. It cannot be ruled out that if the internal legitimacy is questioned (e.g., when the state has no control over the election process, because it has been infiltrated and manipulated by foreign powers), the *external* legitimacy may also be compromised (e.g., the Netherlands as a reliable international partner).

It should be borne in mind that every digitization of government processes creates new vulnerabilities in society, in this case new possibilities of potential influence and disruption of a vital function of our rule of law. This also has an impact on citizens, because the inconvenience caused by and disadvantages of the government’s use of new techniques often end up with them. This affects the constitutional relationship between citizens and the government, where their position and protection are at stake. In an unsolicited advice from 2018, the Dutch Council of State describes the problem aptly:

> “Digitization of decision making threatens to confront citizens increasingly with decisions taken fully automatically, without human intervention. The citizen can no longer check which rules have been applied and it is no longer possible to determine whether the rules actually do what they are meant to do. The citizen also threatens to become a victim of a robotic equality, in which there is no longer an eye for the individuality of his situation. In addition, he threatens to be confronted with decisions based on profiling and statistical correlations. In that case there is no evidence that the citizen has acted culpably; there is only a suspicion based on general characteristics. A statistical reality arises which deviates from the concrete facts. Finally, the citizen is in danger of being confronted with decisions taken on the basis of data obtained from various other administrative bodies. It is then no longer possible to check whether the decisions have been taken on the basis of correct data. Moreover, the citizen himself will have to prove that an error has been made; in the event of errors in the system, he will have to prove his own “innocence”.”[49]

Infiltration of a vital government process can also undermine trust in the rule of law. Illustrative is a recent incident in Germany. In January 2020, *Der Spiegel* reported that the Berlin High Court (responsible for terrorism cases) had been systematically infiltrated by a Russian hacker group probably sponsored by the Russian government, identified as APT 28 (*Advanced Persistent Threat*). This hacker group had

[48] Paul Timmers, ‘There will be no global 6G unless we resolve sovereignty concerns in 5G governance’, Nature Electronics 3, 10-12 (2020). See also the German ‘Industrial Strategy 2030. Guidelines for a German and European industrial policy,’ in which it is recognized that insufficient grip on new technologies poses a direct risk to the preservation of the technological sovereignty of the German economy.

[49] See the Unsolicited Opinion of the Council of State, August 31, 2018, para. 1, https://www.raadvanstate.nl/@112661/w04-18-0230/ See on the impact of digitization on brugers: L. Moerel & C. Prins, *Privacy for the Homo Digitalis: Proof of a new assessment framework for data protection in light of Big Data and Internet of Things, Preadviezen* 2016 Nederlandse Juristen-Vereniging, Deventer: Kluwer juridisch 2016, pp. 9-124.

previously been held responsible for the infiltration of the German Bundestag. The attack focused on data exfiltration, accessing the entire database with identities of suspects, victims, witnesses, and undercover agents and informants.[50]

Another example of undermining trust in the rule of law is the social outcry that arose in Germany when the federal police transferred the *bodycam footage* of police officers into Amazon's public cloud in March 2019.[51] This led to devastating criticism from the German federal privacy regulator that this practice violates privacy laws and that the recordings should be placed in a private German cloud. The regulator's main objection was that Amazon is a U.S. company subject to the U.S. CLOUD Act, which potentially allows U.S. authorities access to this data.[52]

The public outcry in Germany is not so surprising when you consider that bodycam recordings are potentially sensitive material for citizens: these are image and sound recordings that may contain potential evidence of criminal acts, but non-affected bystanders also may be recorded. AI-controlled facial recognition is used to search large amounts of bodycam recordings and *blur* the faces of non-affected persons. How good will the AI be, does it recognize *fake* and manipulated material, and who supervises it? What if fake material is overlooked and ends up in the criminal justice chain? In these cases, the burden of proof lies with the citizen instead of with the criminal law chain, which undermines the functioning of, and trust in, the rule of law. This affects the *internal legitimacy* of the state.[53] Considering the potential impact on trust in the rule of law (again: sovereignty), the European Commission is considering regulation of AI-driven facial recognition and has launched a debate on this issue.[54]

A final example is the previously identified expectation that AI will make it possible to automatically detect and repair vulnerabilities in software. Where AI can make autonomous decisions, this is particularly critical when it comes to state responsibilities. Current cyber defense legislation is not prepared for such autonomous AI. This legislation assumes that consultation takes place on how to deal with threats. However, before the required consultations can take place, a cyber virus will have long since spread and, moreover, have adapted. We therefore need to be able to react with the speed of virus spread, and that is only possible with AI. But what if that AI is actually going to make decisions about life and death, for example by disconnecting part of the electricity network to slow down a cyber virus? If we allow AI at the heart of our cyber defense and at the heart of our state, we will have to clearly define the powers and responsibilities. Again, this affects the organization of the state and is as yet virtually unchartered territory.

[50] https://www.tagesspiegel.de/berlin/cyberangriff-auf-berliner-kammergericht-russische-hacker-koennten-justizdaten-gestohlen-haben/25477570.html

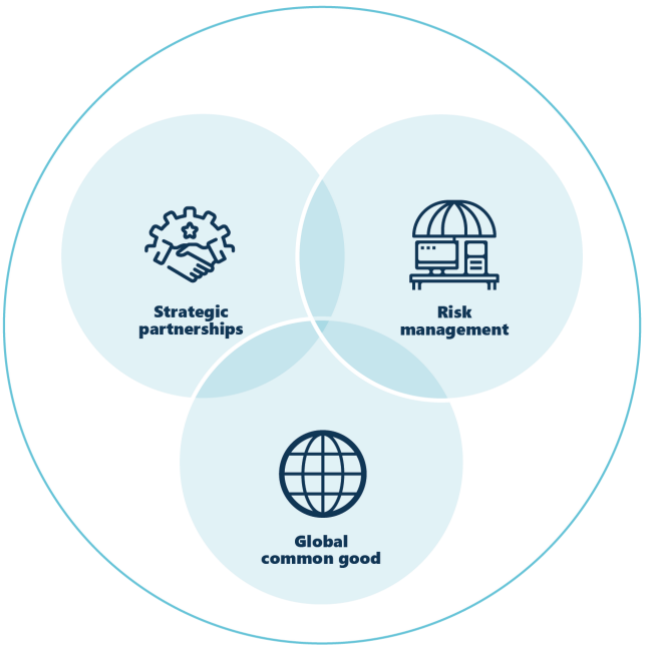
[51] https://www.noz.de/deutschland-welt/politik/artikel/1685384/bundespolizei-geraet-wegen-speicherung-von-bodycam-aufnahmen-unter-druck

[52] The Minister of the Interior replied that the solution would be temporary, until a federal state cloud was set up. Also questions were posed in parliament (including about the risk of the U.S. Cloud Act), after which an official investigation was launched, to which the German federal government responded. This revealed that, at that time, migration to an alternative solution was not yet possible.

[53] This is a fundamental concern of the Council of State, see para. 2 'Growing care citizen in trouble.'

[54] https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-european-approach-excellence-and-trust.

3 Why is digital sovereignty under pressure?



The pressure on (digital) sovereignty comes from three sides, which we will explain in more detail below:

> The increasing dependence on digital technology, which moreover is largely in the hands of a limited number of foreign players[55];

> The increasing cyber threats – in which smaller countries and non-state actors can also enter the global battlefield[56] – are such that they seriously undermine national sovereignty and the international order, thus creating a *sovereignty gap*; and

> The increasing geopolitical tensions, particularly in the U.S.-China, EU-Russia, and transatlantic relationships, leading to extraterritorial claims.[57]

3.1 Dependencies on limited number of foreign suppliers

A number of examples have already been given for why digital sovereignty is under threat. In the following, we will look in more detail at the specific dependencies that arise when organizations use suppliers to deliver their digital infrastructure.

It is clear that if an organization manages the hardware, software, and data required for its work processes, the dependencies on third parties are limited. The dependencies increase as the delivery and management of the various components are outsourced to a supplier. Having its own control over the digital infrastructure is then replaced for components by making contractual agreements. Increasingly, certain dependencies can also be overcome by, for example, technically shielding access to data and systems or by securing the data itself by means of encryption.

The degree of 'control' that the customer has and the grip on security measures over infrastructure and data differ per type of outsourcing. We see this particularly with cloud services. The most far-reaching form of outsourcing is when use is made of so-called SaaS services (*Software as a Service*). In SaaS, both the infrastructure and the software are provided by the supplier as a service to the customer (the customer does not have its own hardware and software licenses), which means that the customer's data is no longer in the customer's own environment. SaaS usually involves a *public cloud*, in which

[55] The Scientific Council for Government Policy, in its advice "Preparing for digital disruption," 2019, Chapter 3, gives a good overview of the far-reaching digitalization of society, the strong interweaving of the digital domain and the physical domain, and the new vulnerabilities that this creates for core societal processes, WRR Advice Digital Disruption , https://www.wrr.nl/adviesprojecten/digitale-ontwrichting/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.

[56] 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 weaponry is changing the (geopolitical) order: "The balance of power is shifting, now that smaller countries can also enter the global battlefield. 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 great clout," https://www.njb.nl/blogs/consequenties-van-een-nieuw-type-oorlogsvoering/

[57] Lucas Kello, The Virtual Weapon and International Order, Yale University Press, 2017.

infrastructure and software are shared with other customers in order to realize economies of scale. When we refer to SaaS services below, we mean a *public cloud* solution.[58]

The international cloud providers compete on security and are *best in class*. The deployment of cloud solutions now offers so many advantages in terms of functionality (e.g., built-in data analysis tools), higher implementation speed, innovation, the possibility of collaboration, and often lower costs, that the use of cloud services is now also seen as 'necessary for a well-functioning government,' making government policy *cloud first*, both in the Netherlands and Europe.

In the market, there is a very limited choice of so-called *hyperscalers* (cloud providers with large capacity). The American and Chinese hyperscalers have 75% market share worldwide (65% already for Amazon, Google, Microsoft, and IBM); and in the EU, European suppliers hardly appear in the picture.[59] The dominance in market positions leads to an imbalance between supplier and customer, with monopolistic behavior in contracts, price, service, and dependencies for the future (not only because of dependencies on contract termination (exit and transition), but also because making changes to standard solutions is difficult).[60]

> ***Exit and Transition***: customer dependencies often arise when contracts terminate because the customer needs the cooperation of the supplier for the transition of data and applications to a successor supplier (who in turn applies its own standards). For this purpose, specific protocols for 'exit and transition' are already agreed upon at the conclusion of the contract.

The major market players offer limited interoperability and portability of data and applications. Because of their scale, they are able to use their own standards – often protected by intellectual property rights – and even build a private internet infrastructure (including even their own submarine cables),[61] which makes them virtually autonomous both physically and legally and makes any interconnection difficult, both in terms of infrastructure and data exchange.[62] To prevent vendor lock-in, clients (as well as the Dutch and European governments)[63] usually have a so-called *multivendor* strategy. However, under current market conditions, this is difficult to achieve.

The current expectation is that – without government intervention – the dominant positions of these market players will only increase. These market players are systematically expanding their ecosystem by integrating new functionalities into their services (such as cybersecurity and data analysis tooling), which will only increase *vendor lock-in*.[64] They are also able to attract the best talent worldwide and have almost inexhaustible access to capital. This enables them to continuously monitor new innovations and start-ups, which they then take over at an early stage and integrate into their own offerings. The strategy

[58] An explanation of cloud and the commonly used terms IaaS, PaaS, and SaaS can be found at https://www.nist.gov/publications/nist-definition-cloud-computing.
[59] Synergy Research Group, October 29, 2019.
[60] European Commission, Communication: A European Data Strategy, https://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1593073685620&uri=CELEX:52020DC0066, 19 February 2020.
[61] Where even their own submarine cables are laid, see for Google, http://www.datacenterknowledge.com/google-alphabet/three-new-submarine-cableslink-google-cloud-data-centers; and for Microsoft and Facebook, https://thenextweb.com/facebook/2017/09/22/microsoft-and-facebook-just-laid-a-160tbpsundersea-cable-17000-feet-deep/.
[62] See farewell speech Jan Smits, https://pure.tue.nl/ws/portalfiles/portal/99880344/Rede_Jan_Smits_LR_15_06_2018.pdf.
[63] See, e.g., Cloud principles JenV, p.2, and European Commission/DIGIT (Appendix 3 - EU Cloud Policy).
[64] This problem is also called out by the European Commission. See European Data Strategy, p. 7. The financial sector (banks, supervisory authorities, etc.) also analyzes the strategic aspects of its own cloud policy. The European Securities and Markets Authority (ESMA) opened the consultation of its directive on cloud outsourcing on June 3. Steven Maijoor, the chairman of ESMA, explained "Financial markets participants should be careful that they do not become overly reliant on their cloud services providers. They need to closely monitor the performance and the security measures of their cloud service provider and make sure that they are able to exit the cloud outsourcing arrangement as and when necessary." https://www.esma.europa.eu/press-news/esma-news/esma-consults-cloud-outsourcing-guidelines.

of the large tech companies to nip competition in the bud by systematically purchasing innovative startups is now being investigated by the American Federal Trade Commission.[65]

Dependence on foreign providers brings with it control from other countries, which have different rules of play with regard to espionage, privacy, and government access to data. For purposes of data analytics, data may well be held either unencrypted in the cloud or with keys held by the cloud provider, which creates foreign interception risks. We will go into these specific dependencies in detail below.

3.2 Cybersecurity threat assessment: the Netherlands

The National Coordinator for Counterterrorism and Security publishes an annual *Cybersecurity Assessment Netherlands*, which provides insight into the digital threats, interests, and resilience in the field of cybersecurity in relation to national security. The Cybersecurity Assessment Netherlands 2019[66] (**CSAN 2019**) reports that there is a "permanent digital threat" in the Netherlands, that the largest (and ever-growing) threat comes from state actors, that countries such as China, Iran, and Russia have offensive cyber programs specifically aimed at the Netherlands, both to achieve geopolitical and economic objectives at the expense of Dutch interests, and in which disruption and sabotage of our critical infrastructure have the greatest impact because of its potentially socially disruptive effects.[67] This picture is perpetuated in the CSAN 2020.[68] Specifically, it is reported that a number of the Dutch top industrial sectors are (or have been) targeted by digital espionage. This mainly concerns high-tech, energy, maritime, and life sciences & health.

The CSAN 2019 also notes that the digital supplier chain (and *Managed Service Providers* in particular) is increasingly vulnerable, that cyber-attacks were "very successful" in the reporting period, and that these are expected to "increase further" in the future.[69] The CSAN 2020 again perpetuates this picture and observes that the supplier chain in particular is being abused because actors are looking for the weak link in chains on which the intended target depends.[70] The U.S. National Security Agency also explicitly warns of the risks associated with the use of cloud services.[71] Precisely because the cloud providers serve so many customers worldwide, their services are a constant target of APTs (*Advanced Persistent Threats*), not only of cyber criminals but also, and above all, of state actors.[72]

The CSAN 2019 further explicitly notes that the dependence on the small group of international suppliers entails risks for national security and the sovereignty and autonomy of the Dutch State and the European Union.[73] Dependencies arise because a limited number of suppliers *de facto* determine the standards, making it possible to strengthen their position in relation to other suppliers, and because the social impact of a disruption or digital attack can be large because many different processes or services depend on a limited number of suppliers. The dependency on this limited number of providers

[65] https://www.ftc.gov/news-events/press-releases/2020/02/ftc-examine-past-acquisitions-large-technology-companies.
[66] Cybersecurity picture Netherlands 2019, https://www.nctv.nl/documenten/publicaties/2019/6/12/cybersecuritybeeld-nederland-2019.
[67] CSAN 2019, p. 7.
[68] CSAN 2020, p. 19, https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
[69] CSAN 2019, p.18; see also AIVD Annual Report 2018, p. 8 https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018
[70] CSAN 2020, p. 19. It is reported that IBM also sees an increase in the use of legitimate tools instead of malware: more than half of the cyber attacks (57 percent) used general management applications.
[71] NSA Releases Guidance on Mitigating Cloud Vulnerabilities | CISA
[72] See, for example, Reuters 2019, Cloud Hopper attack: Eight of the world's biggest technology service providers were hacked by Chinese cyber spies in an elaborate and years-long invasion, Reuters found. The invasion exploited weaknesses in those companies, their customers, and the Western system of technological defense. https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.
See also: Crowdstrike, 2020, About 2019 trends: An alarming trend in targeted ransomware operations is the compromise of managed service providers (MSPs). Subsequent use of remote management software can enable the spread of ransomware to many companies from a single point of entry. WIZARD SPIDER also targeted this sector and impacted cloud service providers. Ransomware is BitPaymer, REvil, Ryuk.
[73] CSAN 2019, pp. 7, 11, and 22.

also creates a dependency on a limited number of countries. These countries apply different rules with respect to privacy and the provision of data, and they can also force the providers to cooperate in (economic) espionage activities and the provision of *backdoors*.

> A ***backdoor*** is a covert method of bypassing normal authentication in software or a computer system that allows hackers and intelligence services to gain illegal access.

Finally, now that cyber threats are high and cloud services are inherently vulnerable, it is important as a customer to be able to (i) monitor the cloud infrastructure for incidents, (ii) perform digital forensic analysis in the event of incidents, and (iii) take mitigating measures. Here, too, specific dependencies arise.[74] In the meantime, both the national government and the Ministry of Justice and Security (including the National Police)[75] have drawn up so-called cloud frameworks for assessing cloud projects, in which the specific risks and dependencies are identified and addressed. The Cloud Framework drawn up by the Ministry of Justice and Security provides a good overview of the *specific dependencies* in terms of threat detection and incident response.[76] When studying the Cloud Frameworks, it is striking that they mainly focus on the direct requirements for a specific cloud project and that they do not include broader considerations of digital sovereignty. We will come back to this later.

3.3 Extraterritorial claims

3.3.1 Access to data by foreign powers

If data are placed in a SaaS cloud, it is possible that these are accessible to foreign states. Although the example of the U.S. CLOUD Act (CLOUD = *Clarifying lawful overseas use of data*) is always mentioned in this context,[77] this is a *safeguarded* possibility for U.S. *law enforcement authorities* to issue and require U.S. cloud providers to hand over data stored on their servers in another country, such as the content of emails, documents, photos and videos, etc. This claim requires a *warrant* from a U.S. court based on the legitimate expectation that the data will provide evidence for the investigation of the crime (*probable cause*).[78]

The Dutch law enforcement authorities also have powers to demand evidence in certain cases, and European legislation is now at an advanced stage, aimed at improving cross-border access to *e-evidence*

[74] For a specific overview, see ENISA paper "Exploring Cloud Incidents," June 2016, in which the technical, organizational, and legal bottlenecks are discussed for both Iaas, PaaS, and SaaS.

[75] The memorandum Exploration of Cloud Policy for the Dutch Central Government, November 29, 2019; the joint documentation for assessment of cloud services JenV: Cloud JenV principles of September 27, 2019; Cloud assessment framework JenV of December 12, 2019; Cloud PIA Model [undated]; Quickscan Information Security JenV of January 2, 2019; and Cloud specific BIO measures JenV of September 27, 2019. The cloud framework of the national police has been drawn up, but has not yet been published.

[76] See, for example, Cloud *specific BIO measures* JenV, para. 4.1 – 4.3:
Incident response. Cloud providers are reluctant to share all kinds of log files and data, especially when these contain data from other customers. In addition, it is not self-evident that if an incident occurs in the cloud environment of the cloud provider, this incident (or a report of it) will also find its way to the Ministry of Justice and Security.
Forensics: Unconditional access to log files and other data is usually a prerequisite for handling incidents efficiently and effectively. However, cloud providers will not be able to share all log files and data, especially if they contain data from other customers.
Logging and monitoring: With the transition from on-premise to cloud environments, the way logging and monitoring is formed is changing. The migration of applications and their data to the cloud provider's systems often leads to (a sense of) loss of control and visibility of log data.

[77] See Rijks Cloudkader, paragraph 3 and letter in next note.

[78] Letter from the Ministry of Justice and Security to the House of Representatives regarding the CLOUD Act, dated October 5, 2018. This letter points out that cloud providers have the possibility of contesting such an order by appealing to the U.S. court in case of conflicting legal rules, according to the *comity procedure within the* meaning of the CLOUD Act. Our information is that the chance of success of such an appeal is very small. The U.S. court also has the option to impose a so-called *gagging order* on the cloud provider, which means that the cloud provider may not inform the client that it has received such an order.

between Member States for European law enforcement authorities.[79] To this end, a European Provisional Warrant and a Detention Order will be created that can be sent to Internet service providers offering services in the EU. The European Commission is also negotiating a bilateral agreement with the United States to allow for cross-border requests for electronic evidence.[80]

In terms of control over European data, more worrying from a sovereignty perspective is that U.S. *intelligence agencies* have certain powers for espionage and counterterrorism purposes to intercept foreign data *in transit* to the United States on transatlantic cables, and also have powers to collect data from U.S. cloud providers if they are hosted on servers in the United States.[81] Two specific interception powers[82] have recently led the European Court of Justice in the well-known *Schrems II judgment*[83] to rule that U.S. law does not provide an equivalent level of protection to personal data of European citizens after being transferred to the United States. U.S. law does not meet the requirements of the General Data Protection Regulation (**GDPR**) and the European Charter of Fundamental Rights of the European Union. The judgment has far-reaching consequences because in countries such as China, Russia, and India, authorities have similar interception powers to U.S. authorities. Therefore, data transfers are also under discussion for these countries.

The Court leaves open the possibility for organizations to take supplementary mitigating measures that in specific cases address the shortcomings, which would allow transfers to still take place.[84] Since U.S. intelligence agencies are not bound by contractual measures between the data exporter and importer, an obvious solution is to seek additional protection in data encryption. The data can then still be intercepted, but the foreign states can do little with this. In this context, it is often overlooked that encryption is only possible for *data at rest* and for *data in transit*. Encryption is so far practically impossible when data are being processed (*data in use*). Here too we see technical innovations in which data in *use* can also be encrypted (so-called *homomorphic encryption*).[85] U.S. cloud providers are the first to come up with practical applications here.[86] This form of encryption ensures that U.S. intelligence services do not have access to identifiable data, even when obtained when the data are in use. At the same time, it ensures that the providers themselves can analyze the data in order to generate insights. This innovation will therefore further strengthen the dominant position of these providers.

> ***Homomorphic encryption*** is a form of encryption that allows operations to be performed on the data without first having to decrypt it.

[79] Regulation on European Production and Preservation Orders for electronic evidence in criminal matters COM(2018) 225 final https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN en Directive laying down harmonized rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings, COM(2018) 226 final.

[80] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890

[81] For a (still up-to-date) overview of the possibilities of interception by U.S. intelligence services of data of non-Americans, see Summary of U.S. Foreign Intelligence Surveillance Law, Practice, Remedies and Oversight, Ashley Gorski, American Civil Liberties Union Foundation, August 30, 2018, https://www.aclu.org/sites/default/files/field_document/cjeu_schrems_report_final_august_30_2018.pdf. This report dates from 2018

[82] This concerns the powers of U.S. intelligence agencies under Section 702 of the Foreign Intelligence Surveillance Act (**FISA**) and Executive Order (**EO**) 12333.

[83] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, ECLI:EU:C:2020:559 (July 16, 2020), http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=10382780.

[84] Ibid, paragraph 133.

[85] See on this topic: Fact and Fiction of Homomorphic Encryption, https://www.darkreading.com/attacks-breaches/the-fact-and-fiction-of-homomorphic-encryption/a/d-id/1333691.

[86] Zie for offering Microsoft: https://azure.microsoft.com/en-us/blog/dcsv2series-vm-now-generally-available-from-azure-confidential-computing/; IBM: https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/ and Google: https://eprint.iacr.org/2019/723.pdf.

3.3.2 Export restrictions imposed by foreign powers

The Netherlands and the EU are increasingly affected by export restrictions as a result of the increasing trade and ideological tensions between the United States and China. Recent examples are the U.S. ban on Huawei as a provider of U.S. telecom infrastructure, mentioned in the introduction, and the restriction on Huawei purchasing computer chips produced with U.S. technology outside the United States.[87]

This plays a role throughout Europe in the choice of suppliers for 5G equipment, for which Huawei is an important potential candidate. If these tensions persist, it should be taken into account that restrictions will extend to other equipment, such as the Huawei servers that support cloud services, the presence of Chinese suppliers in the Internet of Things, cameras, airport scanners, and other surveillance equipment, and drones of Chinese origin. Giving in to U.S. pressure will potentially in turn lead to further Chinese pressure on European governments, including threats of Chinese import restrictions on European equipment and products.

These examples show that the Netherlands and the EU are limited in their sovereignty by geopolitically motivated measures taken by third countries, in particular the United States and China. As a result, 5G, a critical digital infrastructure, is likely to become more expensive as the *multivendor choice* decreases. This ultimately affects our digital sovereignty and makes it more urgent for us to develop our own offerings as well in order to make us less dependent on a multivendor strategy.

4 Approaches to digital sovereignty

In practice, we see three approaches to strategic autonomy, i.e., to achieve digital sovereignty. The first is a *risk management approach*, based on *state of the art* and *best effort*. Examples are the NIS Directive and the European General Data Protection Regulation (**GDPR**). The cybersecurity obligations under these regulations are *risk-based*, where the security measures must be appropriate in light of the state of the art, the implementation costs, and the context (how critical is the system and how sensitive are the application and data).

The second approach is based on relying on strategic partners who are *like-minded*, i.e., entering into strategic partnerships. Like-minded partners can be other states as well as companies, or both, in a public-private partnership. The primary intention is to exclude dependencies on third parties that are not like-minded or to limit them to exceptions (such an intention does not exist in the risk management approach). An example is the aforementioned *European Cloud Federation Initiative* (a public-private initiative). With legislation, there can be strict obligations between the like-minded parties. An example is the *EU Foreign Direct Investment Regulation*, which imposes rules for joint assessment of foreign investments (such as company takeovers) where *essential interests* of member states and the EU may be compromised. Examples of even more limited, inter-state, strategic partnerships are *Maximator*,[88] the five party signals and crypto analysis cooperation (Denmark, Sweden, Germany, The Netherlands and France), the *Five Eyes Alliance* in the field of intelligence (United States, UK, Canada, Australia, and New Zealand) and the SOG-IS cooperation for security certification by 13 European countries.[89] Strategic partnerships can also be combined with *strategic interdependency*, in which *not-like-minded* parties on selected topics are subject to mutual

> **Strategic partnerships can also be combined with *strategic interdependency*, in which *not-like-minded* parties on selected topics are subject to mutual dependencies.**

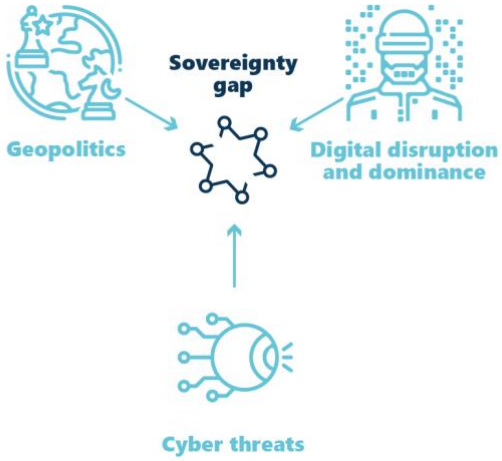
[87] https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html
[88] Bart Jacobs, Maximator: European signals intelligence cooperation from a Dutch perspective, Intelligence and National Security, Volume 35, 2020, Issue 5, https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1743538?src=recsys&.
[89] https://www.sogis.eu/.

dependencies (in EU policy, this is called *open strategic autonomy)*. This concept also has its roots in the military world, such as in arms control treaties.[90]

The third approach is to work together on a global level to find solutions in the common interest (*global common goods*). These go beyond the national interest, or at least do not conflict with it. An example is the Internet as the pioneers originally envisioned it. For some, this vision was motivated by ideology about sovereignty[91] or by techno-idealism. This ideal has proved to be untenable, and the Internet is now increasingly becoming a splinternet.[92] Nevertheless, the Internet still has *global common goods,* such as the Internet domain name system[93] that is largely managed by the global organization ICANN. The *global common goods* approach is also known in other areas. One of its great successes has been the recognition and protection of the ozone layer as an asset and interest of mankind as a whole, thanks to the Montreal Protocol of 1987.

The three approaches do not completely exclude each other, but where they overlap, we speak of the exceptions to the rule. Important, therefore, is the primary starting point of the approach: risk management, strategic cooperation of like-minded parties, or the global common interest. The diagram below shows the three approaches.

Fig. 2. Sovereignty gap



The importance of distinguishing between the three approaches in the context of this article is that the choice of primary approach influences relations between states, with constitutional consequences. In a *global common goods* approach, we think of international agreements in which all countries can participate, such as within the United Nations. For *strategic partnerships*, we think of agreements with an exclusivity of participants such as legislation binding an exclusive group of states (for the Netherlands primarily the EU) or contractual private-public partnerships. For the risk management approach, the whole spectrum of soft and hard agreements is possible, on a national, EU, bi-/multilateral, or global level. Incidentally, we see in the risk management approach that more often the private sector is in charge, rather than the government, even to such an extent that President Macron bemoaned that we put our sovereignty in the hands of the telecom industry.[94] We will discuss this in more detail later.

Due to the wide variety of the reasons why our digital sovereignty is under pressure and rapid geopolitical developments, there is no *one-size-fits-all* solution available. The most obvious way to support our sovereignty integrally is through a 'smart' combination of the three approaches.

A 'smart' approach also means making a cost-benefit assessment. Earlier it was said that it is neither realistic nor desirable for the EU, let alone the Netherlands, to want to develop all kinds of technologies entirely under its own management. Globalization has brought enormous benefits, certainly for the

[90] Paul Timmers, Strategic Autonomy and Cybersecurity, https://eucyberdirect.eu/wp-content/uploads/2019/05/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf, May 2019.
[91] Well known is the Declaration of the Independence of Cyberspace van John Perry Barlow, one of the pioneers of the Internet: "Governments [...] You are not welcome among us. You have no sovereignty where we gather."
[92] Kieran O'Hara and Wendy Hall, https://www.wired.co.uk/article/internet-fragmentation, December 24, 2019.
[93] The domain name system, or DNS, translates internet addresses, such as 145.58.22.3, to more understandable names, such as NPO.nl.
[94] The Economist, November 9, 2019.

Netherlands. Balancing technology and protectionism can hinder global trade and thus cost prosperity and jobs in the Netherlands. The Netherlands would therefore do well to take stock of its dependencies and reduce one-sided dependencies. This should happen not only within the well-known partnerships of the EU and NATO, but we will also have to actively look for countries in other parts of the world that share characteristics such as democratic politics, an open economy, and a policy of peaceful conflict resolution.[95]

Cost-benefit considerations must also be made where sovereignty concerns the protection of values and culture. This is a discussion that should also be conducted in politics. How much are we prepared to invest in our own e-identity solutions to prevent everyone logging on to digital services with a Google or Facebook account? How much risk are we prepared to take that confidence is lost in our justice system by relying on foreign cloud providers? Do we find it acceptable that the big tech companies actually determine what is and is not available on social media?

5 What do we do about it and why is it difficult?

In this chapter, we analyze a number of actions taken to strengthen digital sovereignty, at international, European, and national levels. Again, we will mention the constitutional relevance. Next, we will give three illustrative examples: the cloud strategy, cyber-resilience in the NIS Directive, and e-identity. We conclude with a number of obstacles and challenges, as a stepping stone to the final chapter, which outlines a perspective for the future.

5.1 International level

It is particularly difficult to take action against cybercrime at the national level because ICT systems are being penetrated remotely. It is also extremely difficult to take international action on this – for example, by imposing sanctions – because the perpetrators leave virtually no trace or can impersonate another party (this is the attribution problem in cybersecurity). Where cyber attacks are carried out by foreign states or where cyber criminals are supported by foreign states, requests for legal assistance to these states will not be heard.

The Netherlands, therefore, is strongly committed to making international agreements on standards for the responsible behavior of governments in cyberspace, especially in the United Nations and is consistently committed to the applicability of international law to cyberspace.[96] The EU member states are also trying to strengthen their external legitimacy by acting jointly as the EU in cyber conflicts. To this end, a *cyber-diplomacy toolbox* has been developed that provides escalation procedures. Modesty compels us to acknowledge that these means, and also the UN process, are little effective for the time being. Undermining democratic processes, the use of cyber-weapons in international conflicts, and cyber-espionage continue unabated.

The Netherlands is also a partner in international initiatives for peace and stability in cyberspace, such as the *Paris Call for Trust and Security in Cyberspace*[97] and the *Geneva Cyberspace Accord*.[98] These initiatives do not create international law, but can be trailblazers. We do see a degree of distrust here when large companies are the penholder or even the leader of such initiatives and then take on actions

[95] The WRR specifically mentions as examples countries such as South Korea, Chile, Canada, and New Zealand, see Hollands Spoor debatten strategieberaad Rijksbreed, and WRR, Verslag Toekomst multilaterale orde, p. 3. The EU is also committed to active cyber-dialogues in this sense with, among others, Japan and South Korea.

[96] See for a comprehensive discussion on the applicability of international law: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press 2017. See further collected papers of the Koninklijke Nederlandse Vereniging voor Internationaal Recht, 147: International Law for a digitalized World, October 2020 as well as Eneken Tiik, International Law in Cyberspace: Mind the gap, https://eucyberdirect.eu/content_research/international-law-in-cyberspace-mind-the-gap/

[97] https://pariscall.international/en/.

[98] https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

and status that used to be the exclusive domain of governments. One example is the Geneva Cyberspace Accord, an initiative of Microsoft.

Creeping loss of sovereignty also occurs where the industry, through international standardization, *de facto* sets the standards and governments play the second violin. An example is 5G – a critical digital infrastructure – where the telecom industry sets many of the security standards.[99] There is a strong presence of Chinese companies in these kinds of forums. Some suspect the Chinese government of being the driving force in the background here.[100] 5G is an example where the internal legitimacy of the state is at stake because the state cannot be sufficiently strong externally, i.e., where its external legitimacy is too weak.

Creeping loss of sovereignty also occurs where the industry, through international standardization, *de facto* sets the standards and governments play the second violin.

Digital sovereignty, therefore, also concerns the ability to determine *de jure* and *de facto* international regulations, both as an individual state and increasingly with like-minded partners. These partners should be sought particularly in the EU, but the Netherlands has historically also had close ties with the UK and the United States in the area of security. Despite the recent geopolitical tensions with these countries, these ties remain an opportunity to strengthen Dutch digital sovereignty. The joint action with the UK against Russia's digital espionage against the OPCW in The Hague is an example of this.[101]

5.2 EU level

For a large number of reasons, it is obvious to join forces within an EU context. In the EU context, we can strengthen our sovereignty in all three approaches (risk management, strategic partnerships, and global shared interest).

In the context of risk management, we can, for example, further mitigate cyber risks in the upcoming revision of the European Network and Information Security Directive (**NIS Directive**).[102] Below in the case study, we analyze what a revision from a sovereignty perspective on that Directive would mean.

Within the EU, we can also act inter-state with like-minded parties in technology initiatives in which only EU member states are allowed to participate, such as quantum encryption – thus, in the form of a strategic partnership. We can also think of strengthening exclusive EU regulations such as the *Foreign Direct Investment* Regulation.

The problem is that digital sovereignty easily affects national security, which under the EU treaties is reserved for the Member States.

Finally, in the EU context, we can also focus more on open source development and associated standardization for the global good, such as for the cybersecurity of global logistics systems. Putting the EU on the agenda in this respect also gives us more clout and negotiating power to make agreements at a global level.

Although the EU takes and can take initiatives in a large number of areas to strengthen 'digital sovereignty,' there are a number of obstacles here. In essence, the problem is that digital sovereignty easily affects national security, which under the EU treaties is reserved for the Member States and where the European Union

[99] Paul Timmers, Geopolitics of Standardisation, April 9, 2020, https://directionsblog.eu/the-geopolitics-of-standardisation/.
[100] See the references in Paul Timmers, Geopolitics of Standardisation, https://directionsblog.eu/the-geopolitics-of-standardisation/, April 9, 2020.
[101] https://www.dvhn.nl/binnenland/Defensie-Russische-actie-tegen-OPCW-verijdeld-23618009.html.
[102] European Commission, Annexes to Adjusted Workprogramme 2020, https://eur-lex.europa.eu/resource.html?uri=cellar%3Af1ebd6bf-a0d3-11ea-9d2d-01aa75ed71a1.0006.02/DOC_2&format=PDF.

has a very limited mandate.[103] Article 4(2) of the Treaty on European Union states: "The Union […] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

It is clear that this Article 4(2) is about *national* sovereignty without mentioning it in so many words. The Treaty provides no references, let alone foundations, for *European* sovereignty (the word *sovereignty* does not appear at all in the European treaties).[104] This also means that, for example, the *Regulatory Impact Assessment*, an analysis that is intended to motivate and justify proposals for new European legislation, does not currently provide a framework for analyzing and weighing up the potential impact on sovereignty of the member states and the EU as a whole.

The restriction of the *European* mandate to guard *national* sovereignty has the opposite effect at the present time. Whereas, due to digital and technological developments, Member States are no longer able to protect their sovereignty on their own, and the limited European mandate undermines national security. We illustrate this below with the case study on the NIS Directive.

The fact that the limited European mandate is unnecessarily constraining here is reflected in the recently increased willingness of member states to cooperate at the European level in the digital domain and to pool or share sovereignty. A telling example is 5G security. The member states have asked the European Commission to draw up a joint direction for 5G security, even though the concerns in this area primarily concern national security. This was unthinkable not so long ago.

5.3 National level

There are currently very few actions to be mentioned that are taken at the national level to protect our digital sovereignty.[105] In fact, our observation is that the Netherlands currently has insufficient insight into our new dependencies and is therefore unable to implement sufficiently proactive coordinated policies. The new technologies are so intertwined that with a one-sided focus on cyber resilience, the greater implications for the digital sovereignty of the Netherlands are missed out. Illustrative here is the letter from the Minister of Foreign Affairs on behalf of the Cabinet to the Lower House of Parliament, dated April 17, 2020, regarding the national security strategy.[106] Although it touches on the subject of *economic security*, this is triggered by (and limited to) the discussion about the introduction of the 5G network, concerns about the export of critical technologies to non-affiliates, and economic espionage by China. The role of technology in society is then mainly characterized as an asset in the shift of geopolitical power relations, threatening technological dependencies. The Cabinet then considers that no further specific measures are needed because technological cooperation and mutual dependencies are advantageous for an open and innovative Netherlands.

> "Technology, *in addition to* its great economic and social value, is an indispensable asset in the shift of geopolitical power relations. There may therefore be real threats to technological dependencies on which the Netherlands and the EU must make an independent assessment. The government does not close its eyes to these security risks, but at the same time recognizes that mutual dependency and interdependence can also contribute to stability and security. For an open and innovative country such as the Netherlands, important risks lie in the politicization of the application and cooperation in the field of technological progress."[107] (emphasis added)

[103] See on the European Security and Defence Policy, Adviesraad Internationale Vraagstukken, *Europese Veiligheid: tijd voor nieuwe stappen,* June 2020.
[104] Apart from a very limited reference to some territorial issues under UK sovereignty.
[105] We are still in the exploratory phase, where the Cyber Security Council has announced that it will issue an advisory report on digital sovereignty, and the Ministry of Economic Affairs has also set out a research assignment.
[106] https://zoek.officielebekendmakingen.nl/kst-33694-57.html.
[107] The Parliamentary Letter does, however, refer to protective measures such as the Wet Ongewenste Zeggenschap Telecommunicatie (Act on Undesirable Control of Telecommunications).

In our view, this analysis lacks a more elaborate and balanced consideration when it comes to digital technologies. Namely, a consideration of both their *value* to the economy and society as well as their *threat to* our essential economic ecosystems and trust in the rule of law and democracy. If this deepening is made, a more balanced menu of measures can also be developed. A striking example of the lack of broader sovereignty considerations is our government's cloud policy. Earlier, we saw that within the Netherlands, different cloud frameworks have been drawn up, which are not binding and make different policy choices in important areas.

Furthermore, the cloud frameworks primarily address the direct requirements of a specific cloud project and do not take into account broader considerations of digital sovereignty. As a result, government agencies weigh up the benefits of public cloud (better security, better functionalities) on a project-by-project basis against the specific dependencies in the project in question. Increasing dependencies and loss of sovereignty are not taken into account. As a result, for each project, the decision can be justified, but ultimately these decisions together do threaten our sovereignty (an example of *The Tragedy of the Commons*).[108] The first case study discusses the extent to which European policy and initiatives can change this.

5.4 Case studies

5.4.1 Cloud / GAIA-X

The dependencies of foreign parties and their impact on the EU's digital autonomy and competitiveness have led to a series of EU policy proposals.[109] The main aim of these proposals is to arrive at a joint European digital innovation strategy and agenda, not only for the cloud, but also in the field of AI, and to create so-called *European data spaces*. These proposals are prompted by the concern that these facilities and the related data and knowledge are in danger of coming under foreign control.

Data spaces. An important part of the policy initiatives is to ultimately unlock the value of European data for Europe itself. Clients now put their data in the cloud of the hyperscalers, creating silos as a result of which each user does not have enough data available for AI-related innovation. The aim is to create common data spaces for certain clusters of organizations with common interests (e.g., a certain industry or hospitals, but also governments), so that the scale of data required for innovation for this group can be achieved.

Scaling up through interoperability. The aim of the proposals is to further achieve the required *scalability* of the cloud infrastructure for AI-related innovation, not by creating Europe's own vertical hyperscalers, but by networking (making interoperable) the current European offer of cloud infrastructure, enabling clients to scale up within that network. This is achieved by setting common technical standards and legal frameworks for the digital infrastructure and standardizing contract conditions. This form of interoperability goes beyond portability of data and applications from one vendor to another to prevent vendor lock-in; it really concerns the creation of open APIs, interoperability of key management for encryption, unambiguous identity and access management, etc.

The GAIA-X project is not as comprehensive as the European policy, but it is a concrete realization of the open interfaces, standards, and interconnection needed for the European policy. From a digital sovereignty perspective, the GAIA-X project is a logical and promising initiative.[110] The same applies to the other policy proposals. However, if we look at the policy proposals as a whole, our conclusion is

[108] The Tragedy of the Commons is, in fact, a conflict between individual and collective interests, in which the government's task is precisely to represent the collective interests.

[109] See in particular: European Commission, 'A European data strategy,' COM(2020)66, February 19, 2020; European Commission, White Paper 'On Artificial Intelligence - A European approach to excellence and trust,' February 19, 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*.

[110] In the Netherlands, a coalition of TNO and a number of industry associations are actively contributing to the GAIA-X project, https://www.agconnect.nl/artikel/nieuwe-infrastructuurcoalitie-wil-nederlandse-gaia-x-behoeften-representeren.

mainly that the proposals are not mandatory for the time being. At the moment, there is a high degree of non-commitment, which also means that the required coordination is lacking.

As a result, cloud choices made by Member State governments are currently at best subject to the specific requirements of national cloud frameworks for such outsourcing. The lack of binding European and Dutch cloud policies illustrates a more general pattern of lack of sovereignty considerations that we also see in other areas.

5.4.2 NIS Directive

The NIS Directive concerns the *cyber-resilience* of selected *essential services* such as water, energy, and transport facilities. The Directive also regulates three 'digital services,' namely electronic marketplaces, search engines, and cloud services. The NIS Directive takes risk management as its starting point and imposes cyber security obligations, as well as an obligation to report cybersecurity incidents. The member states must also set up so-called *Computer Security Incident Response Teams* and continue to cooperate with the other member states, both for strategic planning and to deal with incidents. This cooperation is required because incidents in critical facilities can have[111] serious cross-border effects and thus undermine the functioning of the EU internal market as a whole.

When the NIS Directive was proposed by the European Commission in 2013, digital sovereignty was not even known as a concept. The focus was on increasing Europe's cyber resilience. The proposals quickly led to tension with national security, which is reserved for the member states. This meant that the NIB directive in the negotiations was ultimately limited to harmonizing cyber risk management for our vital sectors, which require a territorial presence and only a few digital infrastructures.

The NIS Directive had to be transposed into the national legislation of the Member States by May 9, 2018. However, developments are moving so fast that it already appears that important cyber-vulnerabilities are not being dealt with while they do pose a risk to our sovereignty:

- Active abuse of social media and media in general (such as *fake news*), which is now the order of the day and undermines our democracy and values.[112]
- Vulnerabilities in IACS (or SCADA) systems of the industry in vital sectors such as production and supply of medicines.
- Stealing intellectual property essential to our economic future. According to the CSAN, such intellectual property is stolen on a large scale by foreign powers – in particular by China – and is one of the biggest threats to the economic future of the Netherlands.
- Educational and training platforms which have proven indispensable in COVID-19 times, are mainly operated by non-EU providers.

There are also new essential infrastructures that are completely European and do not fall under the NIS Directive. These thus transcend national sovereignty, do not belong to a single country, and are *de facto* already part of EU sovereignty. They can only be protected in a European context. Examples are:

- The European .eu domain name registration system. There are ongoing attacks on the Internet domain name systems, a major concern for ICANN, the international organization for domain name management. For example, the DYN attack (2016) led to the failure of the Internet in part of the United States.[113]

[111] CSR Advice Cyber Resilience IACS, p. 11, therefore advises to regularly measure international dependencies within the vital infrastructure during cyber exercises.
[112] Below we discuss the need for trustworthy electronic identities for organizations and citizens. When posts on social media for example can be authenticated (e.g., as an official communication from government), many fake news and deep fake issues may proactively be solved. See Bart Jacobs, iBestuur online, 9 December 2019, https://ibestuur.nl/weblog/teken-tegen-nepnieuws
[113] https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

- The announced *European Data Spaces*, such as for health data. These European-wide data infrastructures must play an essential role, for example, in the cross-border fight against infectious diseases such as COVID-19. The protection of these data spaces has yet to be regulated.[114]

On December 16, 2020, the Commission issued a proposal for a revised NIS Directive (**NIS2 Directive**).[115] At the same time, the Commission issued a significantly revised EU Cybersecurity Strategy, which is a non-legislative framework policy,[116] as well as a related proposal for a Directive addressing the non-cyber resilience of critical entities.[117] The NIS2 Directive has extended the scope and now – amongst others - includes the cybersecurity of domain name systems, social networking services platforms, and manufacturing systems of critical pharmaceuticals and medical devices. However, not all of the aforementioned weaknesses are addressed. The limited mandate of the EU where cybersecurity affects national security remains an obstacle, so this would also be easier said than done.

A second obstacle is that the NIS Directive is based on the *Internal Market* article 114 of the Treaty on the Functioning of the European Union (**TFEU**). The Internal Market concerns the free movement of goods, services, capital, and persons in the EU. It is not exactly obvious, for example, that cybersecurity in order to protect intellectual property can fall under this basis. The alternative of leaving the protection of intellectual property to the national level is not very attractive. Attacks know no borders and are so sophisticated that smaller countries risk losing the battle. These will have to be protected in a larger context.

As for combatting the abuse of social media (not for media in general), the Commission has taken a dual approach. Next to the cybersecurity risk management and incident reporting requirements of the NIS2 Directive, the Commission issued a proposal for a Digital Services Act of December 15, 2020, imposing due diligence requirements on social media providers as regards illegal content.[118] The definition of what has to be considered to be illegal content follows from other EU laws and their national implementations. More extensive identification and authentication measures to combat inauthentic use of platforms could also be envisaged (see the e-identity section below).

Finally, there are essential areas such as public health where the EU mandate is even more limited than that of the Internal Market. The table below[119] gives an overview of the provisions for which it can be argued that they should have mandatory cybersecurity, at least if we take sovereignty seriously.

[114] To a very limited extent, cybersecurity is mentioned in the Data Governance Act, a regulation on EU-wide data sharing (proposed by the European Commission on November 27, 2020).
[115] European Commission, 16 Dec 2020, COM(2020) 823 final, https://ec.europa.eu/digital-single-market/en/news/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union
[116] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 16 Dec 2020, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final, https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade
[117] European Commission, 16 Dec 2020, COM(2020) 829 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf
[118] European Commission, 15 Dec 2020, COM(2020) 825 final, Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN
[119] Paul Timmers, When Sovereignty Leads and Cyber Law Follows, October 13, 2020, https://directionsblog.eu/when-sovereignty-leads-and-cyber-law-follows/

Table 1. Cyber-resilience and legal basis in the Treaties

Cyber-resilience of	*Legal basis in the Treaties*	*EU mandate*
Selected physical and digital infrastructure	Article 114 TFEU Internal market	Strong
Telecommunications	Article 114 TFEU Internal market	Strong
Social media and media	Article 6(1) TEU, fundamental rights Art 114 TFEU Internal Market	Weak Strong
Industrial infrastructure	Article 114 TFEU Internal Market Article 173 TFEU Industry	Strong Weak
Intellectual property	Article 114 TFEU Internal market Article 173 TFEU Industry Article 182, 183 Research	Weak Weak Average
Internet domain .eu	Article 170 Trans-European Networks Article 114 TFEU Internal market	Strong Strong
European data spaces	Depending on the area, e.g.: Article 168 Public health Article 114 Internal Market	 Weak Strong
Education	No real legal basis	Absent

It follows from the above table that even if we would have tried to cover as many of the identified vulnerable areas in the NIS2 Directive as possible, the result would have been a jumble of legal bases: Internal Market (Article 114); Public Health (Article 168); Trans-European Networks (Article 172, the basis of .eu); Industry (Article 173), etc. In itself, it would have been possible to base the NIS2 Directive on more than one legal basis. However, the Commission has made the choice to base the NIS2 Directive, like its predecessor, exclusively on a single article, namely Article 114 TFEU: 'The proposed legal act would remove obstacles to, and improve the establishment and functioning of the internal market for essential and important entities by: establishing clear generally applicable rules on the scope of application of the NIS Directive, harmonising the rules applicable in the area of cybersecurity risk management and incident reporting.'[120]

Though the choice for a uniform legal basis is understandable as it is questionable whether the EU would benefit from complex legislation based on several articles from the EU Treaties, we note that the real common denominator for this legislation is not the Internal Market, but the protection of sovereignty. In the concluding chapter, we will address this question.

[120] European Commission, 16 Dec 2020, Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

5.4.3 E-identity

A similar reflection is needed for the ongoing revision of the eIDAS Regulation, which regulates mutual recognition in the EU of notified national electronic identities for citizens (eIDs). This Regulation encourages member states to make their electronic identification of citizens for logging on to digital government services (in the Netherlands: DigiD) also available for use by the business community for online e-commerce transactions.[121]

For e-commerce to flourish, important preconditions need to be properly safeguarded: security, trust, and reliability of the digital infrastructure. eIDs are a necessary pillar for this. In the physical world, we can hardly imagine economic transactions without certainties about the identity of a counterparty, about ownership of real estate, and whether someone is authorized to do something. To this end, the government in the physical world has developed a whole system of means and organizations, such as passports and identity cards, the land register for security of ownership of real estate, the chamber of commerce for security of powers of representatives of companies, notaries, and municipal desks. Legal frameworks and guarantees exist for these structures.

The government has developed DigiD for access to digital government services, but authentication of business representatives and authentication of citizens in the private domain have been left to the market for the time being. As a result, citizens do not yet have a secure and privacy-friendly eID that can be freely used for e-commerce.

At the moment, therefore, for almost every commercial service, citizens still have to login with the vulnerable system of user name combined with password and manually enter and disclose (always the same) personal data. To simplify login, many websites offer citizens the option to authenticate via their account with one of the major foreign platforms, such as Facebook, Apple, Amazon, Google, Alibaba, or Tencent. This creates large concentrations of both Dutch business and personal data on these platforms, which has a direct impact on our privacy and digital sovereignty.

The question is whether in the Netherlands we are sufficiently on track to establish a solid digital infrastructure that protects citizens and businesses in the digital age and facilitates economic growth in the next phase of the Digital Single Market.[122] Note that where for example posts on social media can be authenticated (e.g., as indeed coming from a minister or government official), many of the fake news and deep fake issues may be proactively solved.[123] The proposed Digital Services Act does require large online platforms that are designated as 'gatekeepers', to make a risk assessment of inauthentic use (e.g., identify posts to be likely a deep fake), fake but does not require trustworthy *authentication* as a risk mitigation measure.

Regarding the eIDAS Regulation, Ursula Von Leyen announced in her first *State of the Union* (September 2020) that there will be a European e-identity, against the background of the loss of control over the data of European citizens. This is a good step, provided that it is also linked to an obligation for companies (and in particular the aforementioned platforms) to *accept* the EU-wide eIDAS, and also the compatible DigID,[124] as a login tool. The sovereignty perspective therefore mandates not only a European e-identity, but also mandatory acceptance thereof in a revised eIDAS Regulation,[125] We note that the the proposed Digital Market Act does require the large platforms that are designated as gatekeepers to 'refrain from requiring business users to use, offer or interoperate with an identification service of the gatekeeper in the context of services offered by the business users using the core platform

[121] See recital 17 of eIDAS.
[122] The CSR does not think so; see CSR Advice Towards a secure eID system, November 7, 2019, https://www.cybersecurityraad.nl/binaries/CSR_Advies_eID_NED_DEF_tcm107-415886.pdf
[123] Bart Jacobs, iBestuur online, 9 December 2019, https://ibestuur.nl/weblog/teken-tegen-nepnieuws
[124] https://www.eherkenning.nl/vraag-antwoord/eidas
[125] A proposal by the European Commission is expected for early 2021.

services of that gatekeeper', however, this does not yet entail that the platform itself should accept the European e-identity for access to its core platform services.

6 Where do we go from here?

Developments continue, at a high pace and we see that sovereignty has now become *Chefsache* at the European level and in several Member States. However, the consequence of thinking in terms of sovereignty has not yet really penetrated into policy and legislation. The step we now have to take is the actual embedding of sovereignty thinking: in the Netherlands, as the Netherlands in the EU, and as the Netherlands in an international context. In this light, we give below a number of perspectives for the future, which are relevant under constitutional law. Here we go again from the international, to the European, to the Dutch level.

6.1 International embedding

The firm embedding of the Netherlands in the EU and international organizations (and its adherence to European legislation and international treaties) is both a limitation and an opportunity. It is a limitation because existing frameworks such as the Internal Market and GATT agreements limit the Netherlands' room for maneuver, for example in terms of restrictions on market access. The Netherlands can often not operate autonomously. But as argued, joint action in an EU context also offers an opportunity for the Netherlands to make its voice heard more strongly in an international context.

This is all the more the case if the protection of national or European sovereignty is in line with a *global interest* (and *vice versa)*. Good examples of this are managing critical Internet facilities such as the Internet domain name system, combatting cybercrime in the health sector, and setting standards for the *Internet of Things*. The implication here is that for digital sovereignty, our foreign policy is just as important as our domestic policy. Only through coherent policy is it possible to strengthen both the internal and external dimensions of sovereignty. To be able to play an international role, however, it is also necessary to be able to act as Europe. As we have seen, however, the EU has a limited mandate here. What can be done about this is set out in the next section.

6.2 European embedding and the inadequacy of the EU Treaties

In view of the limitations previously identified in the European mandate on digital sovereignty, it is time for us to think about strengthening the European legal basis for 'EU sovereignty-properly-understood'[126] in terms of strengthening, enlarging, and simplifying the Treaties. The Treaty provides openings for a limited Treaty amendment under Article 48 TEU. The disadvantage of this is that it would still remain patchwork, spread over more *internal policies*, such as the internal market, trans-European networks, and research and development. As far as we are concerned, we must therefore engage in the more fundamental debate, for example, in the context of the ongoing Conference on the Future of the European Union and Article 48(2) TEU.

We realize that some will shy away from this because it opens Pandora's box for all kinds of other treaty discussions. Others will object that further strengthening of European sovereignty goes too far, considering the populist argument surrounding Brexit.

The main arguments[127] for strengthening European sovereignty are:

- European joining forces strengthens national sovereignty. Almost every Member State is otherwise too weak in the fight against cross-border cyber-threats.

[126] This term suggests to address sovereignty in a specific perspective (as iillustrated in the subsequent paragraphs). It is inspired by the 19th century political scientist Alexis De Tocqueville (Democracy in America).
[127] Paul Timmers, When Sovereignty Leads and Cyber Law Follows.

- A strong European mandate contributes to the credible protection – and creation – of European sovereign assets. The domain name system .eu and European *data spaces* are telling examples.
- Owning its own strong digital facilities strengthens the EU's credibility in the world (*external legitimacy*) when it comes to making international agreements and Europe's position vis-à-vis the Internet giants.

Timmers[128] previously suggested that sovereignty, as interpreted above, can be strengthened by supplementing Article 3 TEU as follows: "the Union will strengthen sovereignty in the European Union insofar as it respects or strengthens the sovereignty of the Member States and contributes to common assets and interests of the Union, or strengthens the Union's position in the world." In this light, a debate in the Netherlands on sovereignty in the context of the possible revision of the Treaties would be desirable at the very least. This would not be a revolutionary step but simply in line with the *Zeitgeist*. Incidentally, these three arguments are not new, but have been part of the thinking about European cooperation for about 75 years. In fact, we are talking about adapting the Treaties to the 21st century.

In anticipation of the outcome of a more fundamental debate, we recommend that the Netherlands, in the European context, make a strong case for feasible interventions within the current treaties that can be leveraged to strengthen sovereignty. One tool for that is the recently revised EU Cybersecurity Strategy. The focus should be on *where sovereignty matters most*. One example *par excellence* is the initiative to realize a European e-identity. Providing reliable means of identifying citizens and businesses in order to facilitate trade is a core task of the government. In view of the common interests of the member states with regard to cybersecurity, it is also conceivable that the member states could *pool sovereignty* on specific subjects (such as through joint engagement in international standardization, e.g. on 5G or through cooperation of Security Operations Centres across the EU in a 'European Cyber Shield')[129] and thereby achieve increased European coordination even without fundamental debate.

For the same reason, it is possible to investigate more often whether the Netherlands can reach certain agreements with a group of member states, in a *coalition of the willing*.[130] For the viability of a project, it is often not necessary for all member states to commit themselves, but an initial critical mass is required. This can then be scaled up at a later stage with the affiliation of other member states. In this way, results can be achieved faster than via the vulnerable route of adapting the EU treaties.

Beyond the scope of this preliminary advice, the possible steps that can be taken against dominant market parties for market abuse and violation of consumer law and privacy laws to collect data from European citizens fall outside the scope of this preliminary advice. In the data economy, this often goes hand in hand, and it is particularly obvious to set up a central European supervisor for the enforcement of privacy legislation, just as it does for competition. At the European level, the enforcement by the competition, consumer and privacy authorities should also be coordinated on a mandatory basis.[131]

6.3 Dutch perspective

The Netherlands already has opportunities – also in a constitutional sense – to strengthen its digital sovereignty on a national level. The first steps are certainly not a revolutionary intervention, but rather a matter of 'common sense.' We give a number of suggestions below.

[128] Ibid.
[129] See The EU's Cybersecurity Strategy for the Digital Decade, 16 Dec 2020, ibid.
[130] This is also the first recommendation of the report of the Advisory Council on International Affairs, *European Security: time for new steps*, June 2020: The Netherlands should seek as much connection as possible with Franco-German initiatives for European security: https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2020/06/19/european_security
[131] Caleidoscopische handhaving tegen het datagebruik van ondernemingen, Svetlana Yakovleva, Wessel Geurtesen, and Axel Arnbak, Pre-advice of the Vereeniging Handelsrecht 2019, p. 77.

From national security to digital sovereignty. Earlier, we found that while our national security strategy addresses economic security, it does not sufficiently recognize that digital technologies not only have *value* for the economy and society, but also *threaten* our essential economic ecosystems and trust in the rule of law and democracy. We also noted that the Netherlands currently has insufficient insight into our new dependencies and is therefore unable to pursue a sufficiently proactive coordinated technology policy in the area of research, valorization, and industrial capabilities. This also requires that companies in the Netherlands operate in a flourishing ecosystem; an ecosystem in which they have the opportunity to grow through sufficient access to talent, data, and financing, among other things. To this end, it is necessary to make a conscious inventory of which startups, technology, knowledge, and infrastructure are of strategic importance, making it clear when sales to or departures from abroad could be detrimental to the Netherlands' strategic position. We then need to draw up a proactive strategy, which also includes strategic use of the *aggregate* purchasing power of the government.[132] Without such a comprehensive plan, our country will end up on an irreversible path of gradual erosion of our national technological and industrial capabilities.

Cloud policy. Specifically, with regard to cloud policy, our recommendation is to arrive at an integrated and binding cloud framework and to investigate how the Netherlands can maximally align with the concrete development of GAIA-X based on considerations of digital sovereignty and even to commit to it together with a group of member states. Meanwhile, Dutch cloud, hosting, and infrastructure companies have formed a coalition to contribute to GAIA-X.[133] A good connection requires that the purchasing power of the Dutch government is also used for our knowledge and competitive position in the longer term.

Coherent governance. Because the question of sovereignty is touching more and more areas of the economy, society and democracy, governance must take place centrally. The business community is more aware of this. ICT is now a strategic factor for competitiveness and is the subject of the board table (**C-level**).[134] The government is being driven in the same direction, but we see that the various departments mainly operate in silos and the necessary integration of policy is lacking. Although this has already been proposed on several occasions, it remains obvious to appoint at least a digital affairs coordinator who reports directly to the prime minister, with his own budget and perseverance power.[135]

Explanatory memorandum. Our legislative proposals must be substantiated and justified in an explanatory memorandum (in European policy development, this is the regulatory impact assessment). There is currently no framework to analyze and weigh possible impact on sovereignty. Such a framework should be made available as a matter of urgency prior to legislative preparation, in order to prevent sovereignty from remaining an afterthought.

---

[132] A Dutch example of a proactive strategy is the Defense Industry Strategy. This strategy assesses from a national security perspective (which also includes cyber threats) which knowledge, technology, and industrial capabilities the Netherlands needs to have in-house to safeguard our national security, and how this can be safeguarded with active Dutch innovation and industrial participation policies, with the Ministry of Defense acting more often as a launching customer.

[133] http://www.tno.nl/nl/over-tno/nieuws/2020/11/nederlandse-cloud-infrastructuur-coalitie-cic-eerste-stap-naar-slagvaardig-digitaal-nederland/

[134] C-level refers to the 'C' in the titles of directors of companies, such as CEO (Chief Executive Officer) and CFO (Chief Financial Officer).

[135] Although late in the day, a step in the right direction has been taken by the Dutch Lower House, which has now come to the conclusion that a separate standing committee for digitization should be set up, https://www.digitaleoverheid.nl/nieuws/tweede-kamer-krijgt-vaste-commissie-voor-digitale-zaken/
See also https://www.tweedekamer.nl/nieuws/persberichten/eindrapport-tijdelijke-commissie-digitale-toekomst-%E2%80%9Cupdate-vereist%E2%80%9D

About the authors

Prof. Dr. Lokke Moerel is professor of global ICT law at Tilburg University and Senior of Counsel with the leading global technology law firm Morrison & Foerster (Brussels). She provides strategic advice to the world's most complex multinational organizations on global implementation of new technologies, digital transformation and cyber security. She is a member of the Dutch Cyber Security Council (the advisory body of the Dutch cabinet on cybersecurity), member of the Monitoring Committee of the Dutch Corporate Governance Code, cyber expert on the European Commission's Horizon2020 Innovation Program and member of the Ethics Board tasked by the Dutch government with reviewing the implementation of the Covid tracing app. She received the 2018 International Law Office Client Choice Award for Best Internet & Technology lawyer Germany and the 2018 Acquisition International Global Excellence Award for Most Influential Woman in Data Protection Law.

Prof. Dr. Paul Timmers is research associate at Oxford University for cybersecurity and digital transformation, adjunct professor at European University Cyprus, visiting professor at Rijeka University, senior advisor to EPC Brussels, board member of Digital Enlightenment Forum and of the Estonian eGovernance Academy supervisory board. Previously he was Director at the European Commission dealing with EU legislation and funding for cybersecurity, digital health, smart cities, e-government. He was cabinet member of European Commissioner Liikanen, manager in a large ICT company, and co-founded an ICT start-up. Physics PhD from Nijmegen University, MBA from Warwick University, EU fellowship at UNC Chapel Hill, and cybersecurity qualification at Harvard.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.