



Strategic Autonomy and Cybersecurity in the Netherlands

Paul Timmers

Freddy Dezeure

January 2021

This study has been commissioned by the Cyber Security Council (CSR)



This document is a draft translation from Dutch to English

1	EXECUTIVE SUMMARY	4
2	BROADER CONTEXT AND HISTORICAL PERSPECTIVE	5
2.1	INTRODUCTION	5
2.2	STRATEGIC AUTONOMY AND SOVEREIGNTY	6
2.3	THE DIGITAL SECURITY RISKS	7
2.3.1	CASE: DISRUPTIVE RANSOMWARE	9
2.3.2	CASE: DISINFORMATION AND FAKE NEWS	10
2.3.3	CASE: LAWFUL INTERCEPT - SURVEILLANCE	10
2.4	STRATEGIC AUTONOMY APPROACHES	12
2.5	CASES	12
2.5.1	CASE: GPS - GALILEO	12
2.5.2	A BROADER PERSPECTIVE ON EUROPEAN SUCCESS STORIES	14
2.5.3	CASE: CLOUD - HYPERSCALERS	15
2.6	POLICY AREAS AND -INSTRUMENTS UNTIL RECENTLY	16
3	CURRENT SITUATION	17
3.1	CURRENT CASES AND TOPICS	17
3.1.1	CASE: MANDATE FOR CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE AND SERVICES	17
3.1.2	CASE: E-ID, DIGITAL SECURITY, DEEP SECURITY	19
3.1.3	CASE: 5G PROTECTION	20
3.2	RESEARCH AND DEVELOPMENT	23
3.2.1	GEOGRAPHICAL PERSPECTIVE	23
3.2.2	CASE: R&D IN HOMOMORPHIC ENCRYPTION AND DIFFERENTIAL PRIVACY	24
3.2.3	ACADEMIC EXPERTISE TO VALIDATE KEY TECHNOLOGIES	26
3.2.4	PRIVATE SPONSORSHIP OF ACADEMIC RESEARCH	26
3.3	R&D AND START-UP FINANCING (BUSINESS ANGELS, SEED, VC, PRIVATE EQUITY)	27
3.3.1	GEOGRAPHICAL PERSPECTIVE	27
3.3.2	CASE: STARTUPS IN PRIVACY PROTECTION TECHNOLOGIES	30
3.4	STANDARDIZATION AND MARKET STANDARDIZATION	33
3.4.1	CASE: PRIVACY-PRESERVING DATA PROCESSING	34
3.5	PROCUREMENT POLICY (PUBLIC AND PRIVATE)	36
3.6	ACQUISITIONS (M&A)	37
3.7	COMPARISON OF POLICY APPROACHES	38
3.7.1	THE AMERICAN APPROACH	38
3.7.2	THE BRITISH EXAMPLE	39
3.7.3	CHINA	40
3.7.4	THE SITUATION IN THE NETHERLANDS	41
4	POLICY INSTRUMENTS	42
5	ASSESSMENT FRAMEWORK	47
5.1	FOCUS	47

5.2	KEY TECHNOLOGIES	47
5.3	ASSESSMENT FRAMEWORK OVERVIEW	49
5.4	TRIGGER DIAGRAM	50
5.5	PORTER MODELS	53
5.6	RELEVANT DOMAINS, CONTROL AND STRATEGIC AUTONOMY TEST	54
6	APPLICATION AND VALIDATION OF THE ASSESSMENT FRAMEWORK	56
6.1	5G SECURITY	56
6.2	NIS DIRECTIVE	57
6.3	E-ID	57
6.4	HOMOMORPHIC ENCRYPTION	58
6.5	M&A OF A STRATEGIC AUTONOMY-ESSENTIAL COMPANY	58
6.6	EU POLICIES AND LEGISLATION	58
6.7	OTHER TRIGGER CASES	60
6.7.1	PROTECTION OF SENSITIVE PUBLIC SECTOR INFORMATION.	60
6.7.2	ESPIONAGE AND STEALING OF INTELLECTUAL PROPERTY.	60
6.7.3	ONLINE DISINFORMATION AND FAKE NEWS	60
7	RECOMMENDATIONS	61
7.1	STRATEGIC AUTONOMY IS CRUCIAL IN CYBER SECURITY	61
7.2	PROACTIVE AND COMPREHENSIVE APPROACH	61
7.3	REINFORCING EXISTING STRENGTHS	61
7.4	A PRACTICAL APPROACH	62
8	ANNEXES	64
8.1	ANNEX 1: CYBERSECURITY STARTUPS: SUCCESS AND FAILURE	64
8.2	ANNEX 2: LEGEND OF DOMAINS	65
8.3	ANNEX 3: PORTER MODELS	67
8.4	ANNEX 4: EXAMPLE OF MEASURES VS DOMAINS (5G-SECURITY)	68
8.5	ANNEX 5: AUTHORS	69

1 Executive Summary

Growing dependence on digital information systems means that the impact of cyber-incidents on our society, economy, democracy and fundamental freedoms is increasing. There are also new threats that have not been assessed before. So far, cybersecurity has rather been addressed from a technical perspective and not from the concern for strategic autonomy and sovereignty. Until 2017, strategic autonomy, and certainly in the digital domain¹, was almost unknown, while today it is *Chefsache*. Challenges and threats to strategic autonomy in cybersecurity are too important not to be viewed from a broad perspective and be taken up at the top.

This study analyzes strategic autonomy in relation to cybersecurity, both in general terms and from specific cases. The study also provides an impetus for a better understanding of "control" in this context. The analysis produced observations that guide methods and recommendations. The study provides a concrete assessment framework to address digital strategic autonomy in relation to cybersecurity in the Netherlands in a strategic and at the same time practical way.

The study contains a variety of insights that can provide a source of reflection and action. The proposed methods have been assessed against the cases. They can easily be put into practice in everyday situations.

There are many existing factors, structures and processes in the Netherlands that allow cybersecurity and digital strategic autonomy to be addressed in a permanent, coherent and integrated manner. However, many of them have still been applied infrequently or are not sufficiently known. But there's a good basis for greater impact.

Greater policy coherence and explicit prioritization of digital strategic autonomy is both desirable and necessary. Moreover, it would be valuable to combine reactive behavior with proactive monitoring and anticipation. This would also include connecting multiple policy areas and interests closely, with top-level governance (Whole-of-Government).

The various departments should make their cooperation permanent at operational policy level. Revising the organization and governance in view of digital strategic autonomy is an ambitious step. Nevertheless, the longer-term perspective is anchoring in the organization and governance of the Dutch government.

It is feasible in the short term, and highly relevant, to develop the cases from the study as a starting point for interdepartmental cooperation and to put the proposed methods into practice. Many of these cases are the result of concrete triggers that are urgent and relevant today or in the near future.

Equally, it is feasible in the short term to develop a number of concrete action points that will enable the Netherlands to demonstrate leadership within the EU and achieve impact that would create and sustain digital strategic autonomy with regard to cybersecurity.

¹ See terminology below. This document uses digital strategic autonomy rather than digital sovereignty where possible.

2 Broader context and historical perspective

2.1 Introduction

Since 2000 and accelerating since 2010, cybersecurity has been on the agenda. Cyber incidents did not seem to stop and – more worrying - threaten critical infrastructure. Alongside criminals, increasingly state actors have appeared on the scene. As long ago as 2007, there was a real cyber-attack on Estonia, attributed to Russia. In Ukraine, part of the electricity network was shut down in 2015 and 2016 (also attributed to Russia). Large-scale theft of intellectual property, including by the well-documented APT1 group², urged President Obama to agree with President Xi Jinping on a code of conduct, however with little impact. The Mirai Internet of Things attack in 2017 shut down part of the Internet.

Table I. Frequency of use of the notion of “sovereignty” as related to the digital (using ProQuest Central).

	Data sovereignty		Technological sovereignty		Digital sovereignty	
	Academic	Other	Academic	Other	Academic	Other
Before 2011	0	23	12	81	0	6
2011–2014	18	794	6	101	2	49
2015–2018	89	2459	20	131	22	239

3

We began to realize that the functioning of the state may be fundamentally threatened. Either by shutting down critical facilities or by systematically leaking national knowledge and continuous disturbances (a situation of ‘unpeace’). The preliminary conclusion was that states could not adequately defend their sovereignty with their traditional military/defense approach to national security and inter-state consultations. Kello calls it the sovereignty gap⁴.

However, the situation has worsened. Developments in Europe increasingly took distance from sovereignty. We unconditionally embraced and encouraged digitization. A great success, especially for US and Chinese suppliers. The cloud market in Europe is two-thirds owned by Amazon, Microsoft, IBM and Google. Social media are almost completely American. European telecom hardware and software vendors were forced to give up on a massive scale to Huawei and ZTE. European countries' autonomy is now threatened not only by third countries but also by non-European mega-companies.

More indicators turned to red when critical European technology fell into foreign hands: ARM went to Softbank and then to Nvidia, Kuka robots was sold to Chinese Midea.

The story is not finished: fake news and hacking in the 2016 US elections and in several European countries showed that cyber threats were no longer confined to the economy. Even democracy is under threat.

Europe was already wobbling when it became a game ball in the geopolitical game of the US and China. Europe was targeted in increasing transatlantic tensions such as around NATO and was a ‘sitting duck’ in the rising trade war between the US and China. China’s creeping infiltration into Europe with its ‘Belt and Road’ initiative led to growing unrest in Brussels.

² Mandiant, 2017, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

³ Stéphane Couture, <http://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/>

⁴ Lucas Kello, *The Virtual Weapon and International Order*, Yale University Press, 2017

Merkel stated that it was time for Europe to take control of its own future. Macron lamented that we had given sovereignty to (telecom) companies⁵.

A systematic analysis shows that until 2016 strategic autonomy was only known in the military/defense thinking in France (“force de frappe”) and the economic/military thinking of India (Washington independence, Moscow, and Beijing). But in the pressure vessel of international tensions, profound digitization driven by foreign mega-companies, and explosively growing cyber threats, the realization emerged that strategic autonomy needed a broader interpretation. The European Commission discussed the ability to safeguard⁶ the economy, society and democracy in the 2017 Cybersecurity Strategy review.

What policy instruments are on the table to reverse the trend? The reality is that, until recently, a bold and coherent policy on digital strategic autonomy has hardly existed in Europe or in the Netherlands. One reason for this is, of course, that the threats have only recently become a broader issue. At European level, there is another reason: until recently, ‘sovereignty’ was a taboo. When Juncker declared in his *State of the Union* in 2018 that the hour of European sovereignty had come, half of Europe fell over him. Even the European Treaties mention ‘sovereign’ only to refer to UK military bases in Cyprus. Europe is struggling with ‘sovereignty’, where others such as the US and China are taking measures without hesitation, referring to their national security, self-determination, territorial protection and also claiming sovereignty in cyberspace.

Europe and the Netherlands, therefore, had to make do with the oars that it had - oars that were not all designed from the point of view of protecting sovereignty and which, moreover, were mainly aimed at protecting critical infrastructure such as electricity, water and transport and combating cybercrime. It is only logical that, without a binding principle and a broad perspective on the threats, the policy has so far been limited and inconsistent.

2.2 Strategic autonomy and sovereignty

Sovereignty is generally associated with territoriality, territory, jurisdiction, a population, authority with internal recognition (internal legitimacy) and external recognition (external legitimacy). In order to achieve/maintain sovereignty, the concept must be made operational. When and how can sovereignty be achieved? This is often called *strategic autonomy*, a concept that comes out of military/defense but is now seen as the capabilities and capacities to decide and act upon essential aspects of the longer-term future in the economy, society, and democracy⁷.

From 2016 onwards, the terms strategic autonomy and (digital) sovereignty began to appear in political speeches and policy documents. European leaders are increasingly placing strategic autonomy on their agenda. It is starting to become *a Leitmotif* for European policies on trade, security, industry, foreign investment and takeovers⁸, health (COVID-19) and, of course, digital policy. In 2020, the topic of political agendas was raised to the top of the agenda.

⁵ Interview in *The Economist*, 9 November 2019.

⁶ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 13 September 2017, <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>

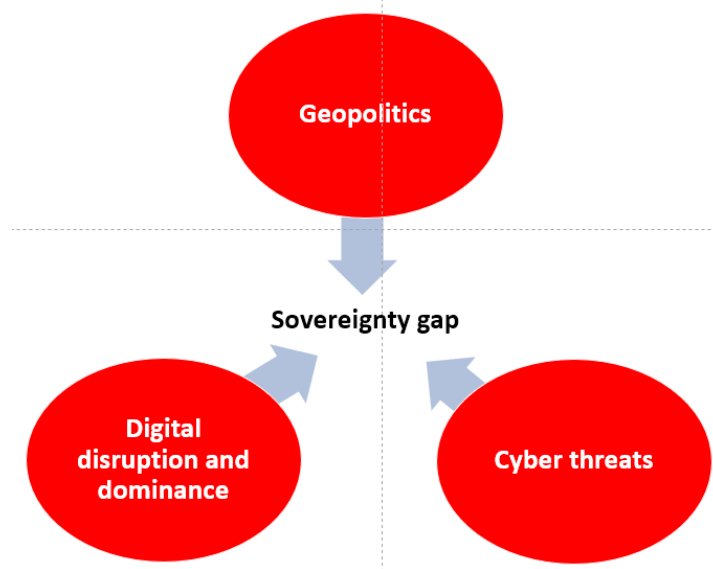
⁷ Timmers, P., *Strategic Autonomy and Cybersecurity*, European Institute of Security Studies, May 2019

⁸ A reason for the EU Foreign Direct Investment Regulation was that Kuka, the German manufacturer of industrial robots, was taken over by the Chinese company Midea in 2017. Since then, Germany has further tightened up national legislation (Kartellamt) to intervene in the event of a threat of international takeover of German companies

Observation: until 2017, the term "strategic autonomy" was almost unknown, whereas today it is *Chefsache* in Europe. Nevertheless, the specific policies and the corresponding investments are still limited and we are still being driven by historical policy. Certainly, cybersecurity was taken seriously, but hardly from a concern for sovereignty. Moreover, policies are not coherent and are therefore less effective in the geopolitical power game.

Observation: strategic autonomy is a means of achieving and maintaining sovereignty. It consists of the capabilities and capacities to decide and act upon essential aspects of the longer-term future in the economy, society, and democracy⁹.

Cybersecurity threats can lead to a real risk for sovereignty. But cybersecurity threats can also emerge from geopolitical power struggles or radical digital transformation and digital market dominance (see diagram). These forces may also create risks to sovereignty and create the sovereignty gap mentioned. However, this study is limited to cybersecurity-related situations.



This study analyzes the combination of strategic autonomy and cybersecurity. This means direct control over strategic cyber-security assets and capabilities as well as strategic autonomy that indirectly affects cyber-resilience.

2.3 The digital security risks

Cyber security threats can undermine sovereignty. We are talking about the whole spectrum of availability, integrity and confidentiality of critical information and services with a potential impact on essential services (energy, water, transport, communications, health, the financial system, etc.) up to and including the functioning of democratic processes, public confidence in the government, the functioning of the rule of law, freedom of expression and freedom of the press, reliability of communication...

⁹ 'capabilities and capacities' originates from the military understanding of strategic autonomy and includes *intangibles* such as knowledge, skills, organization processes and procedures, decision-making culture, politics, etc. and *tangibles* such as resources in financial, human, industrial production, and otherwise physical. For a defence perspective on strategic autonomy, see e.g. IFRI, 'France, Germany, and the Quest for European Strategic Autonomy', p.10, https://www.ifri.org/sites/default/files/atoms/files/ndc_141_kempin_kunz_france_germany_european_strategic_autonomy_dec_2017.pdf

The potential threat comes not only from hostile nations but also from traditional partner countries and possibly even from within our own state structures. Recent developments also show that well-organized criminal gangs (including white-collar crime and digital extortion) have become a real and relevant threat.

Increasingly, this potential undermining is such that our future and that of society as we know it can actually be at stake. This risk is exacerbated by rising geopolitical tensions, increasing digital dependence and the complexity of digital infrastructure.

The term '*digital sovereignty*' is often used. This is the digital dimension of strategic autonomy.

Our society, our economy, our daily lives and even our lives are increasingly dependent on information technology and connectivity. It is positive that this digital transformation also brings us a lot of benefits. Just think of the even greater economic disruption that COVID would have caused if we could not telework from home.

But this increasing dependence also carries an increased risk. The connection of increasingly complex systems exposes us to new vulnerabilities. The devices we rely on are becoming more autonomous and uncontrolled/unmanageable. New threatening actors are emerging, be they states outside the traditional group of advanced countries or organized cybercrime groups. Moreover, these two threat groups are increasingly linked and use similar tools which are increasingly difficult to combat.

Some specific cybersecurity threats to sovereignty expressed in the CIA of information security (Confidentiality, Integrity, Availability) are:

Confidentiality (Confidentiality)

- Systematic stealing of intellectual property from Dutch companies¹⁰
- Misuse of politicians' private data to influence the elections in the US and France¹¹
- Spying on the Netherlands by 'friendly' nations¹²

Integrity (Integrity)

- Fake news/disinformation to influence elections or stability in a country
- Compromising certificates, such as the DigiNotar incident in 2011¹³
- Use of deep fake technology to falsify the identity of executives

Availability (Availability)

- Disruption of essential services as the Ukrainian electricity network in 2015-2016¹⁴
- Disruption of the media, e.g. TV5Monde TV broadcasts in 2015¹⁵
- Systemic incidents that can disrupt the entire financial system, of which we have an idea in view of the attacks against the SWIFT backbone since 2017¹⁶
- Coordinated ransomware attacks that lead to major economic consequences as simulated in the Bashe attack¹⁷
- Possible disruption of the electoral system, either electronically or by post

¹⁰ Cybersecurity Assessment Netherlands CSAN 2019 (in Dutch: CSBN)

¹¹ https://us-cert.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf re

¹² <https://nos.nl/artikel/2356718-vs-bespioneerde-vanuit-denemarken-bondgenoten-waaronder-nederland.html>

¹³ <https://www.onderzoeksraad.nl/nl/page/6749/onderzoek-diginotar-digitale-veiligheid-overheid-moet-sterk-verbeteren>

¹⁴ https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

¹⁵ <https://www.bbc.com/news/technology-37590375>

¹⁶ <https://www.swift.com/news-events/news/how-cyber-attackers-cash-out-following-large-scale-heists>

¹⁷ Bashe attack: Global infection by infectious malware, CyRim Report in 2019

Cyber "insider threats" are also beginning to appear at state level. One example is the financial impact in the 1MDB case in Malaysia. In information manipulation, we can think of the Cambridge Analytics scandal in the political manipulation of citizens' opinion and in influencing elections.

A modern approach to cyber security risk also involves containing and approaching all aspects of the risk: assets, threats and vulnerabilities/resilience.



Figure 1 Interest, threat, resilience - source: CSAN 2019

Observation: our increasing dependence on information systems and connectivity also means that cyber-incidents are increasingly affecting our society, economy, democracy and fundamental freedoms, and that we need to look beyond what we have so far defined as 'vital' in ensuring our protection and also look beyond resilience to include a good understanding of the threats and the assets in our approach. This also has an impact on the renewal of the NIS Directive, the role of the NCSC and the possible role of telecoms operators in providing a secure network to the end-user. In this context, see also the CSR Opinion on the WRR report on cyber resilience¹⁸ and the CITRIX evaluation¹⁹.

2.3.1 Case: Disruptive ransomware

2019 was characterized by the emergence of large-scale cyber-extortion incidents (ransomware). In March 2019, it was announced that the Norwegian energy and aluminum group Hydro had been contaminated with ransomware. Hydro, which also has branches in the Netherlands, was forced by the attack to stop production at various locations in Europe and the USA and switch to manual operations whenever possible. The University of Maastricht also suffered a ransomware attack on 23 December 2019. Because backup servers had also been hit, the recovery was complex. The university decided to pay ransom to the criminals in order to get access to its own encrypted files.

Ransomware attacks were increasingly in the news in 2020. The cyber criminals are increasingly reckless and sophisticated in their methods. Some ransomware variants are specifically designed to attack industrial control systems. It is becoming more and more difficult to stop these attacks and their impact of encrypting or leaking information is

¹⁸ <https://www.wrr.nl/publicaties/publicaties/2020/06/16/kwetsbaarheid-en-veerkracht>

¹⁹ https://www.cybersecurityraad.nl/binaries/CSR_Advies_kabinetsreactie_WRR-rapport_en_Citrix-evaluatie_NED_DEF_tcm107-463191.pdf

increasing. And the criminals do not spare any organization, certainly not the critical infrastructure because there is an even higher chance of a ransom.

Observation: the disruptive and financial impact of ransomware on our economy is growing and is "country-wide". Traditional police and judicial working methods until today have little or no grip on this.

2.3.2 Case: Disinformation and Fake News

A proven technique in the strategic power play is the use of disinformation. Regime changes were triggered and politicians' careers were created and terminated by such manipulations. More recent is the widespread use of disinformation through social media. The problem has already been documented in detail with regard to the 2016 and 2017 elections in the USA and France, as well as with regard to Brexit. At European level, the problem has not only been recognized but a dedicated service has been set up to detect and combat²⁰ disinformation campaigns. The Netherlands is also been the scene of disinformation campaigns, and one example of this is the MH-17 trial²¹. The EU database contains almost 300 cases of disinformation relating to this trial in early November 2008.

The COVID crisis was also used to disseminate false information. In the first three months after the crisis broke, Twitter found over 3.4 million suspicious accounts that started discussions with Coronavirus. YouTube examined over 100,000 videos of dangerous or misleading information about the coronavirus during the same period and removed 15,000 of them.

A 'Code of Practice on Disinformation' was adopted²² at EU level, signed by Google, Facebook, Twitter and Mozilla, among others.

Observation: Disinformation has been used since time immemorial by state actors to intervene in the stability of other countries. Using social media as a channel of influence has made it an acute challenge for citizens and respectful government. International norms and cooperation with the major private players are necessary.

2.3.3 Case: Lawful intercept - surveillance

There is an ongoing discussion on the dual use of technical means of lawful interception. On the one hand, there is the legitimate aim of the security and intelligence services to protect society from criminal and terrorist threats and the technical means to understand the opponent's intentions before the damage is done, or to trace and attribute the events afterwards. The use of these technical means of lawful interception is laid down in the legislation and is monitored by oversight mechanisms aimed at limiting the use of these technologies to what is considered to be 'legitimate'.

On the other hand, the same technical means can also be used for surveillance in all its variations; to gain strategic advantage, to monitor internal opposition, to locate and eliminate political opponents, to gain commercial or competitive advantages.

The position of the Dutch Government on strong encryption of January 2016²³ states: "The Cabinet is responsible for ensuring the security of the Netherlands and for detecting criminal

²⁰ <https://euvsdisinfo.eu/>

²¹ <https://euvsdisinfo.eu/mh17-desinfo-sinds-start-proces/>

²² <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> and related initiatives built upon by the proposed Digital Services Act (see also section 6.6)

²³ https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015

offenses. The Cabinet underlines the need for legitimate access to data and communication. In addition, maximum security for digital systems will benefit governments, businesses and citizens. The Cabinet endorses the importance of strong encryption for Internet security, in support of the protection of citizens' privacy, for confidential communication by the government and companies, and for the Dutch economy. Therefore, the Cabinet considers that it is not appropriate at present to adopt restrictive legal measures regarding the development, availability and use of encryption within the Netherlands. In the international context, the Netherlands will convey this conclusion and the considerations underlying it. With regard to the promotion of strong encryption, the Minister for Economic Affairs will follow up the spirit of the amendment to the budget of the Ministry of Economic Affairs."

Without going into the merits of the various arguments, here are some points in this dilemma:

- Huawei has recently responded to allegations of built-in backdoors by indicating that they, like other suppliers, offer lawful interception functionality according to industry standards²⁴. It draws attention to suppliers from other countries with similar functionality and with similar possible threats of sovereignty.
- Many Corona contact tracing apps protect privacy because they are based on Bluetooth proximity held inside the phone. Google and Apple have changed their operating systems to make that possible, in collaboration with the academic world. In some countries, however, the government has opted for a centralized approach that does not provide the same protection of privacy.
- Digital certificates used in SSL/TLS and code signing are an important cornerstone for cyber security. If a certificate is tampered with, or if it falls into the wrong hands, this may lead to interception of encrypted traffic. Since 2005, the providers of such certificates have organized themselves in the CAB Forum²⁵. Attempts to build a safe and transparent register of certificates have so far failed because some countries and suppliers are opposed to it.
- In many countries, digital identity implementations are being developed and also offered by commercial parties. Most systems are based on a centralized platform that enables identity owners to identify in applications but also centralizes (and potentially exposes) all identity attributes and metadata of the transactions. There are also sovereign, decentralized identity implementations (such as IRMA), but they have not reached the same level of adoption.
- There is a lot of discussion about offensive commercial tools from companies such as Hacking Team and FinFisher who claimed to offer only services to law enforcement and security services, but have been shown to have also sold their products to repressive regimes.
- Also, the use (and non-disclosure) of *zero days* by intelligence services worldwide has led to enormous security risks, visible in the WannaCry and NotPetya incidents, using the zero day 'EternalBlue'.

Observation: Legal interception of information also opens the way to illegal interception and thus creates a risk to national sovereignty.

²⁴ <https://www.huawei.com/en/facts/voices-of-huawei/media-statement-regarding-wsi>

²⁵ <https://cabforum.org/>

2.4 Strategic autonomy approaches

Strategic autonomy does not mean self-sufficiency. This is not possible for the Netherlands and, in many cases, not for Europe. And this would not even be desirable. There are three realistic approaches to strategic autonomy, and possibly in combination:

1. The risk management approach
2. Strategic cooperation: rely on strategic *like-minded* partners, possibly combined with *strategic interdependency*, i.e. a strong and reciprocal dependence with respect to key *'not-like-minded'* parties.
3. Working together globally towards solutions that respect sovereignty and ensure the global common interest (*global common goods*).

Ideally, sovereignty is tackled in an integrated manner, i.e. in a smart combination of the three approaches and not just in the digital dimension. That awareness is growing in Europe since 2019: mention is being made of *materials autonomy* for the European Green deal, *health sovereignty* as regards COVID, *financial sovereignty* triggered by Iran's sanctions²⁶, *energy autonomy* over Russia²⁷, autonomy in electric car batteries to avoid losing²⁸ our car industry to China. The list is growing...

Currently popular at European level is to talk about 'open strategic autonomy'. This is a selective combination of strategic partnership and strategic interdependencies, the second approach as outlined above. Foreign companies are and will continue to be welcome to the EU in this approach, provided that they meet certain requirements, so are convincingly *'like-minded'*.

Observation: a realistic approach to strategic autonomy for the EU and the Netherlands requires a combination of risk management, strategic partnerships, and the promotion of global common interests.

2.5 Cases

2.5.1 Case: GPS - Galileo

The Global Positioning System (GPS) satellite navigation system is owned by the United States and is managed by its armed forces. The GPS project was launched by the US Department of Defense in 1973 and the first satellites were launched in 1978. Civilian applications have been allowed since the 1980s. GPS has more secure and accurate features (PPPs) that can only be used by the US.

China and Russia have autonomous competing systems, BeiDou (first launch in 2000) and GLONASS (first launch in 1982). The GLONASS system was in decline for many years, but the Russian Government made it a new priority in 2001.

The GPS quality may be restricted by the US Administration using *Selective Availability* (SA). SA was used during the first Iraq war in 1991, but the US stopped it because the US military forces did not have enough GPS military receivers on the ground. SA was used against the Indian army in the war against Pakistan in Kargil in 1999. As a result, India decided to design its own GPS system²⁹ (IRNSS).

²⁶ The related financial instrument is INSTEX, <https://instex-europe.com/about-us>

²⁷ 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>

²⁸ <https://ec.europa.eu/growth/industry/policy/european-battery-alliance>

²⁹ <https://timesofindia.indiatimes.com/home/science/How-Kargil-spurred-India-to-design-own-GPS/articleshow/33254691.cms>

In 2000, the US decided to shut down SA in response to the threat posed by the EU's Galileo system³⁰. In the second Iraq war in 2003, the GPS system was modified by the US to provide eight times more precision to its satellite-led missiles.

The Galileo program was launched by the EU in the mid-1990s. Already in 1994, the European Commission expressed its dissatisfaction with its strategic dependence on the United States' global positioning system. The European Commission stated that "if Europe does not act quickly, control of the whole system from abroad will be exercised by introducing a civilian American complement to the military GPS system. The standards for the user requirements and the certification schemes for equipment shall be set by those who own and operate the system. The result would be Europe's dependence on the supply of a strategic asset for the future and a poor prospect for industry to enter the vast market for utility equipment"³¹.

In 1998, the European Commission expressed serious concerns about the continued dependence on positioning and navigation systems of third countries³²:

- It was necessary to ensure that European users were not held hostage by possible future charges or fees that appear excessive: if a dominant position or a virtual monopoly were to be created, it would be difficult to oppose such charges and it might be impossible to develop alternatives quickly.
- The competitiveness of EU industry in this lucrative market would be severely restricted if Europe does not have equal access to technological developments in the system itself. In particular, the US has shown that it will use the strategic advantage of its military positioning system to dominate the global market for systems and services.
- There would be serious problems in terms of strategic autonomy and security if European navigation systems were outside Europe's control.

The first operational Galileo satellite was launched in 2011. The system has been fully operational since 2019, more than 10 years later than originally planned. Galileo was originally intended to be built by a public-private partnership (Galileo Joint Undertaking) in which two-thirds of the costs of introducing the system would be borne by private concession holder who would operate the system at a profit. The PPP efforts broke down in mid-2006 and the European Commission and the European Space Agency (ESA) decided to transform the program into a traditional public procurement.

During the development of the Galileo system, the EU has come into conflict with the US over the use of frequency bands. With the original choice of the Galileo frequency band, the US would hinder its own GPS system if it would block the Galileo system. In 2001, the US intervened to change this choice of frequency bands. In 2004, the dispute was resolved, and the EU accepted the use of frequency bands that allow the US to block the Galileo system without affecting the military frequency bands of its own GPS system. If the US decides to block the civilian use of its GPS system, it will also do so for the signal³³ of Galileo, thus nullifying part of the original objective of Galileo.

Recently, as a result of the Brexit, the UK has been excluded from the development of the Galileo encrypted system, which is due to become operational by 2026. The UK has therefore decided to withdraw completely from the Galileo system because it would not be in the UK's

³⁰ https://media.defense.gov/2017/Nov/22/2001847932/-1/-1/0/WP_0012_CONSTANTINE_GPS_AND_GALILEO.PDF

³¹ COM (94) 248 final

³² COM (1998) 29 final

³³ https://media.defense.gov/2017/Nov/22/2001847932/-1/-1/0/WP_0012_CONSTANTINE_GPS_AND_GALILEO.PDF

interest to use the secure elements of the system if it was not fully involved in its development. The development of an autonomous satellite navigation system is currently under discussion in the UK for strategic reasons.

Observation: GPS-Galileo is a good example of a new technology/service that was developed for strategic purposes but also intended for wider use (dual technology). Europe has made a catching-up to become strategically independent and has succeeded to some extent, after a lot of trial and error and with a lot of delay. Galileo is an example of strategic autonomy and an integrated policy to strengthen European sovereignty³⁴ in both security and the economy.

2.5.2 A broader perspective on European success stories

In a number of areas, Europe has in the past been able to build world-class industrial champions and infrastructure. Examples of industrial champions are:

- Chip technology, micro-electronics: ASML, Infineon, NXP, IMEC
- 5G Network Infrastructure: Ericsson/Nokia
- IT for the automotive industry: Bosch, Continental. Magneti Marelli, on the other hand, was recently sold by FCA to Calsonic (JP), supported by KKR (USA)
- Information technology (Thales, Atos, SAP, F-Secure).

All these companies benefit from EU and national research and innovation funding on a regular basis. They know how to find the way to public funding and they are also very active in providing input to the research funding agenda. This is in fact both a strong and a weak factor in the allocation of these funds. The procedures for setting the agenda, setting up consortia and evaluating the proposals are heavily influenced by the established players (industry, universities and research centers). The processes have a long lead time and an administrative overhead that few small organizations can afford.

Many R&D investments are currently taking place in a separate way from a strategic perspective and are not combined in a coherent and coordinated way with other, reinforcing measures. They do not generally lead to industrial breakthroughs or to the creation of new global players in Europe.

And yet Europe has in the past achieved success in coordinated efforts to create new industrial champions in areas such as aviation (Airbus) and space (Ariane). Similarly, Europe has been successful in building world-class navigation infrastructure (Galileo) and earth observation (Copernicus). Particle physics research (CERN) is also an illustration.

Observation: European success stories from the past (Airbus, Ariane, Galileo, Copernicus) point to the importance of strategic perspective and a targeted, coordinated and integrated approach rather than subsidizing mediocrity.

All these cases have a number of common aspects. They have a strategic perspective, a clear objective, a sustained and adapted budget, a project-based, focused and coordinated approach combined with regulation, standardization, public procurement and a market situation that was/is not self-regulating. And they supported *excellence* above mediocrity.

³⁴ Sovereignty as an objective is explicitly mentioned, see <https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system>

2.5.3 Case: Cloud - Hyperscalers

The current cloud provider market is dominated by four major players; Amazon, Microsoft, Google and Alibaba. Together, they account for almost two-thirds of the market, with Amazon and Microsoft taking the lion's share.

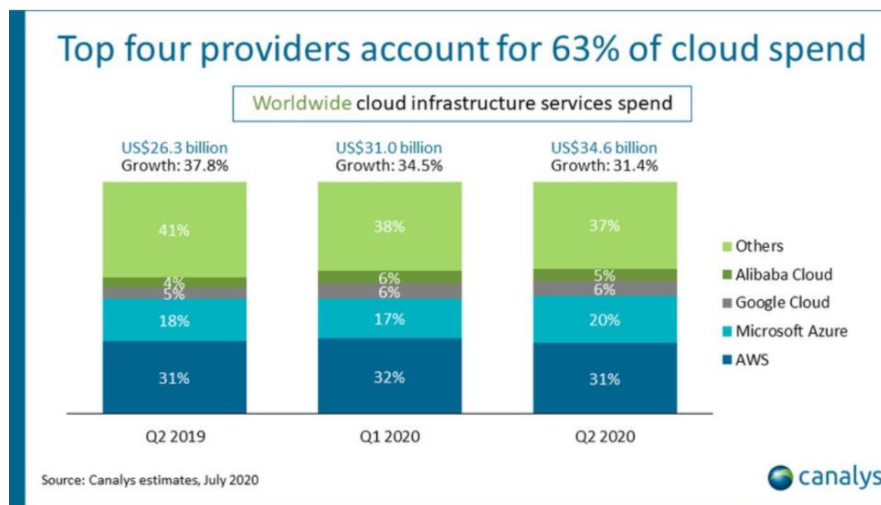


Figure 2 Global cloud provider market share - source Canalis

Amazon continues to benefit from the fact that it was the first to announce³⁵ in 2006 a service of scalable infrastructure for shared computing (EC2) and Storage (S3). The solution was the result of an internal project to harmonize and facilitate the development of infrastructure for the Amazon website, but the project was already intended as a third-party service at the outset and subsequently it became AWS.

Microsoft Azure was launched in 2011 after a pilot period between 2008 and 2011. Microsoft completely shifted its strategy to cloud services in 2014. Azure and Office 365 benefit from the same infrastructure and scale.

The Google Cloud Platform (GCP) grew out of the App Engine, which was launched in April 2008 as a platform as a service. The App Engine was trialed in 2011 and the GCP name has been in use since 2013. GCP runs on the same infrastructure that Google uses for its end-user products such as Search, Gmail and YouTube.

Local players in the European market are very much behind in market footprint (OVHcloud has an annual turnover of EUR 600 million)³⁶.

Cloud Services Leadership – Europe

Rank	Total Europe	UK	Germany	France	Netherlands	Rest of Europe
Leader	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft
#3	Google	Google	Google	OVH	Google	Google
#4	IBM	IBM	Deutsche Telekom	Orange	KPN	IBM
#5	Salesforce	Rackspace	IBM	Google	IBM	Salesforce
#6	Deutsche Telekom	Salesforce	Oracle	IBM	Oracle	Swisscom

Based on IaaS, PaaS and hosted private cloud revenues in Q1 2020.

Source: Synergy Research Group

Figure 3 European market share of cloud providers - source Synergy Research Group

³⁵ <https://techtv.mit.edu/videos/16180-opening-keynote-and-keynote-interview-with-jeff-bezos>

³⁶ <https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries>

Deutsche Telekom and OVHcloud have recently announced the GAIA-X cloud partnership³⁷. The announcement refers to compliance with GDPR rules, open standards, but also portability, user privacy and the highest security standards. It remains to be seen whether this initiative will be successful and whether emerging techniques such as homomorphic encryption and privacy protection data processing will also be included.

Meanwhile, the three leaders are not standing still and have begun to provide encryption solutions and privacy-protected computations. Sometimes they offer hybrid clouds with their competitors³⁸. All three now also have a market place in which third parties offer their solutions. For the vendors, it appears to be an efficient way to reach new customers and the platform supplier takes advantage of it without much effort.

Observation: Cloud hyperscalers is a case where Europe has completely abandoned the initiative and where the gap with the market leaders seems to be unbridgeable. Europe is trying to create a cloud *flagship* with GAIA-X, but its success is yet uncertain.

The strengths of GAIA-X appear to be that a technical architecture, standardization, legislation, economic incentives, investment (EUR 10 billion) and EU policies are combined. The weaknesses are that it is a catching-up operation that has to match the huge existing investments of the hyperscalers with many elements that still need to be clarified, such as migration, hybrid cloud, and participation of non-European suppliers. It shows that a large infrastructure initiative needs a lot of consistency in action and for a long time and this not within reach of an individual country.

2.6 Policy areas and -instruments until recently

Most of the EU policies on cybersecurity that could contribute to digital strategic autonomy have so far been driven from a risk management perspective and fit for the open, global, liberal market economy perspective. Both perspectives are now considered³⁹ 'insufficient' or 'naïve'. Strategic autonomy is now increasingly mentioned in policy statements and legislation, and not just in cybersecurity⁴⁰.

Observation: strategic autonomy as a driving force is gradually beginning to be introduced into new EU policies.

³⁷ <https://www.telekom.com/en/media/media-information/archive/t-systems-and-ovhcloud-cooperate-for-gaia-x-607634>

³⁸ <https://azure.microsoft.com/en-us/overview/security/>

³⁹ The most explicit reference to the relationship with China is the European Commission/EEAS, 12 March 2019, EU-China - A Strategic Outlook, <https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf>.

⁴⁰ An example is the proposed EU Data Governance Act of 25 November 2020, a European regulation whose presentation indicates: 'The data governance regulation will ensure access to more data for the EU economy and society and provide for more control for citizens and companies over the data they generate. This will strengthen Europe's digital sovereignty in the area of data.'

3 Current situation

3.1 Current Cases and Topics

3.1.1 Case: mandate for cyber resilience of critical infrastructure and services

The Network and Information Security Directive (NIS Directive, transposed into WGNI in the Netherlands) for a common approach to cyber-resilience of essential infrastructure services is one of the most important pieces of cyber legislation in the EU. The proposal dates back to 2013, was agreed in 2016 and is now in force.

Initially, this legislation was contested because it would affect national security and "national security remains the sole responsibility of each Member State" (Article 4 TEU). However, the European Commission had proposed the NIS Directive on the basis of the internal market, Article 114 of the Treaty on the Functioning of the European Union, TFEU. In this area, the EU has a strong mandate: Member States cannot deviate from internal market approaches, as otherwise the free movement of people, goods, services and capital would be impeded.

The current NIS Directive deals with cyber-resilience, protection and recovery of cyber-incidents, and explicitly states that they should be based on a risk management approach. It covers cyber-resilience of selected vital infrastructure (such as electricity, water and transport) and digital infrastructure/services and currently covers only three services (cloud, electronic markets, search engines).

In 2020, concerns about sovereignty and strategic autonomy have become an important political driving force. It is clear that various essential digital infrastructure and services are not covered by the NIS Directive in force and are limited by other EU legislation⁴¹. Examples are:

- Social media and media in general, where the daily reality is actively to undermine by attacks, intrusions, hacking, theft and abuse, for example by fake news. The *mainstream* political world is very concerned about the continuing undermining of our democracy and values.
- Industrial and other physical infrastructure (e.g. steelworks where attacks have been seen!) which is increasingly based on the Internet of Things (IoT). IoT security is almost entirely owned by industrial consortia - in which many Chinese participants - but we are more and more critically dependent of it.
- Critical Intellectual Property (IP) for our economic future. Cyber theft of IP is one of the greatest threats to the future of our countries. However, there is no systematic and compulsory protection of intellectual property. Not even as a condition for the use of EU R&D money.
- The emerging European data spaces, such as industrial, public services, health and environmental data. These data infrastructures at European level are essential for the competitiveness of European industry or for combating cross-border communicable diseases such as COVID-19.
- Education and training, where digital platforms have become indispensable in COVID time, while they are largely owned by non-EU providers.

⁴¹ For recent European Commission proposals (end 2020) see also chapter 6 and section 6.6.

The sovereignty perspective gives a very different view of cyber resilience. It points out that cyber protection of all the crucial resources for our economy, society and democracy must be considered.

On 16 December 2020, the European Commission proposed a revision of the NIS Directive ('NIS2 Directive'), together with a significantly adapted Cybersecurity Strategy. Although the revised NIS Directive covers a wider area, not all the above-mentioned gaps are covered in it. There are indeed considerable obstacles to doing so. These are partly political: Is the pooling of strategic autonomy through joint action the right way forward for these issues? Is market intervention by means of legislation necessary? Does the EU have a mandate⁴² to act, particularly where national security also plays⁴³ a role?

As regards legal barriers: a legal anchor ('legal basis') in the Treaties is necessary to propose European legislation. In addition to Article 114 TFEU (the internal market), in order to incorporate all these points, a whole series of additional articles of the Treaties have to be invoked. In some cases, it is even very difficult to find a legal anchor, or simply does not exist. Moreover, not every article gives a strong mandate for action at EU level. The following table provides an overview.

Cyber resistance	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	Weak
	Article 114 TFEU Internal market	Strong
Industrial infrastructure	Article 114 TFEU Internal market	Strong
	Article 173 TFEU (Industry)	Weak
Intellectual property	Article 114 TFEU Internal market	Weak
	Article 173 TFEU (Industry)	Weak
	Article 182, 183 Investigation	Average
Internet domain .eu	Article 170 TFEU Trans-European Networks	Strong
	Article 114 TFEU Internal market	Strong
European Data Spaces	Depending on the area, e.g.	
	- Article 168 Public health - Article 114 Internal market	Weak Strong
Education	No real basis	Absent

⁴² L. Moerel and P. Timmers, 'Reflections on digital sovereignty Pre-opinion State Law Conference 2020', 4 December 2020, <https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf>, and P. Timmers, 'When Sovereignty Leads and Cyber Law Follows', October 13, 2020, <https://directionsblog.eu/when-sovereignty-leads-and-cyber-law-follows/>

⁴³ National security is excluded by Article 4 of the Treaty on European Union

Observation: from a strategic autonomy perspective, all assets and infrastructures that are crucial to the economy, society and democracy must be cyber-protected. Cyber security regulation is a tool to do this. At EU level as at national level, a comprehensive approach does not yet exist. This is a significant and urgent strategic autonomy risk.

3.1.2 Case: e-ID, digital security, deep security

Meanwhile, we're all accustomed to different forms of e-ID, from simple user name and password on social media to government-supported e-ID with a hardware device such as a smart card and dual authentication. With different e-IDs, there are also different electronic signatures. EU legislation (eIDAS Regulation) provides that all these instruments have a legal value, even if they are of different strength. A sufficiently strong e-ID notified at EU level can be used to access public services across the EU. eIDAS also covers a number of related digital security or "trusted services" (time stamping, registered delivery and website authentication).

In practice, the use of government e-IDs is overshadowed by the e-IDs of the giant digital platforms⁴⁴. The private sector's acceptance of government e-IDs is promoted but is not mandatory under the legislation and little has been achieved with this promotion.

The dominance of these oligopolistic private e-IDs poses a serious threat to strategic autonomy. E-ID is the key to participating in the digital society, where more and more people live and work. It is linked to personal data such as online behavior and the personal and professional social network and can be combined with derived data on preferences, political opinions, gender, age, etc. A precise picture of us is being built, a picture that is in the hands of a few private companies. These profiles are used for commercial purposes. But, as the Cambridge Analytics scandal shows, it is also the key to political influence. Loss of control over e-IDs undermines sovereignty.

The identification of citizens was previously the exclusive prerogative of the government. The identification of citizens is a state asset and must be carefully protected. Now, however, governments run the risk of playing a sidelined role in the economy, society and even democracy because of the Internet giants. By losing control of e-ID, citizens and governments fear that they will lose control of key decisions in the economy, society and democracy.

Control of e-ID undoubtedly is part of the digital strategic autonomy. The European Commission is considering giving governments and citizens the opportunity to retain control of e-ID when revising the eIDAS Regulation and is already defining a step in this direction in the recent Digital Markets Act⁴⁵. That may not be enough. The use of the government e-ID or the independent e-ID (such as IRMA) will be indispensable. The Netherlands could ensure that a future eIDAS has a greater chance of success by actively promoting the ease of use of sovereign e-ID solutions. In this context, the CSR has already issued⁴⁶ an opinion.

This study focuses on the intersection of sovereignty with cyber security. Cyber security of e-ID should indeed be a source of concern given the increase in online identity theft. With regard to strong e-ID, many EU governments still have an advantage. Yet Internet giants are moving quickly towards stronger private e-ID with two-factor authentication and biometrics.

Given the link to e-ID, we should also focus on digital security services. For these companies, the same concerns exist about private sector control. Perhaps they are even more serious

⁴⁴ Only 15 out of 27 Member States offer e-ID under eIDAS.

⁴⁵ See also section 6.6

⁴⁶ https://www.cybersecurityraad.nl/binaries/CSR_Advies_eID_NED_DEF_tcm107-415886.pdf

because such services are increasingly integrated into the platform. For example, the *security assurance* of apps on Apple's AppStore is exclusively owned by Apple, without any supervision. The safety of Dutch DigID apps (which clearly relate to the use of a state asset) is assessed by a foreign commercial party outside the control of an EU government! No wonder the EU cloud policy and GAIA-X⁴⁷ specify the unbundling of digital security services.

Unbundling would facilitate taking back of sovereign control and could also open up a promising market for digital security. Common certification under the 2018 EU Cyber Act would remove barriers in the EU internal market for such services. However, they must meet ever higher security standards and face growing cyber threats.

In order to ensure a competitive market in the EU and in the Netherlands, it is necessary to invest in technologies such as AI for software inspection, stringent security for certificates, and distributed security controls. This should also be done through greater involvement in standardization, including in international consortia aimed at market standardization. Moreover, it is necessary to promote market acceptance by raising awareness and public procurement of such solutions in the field of cyber security.

Finally, the emergence of a battle between the major Internet and cloud players who are increasingly trying to integrate security and e-ID into their portfolio by acquiring Internet security companies leads to market suppression of the remaining players. This is in itself a worrying development which needs to be monitored closely.

Governments seeking to regain a degree of control should also consider *deep security*: advanced digital security services and solutions, including for highly demanding applications such as government core communications, diplomatic communications, defense and military. These are niche markets, but they are essential for strategic autonomy. *Deep security* can benefit from the same triggers that encourage *unbundling* of trust and insurance services. The Netherlands has a historic strength in *deep security*. An integrated policy for this should be considered.

Observation: e-ID and related trust services are essential for digital strategic autonomy, but are increasingly escaping from governments. Strengthening EU legislation may be useful, but it is not enough. A smart integrated policy can enable EU governments to regain control, open promising markets for trust services, also the Netherlands, for *deep security*.

3.1.3 Case: 5G protection

In 2017, the issue of 5G security in the telecommunication sector was rapidly put at the top of the global agenda. The reason was an offensive by the Trump government to put pressure on befriended governments to exclude Huawei from new 5G contracts. 5G is becoming the basic digital infrastructure of the future. The USA argued that Huawei's equipment could not be trusted as the company would be controlled by the Chinese State. National security would be threatened by espionage or a hidden "*kill switch*". In addition to security concerns were raised about China's dependence and a possible disruption of the 5G supply chain.

⁴⁷ GAIA-X is an initiative from Germany and France and is a concrete instantiation of EU cloud policy

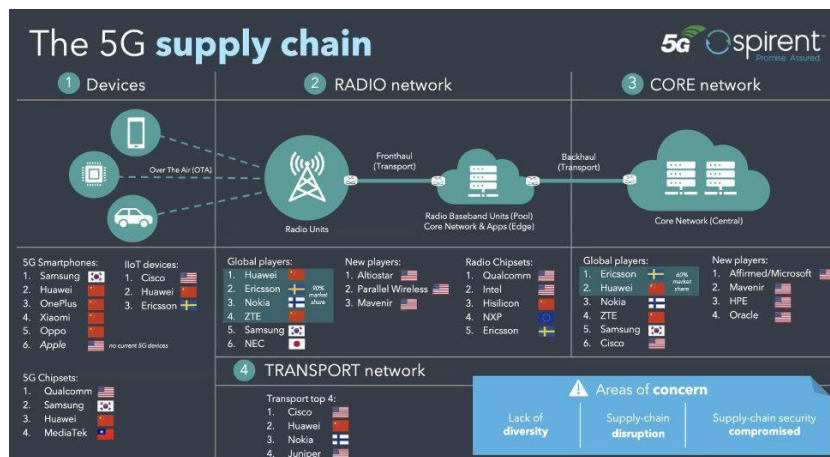


Figure 4 5G supply chain - source Spirent

For a number of years, the United States has been very concerned about China's theft of intellectual property, China's continued cyber threat and China's successful economic growth without the Communist dictatorship decreasing in strength. The US had intensified restrictions on Chinese foreign direct investment (FDI) in key technologies such as semiconductors, telecommunications, robotics and AI. Peter Navarro, director of the White House for Trade and Industrial Policy, stated that otherwise the US would have "no economic future".

EU governments were warned and concerned about national security, but were not convinced by the US. They preferred more objectivity, but that was difficult to achieve individually. They realized that they were not sufficiently aware of the 5G technologies and standards and that 5G is extremely complex. The European Commission subsequently managed to get all EU Member States around the table to adopt a common approach to risk management, the 5G Cybersecurity Toolbox⁴⁸. It consists of a technical cyber security assessment and a political assessment of the government of the country of the equipment supplier.

The concern about 5G is mainly about national security and is at the heart of strategic autonomy and hence of sovereignty. However, national security is explicitly excluded from the EU's mandate. It is therefore remarkable that the Member States accepted such a central role for the European Commission to make recommendations on the safety of the 5G!

However, the 5G toolbox still allowed countries to draw up their own roadmap and buy from Huawei. The United States therefore did not reduce political and diplomatic pressure. As a result, a growing number of countries decided to exclude Huawei, also because of US sanctions imposed on companies that supply technology to Huawei to design and manufacture and maintain components in 5G.

For the EU, the fact that the two largest alternative suppliers, Ericsson and Nokia, were losing market share to Chinese suppliers Huawei and ZTE also plays a role. In the years 2017-2019, there was a lot of speculation about other measures to strengthen alternatives to ensure the diversity of suppliers, such as an open source 5G with support from a 'coalition of the willing' and the suggestion to take over Nokia and Ericsson with US investment funds. A technological (partial) alternative has recently been receiving a lot of attention: OpenRAN.

⁴⁸ <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>

Why have we found ourselves in this rather uncomfortable situation? One of the reasons is that the governments in the West have not followed closely the work on 5G standardization. These are mostly industry-led consortia such as 3GPPP⁴⁹. This opened the door so as not to put national security at the center of the 5G architectures. There is also a suspicion that the Chinese Government has actively controlled companies such as Huawei and could thus undermine the safety of the 5G. Many of the 5G patents, although not all of them may be very relevant, are now also owned by Chinese companies.

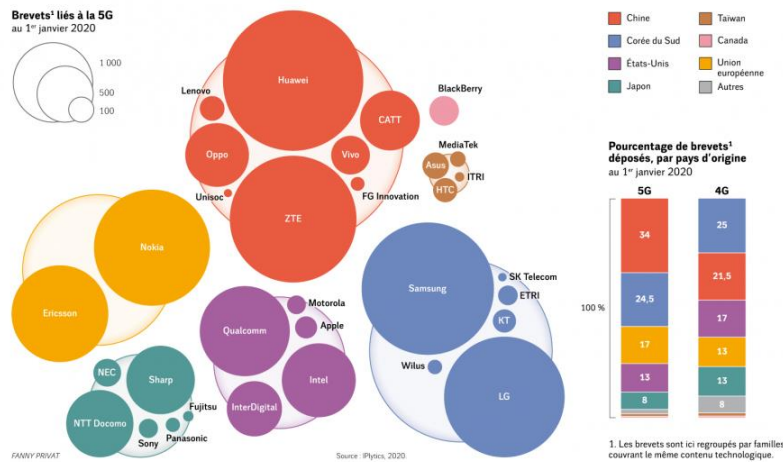


Figure 5 5G Patents - Source Le Monde

Another reason, which is often mentioned in the US, is that since about 2000 the US Government has ignored and thus lost control of the telecommunications equipment sector. In the EU, the development of the next generation of networks was supported by the EU's R&D framework programs, the motto of which was at the time: "We are open to the world". Huawei was an important participant in the EU-led 5G R&D consortia. In general, cooperation with China in the field of R&D and business has been considered positive for many years. But today, China is regarded by many in the EU as a 'systemic competitor'. The free global market approach of the past is considered to be 'naïve'.

Observation: The security of the 5G is a driver of digital strategic autonomy. The reason for this was the pressure from the US, but important weak signals should also have been of concern (no public interest in a key future digital infrastructure, growing disappointment with China's policies). The answer to the 5G security challenge shows that there is a willingness to mobilize various policy instruments (cyber security certification, R&D, standardization, procurement policy), but also that there is still no fully coherent and solid strategy at EU and national level. In the meantime, new technology can disrupt the field. The security story of the 5G threatens to repeat itself for another future digital infrastructure, the Internet of Things (IoT).

⁴⁹ Paul Timmers, Geopolitics of Standardization, April 9, 2020, <https://directionsblog.eu/the-geopolitics-of-standardisation/>

3.2 Research and development

3.2.1 Geographical perspective

R&D spending has grown steadily in recent years, with the EU following a similar curve to the US, and China growing faster in absolute terms than both the US and the EU⁵⁰.

Gross domestic expenditures on R&D, by selected region, country, or economy: 2000–17

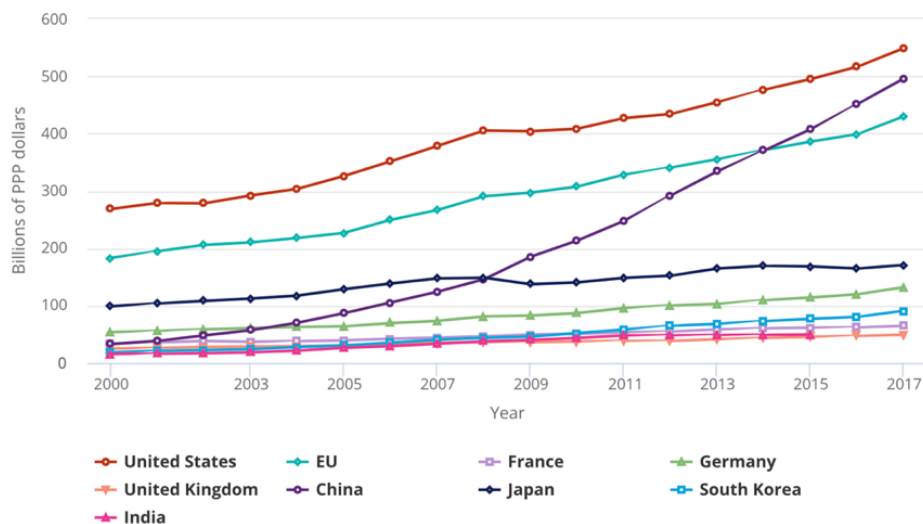


Figure 6 Expenditure on R&D - Source National Science Board

The research funding comparing to GDP (research intensity) shows that the EU (2% in 2018) is lagging behind the US (2.8%) but is investing roughly as much as China (2.1%). The Netherlands is also at 2.1%⁵¹. The leader is Israel with almost 5%.

A very different picture seems to be given in the statistics of patent families by region. Here, the US and the EU are clearly lagging behind Asia. China is mainly responsible for 50% of the patent families granted in 2018.

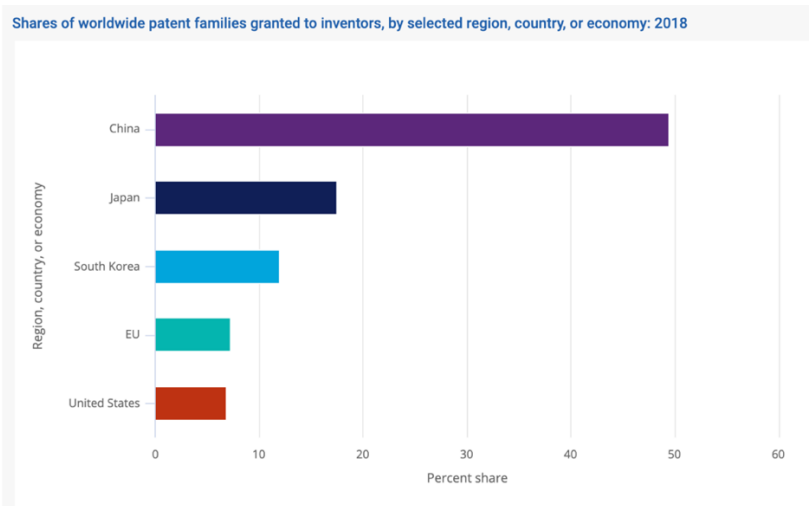


Figure 7 Patent families by region - source National Science Board

⁵⁰ <https://nces.nsf.gov/pubs/nsb20201>

⁵¹ <https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm>

Discussions with academics and entrepreneurs reveal a number of points of attention. It was indicated that the budgets for scientific research are sufficiently available at EU and national level. However, a number of differences in comparison with the USA were also pointed out:

- Programme priorities are set in multi-annual cycles and are not sufficiently agile
- High bureaucracy in project selection and monitoring
- Lack of excellence and too many compromises in R&D funding
- Lack of direct link to product development in R&D funding.

The EU is strong in investing in basic research, much less in generating innovation. Large industrial companies participating in EU funded projects do not do so because they want to develop new products but to cover costs and train new employees. Instead of participating in the most modern research and innovation, the major European industrial companies prefer to buy or acquire technology through M&A.

EU funding is too much spread/redistributed on the basis of compromises and taking into account vested interests. There is little room for disruption, the agenda and the distribution of funding are determined by established players.

Observation: In terms of research intensity, Europe and the Netherlands are moving in parallel with China and are lagging a little behind the US. The US and China are more efficient in transforming research into innovation.

3.2.2 Case: R&D in homomorphic encryption and differential privacy

In this case, a specific domain is analyzed in more depth, namely homomorphic encryption and secure (privacy-preserving) computing. Strong encryption as a means of guaranteeing security on the Internet, in support of the protection of the privacy of citizens, for confidential communications by public authorities and businesses, and for the Dutch economy is an important objective of the Dutch Government and these, although very specific key technologies, could make an important contribution in the future.

Homomorphic encryption is a form of encryption that allows calculations to be performed on encrypted data without decrypting it. Homomorphic encryption can be used for privacy-preserving storage and processing. This allows data to be outsourced to commercial cloud computing environments while remaining encrypted. The idea was first suggested in 1978. For over 30 years, it was unclear whether a solution could be found. The scientific basis for the mathematical solutions for homomorphic encryption was laid in the USA by Craig Gentry (Stanford, now IBM), Marten van Dijk (now at the CWI in the Netherlands), Shai Halevi and Vinod Vaikuntanathan. Shafi Goldwasser (two-time winner of the Gödel Prize and also winner of the Turing Prize) also made major contributions. The next picture clearly shows the leap in publications in 2009 and the steady increase in the number of publications in recent years.

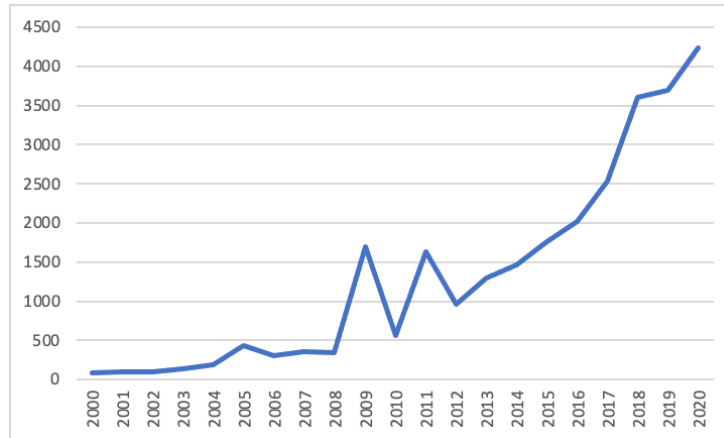


Figure 8 Scientific publications homomorphic encryption - source Dimensions

Differential privacy is a system for sharing information about a dataset by describing the patterns of groups within the dataset while specific information about individuals in the dataset remains secret. First technical solutions were proposed in 2006. Basic research on differential privacy⁵² was conducted by Cynthia Dwork (Microsoft), Frank McSherry (Microsoft), Kobbi Nissim (Ben-Gurion University) and Adam Smith (Weizmann Institute). The growth of differential privacy publications follows a similar curve to that of homomorphic encryption.

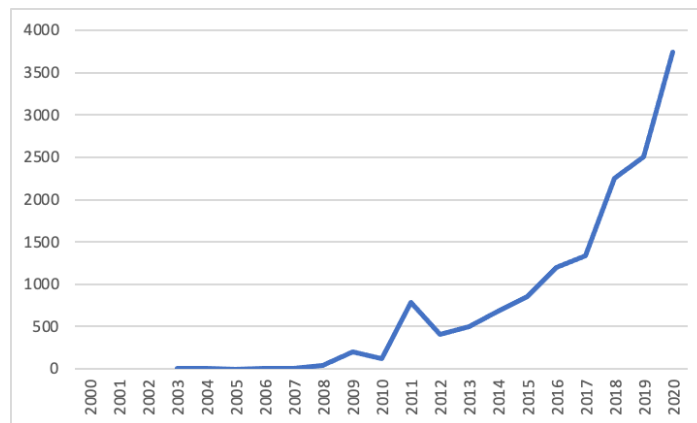


Figure 9 Scientific publication actions "Differential Privacy" - source Dimensions

DARPA and IARPA have already established funding programs for homomorphic encryption and privacy-safe data processing since 2011, PROCEED⁵³, SPAR⁵⁴, BRANDEIS⁵⁵ and HECTOR⁵⁶. MITRE's Mission Assurance program also funded such research over the same period, for example the DataStorm project. NIST has also funded research in this area (PEC project) and the NSF has also funded research.

The first EU-funded projects related to homomorphic encryption and differential privacy were launched in 2014 (Horizon 2020 program). Since 2015, more than EUR 100 million of EU funds

⁵² https://link.springer.com/chapter/10.1007%2F11681878_14

⁵³ <https://www.darpa.mil/program/programming-computation-on-encrypted-data>

⁵⁴ <https://www.forbes.com/sites/andygreenberg/2011/04/06/darpa-will-spend-20-million-to-search-for-cryptos-holy-grail/#23eb92287613>

⁵⁵ <https://www.darpa.mil/news-events/2015-03-11>

⁵⁶ <https://www.iarpa.gov/index.php/research-programs/hector>

have been invested in homomorphic encryption projects and around EUR 20 million in projects related to differential privacy.

This substantial EU R&D funding has not (yet) led to strong start-ups in this area in Europe. Almost all research funds have been paid to universities, public research institutes (TNO, CWI, CNRS, INRIA) and large industrial groups (Thales, NXP, IBM, Atos, Orange, Philips).

There are a number of academic centers of excellence in the Netherlands that can compete in encryption at world level (CWI, Radboud University, TU Delft, TU Eindhoven). The industrial situation is less favorable. Expertise was discontinued (Philips, NXP) and new promising start-ups have not been launched in this particular domain in the Netherlands.

It can be seen from these cases that two years after the publication of the feasibility of the technical concepts in 2009, the US was able to channel research funds into homomorphic encryption. The EU followed only three years later in 2014-2015 but without much transformation into industrial products and growth.

Observation: Europe is not well able to respond quickly to new scientific areas and turn research investment into innovation.

3.2.3 Academic expertise to validate key technologies

The Netherlands (and even the EU) cannot build industrial capacity in all key technologies that are important for cyber security. We must assume that we will continue to involve technological solutions and services from third-country companies. Control and autonomy in the strict sense is difficult to achieve.

In order to achieve the risk mitigation objectives, it will therefore be necessary in some cases to validate and certify in an independent and competent manner the claimed functionality of technical solutions. The new role of ENISA⁵⁷ can also support this.

To give an example in the encryption and privacy domain, if a cloud provider indicates that they retain the data in a way that guarantees total privacy and that the provider does not have the keys to the data, it should be possible to validate it in strategically important situations (but probably also in a broader context).

An in-depth understanding of key technology is needed to validate its effectiveness independently and to prevent cryptographic back doors, as happened in the past with the "elliptic curve random generators"⁵⁸ integrated into many security products.

Observation: If academic expertise is present, it can be called upon to achieve the "control of controllers" of key technologies. Provided that processes exist, budgets are available and independence can be guaranteed.

3.2.4 Private sponsorship of academic research

Research spending in the EU is for 66% in the private sector, 22% in academic research institutes and 11% in the public sector. In the Netherlands, the proportion of companies is somewhat lower and of universities somewhat higher (2017 data)⁵⁹. Of the research funding in Dutch universities, €300 million comes from business to a total of €1770 million, or 17%⁶⁰.

⁵⁷ European cybersecurity agency, with renewed mandate: <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act>

⁵⁸ https://en.wikipedia.org/wiki/Dual_EC_DRBG

⁵⁹ Eurostat, <https://ec.europa.eu/eurostat/documents/2995521/9483597/9-10012019-AP-EN.pdf/856ce1d3-b8a8-4fa6-bf00-a8ded6dd1cc1>

⁶⁰ Rathenau Institute, <https://www.rathenau.nl/nl/vitale-kennisecosystemen/financiering-van-onderzoek-aan-universiteiten>

Private sponsorship of academic research therefore seems relatively minor. Nevertheless, this does not reflect the influence of business, let alone foreign companies, on strategic autonomy through this type of sponsorship and the possible influence of foreign powers. A better understanding of with respect to the situation in key technologies is desirable⁶¹.

3.3 R&D and start-up financing (Business Angels, Seed, VC, Private Equity)

3.3.1 Geographical perspective

In 2019, the volume of private risk funding in European start-up companies increased by 40% to over USD 34 billion. During the same period, US investment remained stable at around USD⁶² 118 billion, three times higher than in the EU. Investment in Asia decreased significantly in 2019.

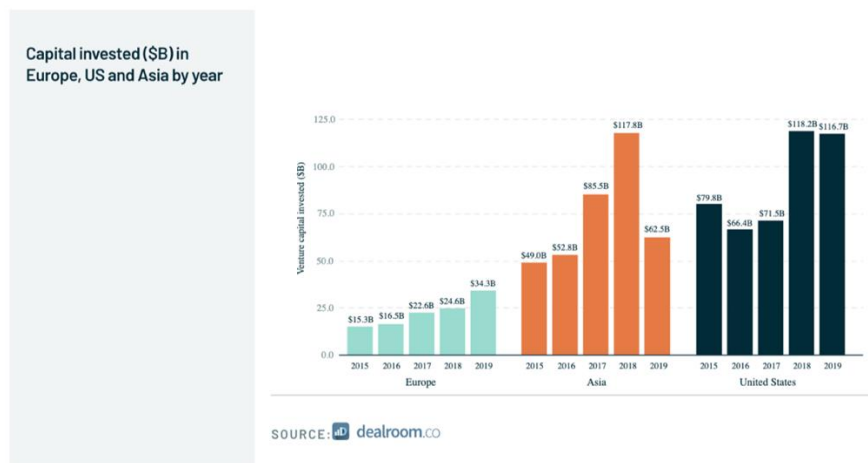


Figure 10 Risk investments in startups - source Dealroom

It is notable that USD 8.6 billion was invested by Angel investors in Europe in 2018.

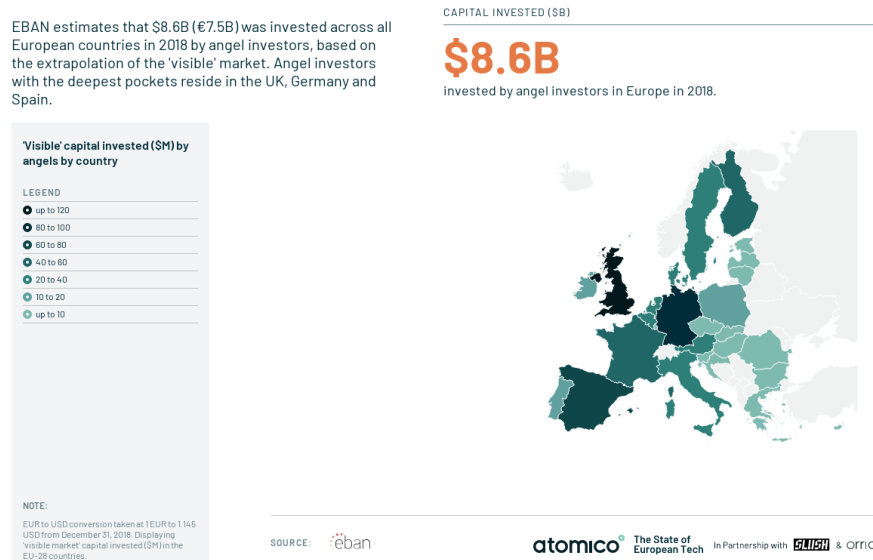


Figure 11 Investment by Business Angels in 2018 - source EBAN

⁶¹ We think of key technologies like quantum computing or, in general, China's presence in Dutch academic research (through companies like Huawei, or through collaborative relationships with Chinese universities)

⁶² <https://2019.stateofeuropeantech.com/chapter/key-findings/>

The top business Angel investors (except 3) in the EU are founders who have previously achieved an exit. Examples are:

- Xavier Niel (Free Mobile and Worldnet), with 54 investments in 2015-2018
- Pierre Kosciusko-Morizet (PriceMinister), with 23 investments
- Taavet Hinrikus (TransferWise), with 22 investments

This is part of a more general trend in which former founders with a successful exit become major investors at an early stage in new ventures. Additional examples are:

- Daniel Ek (Spotify), who wishes to invest EUR 1 billion in deeptech start-up⁶³;
- Niklas Zennström (Skype), who created Atomico (<https://www.atomico.com/>) in 2011 and a.o. invested in Rovio (Angry Birds), which achieved IPO in 2018,
- Jaan Tallin (Skype), who launched Ambient Sound Investments (<https://asi.ee/>),
- Illka Paananen, who, after selling Supercell to Tencent Holdings, set up the Illusian Group Oy as an investment vehicle and recently invested in n8n and Hopin,
- Oliver Samwer (Rocket Internet), with Global Founders Capital, has already invested in over 400 startups.

While these developments in the EU show a positive trend, there are still significant differences between the EU and the US. Start-up investments are easier in the US, especially if the company has no or little demonstrable income. It is not unusual for a start-up in Europe to talk with 100 venture capitalists to find early financing, if they do not yet have a substantial and predictable ARR, also because they are afraid of diluting their founders' equity. The investment climate in the US is, to say the least, much more geared to growth than to profit.

The following tables also show that, on average, the transaction size in the US is 2-fold higher than in the EU and that pre-money valuations in companies are considerably higher and increase over the lifetime of companies.

	US	EU
Angel/Seed	USD 0,6-2 million	EUR 0,9 million
Early VC	USD 6 million	EUR 2,5 million
Late VC	USD 9 million	EUR 5,1 million

Figure 12 Size of transaction - source Pitchbook

	US	EU
Angel/Seed	USD 6,5-7,5 million	EUR 4 million
Early VC	USD 30 million	EUR 8,5 million
Late VC	USD 110 million	EUR 14,4 million

Figure 13 Median Valuation - Source Pitchbook

When it comes to later stage VC (D, E-Round) or private equity investments in cyber security, companies in Europe are in unexplored territory. Most European start-ups have to look at the US, JP (SoftBank) or CN (Tencent), if they want to raise more than EUR 100 million, not to mention more than EUR 1 billion. In 2019, only one EU company (Northvolt) raised 1 billion,

⁶³ <https://techcrunch.com/2020/09/24/spotify-ceo-daniel-ek-pledges-1bn-of-his-wealth-to-back-deeptech-startups-from-europe/>

and this was done in a combination of a business round (Goldman Sachs, Volkswagen) and debt financing (European Investment Bank EIB).

The reason seems not to be the lack of available private money in Europe, but rather a difference in risk acceptance and perhaps a lack of knowledge of technology in the large private equity funds in the EU. The US private equity funds investing in cyber security are KKR, Advent, Insight, Blackstone and Thoma Bravo. In Europe, we only have EQT.

Observation: In the US, venture capital is invested significantly (three times) more in the technology sector than in the EU. Investment in start-ups is easier, especially if the company has no demonstrable income, growth is faster. Individual investments have a deal size two to three times larger in the U.S. and the valuation is also two to three times higher.

From the conversations with entrepreneurs, we noted:

- that they have a lot of problems selling their products to large companies and governments in Europe. There are too many formal obstacles (company age, certification, solvency, etc.);
- that they face major regulatory challenges. In Europe, companies (and their customers) must comply with individual national regulatory requirements, even in areas that are common in the EU (data protection, health, finance). This leads to a lot of overhead and delays. It is not possible to have knowledge of all these national regulatory restrictions. The EU-wide recognition of regulatory licenses should be promoted. In the US, there are far fewer problems of this kind, which clearly benefits start-ups on the US market. The US market is much more a single market than the EU.
- There is a difference in investment culture and ecosystem between the US and Europe. The existence of a 'starter ecosystem' in the US is seen as particularly attractive;
- Switzerland appears to have a very active startup scene. It has a very favorable arrangement for founders. There is a favorable regime for stock options (no capital gains tax) and the recruitment/dismissal of employees is not problematic. There is, however, a problem in immigration legislation, which hampers the recruitment of talent from outside the EEA.

From the discussions with investors, we noted as follows:

- Risk capital is widely available, including in Europe. The COVID situation has not dried up the sources of funding. On the contrary, investors are actively seeking a better return for their available capital;
- There are no significant legal or regulatory constraints for the fund managers that are perceived as cumbersome;
- Support mechanisms for risk investors have been established in Europe (European Investment Bank, European Investment Fund). However, they risk being adversely affected by Brexit. Given that a large proportion of investment opportunities are in cybersecurity in the UK, this is a real problem for fund managers. Acceptance of the European Investment Fund terms excludes the fund from investing in UK startups;
- Access to people/networks is important as a differentiator against the US. Founders with high visibility and good connections are very successful in attracting resources and starting/expanding their business, even in Europe. Founders without a network/visibility have difficulty in raising money;
- Everyone mentioned the importance of the ecosystem. But the biggest disadvantage for founders in Europe compared to the US is the difference in the human ecosystem.

In the US hotspots (NYC, Boston, Seattle, SFO) there is a much higher concentration of technology/technologists and founders and a much greater willingness to interact and help, even among competing startups. In the US, there is an ecosystem that promotes excellence and competition, which is very healthy and provides energy to founders. Every European founder would have to spend six months in the US. There's more energy, more open and more intensive networking. This difference is a decisive factor, including for investors. It may partly explain the differences in ticket size and valuation (in addition to the difference in risk culture);

- The availability of an attractive legal framework for share options is very important. Employees are currently required to invest to acquire shares in their business and capital gains are subject to a very complex tax system in most countries in Europe (including the Netherlands). This makes it difficult to attract talent. This is a reason for companies relocating to the US or the creation of subsidiaries to resolve it;
- Favorable reinvestment conditions for founders who realize an exit could also stimulate Angels' activity in the sector;
- Legislation allowing flexible recruitment/dismissal would be very helpful for start-ups.
- The biggest problem for start-ups is the availability of sufficient capital at an early stage, when the company does not produce a continuous and predictable revenue stream. Venture investors in Europe are more risk-averse;
- The feedback that the risk of investors in Europe being too soft on the founders after investing was interesting. They provide too much room for maneuver for (unsuccessful) founders and wait too long before they turn the screws or pull the plug. Investors in the US are far less tolerant of companies that miss their milestones;
- Another problem facing Europe is the difficulty of selling products to large companies and governments at an early stage. These are very reluctant to buy from companies that have existed for less than three years and cannot demonstrate a large customer portfolio. The risk may be partially offset by facilitated/privileged public procurement, grants or by public investment in equity of undertakings considered to be strategic;
- European venture investors do not see a (minority) participation of a US-based venture capital company as a problem for strategic autonomy. Minority shareholders do not have access to the technology of the company in which they invest. Some precautions may be taken (or even extended) in the term slides for the subjects. In the case of key technology, this may also constitute a potential protection that can be imposed by the government (40-50% of the valuation);
- Various fund managers indicated that they wish to build/maintain a strong reputation, including in the social sphere, but the main driver remains the creation of value for investors. It's not a problem to sell a company to the U.S. If the EU/NL wants to control the company, the state must be prepared to compensate for the difference.

Observation: There is no shortage of risk capital in Europe. But there is a big difference with the US in terms of the start-up ecosystem, investor risk assessment, a true single market (including regulation) and the legal framework in terms of stock options. It is also interesting in this context to study the example of Switzerland as a successful startup country.

3.3.2 Case: Startups in privacy protection technologies

In order to better understand the start-up dynamics in specific key technologies, this study examined technologies that can be an important part of the practical implementation of the GDPR and of privacy-protected data processing, including in the cloud.

The analysis was facilitated by the Momentum Cyber⁶⁴ CYBERScape inventory, in particular the companies listed under the categories 'Encryption' and 'Data Privacy'.



Figure 14 Startups in encryption - Source Momentum Cyber



Figure 15 Startups in Data Privacy - Source Momentum Cyber

Of course, Momentum Cyber has an incomplete and somewhat US-centric perspective, but an analysis of the selected companies provides some interesting insights. Of the 33 companies included in Momentum's 'Encryption' segment, only 5 are located in the EU and none has been established since 2015. Four new companies have been set up in the US since 2015, and they have already raised USD 75 millions in risk funding.

In the case of Data Privacy, only 1 out of 21 companies is established in the EU (established in 2013). Since 2015, seven new companies have been set up in the US, raising USD 2.6 billion(!) in risk capital. All these recently launched American companies refer to the GDPR in their positioning. Pro Memory, the GDPR was adopted on April 14, 2016 and entered into force in May 2018. The following picture shows the growth of scientific publications with "GDPR" in the title or abstract.

⁶⁴ <https://momentumcyber.com/docs/CYBERScape.pdf>

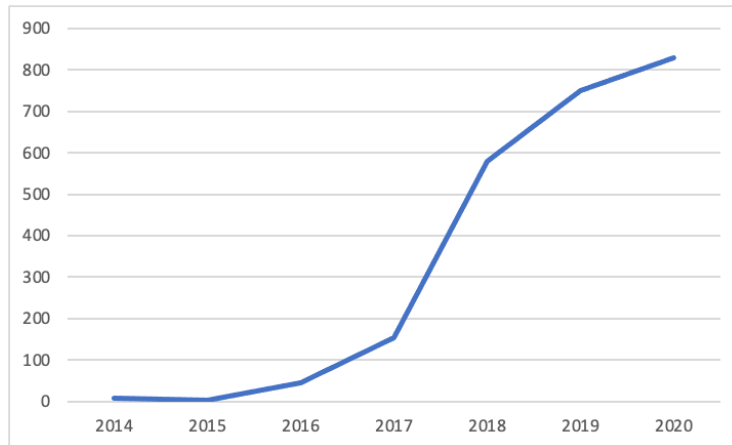


Figure 16 GDPR in title or abstract - source Dimensions

In two consecutive years (2017 and 2018), the RSA Innovation Sandbox winner came from these two segments of the CYBERScape. In 2018 and 2019 there was also a ‘runner-up’:

- Homomorphic encryption: **Enveil** (2017 winner), created by a former NSA and DARPA employee. Initially funded by Datatribe (US), followed by a round in which In-Q-Tel also invested. The 2020 A Round was run by a fund based in the United Kingdom (C5). USD 15 million already collected.
- Data privacy: **BigID** (winner in 2018) has already raised USD 146 million. The remarkable thing is SAP's investment in successive rounds. **Fortanix** (runner-up in 2018) has already raised USD 30 million, including from Intel.

Not included in the Momentum Overview is **Duality Technologies (US and IL)**. This company was established in 2016 and co-founded by Shafi Goldwasser. It specializes in homomorphic encryption and secure data processing. In 2019, it was a runner up in the RSA Innovation Sandbox. It's already raised \$20 million in Israel (Team8) and the U.S. (Intel). They have also received support from DARPA⁶⁵.

On the European side, the following companies (not included by Momentum) were identified:

- **Cosmian**, established in 2018 in Paris. USD 1,4 million collected from Angels, Elaia (FR), Blacailoux (FR) and Acecap (USA). Member of the Confidential Computing Consortium.
- **Decentriq**, established in 2019 in Zurich. Seed round of EUR 3,8 million by BToV (DE), Palladin (US) and Atlantic Labs (DE). Member of the Confidential Computing Consortium.
- **CYSEC** (formerly ArcaTrust), established in 2019 in Lausanne. Raised CHF 1,5 million in seed in 2020 (investor not publicly available). Member of the Confidential Computing Consortium. In 2019, the Commission received a grant of EUR 50 000 from the EU SME instrument. Also supported by Innosuisse, Eureka, FIT and ESA.
- **EXEC**, established in 2017. Raised EUR 12 million through an ICO.
- **Zama**, founded in Paris in 2019. Initial funding from the founder of Snips (Rand Hindi). A-round by Plug and Play (USA). CTO comes from CryptoExperts, which received EUR 1.85 million in EU research funding for homomorphic encryption.

⁶⁵ <https://www.prnewswire.com/il/news-releases/darpa-contracts-with-duality-technologies-to-develop-privacy-preserving-machine-learning-for-covid-19-research-301096126.html>

- **Stattice**, established in Berlin in 2017, seed funding from Capnamic (DE) and WestTech (UK). The company was hosted by DataPitch (<https://datapitch.eu/>), an EU-funded accelerator.
- **Madana**, set up in Berlin in 2017, has not yet raised venture capital.
- **Collibra** has also benefited from the GDPR requirements, even though it was established much earlier (2009). Raised USD 347 million. All the funds collected in subsequent rounds came from the US. Their solutions are not directly in the domain of encryption or differential privacy but rather in data classification.
- **Privatar**, founded in London in 2014, has already raised USD 150 million from 19 investors in the EU and the US. Offers privacy protection data solutions. Privatar and Collibra recently announced a cooperation. Privatar also cooperates with BigID.

Observation: Although significant investment has been made in EU research funding in these two areas in 2014-2020 and substantive legislation has been adopted (GDPR, *Privacy Shield*), this has not led to the creation of recent (created after 2015) global players in Europe. The incumbent European industrial groups have also been technically unable to capitalize on the privacy regulation in which the EU took the lead. Two European outliers (Collibra and Privatar) have been in existence longer and were successful without EU funding.

In the US, on the other hand, at least 14 companies have already been set up in these two areas since 2015, they have already received significant amounts of private investment. Some of them come from research that was partly funded by DARPA.

3.4 Standardization and market standardization

The Financial Times⁶⁶ recently reported on China's domination in setting standards for facial recognition and surveillance at the UN International Telecommunications Union. Similar observations have been made on 5G standards and related 5G security. ICT standardization is a future geopolitical battlefield.

Standardization provides widely agreed norms, rules, guidelines or specifications. They offer economies of scale, resulting in lower production costs, lower prices and greater consumer choice. They can ensure better protection of fundamental values such as privacy and common goods such as the environment. Standards enable connected infrastructure that span the world. Optimized digital standardization is global because most digital services are globally relevant and operate thanks to standards-based interoperability.

However, governments are now aware that they have given too much control over certain elements of critical digital infrastructure to the industry. This would not be a problem if the private sector were to deliver what governments want in terms of security. But this is not the case. Standardization should therefore be revalued as a matter of strategic autonomy. But the benefits of global standardization should not be lost⁶⁷. How can this challenge be addressed?⁶⁸

First, companies and technology experts, who are largely still implementing standardization processes today, should proactively cooperate with governments and address their concerns.

⁶⁶ <https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385>

⁶⁷ Bildt Report, Standardization for EU Competitiveness in the Digital Era, October 2019, <https://www.etsi.org/images/files/Calling-The-Shots-Standardization-For-The-Digital-Era.pdf>

⁶⁸ Paul Timmers, Geopolitics of Standardization, April 9, 2020, <https://directionsblog.eu/the-geopolitics-of-standardization/>

The time that engineers/engineers and policymakers lived in the separated worlds is over forever. Policymakers must also invest more time and resources in standardization.

Secondly, cybersecurity standardization should be discussed at the United Nations (where the Netherlands is very active). Measures to build cyber confidence will be effective if supported by standards, such as standardized information exchange on vulnerabilities and security certification of critical infrastructure.

Thirdly, a role should be given to stakeholders who consider cyber security standardization not to be geopolitical but rather to be a matter of global cooperation. They are looking for the proper functioning and continuity of their core activities, such as health, production or even the global Internet itself. This should not, in their view, be about narrow national security. They can use open source, open standards, standardized cyber security skills and promote globally recognized security standards such as ISO 27000.

Such actions would enable Dutch and European actors to take the lead in a revised standardization policy that is both suitable for global cooperation and respects sovereignty⁶⁹.

Observation: EU governments have long left standardization to industry and technology consortia. However, part of this industry is possibly steered by their Chinese government. Another part of the industry, including the US, is using standardization as a means of upholding commercial dominance. International digital standardization has thus de facto a delegated control over national security and cybersecurity from EU countries. The cause lies in the liberal market economy thinking ('the market is better placed to take decisions than the government') and in some cases in limited capacity and skills in the government (i.e. lack of strategic autonomy in the government).

3.4.1 Case: Privacy-preserving data processing

Key technologies for privacy-preserving data processing are very promising, but it remains a challenge if the company providing the services has access to the encryption keys and thus does not fully preserve privacy. A lot of market standardization is being done by the large cloud and network players from the US and China. These price their solutions as reliable and try to position their own solutions as standards. They use different methods for this purpose:

- Making their algorithms and software libraries available in open source
 - Microsoft has released a homomorphic library (Microsoft SEAL⁷⁰) and the Confidential Computing Framework⁷¹ as an open source.
 - IBM has released a homomorphic library into open source⁷²
 - Google has released "Private join and computer" into open source^{73, 74}.
- Consortia to define interoperability and industry standards:
 - The Confidential Computing Consortium⁷⁵ was established under the umbrella of the Linux Foundation. The members include Google, Facebook, Intel, Microsoft, Huawei, ARM/nVidia and ByteDance (TikTok). On the European side

⁶⁹ The revised EU Cybersecurity Strategy (16 December 2020) calls on the EU to 'strengthen its involvement and leadership in international standardization processes and to strengthen its representation in international and European standardization bodies and other standard development organizations'.

⁷⁰ <https://www.microsoft.com/en-us/research/blog/the-microsoft-simple-encrypted-arithmetic-library-goes-open-source/>

⁷¹ <https://github.com/Microsoft/CCF>

⁷² <https://github.com/homenc/HElib/releases/tag/v1.1.0-beta.0>

⁷³ <https://github.com/Google/private-join-and-compute>

⁷⁴ <https://cloud.google.com/confidential-computing>

⁷⁵ <https://confidentialcomputing.io/members/>

we can find Cosmian (FR), Decentriq (CH), Cysec (CH), Exec (FR) and Swisscom (CH). None of the major European industrial players are present at present;

- The Homomorphic Encryption Standardization Consortium⁷⁶, including participants such as Microsoft, Intel, IBM, Google, and Alibaba. On the European side, we find SAP, Mercedes Benz and Crypto Experts. Public organizations and academia participate, but European participation is very limited;

Intel plays an important role in this domain with its Software Guard Extensions (SGX) built into all modern Intel processors since 2015. SGX enables to create secure enclaves. Data is always encrypted, even in memory. Encryption is performed by the SGX hardware and is much more efficient than software alternatives (Trusted Execution Environment of TEE). Intel SGX is becoming a de facto standard for confidential computing, with large industrial players basing their offers on SGX.

Intel SGX is challenging digital strategic autonomy due to dependency on Intel, lack of accountability, and the risk that all encryption controls may be embedded in the hardware and be available to Intel. In addition, proof-of-concepts of successful and extremely difficult to detect malware attacks against SGX are already documented⁷⁷.

The traditional technical and market lead of European companies in the field of encryption by *hardware security modules* (HSMs) is eroding. The situation was further exacerbated by the condition of the European competition regulator for Thales when it took over Gemalto. It was considered that the acquisition of Thales would create a dominant position in HSMs. As a condition for the acquisition, a sale of subsidiary nCipher was imposed.

Observation: Large American companies have already invested heavily in research and technology in *confidential computing*, and they are determining the standards by imposing them through their cloud product footprint, by actively promoting some of their tools in open source or through industrial consortia such as the Confidential Computing Consortium. China's global players are also determining the level of play. European industrial partners should join the table to influence the outcome, and this is currently not the case.

Observation: With the widespread deployment of Intel's SGX cloud-encryption system, another dominant situation is emerging in which European industrial players are being sidelined. This is all the more painful because Europe was the technology and market leader in HSMs. The situation was facilitated by the strict application of European competition policy.

Observation: There is little industrial capacity and expertise in the Netherlands to meet the need for *high assurance* solutions from the Dutch authorities. The commercial market for this type of technology is insufficient to sustain its economic activity. Solutions by the major players in the US have inherent limitations. Alternative solutions can be obtained from European countries (FR, DE, CH). High-quality and reliable knowledge in the Netherlands to validate those solutions for the Dutch strategic autonomy should remain present in the Netherlands.

⁷⁶ <https://homomorphicencryption.org/>

⁷⁷ <https://arxiv.org/abs/1902.03256>

3.5 Procurement policy (public and private)

One of the tools for strengthening strategic autonomy is the public procurement policy. A number of aspects are well developed in Chapter 4 of the Defense Industry Strategy 2018⁷⁸. These can be applied in the broader domain of cyber security, extending the group of relevant departments from Ministries of Defense, EZK and BZ to JenV and BZK:

- The concepts of ‘open innovation’ and ‘fieldlabs’ and mission-driven innovation policy;
- Strengthening cooperation between Central Government, industry and knowledge institutions over the whole life cycle of critical components;
- Alternative forms of contract;
- Targeted acquisition strategy and proper balancing of exception clauses in the 2012⁷⁹ Procurement Act and the Public Procurement Act on Defense and Security⁸⁰. The definition of ‘sensitive material’ and ‘classified information’ is important here for the *high assurance* solutions. Due consideration should be given to the interpretation of the European Court of Justice in relevant cases such as C-187/16⁸¹ and C-615/10⁸²;
- ‘smart buyer’, ‘smart specifier’, ‘smart developer’ and ‘launching customer’;
- Industrial participation linked to procurement contracts in defense and security.

It is also appropriate to give greater visibility to the capabilities of the Committee on Defense Equipment Development (CODEMO) scheme⁸³ and to use it in a broader way to support strategic autonomy in the digital domain.

Purchases of cybersecurity-relevant infrastructure by private operators are not subject to public procurement laws. However, the government has the ability to influence private parties' purchases of key components in critical infrastructure. This could be achieved by:

- The application of the General Security Requirements Defense Contracts 2019⁸⁴ in a broader sense. More extensive application could have a broader impact on cyber security in the Netherlands and on strategic autonomy;
- Government procurement of key components and their mandatory use by critical infrastructure operators, such as in the National Discovery Network;
- The imposition of technical framework conditions on private operators as a condition for an operating license.

The General Security Requirements for Defense Contracts (ABDO) also include an obligation to report planned changes in control and corporate structure. Since 2014, the cabinet has the possibility to assess whether additional measures are needed to ensure sufficient national security in the event of a takeover or investment. For each vital process, an ex-ante analysis shall be carried out to assess whether protective measures against unwanted acquisitions and investments should be taken.

Observation: In the Netherlands, in the Defense and Security domain, there are already a number of legal provisions and processes in place that allow cyber security and digital strategic autonomy to be supported in a more structural and strategic way. However, many

⁷⁸ <https://www.defensie.nl/downloads/beleidsnota-s/2018/11/15/defensie-industrie-strategie>

⁷⁹ <https://wetten.overheid.nl/BWBR0032203/2019-04-18>

⁸⁰ <https://wetten.overheid.nl/BWBR0032898/2019-04-18>

⁸¹ <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A62016CJ0187>

⁸² <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:62010CA0615>

⁸³ <https://www.rijksoverheid.nl/ministeries/ministerie-van-defensie/contact/zakendoen-met-defensie/codemo>

⁸⁴ <https://www.defensie.nl/downloads/beleidsnota-s/2020/02/04/abdo-2019>

of them are still embryonic, too limited or insufficiently known. But a good basis has already been laid for greater strength.

A number of innovative ideas to safeguard the resilience of Defense could be applied in the broader field of (cyber) security.

The Defense Industry Strategy could play a broader and driving role in preserving and strengthening digital strategic autonomy.

3.6 Acquisitions (M&A)

The realization that takeovers can affect strategic autonomy is starting to grow, and we in Europe are beginning to realize that we have been too naive and too market-oriented in dealing with this for a long time. Known recent cases are in Germany with Kuka (sold to a Chinese company) and ARM (sold to nVidia in the USA via an intermediate step). Germany has amended its legislation on acquisitions of high-tech companies following the acquisition⁸⁵ of Kuka. This was also a reason to propose⁸⁶ the EU Foreign Direct Investment Screening Regulation.

State intervention (regulation, *golden share*, research funding) prevented acquisitions in Germany of, among others, Curevac and IMST⁸⁷. In the Netherlands, a recent example is Smart Photonics.

It is important to point out the widespread (active) market suppression of cybersecurity startups by the large incumbent players. Dominance as an economic objective is used, in a playing field without a lot of game rules, to prevent new players from entering the market, suppress or absorb them.

Economic boundary conditions for the investors in start-ups is, of course, also a factor in this. And for the founders there is the choice between becoming rich quickly or becoming economically powerless. Considerations of strategic autonomy must come from the public authorities. This requires a proactive and realistic approach, including in terms of the protection of start-ups and economic compensation. Innovative and integrated support for the crown jewels of the high-tech industry within the strategic autonomy in cybersecurity.

⁸⁵ <https://www.dw.com/de/altmaier-will-%C3%BCbernahmen-deutscher-hightech-firmen-erschweren/a-51447649>

⁸⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2019:079I:FULL>

⁸⁷ <https://uk.reuters.com/article/uk-germany-china-m-a/germany-blocks-chinese-takeover-of-satellite-firm-on-security-concerns-document-idUKKBN281U0>

Observation: Acquisitions are used by the incumbent players in the market to strengthen their dominance and absorb new, innovative companies. These developments should be closely (actively) monitored in terms of strategic autonomy. New tools with a combination of regulation, participations and conditions in term sheets, smart purchasing policies, innovation support can selectively and in combination deliver optimal results.

It would be useful to compare the Dutch approach with the experience in other European countries (UK, FR, DE, CH, FI).

3.7 Comparison of policy approaches

3.7.1 The American approach

Compared with the EU, the US has adopted a more strategic, forward-looking and coordinated approach to scientific and technical developments, strongly anchored in the desire to remain the strongest nation in terms of military power.

The US approach combines the selection of themes with research funding, public procurement, government-funded early-stage investment, export restrictions and merger and acquisition intervention. The center is their understanding of "foundational and emerging technologies". The selection of strategic topics is used to define scientific and technical areas that deserve funding by public authorities such as DARPA, IARPA, NIST, MITRE, NSF, etc. It is also the driving force behind the NSA's (non-public) internal research and development.

The Bureau for Industry and Security (BIS) maintains two lists of technologies of strategic importance under the Export Control Reform Act (ECRA), basic technologies and emerging technologies⁸⁸. Contributions to these lists were recently requested. They offer an interesting perspective. They include topics like computer vision, expert systems, speech and audio processing, AI, cloud technology, quantum computing, quantum encryption...

These lists of "foundational and emerging technologies" in the US can be seen as a useful input into the decision-making process in selecting topics for EU and/or national research funding.

It is also interesting to analyze recent investments by the CIA's funding instrument, in-Q-Tel.

	Lead	Country		Created
Truwave		US	Machine vision	2017
Morpheus Space		DE	Space, propulsion technologies	2018
Snorkel AI		US	AI	2019
Sayari Labs		US	Fraud and threat detection	2018
Ocient		US	Big data analysis	2016
Lilt		US	AI	2015
Toposens	Yes	DE	Machine vision, autonomous driving	2015
Coder		US	Software quality, Kubernetes	2015
AI.Reverie		US	Synthetic data, training AI	2017
Q-Ctrl	Yes	AU	Quantum computing	2017

Figure 17 Recent investments in startups through In-Q-Tel - source Crunchbase

⁸⁸ <https://www.federalregister.gov/documents/2020/08/27/2020-18910/identification-and-review-of-controls-for-certain-foundational-technologies>

Surprisingly, two out of ten investments were in start-ups in Germany. In one case, In-Q-Tel was even the main investor. The case of Morpheus Space is particularly intriguing as it was founded on a seven-year research effort at Dresden University in 2018. The company has developed a propulsion system for small satellites.

In 2018, Morpheus Space received technology transfer support from Dresden-Exist, but then it went to the U.S. for growth. In 2019, the company started operating at the Techstars Starbust Space Accelerator in Los Angeles. The A round was led by Vsquared (DE) and included Airbus, Lavrock (US), Techstars (US) and Pallas (US).

There is no evidence that EU or ESA funds (research, innovation or procurement) have been provided to Morpheus Space. Given the time frame (creation in 2018 and venture capital financing in 2019), it would anyhow have been difficult to obtain research funding in the light of the existing administrative processes.

The Morpheus Space case shows the flexibility and effectiveness of the US in a strategic area and in a practical case where the opportunity was created by EU research and expertise.

More generally, the previous chapters on science and finance show that the US, with similar levels of investment in science and technology, is two to three years ahead of the EU, focusing efforts on areas of strategic importance and is much more efficient in stimulating start-ups and growth in these areas.

Some instruments used by the US deserve to be assessed on their merit for the EU:

- In-Q-Tel as a government-funded investment vehicle at startup finance
- The rapid funding of research in science and start-ups by DARPA and IARPA
- Exceptions for public procurement

Reference is often made to how the US public departments of DARPA/IARPA are driving academic R&D and industrial R&D, strategically oriented on a selection of relevant technology. Low threshold for good projects, quick decisions. But competitive, also on the ball in monitoring and corrective if the milestones are not respected. Some European academics and companies have already found the way to DARPA and prefer this funding to EU funding.

DARPA works with a limited number of project managers who are paid competitively and who have a high degree of autonomy. They enjoy a high degree of respect and a high in demand in industry when they leave DARPA. DARPA manages an annual budget of USD 3.4 billion.

In October 2020, the White House identified⁸⁹ the strategic autonomy approach to be used for each of 'Critical and Emerging Technologies': risk management, strategic partnership, or exclusively managed under its own control (this option is not available to the EU or the NL). It is striking that the global common good option is not recognized. This may reflect skepticism about multilateral cooperation.

Observation: DARPA/IARPA have already been taken as an example for initiatives in Europe in the past. The UK is currently considering the creation of a similar organization. In-Q-Tel is also starting to invest in European startups from a strategic perspective.

3.7.2 The British example

The United Kingdom's approach is very much in line with the US in terms of strategic autonomy. In the UK, too, intelligence and defense play an important role in determining the

⁸⁹ <https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf>

agenda and gaining and maintaining control over key technologies. Offensive power is used here as an equally important argument as the defensive.

The Defense S&T strategy has recently been published⁹⁰. It indicates how R&D and R&D investment will be used to support the military's main operational needs. A quote from the foreword; "by excelling in S&T we can secure our future strategic advantage". Prospective research and coordination are important building blocks of the strategy.

Five "capability challenges" are identified:

- Pervasive, full spectrum, multi domain Intelligence, Surveillance and Reconnaissance
- Multi-domain Command & Control, Communications and Computers (C4)
- Secure and sustain in in the subthreshold
- Asymmetric hard power
- Freedom of Access and Maneuver

Efforts are planned to support these five areas. An interesting concept in this document is "Generation after next", looking beyond the horizon in terms of *capabilities* but also the technology that can support such future *capabilities*.

The GCHQ Intelligence Service has its own cyber accelerator and innovation program⁹¹ and invests in R&D and R&D of relevant technology. The Ministry of Defense also has its own DASA accelerator and funding program⁹². At the highest level, there are again plans to set up a DARPA-like organization in the UK.

The UK National Cyber Security Center, NCSC-UK, is part of the GCHQ intelligence service. Information collected by the Intelligence Community is also actively used to secure the security of the public and health network in the Protective DNS system⁹³. This is part of the Active Cyber Defense program in which GCHQ plays a leading role.

3.7.3 China

According to Tai Meung Chang⁹⁴, China's 'strategic industries' are driven top-down by the 'national security apparatus' - which includes the military, internal security, law and order, intelligence and information control devices - [and which] occupies a powerful presence in China's cyber affairs. Moreover, the development of the cybersecurity industry and associated information technology domain is significantly driven by the development of technological capabilities.

China combines protectionism with national champions, technology transfer from abroad to Chinese companies and the promotion of Chinese technology standards both at home and internationally. China also has 'cyber sovereignty' as its primary starting point for several years. Jonathan Holslag argues in detail that China combines this with trade policy and foreign investment (Belt & Road Initiative, M&A) to gain⁹⁵ strategic foreign influence. The EU sees

⁹⁰ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/927708/20201019-MOD_ST_Strategy_2020_v1-23.pdf

⁹¹ <https://techcrunch.com/2015/11/18/uk-gov-to-invest-in-security-startups/?guccounter=1>

⁹² <https://www.gov.uk/government/organisations/defence-and-security-accelerator>

⁹³ <https://www.ncsc.gov.uk/information/pdns>

⁹⁴ Tai Ming Cheung (2018) The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities, Journal of Cyber Policy, 3:3, 306-326, DOI: 10.1080/23738871.2018.1556720.

⁹⁵ Jonathan Holslag, The Silk Road Trap: How China's Trade Ammunition Challenge Europe, Polity Press

China as a 'systemic rival' and proposes a renewed transatlantic alliance to reverse⁹⁶ China's move towards world-domination in technology.

Opinions may differ on the ultimate intentions of the Chinese leadership. However, it is clear that China combines a range of policy instruments, top-down, with a long-term perspective. And so far, to a large extent, successfully.

3.7.4 The situation in the Netherlands

In the Netherlands, there is not such a strong link between defense and innovation policies compared to the US and the UK (and France). And the Netherlands is far away from an integrated approach to policy as it exists in China. More generally, a recent SWOT analysis of the Dutch cybersecurity value chain concludes that: "The Netherlands hardly has a manufacturing industry in cybersecurity. Hardware and software come from abroad. The Netherlands is mainly involved in the provision of services. The landscape is fragmented; both in the business sector and in the public sector. Geopolitical considerations can lead to a desire for greater independence. Well-qualified people are sometimes insufficiently available in the Netherlands'⁹⁷.

Nevertheless, there are a number of concrete strengths that the Netherlands can build on to strengthen its policies, including and without being exhaustive:

- the strategic orientation and broad composition of the CSR
- the authority of the WRR
- the operational effectiveness of the NCSC
- the threat information of the AIVD
- the public-private strength of the Defense Industry Strategy
- the proposals of EZ on a new knowledge momentum
- the innovative approach to broad awareness and knowledge of EPC.NL
- academic reputation in a wide range of areas from quantum technology to privacy and open-source initiatives
- the strong voice of the Netherlands in the EU
- the international authority of Dutch cyber diplomacy.

Observation: The US, the UK and China link their strategic autonomy directly to their desire to become, and remain, militarily autonomous and dominant (and for the US and China also in the digital domain). To this end, they have created processes and resources that continuously link the objectives with all the necessary means to achieve them in a coordinated manner. A key element in this is a list of key technologies.

There is also much greater synergy between the defense/intelligence services and the active cyber security of the countries concerned.

⁹⁶ EC and EEAS, 2 Dec 2020, A new EU-US agenda for global change, https://ec.europa.eu/info/files/joint-communication-new-eu-us-agenda-global-change_en

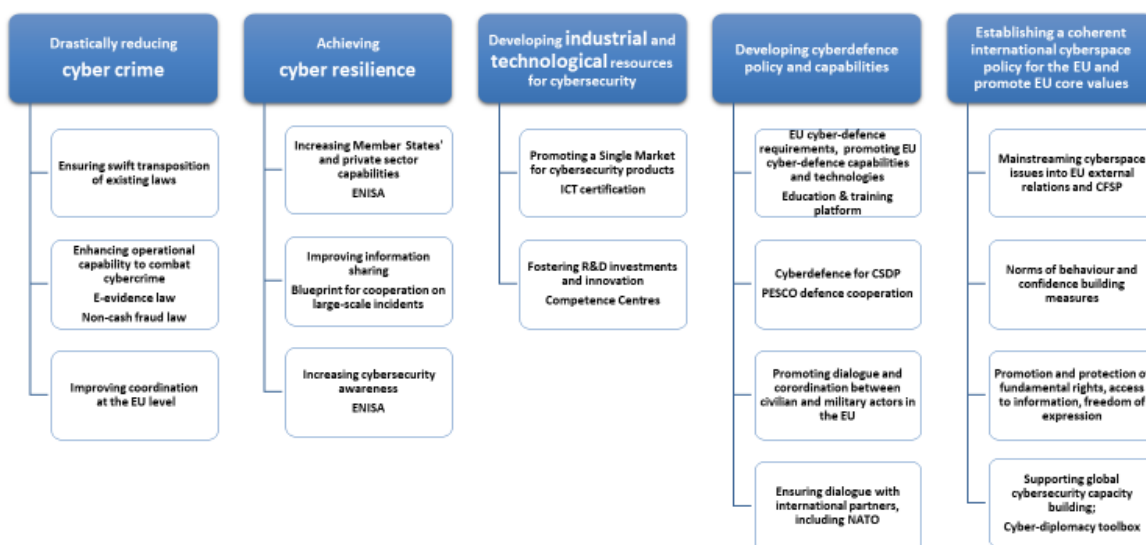
⁹⁷ KPMG, Oct 2020, SWOT Strategic Value Chain Analysis commissioned by EZK

4 Policy instruments

Reference has already been made to policy instruments. In addition, there is a related description of instruments in a recent TNO report⁹⁸.

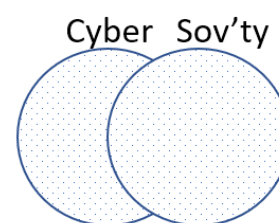
The EU cyber security measures are summarized in the European Commission diagram below. The comprehensive framework is the 2013 EU Cybersecurity Strategy. It was expanded in 2017. A further review has been done end 2020.

EU Cybersecurity Strategy



Picture sources: based on EC SWD(2017) 295

The policy instruments are summarized below, indicating their relevance to cybersecurity and sovereignty. It shall also indicate the current status and motivation and, where appropriate, what is expected in the future.



This study focuses on measures that concern both cybersecurity and sovereignty, and therefore shows some overlap between these two areas. Symbolically marked with:

Cybersecurity-motivated measures relevant to sovereignty:	
Sovereignty-motivated measures relevant to cybersecurity:	
The measures most closely linked to both the broader cyber security policy and the broader sovereignty policy:	

⁹⁸ TNO 2020 R11599 'Strategische Autonomie op Cybersecurity'.

For the most coherent and strong policies, it is advisable to include cyber-security measures that take strategic autonomy in the broader framework of strategic autonomy policies⁹⁹. Conversely, where strategic autonomy measures are taken, it is strongly recommended that their possible relationship with cybersecurity be included¹⁰⁰.

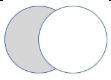
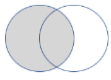
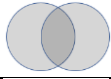

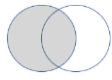
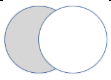

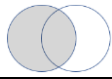
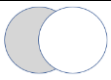





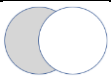

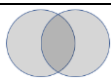











Some observations on the detailed (but not exhaustive) overview given in the following tables:

- Only part of these measures concern both cybersecurity and sovereignty. The overview suggests areas where a stronger focus on the combination of cybersecurity and sovereignty is needed or desirable in the future
- This overview allows policymakers to analyze whether sovereignty and/or cybersecurity might have a role to play in their policies in general¹⁰¹.
- Further policy instruments could be envisaged such as:
 - o Supplier exceptions for cyber security public procurement
 - o Tax policy/capital gains tax
 - o Open-Source Policy
 - o Competition policy
 - o Public participation in risk capital (cf. In-Q-Tel in USA)
 - o Investment support.
- The strength of measures cannot be derived from the list. For example, EU industrial policy is voluntary and lacks legislative power or funding.
- Not directly derived from the tables, but following the case analyses, there is little synergy between measures. Nevertheless, integrated policies are a necessity given the threats and an opportunity to be more effective with measures.
- Italics in the tables indicates future policy (announced or suggested in this study).
- Section 6.6 goes into more detail on recent and announced EU policies and legislation.

⁹⁹ This will be opened up at European level by closely linking legislation on cyber and non-cyber protection of critical entities (i.e. the NIS2 Directive and the CER Directive, see Chapter 4 and Section 6.6).

¹⁰⁰ One example is the digital euro, which can strengthen financial autonomy but must also be cyber-safe.

¹⁰¹ The method of analysis is therefore also applicable to situations which concern sovereignty but not cybersecurity, such as the impact on sovereignty of European/NL telecoms policy, where prices are depressed and competition is increasing, but also domestic innovation and independence are at risk of erosion.

Facilitating				
	EU measure	Cybersecurity and/or Sovereignty	Netherlands measure	Cybersecurity and/or Sovereignty
Strategy and Agenda	CS Strategy 2013 - 2020 CS 2020 Strategy - EU-US Agenda 2020	  	CSR to recent <i>CSR future?</i>	 
Monitoring	ENISA threat report		NL threat report; <i>Strategic Autonomy Monitor?</i>	 
Knowledge	EU R&D AI policy Quantum R&D flagship	  	Current R&D cyber <i>Future R&D Cyber?</i> NCSC	  
Cyber Skills	Cyber Month (ENISA)		ECP-NL Cyber	
Support Infrastructure	Connecting Europe Facility Cloud Policy, GAIA-X	 	NL Cloud policy	
Market stimulating	Resilience & Recovery Fund Purchase R&D	 	<i>Government as launching customer?</i> <i>Government cyber-R&D purchase?</i>	 
Ecosystem (industrial, innovation, knowledge, policy)	Cyber Competency Centers; ENISA; Industry, 2020 ¹⁰²	  	EZK Platform ¹⁰³ StartupDelta	 









¹⁰² COM(2020) 102 final, 3 March 2020.

¹⁰³ Cybersecurity and Innovation Cooperation Platform

Regulatory				
Market-prescriptive or market-monitoring	GDPR		AVG	
	CyberAct Certification			
	FDI Regulation		M&A/FDI control agency	
	EU export controls		<i>For specific companies:</i>	
	Wassenaar		- <i>poison pill</i>	
	<i>AI liability</i>		- <i>golden share</i>	
	Digital Services Act, Digital Markets Act		- <i>public participation</i>	
			- <i>financial support</i>	
			- <i>clauses in term sheets</i>	
			<i>Investment Review Act</i>	
Operational cyber-resistance	CERT-EU		NCSC	
Cyber-crime	Non-cash fraud		<i>Judiciary-chain cloud?</i>	
	E-Evidence			
Critical infrastructure and services	NIS Directive 2016		NIS Directive	
	NIS2-Directive 2020			
	5G Security Recommendation		WOTZ ¹⁰⁵	
	CER Directive ¹⁰⁴			
Critical assets (state secrets, industrial knowledge/IP, data spaces, identification of citizens and businesses)	IP Action Plan 2020		State secrets	
	.eu Regulation 2003		<i>Knowledge security initiative EZK</i>	
	<i>EU Data Spaces '21</i>			
	eIDAS 2014			
	<i>eIDAS 2021</i>		<i>Deep security?</i>	

¹⁰⁴ Critical Entities Directive, 16 December 2020 (successor to Directive 2008/114/EC — identification and designation of European critical infrastructure)

¹⁰⁵ Wet Ongewenste Zeggenschap Telecom

International				
International standardization	ETSI, CEN/CENELEC			
	CS 2020 Strategy			
Rights and values	UN OEWG, GGE			
	CS 2020 Strategy			
International Conventions	Budapest Convention on cybercrime			
Defense	CSDP		Defense Industry Strategy	
	NATO			

5 Assessment framework

The observations in this study lead to a rich set of insights and triggers for government intervention. The insights and the triggers are the starting point of an analysis to assess whether the state should intervene to strengthen strategic autonomy or to restore balance and how it should do so. All elements shall be collected in a case that is assessed in an integrated manner and potentially leads to an intervention.

A case is expressed in a number of relevant domains in which it is or may be handled. In these areas, information can also be gathered in an active and continuous way to identify developments that distort strategic autonomy.

These areas form one dimension of the assessment framework. The second dimension of the review framework is the relevant policy areas.

This chapter provides the presentation and explanation of the assessment framework. The following chapter applies the framework to concrete cases.

5.1 Focus

The cases in the previous chapters provide a lot of material to describe the concepts that enable strategic autonomy to be addressed in a strategic but also practical way.

This study and the review framework are limited to those factors which concern both cyber security and influence strategic autonomy. In other words, the digital aspects of strategic autonomy and, in particular, those concerning cyber security. Such a focus corresponds to the mission and (limited) scope of this study.

One criterion for translating this focus into practice is to verify whether a case concerns ‘key technologies’. Another form of focus could be to limit the possible policy instruments. However, this would not be justified. A general observation is that:

General observation:

1. Coherent and integrated policies are needed, others are doing so in the geopolitical field, but there is still rare to see this in the Netherlands and the EU.
2. Strategic autonomy and thus sovereignty are hardly taken as a starting point for policy. This poses a high risk.
3. Proactive monitoring of triggers for strategic autonomy and cybersecurity has a great value in responding in a timely and coherent manner.

5.2 Key Technologies

In order to support the focus, a list of ‘key technologies’ that allow cyber security to be monitored or mitigate cyber security risks is useful.

Observation: A list of key technologies should be developed and maintained as an essential tool for identifying, assessing and influencing relevant changes in our environment.

Countries such as the US and the UK use lists of key technologies to guide their interventions related to strategic autonomy. In their case, these lists are not only viewed economically and socially, but are also linked to military strategic objectives.

In the Netherlands too, the concept of key technologies has already been suggested. In this context, the recent CSR opinion *‘Towards structural mobilization of innovative applications of*

*new technologies for the cyber resilience of the Netherlands*¹⁰⁶ is pertinent. The CSR opinion contains four recommendations:

1. The government should develop an integrated policy on new technologies with an impact on cyber resilience.
2. The government should map the technical developments relevant to exploiting and creating opportunities on an annual basis, safeguarding cyber resilience and the wider digital autonomy of the Netherlands.
3. The government should pursue an active industrial policy for cybersecurity.
4. The government shall encourage (inter)national cooperation in relevant technologies for cybersecurity.

Additional existing connecting factors in the Netherlands have been developed by the High-Level Group on Key Technologies in 2017¹⁰⁷ and the AWTI opinion of January 2020, 'Strengthening the choice of key technologies'¹⁰⁸.

The Defense Industry Strategy 2018 Policy Paper also refers to (emerging) technology areas that may be important in the future. This policy paper also balances the need for state intervention and the desired level of government involvement (Defense in this case).

At international level, there is a list of dual-use goods and technologies¹⁰⁹ in the Wassenaar Arrangement. The Wassenaar Arrangement¹¹⁰ is supported by 41 countries, including the US and the EU. Particularly relevant in the list¹¹¹ are Category 5, "Telecommunications" and "Information Security". The Wassenaar List could also contribute to the areas that could be considered important for digital strategic autonomy.

With regard to key technologies, there are several questions to ask:

- Is the technology crucial in the narrow (specific) sense or in the broad (fundamental) sense and therefore essential?
- Is the technology unique (no alternatives) today or in the future?
- Is the technology owned by an organization which is under-controlled from a strategic perspective?
- Can the risk be reduced by other technological components or by regulation or market access conditions?

¹⁰⁶ 18 September 2020 CSR opinion 2020, No 5

¹⁰⁷ <https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/kwantitatieve-analyse-van-onderzoek-en-innovatie-in-sleuteltechnologieen-in-nederland>

¹⁰⁸ <https://www.awti.nl/actueel/nieuws/2020/01/30/advies-krachtiger-kiezen-voor-sleuteltechnologieen>

¹⁰⁹ <https://www.federalregister.gov/documents/2019/05/23/2019-10778/implementation-of-certain-new-controls-on-emerging-technologies-agreed-at-wassenaar-arrangement-2018>

¹¹⁰ <https://www.wassenaar.org/>

¹¹¹ <https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf>

5.3 Assessment Framework Overview

The suggested assessment flow and intervention logic shall be:



1. **Identify** the **trigger(s)**, which can be identified in a reactive or proactive manner, and may be specific or sector-wide
2. **Analyze** the market and regulatory **dynamics** and the technology dynamics associated with the activated trigger(s), for example with models of Porter
3. Provide the **case description**, a ‘narrative’ in terms of relevant **domains** or factors (from the models), including the level of **control** in the sense of strategic autonomy¹¹²
4. **Focus** on factors affecting cyber security and strategic autonomy
5. Define the **objectives**: define the desired result in strengthening strategic autonomy
6. Identify a coherent set of **measures (interventions)** to strengthen capacity and capacity to build or restore balance.

The overall approach is outlined below and then explained.

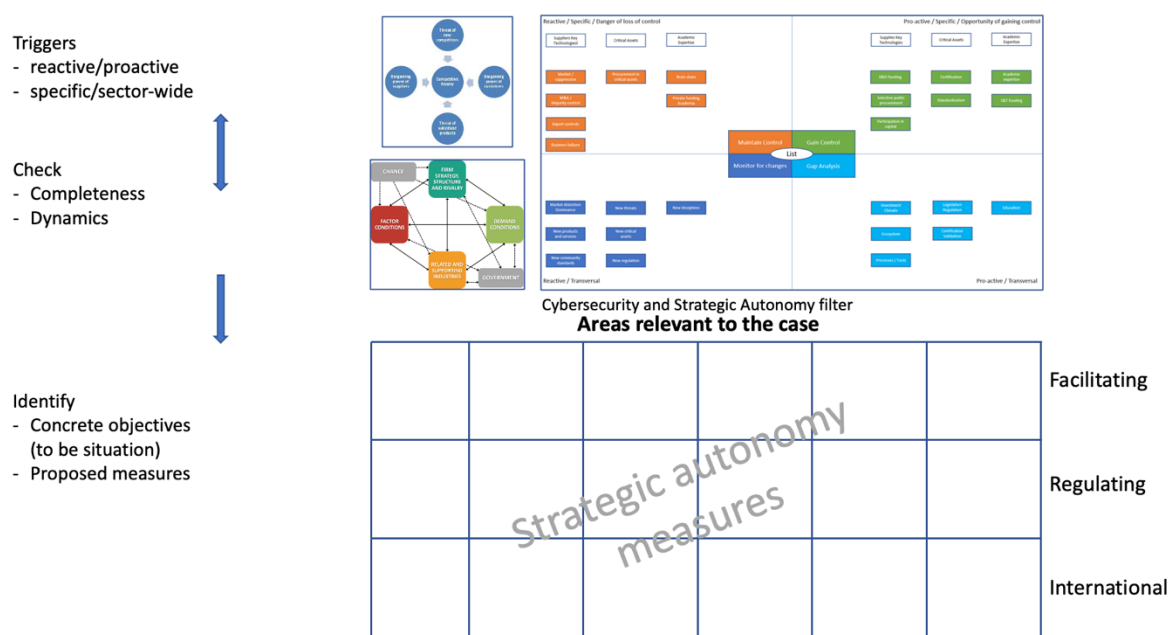


Figure 18 Assessment Framework

This scheme, starting from the top, provides a ‘Trigger Diagram’, whose function is to identify triggers for intervention, and two Porter models to analyze the dynamics of knowledge, industry, market and government. Porter models and trigger diagram serve to provide a complete case description, which then focuses on strategic autonomy in cybersecurity (steps 1, 2, 3 and 4). On the basis of the data collected, control objectives are linked to interventions that are both possible and desirable (steps 5 and 6).

¹¹² Control of the ability and resources to decide on the future of the economy, society and democracy.

One practical approach is to start at the trigger level. Then the entire situation needs to be mapped into a Case (the 'as is' situation) in order to understand the dynamics. Then the desired result must be defined, that is, the goal in terms of strategic autonomy, the 'to be' situation. The next step is to define the relevant instruments for intervention and finally to verify the coherence of these instruments. Where necessary, the monitoring of interventions may also be established.

Two Porter models are used for analysis. The Five Forces model is about the forces that act on a *specific company*, corresponding to the top half of the trigger diagram. The Diamond Model describes forces in a *sector as a whole*, corresponding to the lower half of the trigger diagram.

On the one hand, the two models of Porter are designed to group the origin of "triggers" in order to prevent the loss of certain triggers and the arbitrary choice of triggers to concentrate on. Moreover, models help to see related factors and related policy instruments. They help to understand dynamics such as the interaction between regulation and market development. This can be seen as the **top-down** approach.

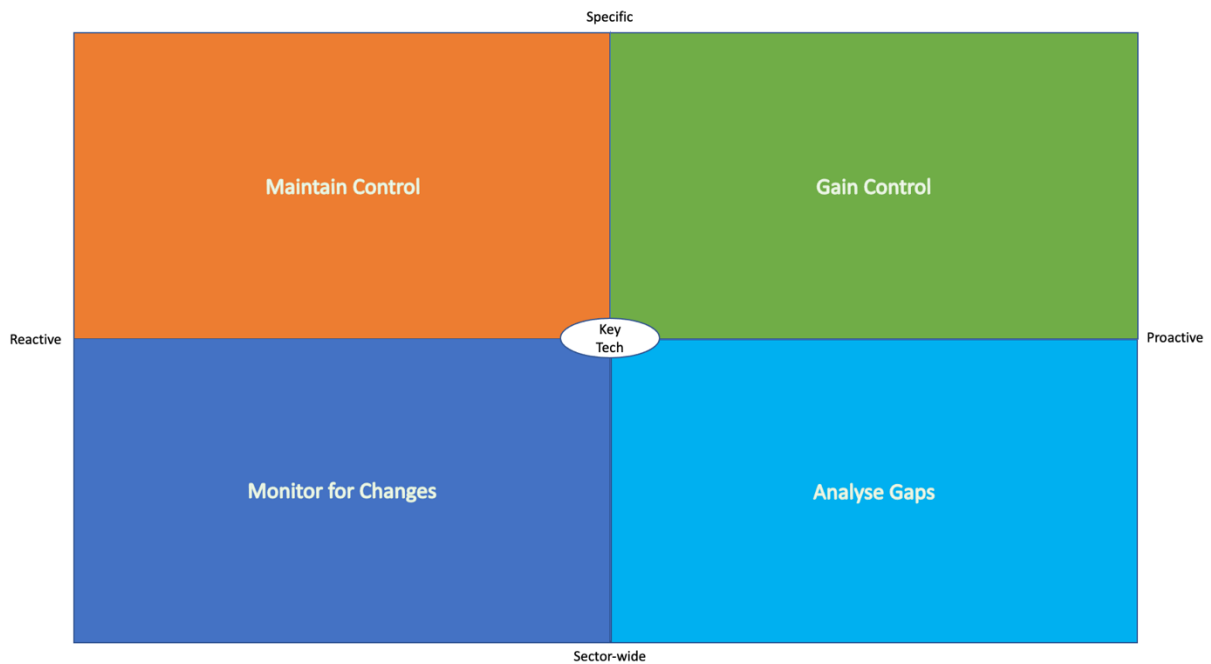
On the other hand, the **bottom-up** analysis follows a series of triggers, grouped together in the 2x2 overview described in the next section. The two dimensions are the identification process, reactive or proactive, and the level of trigger, which is specific or sector-wide.

One reservation is that this will provide a rich but not complete analysis: the interactions will be more complex than provided for in these models. Moreover, the models chosen have largely focused on competitiveness rather than - for example - on government policies, let alone an integrated picture of interplay between government and market dynamics (which use recent *governance* insights). The development of more integrated models is outside the scope of this study.

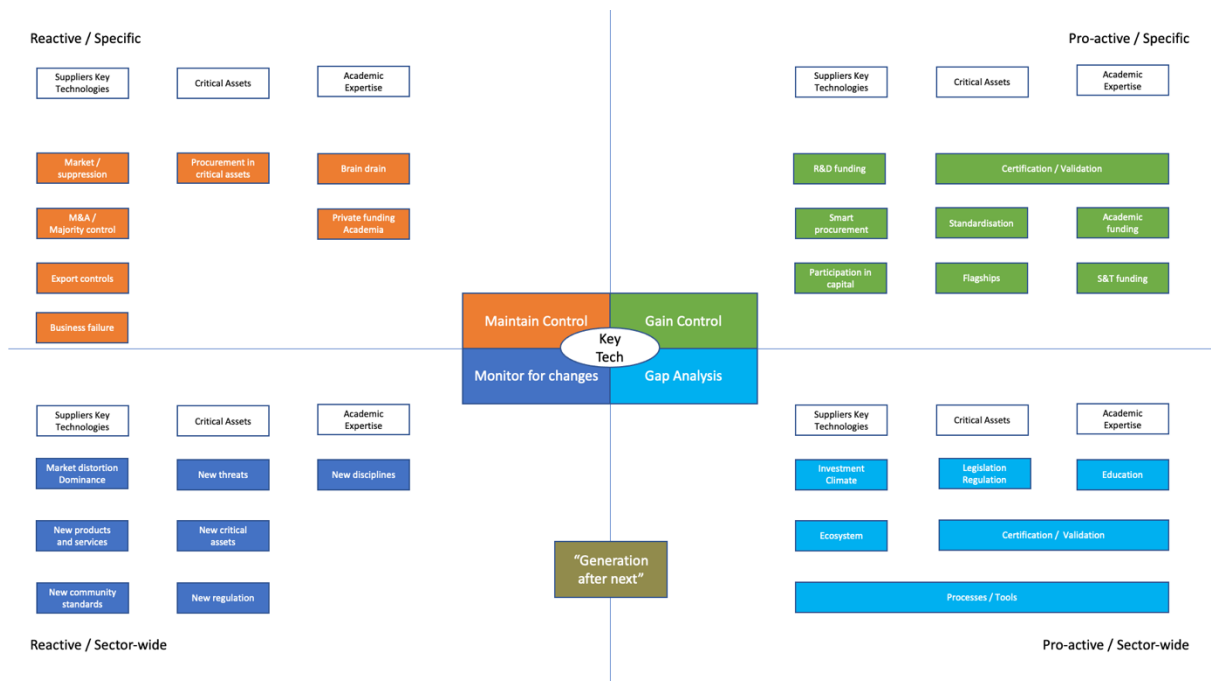
Finally, the assessment framework is modular, in the sense that if desired, the Porter models and the Trigger Diagram can be used separately or replaced by alternative analysis tools, e.g. *agent-based modelling*, *system dynamics*, and *multi-modelling*. What matters is to arrive at a complete and coherent case description that will enable to assess the impact of one or more interventions based on the chosen policy instruments.

5.4 Trigger Diagram

The cases analyzed in our study lead to a summary of relevant domains from which triggers can be collected and where impact is possible. The Trigger Diagram has two dimensions: reactive or proactive and specific or sector-wide. As a result, four quadrants emerge: "Maintain control", "Acquire control", "Observe changes" and "Analyze and close gaps".



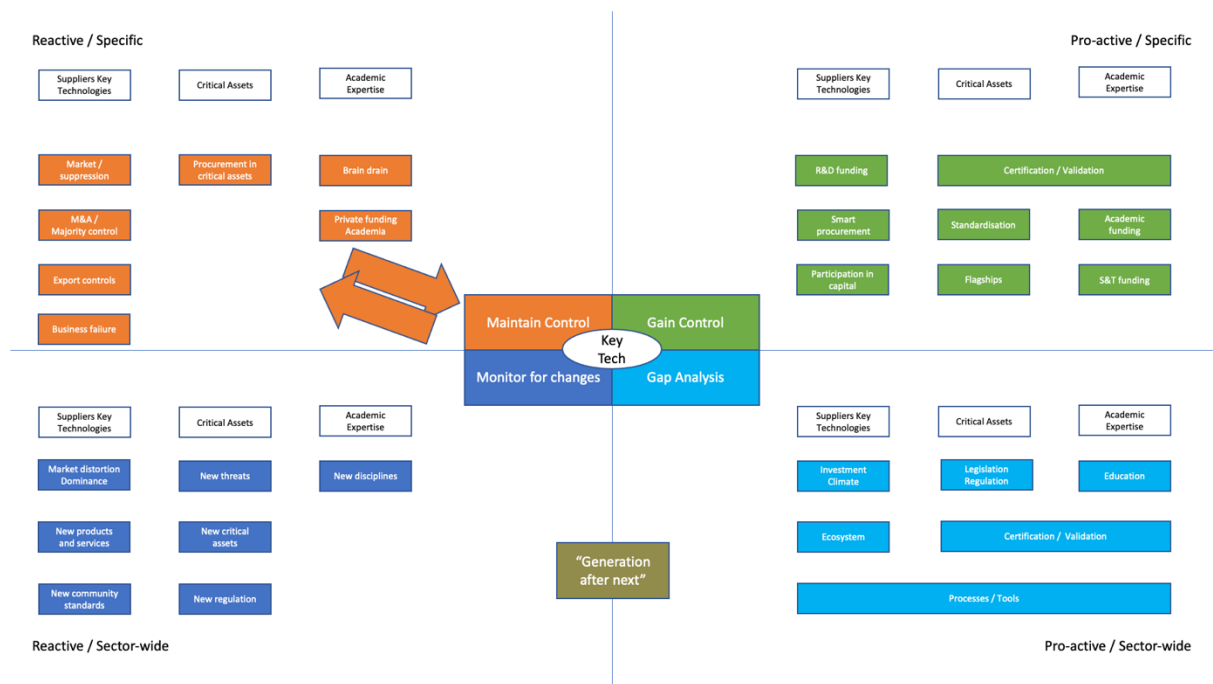
Each quadrant also distinguishes between the domains of key technology providers, the critical assets that use key technology, and the scientific world that lays the foundation for key technologies. An explanatory legend of the different domains and the link to the cases is included in Annex 2.



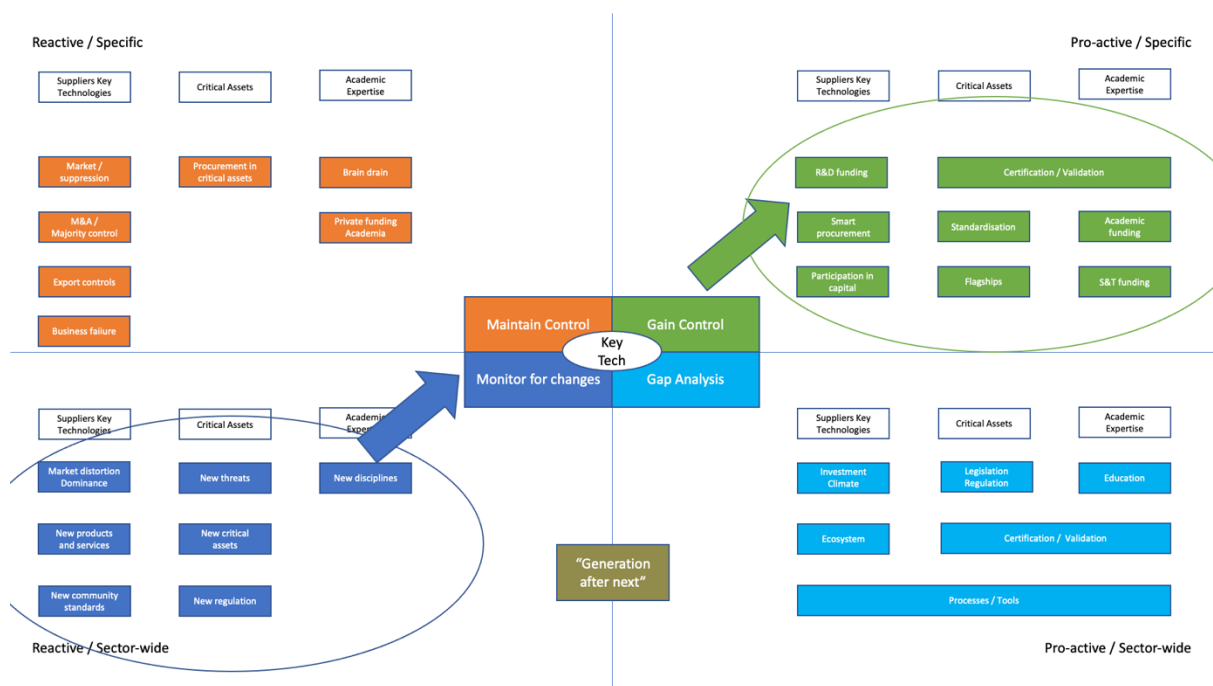
Central in the Trigger Diagram is a permanent (inter-departmental) activity to identify and assess relevant developments in the various domains related to the key technologies.

Observation: relevant developments in the domains should be monitored, analyzed and assessed on a continuous and proactive basis. This activity is **interdepartmental** within the government **and generally involves several stakeholders**.

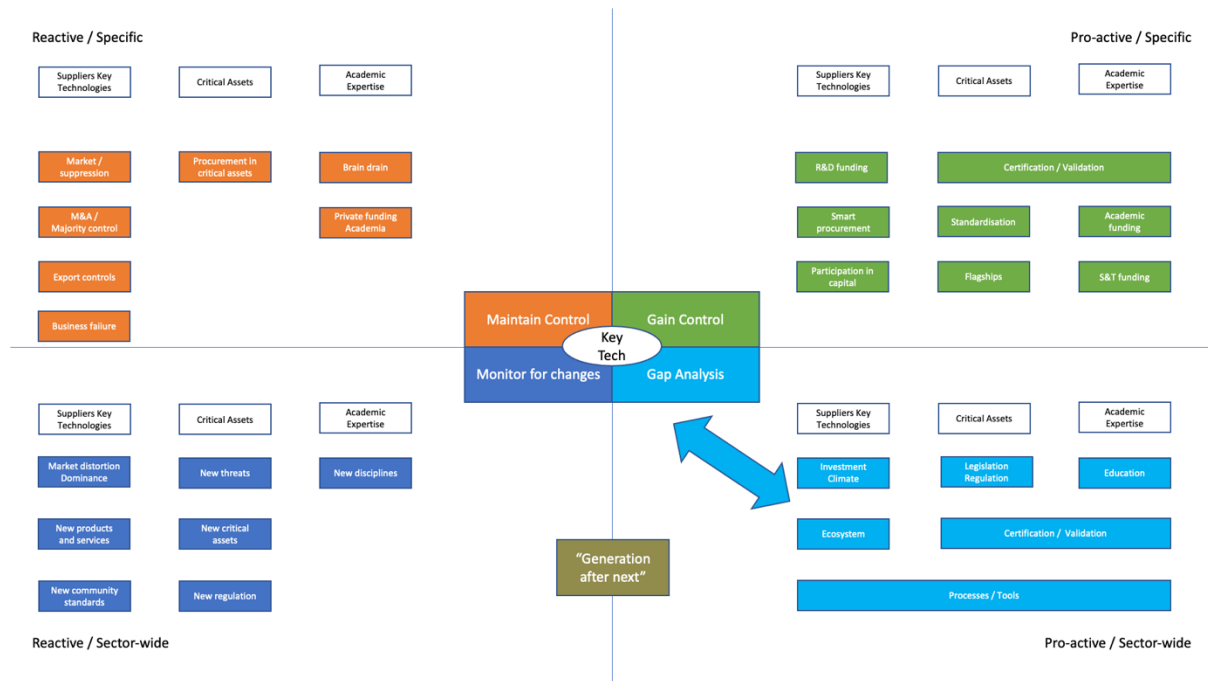
The operation of the Trigger Diagram can be explained with some examples. A trigger in the quadrant on the top left is a specific situation in which an existing control is in danger of being jeopardized. An example of this is the announced acquisition of a unique key technology supplier. From this observation, action can be taken to maintain control.



A trigger in the bottom left quadrant can come from a sector-wide relevant evolution that can trigger a new cyber security threat (or opportunity). One example of this is the development of new key technologies such as privacy-protective data processing. If this is observed, proactive action can be taken by supporting the development and use of this new technology in the areas described in the quadrant right-hand top. This could be combined with legislation and regulation (in the lower right quadrant). One example is the GDPR.



One final example is the comparative analysis of tools and legislation in other countries with regard to digital strategic autonomy. Which countries are doing it differently and better than the Netherlands? What are they doing differently, and can it be transferred to the Dutch situation, and what should be done for this?



5.5 Porter models

Porter's Five Forces model explains the forces that are working on competition at company level. In short, at company level, it explains that competition dynamics are influenced by the power of suppliers and customers, the threat of new entrants (which must overcome *barriers to entry*) and the threat of substitution. This model is well known when it comes to analyzing strategic competition, that is, business strategy.

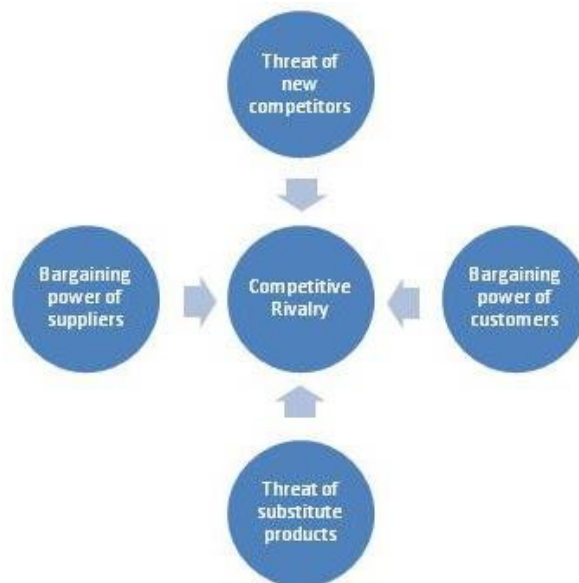


Figure 19 Porter Five Forces model (source: see Annex)

The Porter Diamond model is at a higher, aggregated level and concerns the competitiveness of a country or industry as a whole. As it operates at state level, this model is closest to strategic autonomy. This model explains the relationships between factor conditions (such as capital and knowledge), key features of the industrial ecosystem such as the degree of competition, the demand side at macro level, and the larger ecosystem of upstream industries. This model also reflects the influence of the government. This model has been used, including by the OECD, for strategic analysis of industrial policy in Finland, Mexico and Taiwan.

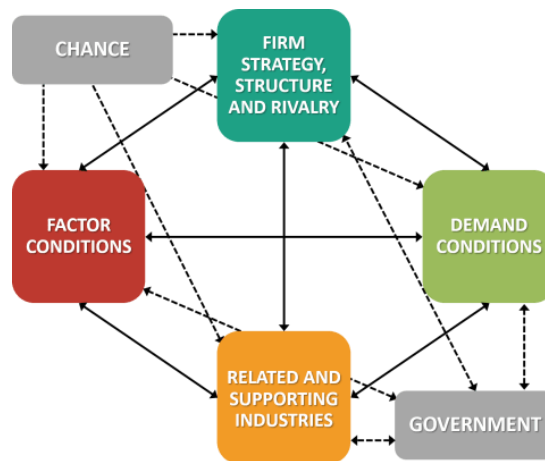


Figure 20 Porter Diamond Model (source: see Annex)

The Porter models do not represent macro-level trends such as geopolitics (e.g. US-China rivalry), social change (e.g. populism), environment (e.g. climate). These are all trends that also concern sovereignty, impact the Diamond model, and then lead to changes in the Five Forces model. Conversely, changes that directly affect companies or organizations (and are therefore analyzed in the Five Forces) may become state level issues, i.e. operate in the Diamond Model and thereby eventually enter into strategic autonomy and thus sovereignty. A brief explanation of the two models is given in Annex 8.3.

5.6 Relevant domains, control and strategic autonomy test

The case description as developed in the trigger and model analysis leads to a number of relevant areas, such as technology suppliers, factor conditions such as academic knowledge and critical resources, and the nature of public procurement. These are areas for considering possible public intervention.

A next element in the analysis is 'control'. The analysis should describe the change - loss or increase - in control over power and resources to determine the own future in the sense of strategic autonomy. From being sufficiently specific in relation to control follow directly concrete objectives for restoring or strengthening strategic autonomy and cybersecurity.

What is the scope of control and what kind of control? Categories of resources and capabilities of strategic autonomy can illustrate this (see footnote 9):

Intangibles:

- Knowledge: brain drain, relocation of R&D abroad (cf: encryption, AI)
- Skills: low government experience with technology and policy combination (cf: cloud)
- Organization of processes/procedures: Inability to check the inspector (cf: 5G)
- Decision-making culture: erosion of business cooperation - public authorities (cf: former industrial policy taboo)
- Cross-compliance: for the participation of foreign companies in the European or Dutch market (cf: 5G, EU Cloud Policy)
- Political: Reflection of priority for strategic autonomy in political party election programs (currently: limited and implied¹¹³).

Tangibles:

- Financial: shift from long-term continuity to short-term profit (case: M&A)
- Staff: no attraction for new entrepreneurs by the departure of large companies (cf: ARM)
- Research facilities: necessary scale-up impossible by M&A legislation (cf: complaints from cyber security industry¹¹⁴)
- Industrial facilities: Outsourcing of industry chains critical to crisis (cf: computer chips for maintenance equipment).

A possible future step in these methods could be a systematic strategic autonomy test in the sense of the EU regulatory impact assessment or the Dutch Explanatory Memorandum¹¹⁵.

¹¹³ Bernold Nieuwesteeg, Cybersecurity in the TK 2021 election programs (v. 0.3).

¹¹⁴ ECIL, European Cybersecurity Industry Leader report, <https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders>

¹¹⁵ L. Moerel and P. Timmers, *ibid.*

6 Application and validation of the assessment framework

This chapter provides for the application of the assessment framework to certain specific cases in order to understand the source of the impetus for public action in the field of strategic autonomy and cyber security.

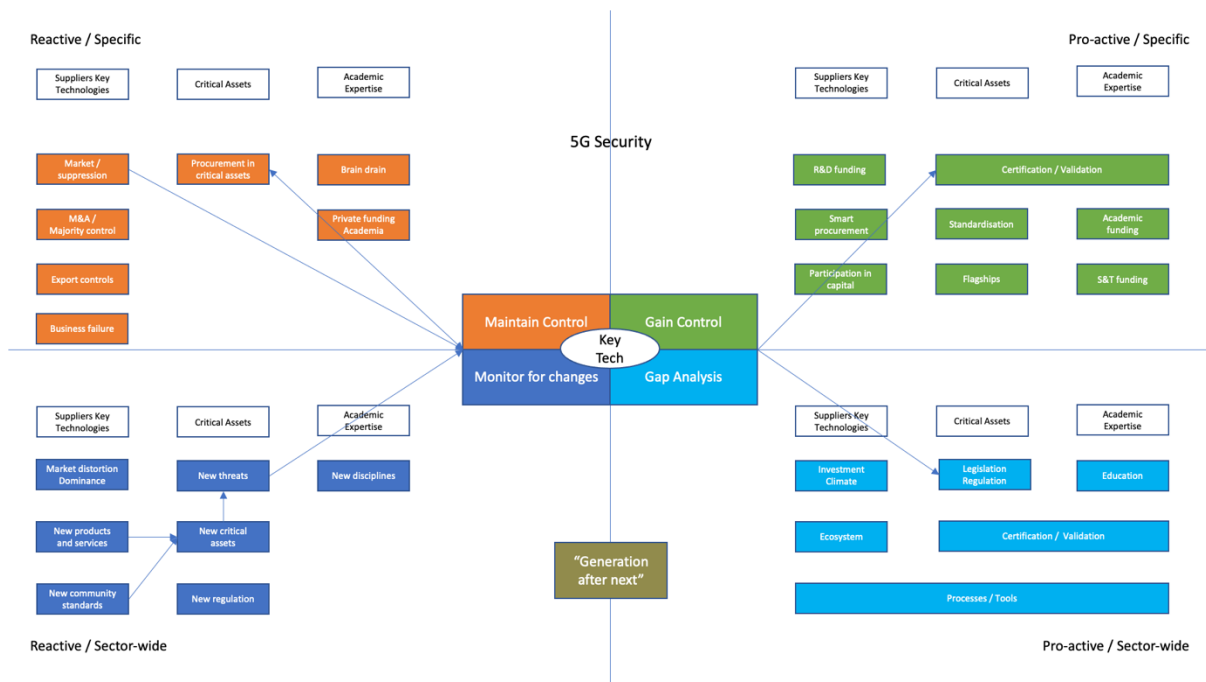
6.1 5G security

One important trigger in this case is the pressure from the US to move away from Huawei as a supplier of telecom equipment. In the Five Forces diagram, this changes the supply side for the telecom operators, it changes the competition between telecoms operators, but it also forms part of the broader public image of the industrial ecosystem for telecoms equipment. Another reason for this is the above-mentioned statement by President Macron: "We have left our sovereignty to the telecoms industry". It is also fits with the relationship between government and industry in the industrial ecosystem in Porter's Diamond diagram. Finally, a trigger that is more gradually emerging is the introduction of 5G as a new (key) technology.

If we look at this last trigger in the Trigger Diagram, we start at the bottom left, when new products and services are created (5G technology developed by the network product manufacturers) and the development of industry standards by suppliers. These products and services are included in new critical assets that are essential for national interest (5G networks replace existing internal company networks, Internet becomes the corporate network) and thus give rise to new cyber security risks (quadrant at the bottom left).

Back to the Trigger Diagram, it is observed that European suppliers (Nokia and Ericsson) are being pushed out of the market presumably with Chinese state aid (for Huawei) and that critical telecom infrastructure operators are opting for the Chinese supplier for cost reasons, among other things. This in turn strengthens the external influence and thus the loss of strategic autonomy or control over these critical assets.

In response, national authorities exerted pressure on telecoms operators and an EU 5G Cybersecurity toolbox was developed that combines legislation (quadrant right bottom) and certification/standardization (quadrant right top) to be implemented by operators.



To date, a number of areas in the scheme have not been applied in a coordinated and integrated manner in this particular case. In particular, there are (as yet) no measures to strengthen the telecom equipment industry in the EU and the Netherlands through:

- Selective use of (EU) R&D funding
- Selective purchase by the government
- Flagships as demand-side incentive (from industry, government, defense)
- Government participation in the capital of 5G vendors
- Transatlantic cooperation.

Furthermore, in 5G Case, it seems advisable to look "strategically" beyond the current horizon and to better address "Generation after next". A summary of the outcome of the 5G Security Assessment Framework application is given in Annex 4.

6.2 NIS Directive

The trigger in this case is the revision of the NIS directive. In the Diamond Model, this trigger comes from the government block (see Figure 20 **Error! Reference source not found.**). The previous analysis has already revealed shortcomings in the directive in force. The most important intervention is a review of the legislation.

The revised NIS Directive was proposed by the European Commission on 16 December 2020 and is still based on risk management rather than strategic partnership building for exclusive competences or cyber resilience as a general good. It has been steered to a limited extent and indirectly only by strategic autonomy.

The analysis of market dynamics suggests looking at related industries in order to strengthen cyber resilience as a sector through this review. This concerns for example cyber-incident analysis, cyber-defense/offensive and cyber-insurance. In some of these, the Netherlands already has a position, but in others it should also consider gaining sovereign control. Moreover, the reality is that some of the sectors covered by the (revised) NIS directive are highly dependent on foreign suppliers. Leaving intervention to the EU may not be enough. There is also an opportunity and need to strengthen cyber skills, both as a factor condition (input) and demand-side condition.

Coherent support measures could then be:

1. promotion of industrial cyber-analysis activities through co-investment, public procurement, industrial-academia-government partnerships, possibly including export promotion
2. strengthening skills in the new areas covered by the NIS revision (e.g. setting up ISACs for the pharmaceutical and medical equipment industry and in the public sector)
3. Promoting internationally the risk management approach of the revised NIS Directive, in particular for the confidence-building measures to implement UN norms and values in cyberspace.

6.3 e-ID

Awareness has grown strongly about the risks of dominant positions of Internet platforms also in the area of identification - for example. via Facebook and Google ID. In the Trigger Diagram the trigger comes from the bottom left quarter. In the Five Forces diagram, this is a trigger that comes from the supply side. This dominance represents a significant loss of strategic autonomy. Another weaker trigger is the emergence of a self-sovereign identity, which is a substitute product.

A third trigger is the forthcoming revision of eIDAS. This is, in the Porter Diamond Model, a government-initiated trigger. This offers an opportunity to lower entry barriers. This is very important because the government, as an e-ID provider, is a late provider, facing significant barriers to entry (*barriers to entry*). This opportunity is also available for *self-sovereign identity* initiatives.

To make the eIDAS review effective as a game changer, more will be needed than a new eIDAS law. The Trigger Diagram suggests possible additional interventions, but before going into these, the question, in the context of this study, is whether e-ID is sufficiently relevant to cyber security.

This is not to a large extent the case for e-ID in itself, but more clearly for the security insurance services (authentication of websites, possible attribute *assurance*) that have related industries and academic skills that are to some extent present in the Netherlands. However, security assurance services are much broader than those covered by eIDAS.

For e-ID, there is therefore a clear need and possibility to strengthen the (digital) strategic autonomy, but intervention should be part of a broader plan that is not just about cyber security. Within this broader policy, the recently proposed Digital Markets Act, even if limited in this context to e-identification (see also Table 1 Recent and Expected EU Legislation below), is also appropriate.

6.4 Homomorphic encryption

This is a technology trigger. These usually lead to replacement products, in this case with implications for the secure data analysis by cloud companies. A short analysis for the follow-up of this trigger is as follows:

If we want national competitiveness to change in the cloud (that is, we want to address a strategic autonomy issue), we need to consider activities in this form of encryption in the Diamond Model. It is then relevant to think about factor conditions (knowledge base, investments in homomorphic encryption), a demand condition (e.g. public procurement), public influence (e.g. mandatory safe data analysis), and an understanding of the desired competitive industrial ecosystem (e.g. industrial alliances, landscape of mergers and acquisitions).

6.5 M&A of a strategic autonomy-essential company

This could be a hypothetical acquisition, e.g. a critical infrastructure operator, or a past acquisition such as FOX-IT by NCC. This is a typical reason for the entry of new competitors. Such a company may, for example, have a basic technology or an essential infrastructure. There are other triggers that can come from one of the Five Forces. A previous example is that Huawei would have entered into the market through price undercutting.

6.6 EU policies and legislation

Relevant EU policies are developing rapidly. Chapter 4 gives an overview of where cybersecurity and strategic autonomy are most important in this policy. The table below summarizes the needs for attention, according to the analyzes in this study, for recent policies from 2020 or for those expected in the first half of 2021¹¹⁶.

¹¹⁶ See European Commission Work Program 2020 (update of May 2020) and 2021 (October 2020).

Table 1 Recent and Expected EU Legislation

Data Governance Act	Nov 27, 2020	Limited relevance to the combination of cybersecurity and strategic autonomy. Skills in the supervisory administration. Opportunity for supporting industry (in security assurance and EU cloud).
NIS2 Directive	Dec 16, 2020	see more detailed analysis in section 6.1.
Cybersecurity Strategy	Dec 16, 2020	coherence of industrial ecosystem measures, R&D/key technologies, cyber certification, cyber resilience, standardization, cyber & defense, international standards and values.
EU-US transatlantic agenda	Dec 2, 2020	Consistency of the EU-US partnership and Cybersecurity strategy, White House strategy, means of multilateral instruments such as international standardization, WTO, cooperation in key technologies, joint agenda of 'global common goods' ¹¹⁷ .
eIDAS	Q1 2021	see more detailed analysis in section 6.3
AI Liability in high-risk applications	Q1 2021	Impact of AI on cyber incident analysis and response to sovereignty, e.g. crisis responsibility; coherence with NIS2 Directive; AI skills. Opportunities and necessity for Dutch knowledge and industry.
Horizon Europe, Digital Europe and Connecting Europe Facility	Q1 2020	10-20 billion work programs in EU R&D, applications, cooperation and infrastructure; For strategic autonomy, choices must be consistent with investments in startups, scaling up and public procurement in the Netherlands and Europe. See e.g. homomorphic encryption, section 6.4 and 5G security.
Digital Services Act	Dec 15, 2020	Large online gatekeeper platforms should perform risk assessment of 'inauthentic' use (e.g. fake news and deep fakes) but are not required to provide reliable authentication as advocated ¹¹⁸ .
Digital Markets Act	Dec 15, 2020	Take back e-ID from gatekeeper platform control. Does not mean that national or European e-ID should be offered (perhaps in the coming eIDAS review?). Neither does it improve the unbundling of trust & assurance services, so strategic autonomy improves only partially.

Negotiations on EU e-evidence are still under way to streamline cooperation with service providers (e.g. cloud providers) in order to provide authorities with rapid tools to obtain electronic evidence. It remains to be seen whether there will be a transatlantic agreement that will bridge the gap between the US Cloud Act and the EU Evidence Act.

¹¹⁷ If the Biden administration consistently shows greater openness to multilateralism, there will be room to promote worldwide common interest in cybersecurity, which is particularly relevant for the Netherlands.

¹¹⁸ Bart Jacobs, iBestuur Online, 9 Dec 2019, <https://ibestuur.nl/weblog/teken-tegen-nepnieuws> and 24 Dec 2020, <https://ibestuur.nl/podium/ontwakende-europese-digitale-sovereiniteit>

6.7 Other trigger cases

Other examples of triggers are:

- A basic technology is taken over by one unique user (European or non-European). This affects the factor conditions in the Diamond Model. An example might be quantum encryption.
- Acquisition of a 'critical' company.
- Discover spying or surveillance, such as the Snowden or Cambridge Analytics Cases.
- Ransomware in hospitals that are widely endangering the continuity of healthcare at a critical time (e.g. during the COVID-19 crisis).
- The ever-increasing debate on the risks of backdoors for lawful interception.
- Critical moments for choices in basic/critical science and technology. See above for the imminent political decision-making on the use of the billions of EU R&D Horizon Europe programme. In addition, the recent White House Critical & Emerging Technologies list¹¹⁹ and **President Xi Jinping's 2025 plan**.

The analytical method is also applicable to larger challenges. Here are three examples.

6.7.1 Protection of sensitive public sector information.

This is of direct importance to the government from justice to defense, but also, for example, to the privacy of individual citizens and confidence in the rule of law. This relates to the aforementioned analyzes of cloud, (homomorphic) encryption, deep security, and also to AI. Given the infrastructural aspects of information and data management, Galileo's experience is also important, and thus the industrial ecosystem. This is a case where the 'Brussels effect'¹²⁰ can be applied internationally, the leverage effect of EU legislation, and also the handling of extraterritorial claims by foreign powers (cf. Cloud Act, Schrems II).

6.7.2 Espionage and stealing of intellectual property.

This is of major direct importance. This relates to the review of the NIS Directive, 5G security, EU rules on the use of European R&D funding, Foreign Direct Investment Regulation and M&A triggers and also to the economic opportunities to stimulate a security assurance industry. This also has a strong international dimension (norms and values of state behavior).

6.7.3 Online disinformation and fake news

This is very important for the functioning of democracy but also for the effectiveness of the state, public sector and business in implementing policies (e.g. having regard to anti-5G and anti-vax campaigns).

¹¹⁹ Ibid.

¹²⁰ Anu Bradford, <https://www.law.columbia.edu/faculty/anu-bradford>

7 Recommendations

7.1 Strategic autonomy is crucial in cyber security

Strategic autonomy is increasingly essential in cybersecurity and requires **continued attention and commitment to the highest level**. This is insufficiently the case at present, leading to a creeping erosion of sovereignty. Increasing digital dependence, new technologies and market players, new threats are catching up with us. If we respond, it is often too late. Letting this to continue is not justified.

We must and can **now** take action to raise political, policy and implementation awareness, provide instruments and act in practice. The Netherlands should step up its efforts with partners in the EU and internationally.

7.2 Proactive and comprehensive approach

An uncoordinated and fragmented approach is of little use. Policy coherence and explicit prioritization are necessary. This has already been noted on several occasions, but where this study differs from previous opinions, this strategic autonomy is a necessity and priority for cyber security and provides a practical framework for assessment and action. In addition, the study provides a large number of relevant and up-to-date topics for getting to work now.

Our first recommendation concerns strategic governance:

1. Organize the cybersecurity policy as a **continuous, proactive, and integrated activity**;
2. Use the proposed methodologies and the **review framework**;
3. Make a **priority** of strategic autonomy in cybersecurity,
4. Define **objectives** for **strategic control** in cybersecurity, both in general and by case. In any case, the priority is to strengthen strategic control in cybersecurity with regard to:
 - Cloud: privacy-protecting, secure for business information and shielded from third-country government intervention, taking into account GAIA-X and EU policies
 - Secure communication: country-wide, robust and secure networks for state, business and citizens (including 5G and next generation security, and IoT)
 - Deep security (advanced digital security services and solutions): long-term (including post-quantum) protection of sensitive information.

In addition, a list of **key technologies** is an important aid for determining objectives.

7.3 Reinforcing existing strengths

There are already a lot of strengths in the Netherlands to address cyber security in a good way in relation to strategic autonomy. These include the strategic orientation of the CSR, the operational effectiveness of the NCSC, the threat insights of AIVD, the public-private strength of the Defense Industry Strategy, the EZK proposals for a new innovation and knowledge boost, academic reputation, and the international authority of Dutch cyber diplomacy.

Our second recommendation is that building on existing strengths, multiple departments, agencies and stakeholders **work together at strategic and policy-operational level**, possibly with further reinforcement, and with guidance from the highest level.

The identification of those relevant parties, their precise role, and organizational gaps to fill in time were not part of this study. Our analysis, however, as a third recommendation highlights **important issues** for each policy area:

- Economic policy and implementation: in particular, investment, FDI and M&A conditions, innovation ecosystem, industrial/logistic flagships, competition policy,

market access, standardization and industrial cooperation, participation and protection of "crown jewelry" against acquisitions

- Knowledge policy and implementation, in particular support for key technologies, interaction with a strengthened ecosystem of innovation and market, pre-standardization
- Defense policy and implementation, in particular coherence of defense industrial policy with economic, knowledge, and intelligence policies, extension of smart purchasing methods to other security domains
- Intelligence on threats, in particular with attention to the threat of potential erosion of values and standards, the threat of loss of intellectual property or sensitive government information and the threat of black swan events
- Operational cyber resilience and response, in particular country-wide approach, closer cooperation with the telecoms operators and strategic interaction with the other functions
- Policy and implementation on crime and public security, in particular where deep security in cloud, AI and the functioning and trust of the rule of law
- Policy and roll-out of digital public services and public procurement in particular as regards cybersecurity and strategic autonomy (e.g. e-ID)
- The EU and international, in particular the Netherlands-EU coherence, contribute to current and nearby EU policies, and a balanced approach to strategic autonomy for a Netherlands that is and remains 'open to the world'.
- Strategic advice, meeting, prospective analysis, independent "control of auditors", and wider implications for the economy, society and democracy.

Other policy areas will, of course, also play a role, for example tax policy to position the Netherlands as an attractive startup country, such as by taxing risk investments in a competitive manner (stock options, angel investment).

Finally, a list of key technologies can be used as a common thread for supporting and coordinating the desired cooperation.

7.4 A practical approach

A concrete result of this study is the **assessment framework**. The recommendation is **to work** with this framework **practically and without delay**. Three examples of using the framework and current triggers to perform the case analysis and illustrate policy coherence are:

5G security: There is a concrete policy framework, namely the European 5G Security Recommendation and the Dutch telecom law. However, the case analysis shows that the 5G security innovation ecosystem can be further strengthened. This may include: by stimulating investment to convert knowledge into innovation, strengthening the cooperation between supply and demand with flagships in the Netherlands (e.g. logistics, health, industry). Greater active participation is also required in international 5G/6G standardization initiatives and a clearer EU/Dutch policy on unfair state aid in China. In addition to the case analysis in section 6.1, Annex 8.4 provides a matrix of measures.

Defense - Civil: the Defense Industry Strategy, with the inception of key technologies, identifies concrete instruments. This includes: innovation support, smart purchasing methods, the use of the CODEMO scheme, and industrial participation. Countries such as France, the UK and the US use defense strategy as a driving force for both cybersecurity and strategic autonomy. As indicated above, materialization is related to knowledge policies (e. g.

deep security, AI), economic policy (e.g. purchase of innovation in security assurance) and intelligence. Some of the tools and processes of the Defense Industry Strategy can be generalized into the broader domain of security and cyber security, contributing to further understanding of government participation in the cybersecurity market in terms of risk capital, government as launching customer, government procurement of R&D, and a sectoral strategy as a driver.

EU - Netherlands: European policy in cybersecurity and strategic autonomy is accelerating. The Netherlands will have to and will be able to play an active or even proactive role. For cybersecurity and strategic autonomy, the key issues from the beginning of 2021 are: the NIS2 Directive, for which the Netherlands could take a country-wide approach, the forthcoming revision of the eIDAS Directive including the relationship with the recent Digital Markets Act, cloud policy, and the forthcoming AI policy for high-risk applications. In all these cases, as illustrated in more detail in the case analyses of the NIS Directive and the eIDAS Regulation, further coherent action is needed. Among other things, this is raising awareness, stimulating trust/assurance services and partially keep these in own hand, and assessing the impact of AI in cybersecurity on democratic control on the rule of law and the economy. There is also a clear need for a better investment climate in order to continue to grow, and for adapting competition law to geopolitics.

These three examples will provide an incentive to analyze other situations. In particular, this can help to formulate **technology policies** that are of great importance and urgently needed from a strategic autonomy and cybersecurity perspective.

This approach can also provide further strategic analysis and coherence in order to address **major challenges for cyber-protection of society, economy and democracy**. These are challenges such as protecting sensitive government information, industrial cyber-espionage, and online disinformation and undermining democracy.

Finally, the study contains a variety of insights (relevant threats, new developments in basic technologies, gap analysis with other countries) that can provide a source of reflection and action. Our advice is therefore to **widely disseminate** the **study** to the relevant departments of ministries and relevant stakeholders.

8 Annexes

8.1 Annex 1: cybersecurity startups: success and failure

Success stories (unicorns) with little or no EU funding for research and development:

Collibra, founded in 2008 in Brussels, has raised a total of USD 347 million. All the funds collected in subsequent rounds came from the US. 700 employees.

Elastic, established in 2012 in Amsterdam, IPO in 2018. Has taken over Endgame in 2019, an American EDR company. All the fund raising came from the U.S. 2000 employees.

Avast, established in 1988 in Prague, IPO in 2018. 2000 employees.

F-Secure, established in Helsinki in 1988, IPO in 2002. 1700 employees.

Darktrace, founded in Cambridge in 2013, has raised a total of USD 230 million from British and American resources. 1 300 employees.

Privatar, set up in London in 2014, raised USD 150 million in the UK and the US, but also from industrial parties (ABN/AMRO, Salesforce, HSBC, CITI)

Cases with significant EU funding for research and development:

Guardtime, established in Tallin in 2007, raised corporate funding (CH) in 2019. More than EUR 5 million in EU research funding. Active in cryptographic authentication and integrity. Certified supplier to US DOD vendor (Lockheed). No VC or PE resources yet. 150 employees.

Gemalto, established in 1979, was taken over by Thales in 2019. Almost EUR 6 million in EU research funding. Strong technology portfolio in digital identity and security (security of payments, wireless data, border management, IOT, mobile, eSIM, reliable ID). 15,000 employees.

Small enterprises with basic technology and limited venture capital financing or EU research funding:

Utimaco, established in 1983 in Germany. VC rounds in 2005 (DE) and 2013 (DE, LU). Taken over by EQT in 2017. Produces HSM modules, 'root of trust' infrastructure and equipment for lawful interception. Works on quantum-safe HSM in collaboration with ISARA (US) and Microsoft¹²¹. Utimaco acquired the key management company Geobridge (USA) in 2018. 170 employees.

A few notable shortcomings in EU "control":

Deepmind, created in London in 2010 and absorbed by Google in 2014

ARM, founded in 1990 in Cambridge, IPO in 1998, was withdrawn from the market and purchased by private equity (Softbank) in 2016 and absorbed by nVidia in 2020.

Skype, established in 2003 in Estonia, absorbed by Microsoft in 2011.

Virustotal, established in 2004 in Spain, absorbed by Google in 2012.

Sophos, established in 1985 in the United Kingdom, acquired by Thoma Bravo (USA)

IDEMIA (Sagem, Morpho, Safran), established in 1982 in France, acquired by Advent (USA) in 2017. Produces facial recognition, biometric identification for financial services, border control and access control. Involved in a UN project for identity to all by 2030. Concerns about the use of the equipment in digital surveillance¹²² and the use of the biometric data.

¹²¹ <https://hsm.utimaco.com/solutions/applications/post-quantum-crypto-agility/>

¹²² <https://www.amnesty.org/download/Documents/EUR0125562020ENGLISH.PDF>

8.2 Annex 2: Legend of domains

First quadrant - maintain control: key technology where control is in danger of being lost

Market/Suppression: a critical supplier of key technology that is in danger of being driven out of the market by competition that is not controlled. Case: European Cloud Suppliers, 5G.

Business failure: a critical supplier of key technology at risk of bankruptcy.

M&A/majority control: a critical supplier of key technology, where control is likely to be lost through a takeover. Case: ARM

Export control: critical technology that is in danger of being exported to countries or companies where this is not desirable from a strategic perspective.

Procurement in critical assets: purchase of key components in a critical infrastructure where it is envisaged to purchase them "externally". Case: purchase 5G equipment.

Brain drain: loss of key talent in academia necessary to provide independent advice on the proper functioning of specific key technology.

Private funding academia: possible loss of control through foreign investment or sponsorship of academia necessary to provide independent advice on the proper functioning of specific key technology. Case: Huawei and the UvA, VU Amsterdam.

Second quadrant - gain control: key technology that can be controlled in new domains or when an opportunity arises

R&D Funding: financing of new key technology development by controlled companies

Smart procurement: privileged purchase of key technology from controlled companies (exceptions to public procurement, operating conditions, smart buyer, smart specifier, smart developer and launching customer).

Participation in capital: government participation in the capital of companies that produce key technology (golden share, controversy stake, controversy term sheets). Case Curevac.

Certification: development and financing of certification schemes that enable operators to operate critical infrastructure or to purchase reliable solutions. Case encryption, Intel SGX.

Standardization: active participation in standardization and inter-operability of key technologies

Academic expertise: developing and consolidating the capacity to provide an independent opinion on the proper functioning of specific key technology. Case encryption.

Flagships: the establishment of large-scale infrastructure providing critical services. Case Galileo.

Third quadrant - gap analysis: develop generic support measures based on an analysis of successful examples elsewhere

Investment Climate: creating a legal framework that promotes risk investment and entrepreneurship (e.g. stock options, hire/fire). Case Switzerland.

Ecosystem: facilitating an ecosystem that helps and encourages start-ups (inventory of funds, Angels, network of entrepreneurs). Case United States

Processes/Tools: Defining and implementing processes and tools that support digital autonomy. Case US and UK, In-Q-Tel, Darpa, Defense Strategy, Selective Purchase Policy, Operating Conditions, Key Technologies List.

Legislation/Regulation: adapt legislation to promote strategic autonomy. E.g. exceptions for public procurement, competition policy (Germany Kuka)

Certification/Validation: infrastructure and processes to promote certification. Case ENISA

Education: training and guidance for entrepreneurship / traineeships

4th Quadrant - monitor for changes: prospective examination of major changes across the sector or in the threat landscape

Market distortion / Dominance: developments in the market which could give rise to uncontrolled dominance. Case hyperscalers, Intel SGX.

New products and services: new products/services with a cybersecurity impact. Case GPS.

New Community standards: industry standards in a relevant domain. Case Confidential Computing.

New Threats: new types of cyber threat for which there is insufficient protection. Case ransomware, disinformation.

New critical assets: the use of new infrastructure in critical areas. Case: cloud, 5G.

New regulation: new legislation containing a cyber security component. Case GDPR, eIDAS.

New disciplines: new scientific disciplines that may have a cybersecurity application. Case homomorphic encryption, differential privacy, multi-party computing.

8.3 Annex 3: Porter models

Michael Porter developed two commonly used models in the 1980s and 1990s¹²³. The first, the Five Forces model, is designed to analyze competitiveness in order to develop business strategy. An excellent explanation is in the 2008 Harvard Business Review¹²⁴.

A brief description of the main elements, from the above reference, is:

New entrant threat: new entrants put new capacity under pressure, prices and investments

Powerful suppliers retain more value for themselves by raising prices, reducing quality, or transferring costs to customers.

Authorized buyers are more valuable to themselves by pushing prices, demanding more quality or service, and playing vendors against each other.

Threat of substitutes: These may replace the product by redoing the same function.

Competition between existing competitors: can take various forms, such as discounts, advertisements, new products, and the improvement of services.

The second model is intended to analyze national competitiveness. An explanation is in the 1990 Harvard Business Review¹²⁵. A brief description of the elements is, from the reference given:

Factor conditions. The country's position as regards factors of production, such as skilled labor or or infrastructure, which are necessary to compete in a given sector.

Terms and conditions. The nature of the demand on the home market for the product or service of the sector.

Related and ancillary industries. The presence or absence in the country of suppliers and other related industries that are internationally competitive.

Business strategy, structure and rivalry. The conditions in the nation that determine how companies are created, organized and managed, as well as the nature of domestic rivalry.

The models allow first to identify and classify phenomena such as the power of suppliers (for individual companies) or the factors that input into an internationally competitive industry sector (national analysis). They also allow the dynamics of forces and factors to be described in a 'narrative'. They're not mathematical models.

¹²³ <https://www.isc.hbs.edu/competitiveness-economic-development/frameworks-and-key-concepts/Pages/default.aspx>

¹²⁴ <https://www.isc.hbs.edu/strategy/business-strategy/Pages/the-five-forces.aspx>

¹²⁵ <https://hbr.org/1990/03/the-competitive-advantage-of-nations>

8.4 Annex 4: Example of measures vs domains (5G-Security)

The application of the 5G security review framework as described in Section **Error! Reference source not found.** creates a matrix of measures and domains:

Strategic Autonomy	Domain	Factor conditions			Demand conditions	Industry, strategy, structure, rivalry	Government
	Trigger	<i>Technology change</i>	<i>R&D investment</i>	<i>Standardization processes</i>	<i>Conditions for buyers</i>	<i>State support China</i>	<i>Pressure by USA; National security; Market access</i>
	Intervention						
Market conditions	<i>Security requirements</i>				EU 5G Toolbox NL Telecom Law		EU 5G Toolbox
	<i>Market access</i>			ENISA specifications			ICT security certification (Cyber Act)
	<i>Public procurement</i>				EU 5G sectoral flagships?		
Financial	<i>Capitalisation by 'like-minded'</i>					Government participation?	
Knowledge / R&D facilities	<i>EU R&D</i>	More EU innovation in addition to EU R&D?	Horizon Europe funding: 1) exclusive participation? 2) patent-protected?				
Industrial facilities	<i>Standardization</i>			Standardization as a priority?			
Politics, Policy, Organisation	<i>Strategy</i>						EU-US strategy vs CN? ENISA / NCSC threat landscape

8.5 Annex 5: authors



Prof Dr. Paul Timmers

Paul Timmers is 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 Governance Academy Supervisory Board. Previously he was research associate at Oxford University for cybersecurity and digital transformation and Director at the European Commission dealing with EU legislation and funding for cybersecurity, digital health, smart cities, e-government. He was a cabinet member of European Commissioner Liikanen, manager of 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.

Contact: paul.timmers@iivii.eu.



Freddy Dezeure, MSc,

Freddy Dezeure graduated from the KUL in Belgium, with a master of science in engineering in 1982. He was CIO of a private company from 1982 until 1987. He joined the European Commission in 1987 where he held a variety of management positions. He founded the EU Computer Emergency and Response Team (CERT-EU) in 2011 and managed it until May 2017. He is an Independent Strategic Advisor in cybersecurity and cyber-risk management and a Board Member and Advisor in several high-tech companies. He is also leading the EU ATT&CK Community.

Contact: contact@freddydezeure.eu.