HCSS GLOBAL TRENDS

Flow Security in the Information Age

Paul Verhagen, Esther Chavannes and Frank Bekkers

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

Flow Security in the Information Age

HCSS Global Trends
The Hague Centre for Strategic Studies

ISBN/EAN: 9789492102737

Authors: Paul Verhagen, Esther Chavannes and Frank Bekkers
Contributors: Tim Sweijs, Patrick Bolder and Giorgio Berti.
The research for the Semicon case (see Annex A) was performed by Datenna, as commissioned by HCSS in the context of this research.
December 2020

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Design: Mihai Eduard Coliban (layout) and Constantin Nimigean (typesetting).

The Hague Centre for Strategic Studies
info@hcss.nl
hcss.nl

Lange Voorhout 1
2514EA
The Hague
The Netherlands

HCSS GLOBAL TRENDS

Flow Security in the Information Age

Paul Verhagen, Esther Chavannes and Frank Bekkers

Table of Contents

1. Introduction 7
1.1 Setting the stage: flows and flow security 7
1.2 Strategic autonomy 9
1.3 The relevance of technology flows 11
1.4 Three cases 13
1.5 This paper 15

2. Economic angle: dependency on risky third-party technology suppliers 16
2.1 Introduction 16
2.2 Critical infrastructure and 5G 17
2.3 The economic appeal versus the risks specific to Huawei 5G 19
2.4 Key areas of potential flow insecurity 22

3. Military angle: lasting dependency on US' military systems 23
3.1 Introduction 23
3.2 European or American? Technological dependencies between military partners 24
3.3 The data streams relevant for the F-35 25
3.4 Advantages of collaboration 27
3.5 Key areas of potential flow insecurity 28

4. Institutional angle: entanglements in the financial system 29
4.1 Introduction 29
4.2 Shielding international financial flows 30
4.3 Securitizing domestic flows 32
4.4 System-level dependencies 33
4.5 Key areas of potential flow insecurity 34

5. Policy implications 35
5.1 Introduction 35
5.2 Policy instruments 36
5.3 Securitizing flow dependencies 37
5.4 Creating flow redundancies 38
5.5 Obtaining flow autonomy 39
5.6 Offensive leveraging of flow dependencies 40

6. Final remarks 42

Annex A: PRC-Taiwan semiconductor case 44

1. Introduction

1.1 Setting the stage: flows and flow security

In a hyper-connected world, which is characterized by a partial breakdown of the multilateral system,[1] the ability to influence or control flows is key to new coercive strategies. As French President Emmanuel Macron put it in a recent speech on defense and deterrence strategy: "Managing tangible and intangible resources and flows is key to new power strategies. The high seas, air space and outer space and the digital realm, common spaces that interpenetrate each other and complicate our understanding of the issues, are becoming or are once again arenas for power struggles and at times, confrontation."[2] In the information age, worldwide flows not only pertain to the physical trade of energy, commodities, and products, but also to the digital exchange of money, data, and ideas. The effects of disrupting or blocking any of these flows could be disastrous–albeit with different time horizons for different types of flows. With this vulnerability in mind, various actors, including the great powers the US, China and Russia, but also the EU and some of its member states, are actively reviewing their current flow dependencies and considering ways to reduce, mitigate or counter some of the associated risks.

The interdependencies in the form of flows have always been part of international relations. Yet the magnitude and depth of international interwovenness in the modern era, not in the least in the digital sphere, has given rise to the new concept of flow security. In short, flow security refers to the need to manage the risks that come with flows between actors in a globalized, highly connected world – while simultaneously fostering the opportunities of such flows.[3] Within the context of this study, we look more narrowly at flow security as managing the risks for obstruction or sabotage of such flows or preventing the malicious use of flows for espionage or interference purposes.

---

1 See Jack Thompson, Rob de Wijk and Esther Chavannes, "Adjusting the Multilateral System to Safeguard Dutch Interests", 2020; https://hcss.nl/report/adjusting-multilateral-system-safeguard-dutch-interests

2 See "Speech of the President of the Republic on the Defense and Deterrence Strategy," Website of the President of the French Republic, elysee.fr, February 7, 2020, https://www.elysee.fr/emmanuel-macron/2020/02/07/speech-of-the-president-of-the-republic-on-the-defense-and-deterrence-strategy.en

3 Of course, flow dependencies also offer great benefits and opportunities. Indeed, most would agree that the overall balance is positive. Flow dependencies have stimulated prosperity across the world (albeit unevenly distributed) and have consequently created considerable incentives for multilateral collaboration rather than conflict. The focus of this paper is to look at flows from a security risk perspective, and at the risks that dependencies on others might bring.

The difference between flow security and a flow dependency is also pertinent. The former refers to the larger objective of managing interdependencies, whereas flow dependency refers to a (existing) flow that carries some level of dependence on an external actor to ensure flow integrity.

It is worth considering the monumental shift that flow security represents. It marks a clear departure from unregulated market reform policies espoused by Western states in the second half of the twentieth century. These policies, in combination with the emergence of the global internet, have facilitated economic globalization to accelerate and grow at a historically unprecedented scale. Especially technological flows lie at the root of both the greatest gains as well as the most entangled risks for disruption. From the 'gains' perspective, mutual dependencies were considered positive, especially if they served to lower the cost of goods and services. Furthermore, mutual dependence was coherent with the widely embraced idea that greater economic integration would drive liberalization and even democratization of non-Western countries. This period of globalization undoubtedly generated tremendous wealth and prosperity, albeit unequally distributed.[4] However, from the 'risks' perspective, greater dependency also comes with novel challenges for disruption to societal integrity or offer vectors for espionage efforts. The increase in geopolitical competition in recent years has highlighted this side of the coin. Yet despite this newfound importance and relevance, outside of military equipment trade states generally have not approached such dependencies and flows strategically.

Modern flow dependencies can no longer be only assessed on financial or economic terms. States are seeking to balance the risks of flow dependencies and to leverage geo-political advantages from global flows. Potential major flow disruptions pose a substantial risk to the EU and its member states. In general, the more Europe is dependent on other parties to generate and secure critical flows across different domains, the more it is vulnerable to those dependencies being leveraged for political pressure. A classic example is Europe's dependence on Russian energy. As the Dutch Advisory Council on International Affairs wrote: "The crisis in Crimea and Ukraine has focused attention on the energy dependency of the countries of the European Union (EU) on Russia [...] This dependency makes the EU vulnerable to political pressure."[5]

Leveraging asymmetric dependencies and flows have become increasingly common in recent years as a method of coercion, not just by adversaries but also by Western states. Following the annexation of the Crimea, both the EU and the US discussed

4 Martin Ravallion, "Inequality and Globalization: A Review Essay," *Journal of Economic Literature* 56, no. 2 (January 2018): pp. 620-642, https://doi.org/10.1257/jel.20171419

5 Adviesraad Internationale Vraagstukken, "De EU-gasafhankelijkheid van Rusland. Hoe een geïntegreerd EU-beleid dit kan verminderen", June 2014, p2, https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2014/06/06/de-eu-gasafhankelijkheid-van-rusland

whether Russia could be denied access to the SWIFT financial messaging system.[6] Potentially, this could have seriously harmed the Russian economy. In response to this threat, the Bank of Russia has created its own System for Transfer of Financial Messages (SPFS) as an alternative to SWIFT. Furthermore, Russia is putting efforts in uniting other countries to circumvent SWIFT. For example, Iranian and Russian banks are now connected through the Russian SPFS and Iran's SEPAM financial messaging services; while China's Cross-Border Interbank Payment System (CIPS) is looking at coordinating with Russia's SPFS to handle all Russia-China transactions. It highlights how these countries believe that they are vulnerable to the interruption of vital flows because of Western coercion, a belief that is reinforced by President Trump's trade wars and sanction politics against China. These developments have increased the awareness of the strategic importance of managing flow dependencies–for defensive but also for offensive purposes.

As a result, various states are looking at possibilities to shift or manage their flow dependencies differently. Indeed, a 2019 EU Commission press release goes so far as to call the challenges surrounding 5G a new security paradigm that requires the reassessment of current security frameworks.[7] Flow security issues are inextricably intertwined with other considerations concerning a country's position in global networks, as exemplified by the US's 'America First' agenda, China's 'Made in China 2025' strategy, and European discussions about 'strategic autonomy'. To better understand the nature and importance of flow security, we take a closer look at this last term.

1.2 Strategic autonomy

The concept of 'strategic autonomy' is often mentioned in the contemporary security debate but lacks a clear delineation. Projected upon the military realm, for instance, the interpretation of European strategic autonomy ranges from European being able to conduct minor military crisis management operations in its periphery without American assistance, to a more comprehensive grand strategic and autarkic defense industrial set of priorities. Where the more minimal former definition is uncontroversial, the latter is not, as critics see this as precipitating a US departure from Europe ('decoupling'), inefficient use of scarce European defense spending ('duplication'), and needlessly complicating command and control arrangements

6 The Society for Worldwide Interbank Financial Telecommunications (SWIFT) system is a vast messaging network used by banks and other financial institutions worldwide to send and receive information, such as money transfer instructions, quickly, accurately, and securely. Without SWIFT, or systems like it, international money transfers would be a cumbersome affair.

7 "Report on EU Coordinated Risk Assessment of 5G," Text, European Commission - European Commission, accessed September 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

because of the partial overlap with NATO ('discrimination'). In that sense, the debate has moved little since the 1990s.[8]

To further illustrate the diffuse ways in which the concept has been defined, the German Institute for International and Security Affairs defines strategic autonomy as "the ability to set priorities and make decisions in matters of foreign policy and security, together with the institutional, political, and material wherewithal to carry these through – in cooperation with third parties, or if need be alone."[9] This definition carries within it two further distinctions which the European Council on Foreign Relations separates as "autonomy from other powers", versus "autonomy to conduct operations". Autonomy from other powers refers to being free from existing dependencies being leveraged by other actors.[10] Autonomy to conduct operations holds the ability to independently pursue EU strategic objectives without needing another party to facilitate this. In the wider sense, within Europe the notion of strategic autonomy is used somewhat interchangeably to refer to the spectrum of policy options that range from complete (military) decoupling of the US to a near continuation of the status quo.

For the purpose of this study, it is sufficient to consider European strategic autonomy in a more minimal and functional – and mostly uncontroversial – sense as Europe being able to generate instruments of power, military and otherwise, to defend its interest anywhere where the US is not able or willing to fully engage. The important take-away from the debates and initiatives on strategic autonomy is the fact that states, often through alliances, are trying to reduce their dependencies on flows that originate from geopolitical rivals in order to protect national security, economic prosperity and longer-term competitiveness, and their ability to reach sovereign decisions. Implicitly, the goal of reducing dependencies is one of various ways to strengthen strategic sovereignty.

For countries like China, Russia and Iran, the global power shift from the West to the East provides space to pursue such a policy. Indeed, with their military capabilities arguably lagging behind their regional or even global ambitions, better protection of their own flows against Western coercion combined with capabilities that enable them to attack flows, is a rational choice for these countries to make their rising power in the international arena manifest.

---

8 van Hooft, P. "Land rush: American grand strategy, NATO enlargement, and European fragmentation". *Int Polit* **57,** 530–553 (2020), https://doi.org/10.1057/s41311-020-00227-7

9 https://www.swp-berlin.org/10.18449/2019RP04/#:~:text=In%20this%20publication%20strategic%20autonomy,or%20if%20need%20be%20alone

10 https://www.ecfr.eu/specials/scorecard/independence_play_europes_pursuit_of_strategic_autonomy

1.3 The relevance of technology flows

The current Sino-American rivalry has been referred to as the New Cold War in popular media,[11] but while there are some superficial similarities there are also crucial differences between the two. Whereas during the Cold War there was a near complete economic separation between the Western and Soviet economic blocs, this is not the case today nor is such a scenario likely to come about because of the degree and scale of global interdependencies.[12] Instead of complete economic decoupling, current trends are more likely to augur in a period of technological fragmentation in which groups of state separate into distinct technological ecosystems.[13] Specifically, countries are managing flow dependencies, by deliberately creating flow dependencies for others and actively reducing their own dependencies. As such, technology is the accelerant, fuel, and instrument by which modern geo-political competition is waged.

This trend is part of a new global power competition which also manifests itself in the race for dominance in key technological sectors. Data are at the center of this race. Breakthroughs in the new mobile 5th generation internet, artificial intelligence, quantum computers, the Internet of Things, robotics, 3D printing, nanotechnology, and biotechnology will transform the global economy in a fundamental, albeit not yet fully understood way.[14] Here, economic power matters. China is using its booming economy to increase its leverage over other countries, to coerce states or, to create divisions within alliances such as the EU. For this purpose, China is using its Belt and Road Initiative (BRI), the 17+1 format and its Foreign Direct Investments (FDI) to unroll Chinese 5G infrastructures together with other 'Made in China 2025' innovations that lie at the heart of the 4th industrial revolution.

The creation of key technology dependencies through the aggressive promotion and export of technology standards may well result in the emergence of separate regional orders that have their own digital standards. Countries or blocs not only set up their own standards but also try to export their standards to other countries, thus in effect creating dependencies from their technological and industrial base. The technologies that drive the shift from the ICT-centered 3rd industrial revolution to the data-centered

---

11 Niall Ferguson, "Opinion | The New Cold War? It's With China, and It Has Already Begun," *The New York Times*, December 2, 2019, sec. Opinion, https://www.nytimes.com/2019/12/02/opinion/china-cold-war.html.

12 Keith Johnson and Robbie Gramer, "The Great China-U.S. Economic Decoupling," May 14, 2020, https://foreignpolicy.com/2020/05/14/china-us-pandemic-economy-tensions-trump-coronavirus-covid-new-cold-war-economics-the-great-decoupling/.

13 Adam Segal, "The Coming Tech Cold War With China," *Foreign Affairs*, September 9, 2020, https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china.

14 Hugo Van Manen et al., "Macro Implications of Micro Transformations: An Assessment of AI's Impact on Contemporary Geopolitics | HCSS," *The Hague Centre for Strategic Studies*, accessed September 10, 2020, https://hcss.nl/report/macro-implications-micro-transformations-assessment-ais-impact-contemporary-geopolitics. Paul Verhagen and Erik Frinking, "Understanding the Strategic and Technical Significance of Technology for Security, Implications of Quantum Computing within the Cybersecurity Domain | HCSS," *The Hague Centre for Strategic Studies*, September 18, 2020, https://hcss.nl/report/understanding-strategic-and-technical-significance-technology-security-implications-quantum.

4th industrial revolution are what matters in this global competition. Historically, the champions of the previous industrial revolutions have become the leading economic power and assumed the role of global hegemon, including Great Britain in the 19th century and the US in the 20th century.[15] The stakes in this race are therefore not only economic but also political. The winner will be able to define the terms of the next world order. Policies implemented today will be important in deciding who will come out ahead in the years to come.[16]

As it currently stands, China might very well be that state. Through a combination of genuine product innovation and economy of scale on the one hand, and a policy of dumping, IP theft, and protectionism on the other, Huawei and ZTE are now dominating the European 5G market at the expense of Nokia and Ericson. Dependencies could grow even bigger if China manages to integrate its Beidou-2/3 GPS-system and 5G, making users reliant on both terrestrial and space-based Chinese infrastructure. A similar development might be underway in AI, another key driver of the new industrial revolution. Although the US vastly outspends China on AI, Beijing's centralized AI-policy and the absence of privacy laws will make the unrestricted use of data for the development of AI applications possible. The BRI is instrumental for unrolling the Chinese infrastructure.

However, the US is certainly in the race. The United States is still home to eight of the world's most valuable and innovative tech companies, even if China is catching up. While the US' based tech giants are still dominant globally, there have been increasingly strong headwinds both foreign and domestic. From Europe the dominance of US tech giants is challenged in court under various anti-monopoly or anti-trust violations. Multiple court cases have been running for several years, most notably three antitrust investigations into Google for allegedly abusing its market dominance. [17] In the US itself Congress has increasingly turned its regulatory attention towards the tech giants, with a congressional investigation faulting Amazon, Apple, Facebook, and Google for engaging in anti-competitive or monopoly-style tactics.[18]

Europe, for its part, has become global regulatory leader, in particular for privacy and data protection. The EU has made considerable legislative progress on privacy regulation in the form of the GDPR (General Data Protection Regulation). However, this regulatory clout is not matched by its technological prowess, with Europe's leaders become increasingly worried about a host of new technologies including quantum

15 Paul Kennedy, The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500-2000, New Ed Edition (London: William Collins, 2017).
16 Sean Fleming, "The World Order Will Be Rocked by AI - This Is How," World Economic Forum, February 13, 2020, https://www.weforum.org/agenda/2020/02/ai-looks-set-to-disrupt-the-established-world-order-here-s-how/.
17 https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581
https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770
18 https://www.washingtonpost.com/technology/2020/10/06/amazon-apple-facebook-google-congress/

computing, cloud services artificial intelligence, and fifth generation wireless. Falling behind on such key technologies would put the EU at a considerable disadvantage. Not only would Europe be less innovative, it would also mean that it would become dependent on other countries for cutting edge technology. The EU currently lags because efforts and investments are too fragmented. It lacks powerful corporate champions that can dictate the market and focus on research that is largely nationally organized. At the same time, the EU is still the world's largest economy and trading bloc, as well as ranking first in both inbound and outbound international investments. Combined efforts may build upon this to favor Europe's chances.

1.4 Three cases

Flows and flow security are catch-all terms that cover a wide range of different flows and a diverse set of security risks and threats that may harmfully affect these flows. Flows may broadly be defined as a transfer between two parties, the exact nature of the transfer may be material goods like oil or gas, or more abstract like information or norms.[19] In order to move beyond high-level observations and to properly develop actionable plans to increase flow security (or decrease flow insecurity, which might not be completely the same thing), it is critical to differentiate between various types of flow and associated security issues. It is self-evident that the flow of cheese products between the Netherlands and Germany faces different types of security risks than a flow between China and the Netherlands on critical pharmaceutical materials. This example is an illustration of a type of flow, namely the trade of physical goods, for which we have a good grasp of the sort of risks that might affect these flows: from trade barriers and boycotts, via piracy and smuggling, to large scale blockades and attacks by state actors.

In this paper, however, we concentrate on a type of global flows for which we have a vaguer idea of the sort of threats that might disturb them. In three case studies, we illustrate different aspects and dimensions in the *global flow of information*, in particular pertaining to *keystone technologies*. These cases are centered on technologies that offer strong competitive advantages and are contingent on the undisrupted flow of information to ensure operation. All three cases pertain to a technological ecosystem for which the keystone technology is critically positioned. As such, these cases encompass security not only in the sense of safety, but also security in guaranteed access to keystone technology. The cases, summarized in the table below, represent the strategic range of flow security, from military to economic to financial, as well as differences between European dependence on China and the US. The first two

19 A higher-level taxonomy on flow security and its components may be found here: https://hcss.nl/report/flow-security-and-dutch-defense-and-security-policies

cases focus on the flows of innovative ideas, technologies, components, and products that flow within global (5G case) and international partnership (F-35 case) innovation and production networks. The third case concerns the indispensable companion of many other flows, namely the financial transactions associated with the flow of goods, services, technology, or information.

5G networks and standards	F-35 continuous development	Entanglements in the financial system
This case discusses the reliance on Chinese companies, Huawei in particular, for 5th generation cellular technology – commonly referred to as 5G. This case is particularly apt considering the ongoing discussion in several (Western) countries on the possible risks associated with the use of Chinese technology (allegedly manipulatable by the Chinese government) in critical infrastructures.	The US-developed F-35 combat aircraft has a planned life of type at least into the 2050s. The focus of this case is not on the F-35 itself, but on the intricate information and support systems that have been set up (under US control) to support actual F-35 deployment as well as the continuous development of the aircraft and the associated technology transfer to F-35 partner nations such as the Netherlands. The F-35 is thereby an example of modern weapon platforms that require a particular data-ecosystem to maintain full combat effectiveness.	This case considers how the SWIFT financial messaging system creates information dependency, and how the de-facto global standard set by SWIFT to facilitate international financial transfers are challenged. The focus of this case is on the strategic capture of institutions that facilitate international commerce.

These cases not only vary in substance but also highlight different angles and illustrate more generic issues, as the table below illustrates.

Case	Angle	Status in time	Specific concern	Generic issue the case illustrates
5G networks and standards	Economic with (geo-) political implications	A flow dependency that has not yet manifested but is being considered	Undue influence by China in European economic affairs and overdependence on Chinese technology products	Global economic *and* (therefore) political competition in a crucial technology / business sector that is a huge market, but also underpins the 4th industrial revolution
F-35 continuous development	Military partnerships over time	A manifested flow dependency that requires continuous managing	Reliance on unobstructed information and data sharing with the US to maintain operational integrity and effectiveness of Dutch Armed Forces	Managing a lasting dependency over several decades, while alliances and allegiances may shift
Entanglements in the financial system	Financial / Institutional	A pre-existent flow dependency that has been politicized over time	Reduced autonomy in pursuing European foreign policy interests by exposure to US-led secondary sanctions	Segmentation of global financial institutions, systems, and standards; and, as a result, of markets

Notably all three cases also reflect a changing relationship and role discussion between governments and private companies in flow management and control.

1.5 This paper

This paper aims to contribute to a better and more detailed understanding of the notion of flow security and of the policy options for the Netherlands and Europe to effectively contribute to flow security to protect vital interests and values. Since 2017, the Dutch Ministry of Defense designated flow security (also known as 'secure connections' or 'veilig verbinden' in Dutch) as one of three principal strategic challenges. Flow security stands on par with the two more familiar challenges of staying secure (territorial defense of Dutch and NATO territory) and of bringing security (peace support and crisis management operations geared towards promoting global stability and maintaining the international order). This represents an acknowledgment – as described in §1.1, Setting the stage – that contemporary security and defense is as much about ensuring uninterrupted access to resources, both tangible and intangible, and markets as it is about safeguarding territorial integrity.

This paper is structured as follows. After this introductory chapter 1, chapters 2 through 4 deal with the three cases introduced above and their (potential) geopolitical consequences in three areas, namely economic, military, and institutional respectively. All three cases address the question of how the position of the Netherlands and the EU within international markets might develop in the mid-term future in relation to certain technological or informational dependencies. These real-world cases serve to get a deeper and concrete grasp of what the very broad notion of flow security could mean in the information and technology domain; and then to identify policies that can be implemented to manage or mitigate flow (in)security issues. The latter is the subject of Chapter 5, which discusses the analysis in the previous chapters in terms of policy implications for the Netherlands and/in the EU. The main topics on which conclusions are drawn, are potential areas for Dutch or European strategic autonomy, preferred partners for the Netherlands to reduce risks of critical dependencies, and a number of strategic choices to mitigate, reduce, or even leverage flow insecurities and vulnerabilities for the Netherlands and its like-minded European partners. Chapter 6, finally, closes off with some high-level conclusions.

2. Economic angle: dependency on risky third-party technology suppliers

2.1 Introduction

The first case focuses on the potentially imminent technological dependency on China, related to the development and roll-out of 5G networks in the Netherlands and many of its partner countries. To assess the flow security risks of 5G, we first examine the intersection between 5G networks and critical infrastructure. Subsequently the idiosyncrasies of specifically Huawei 5G are analyzed. Finally, the economic benefits of using Huawei 5G are assessed and contextualized. These observations are then summarized in key take-aways. Within the broader research question, the 5G case represents a technological flow dependency that has not yet manifested but is actively being considered.

5G represents the fifth-generation technological standard of cellular networks and offers many advantages over earlier generations, including faster data transfer speeds and lower latency. These two properties make 5G a keystone in a host of technologies that are likely to drive the shift from the ICT-centered 3rd industrial revolution to the data-centered 4th industrial revolution. The possible payoff of dominating the next industrial revolution is global and political hegemony. Whoever manages to set the standards of the next technology will have a considerable first mover advantage.

Setting standards is an important part of China's industrial policy.[20] Made in China 2025 highlights this importance. Standard setting will be further elaborated in the China Standards 2035 plan, which is currently being drawn up and will be released late in 2020. China is increasing its influence on the boards of international standards organizations such as ITU, ISO and, IEC. Actively stimulated by the government, participation by Chinese companies in these organizations has sharply increased, especially in the field of new technologies such as 5G, IoT and, AI. For example, many standards in the field of surveillance technology and facial recognition within the

20 John Seaman, "China and the New Geopolitics of Technical Standardization," *Notes D'Ifri*, January 2020, https://www.ui.se/butiken/uis-publikationer/ui-brief/2019/chinas-standard-power-and-its-geopolitical-implications-for-europe/

ITU[21] currently come from Chinese companies.[22] Next to actively participating in international organizations, China is also promoting standards on a bilateral basis. The question then is: what are the relevant flow securities that pertain to the use of risky third-party vendors in general, and Huawei in particular, when it comes to 5G infrastructure?

2.2 Critical infrastructure and 5G

5G is considered a keystone technology in the sense that technological innovations such as autonomous vehicles, smart electrical grids, and the Internet of Things depend on a mature 5G infrastructure. The EU has stated that "5G networks is the future backbone of our increasingly digitized economies and societies", and that ensuring the security and resilience of 5G networks is therefore essential.[23] Because of this importance of 5G networks for vital societal functions, the debate is whether allowing Chinese technology in the heart of 5G networks constitutes a national security risk. The recent EU 5G security toolbox allows for the application of restrictions on high-risk supplier for key assets that are defined as critical and sensitive in the EU coordinated risk assessments.[24] The need to mitigate security risked linked to 5G is explicitly stated, as is the requirement for greater international coordination with EU neighboring countries.

To that end, the existing EU critical infrastructure protection (CIP) program is being revaluated. The priorities of the CIP program were established by the 2008/114 EU Directive on Critical Infrastructure.[25] The 2008 Directive was complemented in 2016 by the Network and Information Security Directive.[26] While the former is specifically focused on energy and transport infrastructure, the latter considers network and information systems infrastructure used by crucial services to ensure proper functioning. However, neither of the two Directives comprehensively capture novelty issues and threats – including 5G, unmanned aircrafts, and pandemics – that the EU is

21 https://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96. We note that the ITU is not the most important standard organization globally. Organizations such as ISO are considered more relevant.

22 Anna Gross and Murgia Madhumita, "China Shows Its Dominance in Surveillance Technology," *Financial Times*, December 27, 2019, https://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96

23 "Report on EU Coordinated Risk Assessment of 5G," Text, European Commission - European Commission, accessed September 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

24 General Secretariat of the Council, "Outcome of Proceedings" (Council of the European Union, June 9, 2020), https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf

25 Council of the European Union, "COUNCIL DIRECTIVE 2008/114/EC, of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection" (Official Journal of the European Union, December 23, 2008), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

26 The European Parliament and the Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union", https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:194:FULL&from=EN

facing, as found by the 2019 evaluation of the Directive.[27] For this reason, establishing new guidelines for coordination regarding Critical Infrastructure in the EU is one of the published initiatives of the Commission.[28] The new version will become available in the fourth quarter of 2020. While the nature of the risks themselves have not changed, the risk level of occurrence for, among others, cyberthreats has significantly increased. The European Commission therefore recognizes the need to increase the resilience of these infrastructures across the EU to ensure that they can recover quickly in case a disruption would happen.[29,30] Attention is also pointed towards the influence of third countries on EU Critical Infrastructures, which could be harmful due to the lack of an updated coordinated program.[31]

Although CIP initiatives exist on the EU level, determining national critical infrastructure plans and strategies remains within the authority of member states. The Netherlands distinguishes nearly 30 'vital processes' and divides the threat into two categories, corresponding to the gravity of the effect. Category A includes threats with more destructive projected economic, social, and physical consequences, while category B includes less destructive potential threats.[32] Threat category A refers primarily to energy and water issues, category B includes ICT, financial, defense, transport, and institutional issues. Similarly, the US Department of Homeland Security has specifically labeled these vital processes as the National Critical Functions Set.[33] The broad consensus on both sides of the Atlantic is that a reliance on risky third-party equipment for 5G could constitute the potential that critical infrastructure functions and processes may be affected or terminated remotely.

27 EU Commission, "Evaluation Of Council Directive 2008/114 On The Identification And Designation Of European Critical Infrastructures And The Assessment Of The Need To Improve Their Protection," July 23, 2019, 23, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf, p 6.

28 EU Commission, "Protecting Critical Infrastructure in the EU – New Rules," Published Initiatives - EU Commission, 2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection

29 EU Commission, "Evaluation Of Council Directive 2008/114 On The Identification And Designation Of European Critical Infrastructures And The Assessment Of The Need To Improve Their Protection" p6.

30 European Parliamentary Research Service, "Digital sovereignty for Europe (EPRS Ideas Paper. Towards a more resilient EU)", July 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

31 EU EU Commission, "Evaluation Of Council Directive 2008/114 On The Identification And Designation Of European Critical Infrastructures And The Assessment Of The Need To Improve Their Protection", p36.

32 Ministerie van Justitie en Veiligheid, "Overzicht vitale processen - Vitale infrastructuur - Nationaal Coördinator Terrorismebestrijding en Veiligheid," Government Website, Dutch Ministry of Justice (Ministerie van Justitie en Veiligheid, October 9, 2019), https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

33 "National Critical Functions Set | CISA," Cybersecurity & Infastructure Security Agency, April 29, 2019, https://www.cisa.gov/national-critical-functions-set

2.3 The economic appeal versus the risks specific to Huawei 5G

Within the burgeoning field of 5G, the primary actor of note is the Chinese telecom corporation Huawei.[34] As it currently stands, Huawei is the largest producer in the world of 5G equipment.[35] The main competitors of Huawei are Ericsson, Nokia, and Samsung. Compared to its competitors, Huawei equipment is recognized for its low cost, speed of implementation and quality that is at least on par, and by some assessments better, than its market equivalents.[36] As a result, many European countries make use of Huawei equipment to implement their 5G networks. The Dutch Vodafone 5G network uses Ericsson equipment, while KPN employs Huawei equipment – albeit with the stipulation that it will only be used in the radial network.[37] In addition, large components of existing 4G networks make use of Huawei equipment. A 2019 GSMA industry report suggests that banning Chinese vendors from Europe's 5G would increase the cost by $62 billion and delay implementation by 18 months.[38] British Telecom estimates the cost of banning Huawei 5G would reach £500 million.[39] Implementing a full Huawei ban that includes everything from 3G to 5G would be even more expensive. There are therefore strong financial and economic incentives that favor the implementation of Huawei 5G.

While the short term economic logic seems to favor Huawei, the flip side is that Huawei has repeatedly been accused of unfair business practices, including IP theft, government subsidizing of research, and protectionist measures to maintain the domestic Chinese smart-phone market. The US have issued explicit objections against the use of Huawei equipment in European 5G networks.[40] While Huawei stringently denies it receives undue support from the Chinese government, it has been labeled as a national champion and is alleged to have received considerable economic support on its R&D as well as benefiting from protectionist policies to ensure sales of Huawei devices inside China's immense domestic market.[41] Indeed, China has executed a

34 Other Chinese companies such as ZTE are also of note but fall outside the current case study. We also note that the contemporary discussion on technological competition centers largely on Huawei, and to a lesser extent TikTok.

35 Robert WIlliams, "Securing 5G Networks," *Council on Foreign Relations*, July 15, 2019, https://www.cfr.org/report/securing-5g-networks

36 Note that this is also the result of many European countries, including the Netherlands, piggybacking for years on Chinese investments in R&D, while consciously cutting back on their own (government) investments in R&D. This approach is now tilting, and European countries must be prepared to invest more in R&D. However, the backlog cannot simply be reversed in the short term.

37 See e.g. Pim Van Der Beek, "KPN sluit Huawei uit voor core-netwerk 5G," *Computable*, April 26, 2019, https://www.computable.nl/artikel/nieuws/mobility/6652075/250449/kpn-sluit-huawei-uit-voor-core-netwerk-5g.html. The exact technical details of 5G are beyond the scope of this paper. The distinction between radial and core networks is commonly used but is also contested by some experts as not being a clear distinction.

38 "Europe's 5G to Cost $62 Billion More If Chinese Vendors Banned: Telcos," *Reuters*, June 7, 2019, https://www.reuters.com/article/us-huawei-europe-gsma-idUSKCN1T80Y3.

39 Mark Sweeney, "Huawei Ruling Will Cost Us £500m, Says BT | Business | The Guardian," *The Guardian*, January 30, 2020, https://www.theguardian.com/business/2020/jan/30/huawei-ruling-will-cost-us-500m-says-bt.

40 Fung Brian, "US Spat with Huawei Explained", *Washington Post*, April 10, 2019, https://www.washingtonpost.com/gdpr-consent/

41 Karl Song, "No Huawei Isnt Built on Chinese State Funding," Company Website, Huawei, accessed September 10, 2020, https://www.huawei.com/en/facts/voices-of-huawei/No-Huawei-isnt-built-on-Chinese-state-funding.

concerted industrial strategy to dominate the race for 5G. A 2015 key partnership between the EU and China is an indication of the long timescale upon which China has sought to develop its 5G networks.[42] While there is no conclusive open-source evidence that there was direct coordination between the Chinese government and Huawei, Chinese telecom corporations are extremely well-positioned to reap the benefits from technological innovation. [43] For example, Huawei's global market share of smartphones has risen from 1.5% in 2010 to nearly 18% in 2019. Part of this meteoric rise has been its dominance in the Chinese domestic market, where it holds a 42% market share.

Beyond the integrity of vital processes, there is also the risk that an (over)reliance on Chinese telecom equipment would allow for the theft of intellectual property. In 2017 the Office of the US Trade Representative has placed China on the priority watchlist for IP theft.[44] The concern here is primarily that Huawei would act as a vehicle for the Chinese government to spy on strategically important technologies to strengthen the competitiveness of Chinese products. As such, this represents a risk to the integrity of intellectual flows that might harm European companies and governments.

Next to the theft of IP, there has also been an increase in legal vectors for acquiring IP, either through corporate takeovers and technical partnerships or through direct legislation. This is further borne out by article 7 of the Chinese National Intelligence Law creates an obligation for all Chinese citizens to support national intelligence work. It is unclear whether the current application of article 7 would also include overseas investments done by Chinese governments.[45] This creates the possibility that the use of Chinese telecom provides opens a legitimate legal route for the collection of data. This in turn problematizes the legal tools available for the prevention and detection of abuse.

---

42 "Autonomic Logistics Information System (ALIS) | Lockheed Martin," accessed September 10, 2020, https://lockheedmartin.com/en-us/products/autonomic-logistics-information-system-alis.html.

43 Allegations from the US regarding the collusion between the Chinese government and Huawei have caused public controversy, yet no conclusive evidence to support these claims has been released. The US has allegedly shared classified information with its 'Five Eyes' allies proving the connection between Huawei and China. After the US' decision to ban Huawei from participating in their 5G network, countries such as Australia and UK followed lead. However, given Huawei's constant rebuttal of the US' allegations, the existence and significance of the evidence is still uncertain. See e.g.: Zak Doffman, "CIA Claims It Has Proof Huawei Has Been Funded By China's Military And Intelligence," *Forbes*, April 20, 2019, sec. Innovation, https://www.forbes.com/sites/zakdoffman/2019/04/20/cia-offers-proof-huawei-has-been-funded-by-chinas-military-and-intelligence/. Bruno Mascitelli and Mona Chung, "Hue and Cry over Huawei: Cold War Tensions, Security Threats or Anti-Competitive Behaviour? - ScienceDirect," *Research in Globalisation* 1 (May 24, 2019): 1–6. https://doi.org/10.1016/j.resglo.2019.100002. Steve McCaskill, "Huawei: US Has No Evidence for Security Claims | TechRadar," *TechRadar*, February 28, 2019, https://www.techradar.com/news/huawei-us-has-no-evidence-for-security-claims.

44 We note that estimates range from $225 billion and $600 billion and that it is difficult to accurately obtain the cost of IP theft. The office of the United States Trade Representative, "2017 Special 301 Report," April 1, 2017, https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF

45 Joseph Lee, "The National Security Risks Over Huawei and Its 5G Network: Is an Outright Ban or a Restricted Access the Answer?," *Oxford Law Faculty, Commercial Law Centre Blog* (blog), May 3, 2019, https://www.law.ox.ac.uk/research-subject-groups/commercial-law-centre/blog/2019/05/national-security-risks-over-huawei-and

Finally, there are considerable privacy concerns, as (user) data collected on Chinese tech platforms might be handed over to the Chinese government. In addition, small tech companies and startups that trade in consumer data, such as marketing companies, may do business with both the Dutch government and Chinese parties (e.g. Huawei). This creates new security dilemma's, because government monitoring of and control over such practices would be hard to build and sustain.

To minimize the impact of risky third-party equipment, various governments have distinguished between the 'core' and the 'edge' of communication networks to reduce the vulnerability. The core refers to the centralized computer servers and sub-networks that route data, while the edge refers to the mobile phone masts and base stations. However, the nature of 5G technology is such that, compared to 4G, more operations and data process occurs within the edge of the network, raising questions as to the saliency of a 'core' and 'edge' separation. The UK was one of the countries that made this distinction before a policy shift that chose to avoid 5G Huawei from the entirety of the network.[46]

In short, while Huawei equipment is recognized for its cost-effectiveness, there are valid concerns around its business practices. The protectionist economic measures applied by the Chinese government to their internal market are well documented and have been beneficial to domestic Chinese corporations. A choice to take Chinese developed 5G could therefore be rewarding economic bad behavior and undercuts European companies that have pursued more transparent R&D trajectories. Broadly speaking, European based firms do not receive the same level of support in the forms of subsidies and protectionist measures, in line with the EU's historical dislike for national champions.[47] While the purchase of Chinese 5G technology may be profitable in the short term, it could harm European innovative capacity and the competitiveness of its products in the long run. In terms of its flow analogy, the innovation risk is that Europe ceases to be a source of innovation and becomes a net importer of technological innovation.

46 "Huawei: What Is 5G's Core and Why Protect It?," *BBC News*, January 28, 2020, sec. Technology, https://www.bbc.com/news/technology-51178376

47 Steven McGuire, "No More Euro-Champions? The Interaction of EU Industrial and Trade Policies," *Journal of European Public Policy* 13, no. 6 (2006): pp. 887-905, https://doi.org/10.1080/13501760600838573.

2.4 Key areas of potential flow insecurity

Key observations and conclusions regarding potential flow security risks for the 5G case:

- There is a strong nexus between national security considerations and the deployment of 5G networks.
- Chinese dominance in standard setting confers innovation and competitive advantages to its high-tech industry.
- There is a direct contradiction between the security incentives and the economic incentives in choosing Huawei 5G.
- The keystone technologies properties of 5G creates a chain of security risks in the national critical infrastructure.
- Dependence on Chinese technology harms European (corporate) innovation and could create more vectors for IP theft through legal and non-legal means.

3. Military angle: lasting dependency on US' military systems[48]

3.1 Introduction

The second case represents the military dimension of technological dependencies vis-a-vis the US, as well as an already manifest flow dependency that will require managing into the future.[49] Many modern weapon systems and platforms rely on continued access to data and information streams to be able to operate at maximum effectiveness. A prime example of such a weapons platform that requires embedding in a data ecosystem is the Lockheed Martin F-35 Lightning II. This case is further examined here. We underline that the case illustrates a broader range of cases where the acquisition of a class of weapon system implies a life-of-type-long relationship with the producer and/or lead nation to guarantee continuous technology insertion and operational data feeds for the upkeep of the operational performance of the platform/system. As such, the case is not centered on the F-35 per se, but particularly concerns the requirement for and dependency on a trusted relationship between partners (in casu the Netherlands and the US) surrounding sharing sensitive, partly highly classified, data and technology. We have also looked at two other illustrative cases, the M982 Excalibur range guided artillery shell and the MIN-104 Patriot surface-to-air missile system. These cases, however, have little to add to the F-35 case and are therefore not contained in this report.

In modern warfare, a meaningful deployment of a complex weapon system such as the F-35 is impossible without the ability to rapidly share operational information analyses with aircraft from partner nations, in particular the US as the largest user of the aircraft. This information sharing ranges from the Autonomic Logistics Information

48 Note that, due to the classified nature of large parts of the F-35 program and the resulting lack of open source information, the assessment in this case is partly based upon interviews with experts within the Royal Netherlands Air Force: Col Tjalling Frieswijk, Defense Material Organization, program manager; Mr. Steven Haijer, Airstaff, Strategy/Business Development; and LtCol Ted Meeuwsen, Dep Cdr Centre for Man in Aviation.

49 Perhaps the most salient example of technological dependence is arms export. The reliance on another country for the supply of arms creates multiple levels of (potential) leverage. The supplier may cut off access to the weapon system itself, to its ammunition or other components that directly contribute towards the operation of the system, or to its support systems (repair, maintenance, and overhaul). For modern weapon systems, an additional complexity may be added, namely that of information environment that it needs to access to properly function. It is this last dependency that this case emphasizes and explores.

System (ALIS),[50] which supports the maintenance, management, and deployment of the F-35, to the myriad of internal mission systems and sensors and allowing those systems to communicate between aircraft in a secure way.[51] In addition, there is an entire software ecosystem that manages and controls the aircraft while in flight that is needed for the airworthiness of the F-35.[52] All these data flows operate based on information sharing. Any disruption or limitation of such information sharing could severely and negatively impact the operational capability of the F-35.

As the F-35 is planned to remain in service for several decades to come, managing these data flows – and therefore the relationship with the US – is crucial for the Dutch defense organization. To contextualize this, we first examine the broader decision of choosing American built fighter jets over European ones. Following this, an assessment of the specific flow concerns with the F-35 is appropriate. Finally, the merits of international collaboration are assessed to balance the discussion. These arguments serve to underpin the question of what the state of military flow security with the US is, and to what consequences.

3.2 European or American? Technological dependencies between military partners

We may distinguish between two groups of European air forces: those that have the American F-16 and those which have a European-built jet aircraft as their main fighter aircraft.[53] The distinction has been dictated by domestic industrial interests, timely availability, participation possibilities (offset), and, not in the least, operational requirements. After World War II, the US provided Western European countries with Marshall Plan aid for economic recovery and later with dedicated 'defense support aid' programs to rebuild their defense structure in the face of the emerging Soviet threat. The Netherlands mostly used these funds to buy American military equipment, thus paving the way to the acquisition of the F-16 in the 1980s. In contrast, some larger European countries started developing and acquiring domestically produced fighter jets. The Multi-Role Combat Aircraft (MRCA) Tornado, for example, was jointly developed and manufactured by Italy, the UK, and Western Germany. The Tornado was succeeded by the Eurofighter, also produced by a European consortium. Naturally, the ability to construct fighter jets domestically removes the issue of flow securities on external parties. As such, decisions made in the US with respect to the sharing of

50 "Autonomic Logistics Information System (ALIS) | Lockheed Martin," accessed September 10, 2020, https://lockheedmartin.com/en-us/products/autonomic-logistics-information-system-alis.html.
51 "F-35 Mission Systems," F-35 Lightning II, accessed September 24, 2020, https://www.f35.com/about/capabilities/missionsystems.
52 "Platform One | Office of the Chief Software Officer, U.S Air Force," accessed September 24, 2020, https://software.af.mil/team/platformone/.
53 Within Bulgaria, Belgium, Croatia, Denmark, Greece, The Netherlands, Norway, Poland, Portugal, Romania, and Slovakia make use of the US produced F-16 Fighting Falcon.

information are less likely to directly impact the operational capacity of European fighter jets.

The Dutch choice to 'buy American', in line with the standing practice after WWII, was built on undisputed strong trans-Atlantic ties. However, recent geopolitical and US domestic political developments have increasingly drawn that relation into question.[54] These developments have accelerated the contemporary discussions in Europe around strategic autonomy. Indeed, various new initiatives, including the Permanent Structured Cooperation (PESCO), have been activated in response to this shifting strategic landscape. [55] While PESCO strengthens the ability of the EU to coordinate on issues of strategic autonomy, it does *not* necessarily reduce technological dependencies on the US.[56]

However, the complexity of reducing dependence on the US in the F-35 and similar cases (such as, for instance, the Patriot system) is considerable and costly. Creating a domestic industrial complex that could offer full serviceability for US-designed military equipment would require support from not only the original equipment manufacturer (OEM), but also from the US government. Indeed, most of the cooperation is arranged government-to-government. Even in cases where (parts of) American equipment is built in countries where these systems are utilized, the dependency on the US remains considerable. Most of the vital information required for a high-quality functioning of the US equipment is controlled by and processed in the US, often by US corporate parties. Hence, if the US loses trust in how, for instance, the Netherlands handles delicate equipment or adheres to data sharing agreements, cooperation could be endangered or unilaterally stopped, thereby preventing the Netherlands from being able to endanger the operational integrity of US-designed military equipment.[57]

3.3 The data streams relevant for the F-35

Several 'information flow'-related dependencies characterize the acquisition of a complex weapons platform such as the F-35. First, there are 'information ecosystem' considerations that apply not just to the F-35 platform as such, but also entail the entire support package. In this case, the platform defines all related business processes. Full logistics support – including spare parts, software inspection regimes and administration, the planning and (automatic) reporting of possible needed repairs

54 Most notably the rise of China, the Brexit referendum, the Russian annexation of Crimea, and the return of American isolationism.

55 Niklas Nováky, "The EU's Permanent Structured Cooperation in Defence: Keeping Sleeping Beauty from Snoozing," *European View* 17, no. 1 (2018): pp. 97-104, https://doi.org/10.1177/1781685818764813.

56 Shannon Togawa Mercer, "No, Europe Isn't Ambushing NATO," *Foreign Policy* (blog), accessed September 24, 2020, https://foreignpolicy.com/2018/01/03/no-europe-isnt-ambushing-nato/.

57 Based on interviews.

– is required to be able to operate the airplane. Acquiring jet fighters also means buying into a specific way of operating. An air force such as the Royal Netherlands Air Force (RNLAF), accustomed to US equipment and the 'way of doing business' that comes with it, would face a major overhaul of its structures, processes, and culture to accommodate the different operational and business principles associated with an European built aircraft. This includes the way data is shared between partners and the mutual trust required for this.

Furthermore, to take advantage of further developments and improvements and to profit from lower costs per flying hour over time, F-35 nations need to participate in the continuous program of F-35 lifecycle improvements. Modern aircraft regularly receive software updates that in turn require further training in the use and sharing of data. In fact, the Chief Software Officer of the US Airforce recently indicated that soon the service will be available to update an aircraft's onboard software whilst in flight.[58]

In practice, acquiring the F-35 also means acquiring Lockheed-Martin's Autonomic Logistics Information System (ALIS).[59] The F-35 comes not only with a dedicated logistic support system, but the philosophy behind the support systems also defines the logistic system and required skills of maintenance personnel involved and the maintenance organization itself. Complex as advanced multiple-task software can be, ALIS has presented difficulties for its operators and will probably be replaced by Operational Data Integrated Network (ODIN), following an announcement in January 2020.[60]

In fact, ALIS has been the cause of several unexpected F-35 groundings, with the US Government Accountability Office finding that ALIS posed several key risks, including data accuracy, accessibility issues, inadequate training, and lack of redundant infrastructure in the event of system failure.[61] The report also stated that ALIS is one of three major components that make up the F-35, together with the engine and the airframe. ODIN will be a cloud-native system that incorporates a new integrated data environment and a new suite of user-centered applications, according to a Pentagon statement. The ODIN is supposed to be designed to substantially decrease F-35 administrative and maintenance workload and increase mission capability rates for all F-35 variants. It will also enable software engineers to rapidly develop and deploy

58 Andrew Eversden, "Updating Software in Flight? The Air Force May Be Close.," C4ISRNET, September 16, 2020, https://www.c4isrnet.com/battlefield-tech/it-networks/2020/09/15/updating-software-in-flight-the-air-force-may-be-close/.

59 "Autonomic Logistics Information System (ALIS) | Lockheed Martin," https://lockheedmartin.com/en-us/products/autonomic-logistics-information-system-alis.html.

60 "Janes | Latest Defence and Security News," *Janes.Com*, accessed September 10, 2020, https://www.janes.com/article/93861/pentagon-announces-replacement-for-f-35-s-alis.

61 United States Government Accountability Office, "WEAPON SYSTEM SUSTAINMENT DOD Needs a Strategy for Redesigning the F-35's Central Logistics System," Report to Congressional Requesters, March 2020.

updates in response to emerging warfighter requirements.[62] The ALIS system provides crucial information on which parts of the aircraft need maintenance or replacement. Limiting access ALIS or its success ODIN could severely limit the ability of the RNLAF to maintain the F-35 in a combat-ready state.

Furthermore, next to logistical support, ALIS (as will its successor ODIN) also supports mission planning.[63] This is a highly information-dependent task, with data essential for safe and effective mission conduct. Parts of the database behind the mission planning system are also embedded in and controlled by ALIS. ALIS knows at least 65 sub-programs which will be updated regularly, just as ALIS as a whole (and ODIN as well).[64] A good example of a crucial sub-program is the threat database. This database contains the characteristics of all ground-to-air and air-to-air threats known and is regularly updated. This data is essential for the aircrew in choosing the best flight routes or in turning to stealth mode when necessary. Moreover, the entire system is highly dependable on the availability of reliable and safe communications to provide the needed cloud-data transfer, which introduces security issues at the user side as well.[65]

In summary, the F-35 capabilities are strongly associated with continuous sophisticated information flows. It is a system of systems of which the airborne platform is only the most visible part. To operate that platform at the required quality levels, now and in the future, a continuous good relationship with the OEM and the US government is of the utmost importance. Without this long-term relationship, it is difficult to deploy the aircraft, keep it in flying condition for a prolonged period, and to use all its advanced features in the long run.

3.4 Advantages of collaboration

The F-35 is the result of the US' most ambitious international military partnership to date. Participation within the Joint Strike Fighter / F-35 program has allowed the Netherlands to incorporate some crucial operational demands of the RNLAF into the design of the F-35. The accompanying co-creation serves to strengthen personal, military, and innovative ties between the US and the Netherlands. Furthermore, while the F-35 is dependent on the continuing open collaboration and information sharing from the US to its partners, the US itself is also dependent on European information

62 Based on interviews.
63 *ALIS: Keeping the F-35 Mission Ready*, 2017, https://www.youtube.com/watch?v=yqShP6R5P6g.
64 "Autonomic Logistics Information System (ALIS) | Lockheed Martin," accessed September 10, 2020, https://lockheedmartin.com/en-us/products/autonomic-logistics-information-system-alis.html.
65 Joseph Trevithick, "Foreign F-35 Users Spend Millions To Stop Jet's Computer From Sharing Their Secrets - The Drive," *The Drive*, September 21, 2018, https://www.thedrive.com/the-war-zone/23052/foreign-f-35-users-spend-millions-to-stop-jets-computer-from-sharing-their-secrets.

streams. These include intelligence sharing (although this has taken a diplomatic hit after the 2015 revelations that the US had surveilled German Chancellor Angela Merkel's personal cellphone).

As it stands, the collaboration between the US and various European countries, including the Netherlands, in the F-35 program has had, and still has, significant benefits. Nonetheless, in a shifting geopolitical environment, it is prudent to assess vulnerabilities and take proactive steps to minimize those. With a US that is increasingly ambivalent about its security obligations to and ties with Europe, a new paradigm in European security collaboration is emerging.[66] It is therefore paramount to, at the very least, map out potential flow security concerns that could directly impact the ability of the Dutch armed forces to execute its mandate.

3.5 Key areas of potential flow insecurity

Key observations and conclusions regarding potential flow security risks for the F-35 case:

- Dependence on the US-made military equipment has been beneficial for both the US and the Netherlands, and has made the Netherlands safer, stronger, and more secure.
- The benefits of US-Dutch military collaboration are contingent on adequate sharing of information; there are several ways in which limiting information sharing can negatively impact the combat effectiveness of US-made equipment.
- Besides classical considerations like supply chains and maintenance, there are also real-time data dependencies that must be managed appropriately to ensure the operational integrity of the Dutch armed forces.
- Several critical information-sharing agreements are necessary to keep the F-35 combat-ready. Temporary or permanent breaks in such systems can have immediate effects on the operability of the airborne platform.
- Frequent software updates are required and can be deployed in flight, creating scenarios where the airworthiness of the F-35 could theoretically be compromised while airborne.
- Current European alternatives to US-based military assets are neither adequate nor designed to be a direct replacement.

66 As exemplified by the September 2020 results from the 'Buitenland Barometer' of Institute Clingendael (https://www.clingendael.org/research-program/foreign-affairs-barometer). As the *Volkskrant* puts it: "Many now see the US as almost as great a threat as China and Russia, and believe that the Netherlands is better off with its European allies for its security" (https://www.volkskrant.nl/nieuws-achtergrond/onderzoek-nederlander-wil-neutraal-blijven-in-nieuwe-koude-oorlog-tussen-vs-en-china~baa2967e/).

4. Institutional angle: entanglements in the financial system

4.1 Introduction

This final case centers on the issue of institutions creating dependencies and flow insecurities. As certain systems of digital sharing and transfer of essential information, such as financial transactions, become more institutionalized and are being used globally, there is also the potential to politicize these systems – and especially the access thereto. As a result, countries or country blocs may opt-out of the widely institutionalized system and develop more entrenched, alternative versions. To illustrate this, we look at the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system. Related is the world's dependency on the US dollar as the world's reserve currency. Global financial dependencies on the US dollar create tools of leverage and potential flow insecurities, as it allows for greater access and control over various instruments of statecraft, including sanctions, capital and exchange-rate gains, and policy autonomy.[67] A summary of the influence of US dollar hegemony is beyond the scope of this study, but it is considerable and well documented.[68] Underpinning the global financial order and its dependence on the US dollar is SWIFT, the messaging system between financial institutions that allows for the international transfer of capital.

The later decades of the 20th century ushered in a period of globalization that has seen both cultural and economic interdependencies reach unprecedented levels of complexity. Economic globalization has been driven by global capital mobility that has allowed for the reorganization of global supply chains and the shift towards a focus on foreign markets instead of domestic production and consumption.[69] As a result, trade as a share of global GDP rose from 27% in 1970 to 60% in 2018. Given the global supply chains and increased dependency on international trade, this period also saw the emergence of international institutions to regulate and facilitate these globalized economic and financial flows, including the creation of SWIFT in 1973 and the WTO

67 Carla Norrlof, "Dollar Hegemony: A Power Analysis: Review of International Political Economy: Vol 21, No 5," *Review of International Political Economy* 21, no. 5 (April 17, 2014): 1042–70.
68 Carla Norrlof, "America's Global Advantage: US Hegemony and International Cooperation" (Cambridge: Cambridge University Press, 2010).
69 William Robinson, "A Theory of Global Capitalism" (Johns Hopkins University Press, 2004).

in 1994. Both SWIFT and the WTO have become increasingly politicized, especially following the 2016 US election and the subsequent start of the Sino-American trade war. In this case, we will focus on SWIFT as it ties closer to our overarching technology dependency angle.

Despite it being ostensibly neutral,[70] SWIFT has become a vehicle for geopolitical influence, particularly by the US. Examples include attempts to choke off funding to terrorist organizations after 2001, targeting various Russian economic sectors following the invasion of Crimea in 2014, and cutting off Iran from the global financial system after the decline of the Iran nuclear deal. Seeing the increased politicization of SWIFT, China[71], Russia[72], and the EU[73] have attempted to create alternative systems. Indeed, control over financial flows has both international and domestic incentives, the first in the form of protection of (domestic) assets and flows against external coercion and the latter in the ability and inclination to attack flows to coerce the external actors into making favorable geopolitical choices.

4.2 Shielding international financial flows

The defensive angle of financial flow security centers on the ability to shield one's own financial flows from external influence. The clearest application of this is the ability to avoid international sanctions, with the Iran Nuclear deal as a recent case. This example shows that financial dependencies may become a liability when strategic interests diverge. The European strategic interest is closer economic ties and investment opportunities in Iran, the American strategic interest under the Trump Administration is to pursue a maximum pressure campaign to starve Iran of foreign sources of capital. The strategic issues emerge from the lopsided ability of the US to force Europe into pursuing American interests that not necessarily align with Europe's own interests. In 2012, US Congress adopted legislation authorizing the president to impose sanctions on persons that provide financial messaging services to

70 SWIFT is an independent company that strongly upholds neutrality for its customers all around the world. Despite this core tenet of SWIFT, it has over time received requests to remove countries or institutions from its networks. This was especially the case in 2014, when SWIFT was asked to cease activity in Russia and Israel. The organization strongly refused compromising neutrality toward its customers and resisted political pressures to do so. Political sanctions, however, need to be respected by SWIFT given that it operates under Belgian – and EU – law. As such, if the EU were to implement sanctions against a country and if these sanctions referred, among others, to financial services like SWIFT, the organization would be obliged to comply. Ceasing activities in Iran, for example, occurred as a result of EU sanctions. See e.g. SWIFT. "SWIFT Sanctions Statement." SWIFT - The global provider of secure financial messaging services, October 6, 2014. https://www.swift.com/insights/press-releases/swift-sanctions-statement-0.

71 CIPS, "Company Profile," CIPS Co., Ltd., accessed September 2, 2020, http://www.cips.com.cn/cipsen/7052/7046/index.html.

72 National Settlement Depository. "NSD Receives the Status of Bank of Russia's SPFS Service Bureau," May 19, 2020. //www.nsd.ru/en/publications/news/press-releases/nsd-receives-the-status-of-bank-of-russia-s-spfs-service-bureau/.

73 Foreign & Commonwealth Office, and Jeremy Hunt. "New Mechanism to Facilitate Trade with Iran: Joint Statement." GOV.UK, January 31, 2019. https://www.gov.uk/government/news/joint-statement-on-the-new-mechanism-to-facilitate-trade-with-iran.

the Central Bank of Iran (CBI) or any other designated Iranian financial institution.[74] This legislation led to the disconnection of the CBI and other Iranian banks from the SWIFT financial messaging service. This was widely seen as one of the most powerful sanctions imposed on Iran prior to the 2015 nuclear deal formally known as the Joint Comprehensive Plan of Action (JCPOA).[75] The termination of Iran's connection to SWIFT was utilized to further the geo-political interests of the US and had a significant negative impact on the Iranian economy.[76] The subsequent decision by the Trump administration to retract from the JCPOA caused a strategic rift between the US and Europe. While the US aimed to cut off Iran from sources of international finance, the EU had sought to invest in the Iranian economy. However, given the dependence on the US financial system, European countries were unable to continue trading and investing in Iran for fear of being targeted by US sanctions. Any European corporation that continued seeking business in Iran could be subject to US secondary sanctions.[77] In fact, the mere threat of the US pulling out of the JCPOA slowed down European investment in Iran.[78]

This divergence of strategic objectives therefore gave rise to the contemporary discussion on how be able pursue geo-political interests without being subject to consequences from the US. One answer to this strategic leverage is to set up a parallel system, as evident by the multitude of (semi-)international alternatives. For example, the Bank of Russia has created its own System for Transfer of Financial Messages (SPFS) as an alternative to SWIFT, although its effectiveness is unclear. The SPFS system was created in direct response to the 2014 Invasion of Crimea and the American threats to remove Russian access to the SWIFT system. Fundamentally, SWIFT Is an international financial messaging system, and Russia is putting efforts in uniting other countries to circumvent it. For example, Iranian and Russian banks are now connected through the Russian SPFS and Iran's SEPAM financial messaging services to handle two-way banking transactions[79] China's Cross-Border Interbank

74 22 USC, "IRAN THREAT REDUCTION AND SYRIA HUMAN RIGHTS ACT OF 2012," 8701 § (2012). https://www.congress.gov/112/plaws/publ158/PLAW-112publ158.pdf

75 Rachelle Younglai and Roberta Rampton, "U.S. pushes EU, SWIFT to eject Iran banks," *Reuters*, February 15, 2012. (https://www.reuters.com/article/us-iran-usa-swift-idUSTRE81F00120120216); Rick Gladstone and Stephen Castle, "Global Network Expels as Many as 30 of Iran's Banks in Move to Isolate Its Economy," *The New York Times*, March 15, 2012, sec. World, https://www.nytimes.com/2012/03/16/world/middleeast/crucial-communication-network-expelling-iranian-banks.html.

76 Sajjad Faraji Dizaji and Peter A G Van Bergeijk, "Potential Early Phase Success and Ultimate Failure of Economic Sanctions," *Journal of Peace Research* 50, no. 6 (2013): pp. 721-736, https://doi.org/10.1177/0022343313485487. Fatemeh Kokabisaghi, "Assessment of the Effects of Economic Sanctions on Iranians' Right to Health by Using Human Rights Impact Assessment Tool: A Systematic Review," *International Journal of Health Policy and Management* 7, no. 5 (2018): pp. 374-393, https://doi.org/10.15171/ijhpm.2017.147.

77 Secondary sanctions are defined as sanctions that target third country actors doing business with a targeted regime, actor, or person. In this case the targeted regime is Iran, the third-party actors would be European corporations doing business with Iran.

78 Ellie Gernamyeh and Manuel Lafont Rapnouil, "Meeting the Challenges of Secondary Sanctions" (European Council on Foreign Relations, June 2019), https://www.ecfr.eu/page/-/4_Meeting_the_challenge_of_secondary_sanctions.pdf.

79 "Banks in Iran, Russia Connected via Non-SWIFT Financial Messaging Service," *Financial Tribune*, September 19, 2019, https://financialtribune.com/articles/business-and-markets/99912/banks-in-iran-russia-connected-via-non-swift-financial-messaging.

Payment System (CIPS) is looking at coordinating with Russia's SPFS to handle all Russia-China transactions. Likewise, several European countries have created Instruments in Support of Trade Exchanges (INSTEX), a special financial vehicle to continue trade with Iran while circumventing the SWIFT system[80] All these initiatives are broadly aimed shielding international financial flows from interference by third parties, most directly in the form of US sanctions. The goal is to create a separate financial ecosystem in which the US is not able to unilaterally block international financial transactions.

4.3 Securitizing domestic flows

In the event where multiple countries have adopted a standard other than SWIFT, it becomes possible to leverage dependencies in an offensive fashion. This falls into the broader strategic goal to reduce the power of the US financial hegemony and dependency on the US dollar. Specifically, the goal is to force other external actors to compete on terrain that is financially advantageous to yourself. Not only is the goal to minimize the ability of the US to block financial flows, but also to be able to actively interfere in others financial flows. This is pertinent to controlling flows in the domestic market. There are several ways to achieve this objective, including protectionist measures, state owned enterprise, trade policy, and setting of technical standards. We here will focus on the last: financial standard setting. This field is related to the term FinTech, which may broadly be defined as new technology that seeks to automate the delivery and use of financial services.[81]

China has arguably been most comprehensive in its attempts to develop a unique FinTech ecosystem, by its use of disruptive technologies like e-wallets, QR codes, and domestic protectionist measures. These serve not only to reduce dependence on the US dominated financial services (such as global credit card companies), but also to grow China's domestic financial ecosystem on its own terms. Alipay, the world's largest mobile pay platform currently counts over 1 billion users and has recently made the step to internationalize its platform.[82] Multiple European countries have partnered with Alipay system to streamline QR-based digital payment. Globally, over 55 (including 29 European) countries have accepted Alipay as a payment method. While dependencies are currently too low to leverage as geo-political tools, the growing importance of the Chinese consumer market allows for the leveraging of tech

80 "Trading with Iran via the Special Purpose Vehicle: How It Can Work | European Council on Foreign Relations," accessed September 10, 2020, https://www.ecfr.eu/article/commentary_trading_with_iran_special_purpose_vehicle_how_it_can_work.

81 Anne-Laure Mention, "The Future of FinTech," *Research-Technology Management* 62, no. 4 (2019): pp. 59-63, https://doi.org/10.1080/08956308.2019.1613123.

82 Sito Peggy, "Alipay Launches International E-Wallet, Giving Foreigners Access to Mobile Payment Platform in First for China | South China Morning Post," *South China Morning Post*, November 5, 2019, https://www.scmp.com/business/article/3036366/alipay-launches-international-e-wallet-giving-foreigners-access-electronic.

standards in the future. If Chinese FinTech can set the standards and best practices for the industry it would confer sizable strategic advantages both in terms of innovation but also the overall design of the system to further Chinese strategic purposes. In addition, if Chinese FinTech becomes increasingly dominant other countries may choose to adopt the Chinese standards over Western ones, further strengthening the ability of the Chinese to control financial flows in more proactive terms. Failure to comply according to the domestic Chinese standards could be basis upon which Western corporations are prevented from operating in the Chinese market.

4.4 System-level dependencies

The global financial system is largely underpinned by the value of the US dollar, with over 80% of international financial transactions and 61% of global reserve currencies denominated in US dollars.[83] Such a deep dependency, together with global financial integration and dependency on US based banking institutions, creates possible vulnerabilities for localized financial crisis to have global impact, most clearly seen in the 2007-08 global financial crisis.[84] While the collapse of the US dollar has been predicted by analysts for decades,[85] the 2020 Covid-19 crisis saw a global surge of lending in US dollar denominations from the Federal Reserve amounting to $450 billion.[86] Part of the strength of the US dollar is trust in the US as the global financial hegemon, and the perception that the US Treasury bond are risk-free assets.[87] As a result, times of high global risk often see a 'flight to safety' to US treasury bonds.

However, recent political developments have problematized this perception. The 2007-08 global financial crisis showed that the US banking sector could have considerably negative impacts on the US economy that required direct policy intervention such as quantitative easing. Trust in the stability of the US dollar is increasingly being drawn into question, as evidenced by the S&P-rating downgrade from AAA to AA+ in 2011. Under the current Trump administration this discussion has been further accelerated, most notably due to the idea to directly manipulate the US currency in 2019;[88] an idea

83 International Monetary Fund, "Currency Composition of Official Foreign Exchange Reserve - IMF Data" (International Monetary Fund, June 30, 2020), https://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4.

84 OECD Economics Department Policy Notes, "Financial Contagion in the Era of Globalised Banking?," June 2012, http://www.oecd.org/economy/monetary/50556019.pdf.

85 Doug Stokes, "Achilles' Deal: Dollar Decline and US Grand Strategy after the Crisis," *Review of International Political Economy* 21, no. 5 (August 2013): pp. 1071-1094, https://doi.org/10.1080/09692290.2013.779592.

86 Lindsay Dunsmuir and Howard Schneider, "Fed Opens Dollar Swap Lines for Nine Additional Foreign Central Banks," *Reuters*, March 19, 2020, https://www.reuters.com/article/us-health-coronavirus-fed-swaps-idUSKBN2162AX.

87 Wenxin Du, Joanne Im, and Jesse Schreger, "The U.S. Treasury Premium," 2017, https://doi.org/10.3386/w23759.

88 We note that there is considerable discussion on whether Central Banks and specifically quantitative easing should be considered currency manipulation. While we do not take a position on this, the 2019 proposal was widely seen as recognizable currency manipulation, and a considerable shift from previous US Treasury policy.

that was ultimately rejected.[89] The current domestic political turmoil, polarization and associated political norm breaking further undermines trust in the dollar.[90] The Eurasian Economic Union has de-dollarized its trade by 70% with the aim to reduce dependency on the US dollar entirely. If such attempts to create greater economic and monetary autonomy catch on, this could cause large scale fluctuations in currency exchange rates that may have far reaching consequences or otherwise offer geo-political vectors.

4.5 Key areas of potential flow insecurity

Key observations and conclusions regarding potential flow security risks for the Financial Entanglements case:

- The leveraging of financial messaging systems and FinTech could compromise international financial markets.
- Coercive use of financial institutions would lead to the blocking of certain international transactions, limiting ability to trade and undermining strategic autonomy.
- Technological incompatibility in finance could cause fragmenting of financial system, and creating unequal playing fields within different markets
- Lack of global financial hegemon makes sanction-based adjudication of international conflicts impossible.

89 Alan Rappeport and Jeanna Smialek, "White House Considered Weakening U.S. Dollar Before Ruling It Out - The New York Times," *The New York Times*, July 26, 2019, https://www.nytimes.com/2019/07/26/us/politics/trump-dollar-currency-manipulation.html.

90 Alan Rappeport, "U.S. Says China Is No Longer a Currency Manipulator - The New York Times," The New York Times, January 15, 2020, https://www.nytimes.com/2020/01/13/us/politics/treasury-china-currency-manipulator-trade.html.

5. Policy implications

5.1 Introduction

The three cases examined in this paper each represent technology flows that come with high, potentially unacceptable, levels of risk to Dutch national security. Their interruption would have an immediate and severe impact on critical functions of the Dutch government or Dutch society, and no ready alternatives are available. The 5G case highlight risks to national security, to long term economic competitiveness, and to data and privacy protection. The F35 case illustrates a clear dependence on the US for the military operational readiness of Dutch armed forces. The financial entanglements case, finally, represents how the weaponization of financial institutions undermines global trade and investment, spurs the fragmentation of financial systems, and decreases the coercive leverage of Western states.[91]

The three cases each represent different risks, but together highlight that flow security requires proactive management at the national and at the European level. Failure to do so will severely limit Europe ability to set and pursue its own geopolitical objectives and, as a result, curtail European strategic autonomy. Reaction to the manipulation of flows by third actors only after the fact is detrimental to vital security and economic interests and undermines Europe's ability to effectively operate in today's geo-political environment.

Case	Domain	Risk	Costs	Benefits
Huawei 5G	Economic & Information	Losing autonomy over critical infrastructure	• Compromised information flows • Reduced European innovation • Technological lock-in	• Low financial costs • Faster adoption of keystone technology
F-35	Military & Territorial	Failure to maintain combat readiness	• Reduced combat effectiveness	• Access to most advanced weapons platforms • Closer integration into US defense deterrent
Financial entanglements	Economic & International security and order	Fragmentation and isolation from international finance	• Secondary sanctions impact European businesses	• Access to global financial system • Greater integration into the global economy

91 In the systematics of the risk assessment process of the National Security Strategy, security risks are categorized according to their impact on six categories of vital interest: economic security, territorial security, ecological security, physical security, social and political stability, and international law and order. Risks associated with the type of information / technology flows covered in the 5G case and SWIFT case relate to economic security, but may indirectly also challenge social and political stability, and international law and order. The F-35 case pertains to territorial security and international law and order.

5.2 Policy instruments

While there are considerable risks associated with flow security, these are to a large extent the flip side of sizable advantages. For the Netherlands, some degree of dependence is inherent to being part of both the global community through the UN, NATO, the EU, and myriad other fora, as well as being a nation closely engaged in trade and commerce. On an abstract level, one of the solutions available to solve the issue of flow security is autarky. The contemporary return of populism has come with strong autarkic undertones, including anti-globalization, anti-EU sentiments, and 'America First' type of sentiments.[92] While such (economic nationalist) solutions may be politically expedient in the short term, we emphatically argue against such an approach. As a country, the Netherlands benefits enormously from multilateralism and the international rules-based order.[93] Flow dependencies certainly come with benefits and advantages. An autarkic Netherlands, if possible at all, would be weaker, less prosperous and less influential. Furthermore, it is difficult to detach domestic security from international security, and in many cases impossible (e.g. in the case of ecological security).

Instead, the goal should be more selective in which flows are of strategic importance and therefore in need of management. There is a strong nexus between the topic of flow security and the larger notion of strategic autonomy.[94] As such, some (but not all) policies that are in the pursuit of strategic autonomy are relevant for flow security. Four such recommendations that pertaining more narrowly to the policy recommendations stemming from the case studies include:

- Demarcation of sectors of strategic importance.
- Manage sensitive data transfers between Europe and potentially malicious actors.
- Calculate-in market distortions and unfair economic advantages associated with foreign-made technology.
- Strengthen the (international) role of the Euro and associated central bank institutions.

These recommendations allow the Netherlands, through Europe, to remain a global actor, but simultaneously offer a greater range and flexibility of strategic options. In addition, the principles outlined in the Dutch Defense Vision 2035[95] of innovative capacity, authoritative information position, and a stronger more self-sufficient Europe logically concur with these policy recommendations. In its bleakest interpretation,

92 Lubos Pastor and Pietro Veronesi, "Inequality Aversion, Populism, and the Backlash Against Globalization," 2018, https://doi.org/10.3386/w24900
93 https://hcss.nl/report/adjusting-multilateral-system-safeguard-dutch-interests
94 https://ecfr.eu/publication/defending_europe_economic_sovereignty_new_ways_to_resist_economic_coercion/
95 Ministerie van Defensie, "Defensievisie 2035. Vechten voor een veilige toekomst", October 2020.

Europe imports a sizable fraction of innovation, is dependent on foreign-made technology and data streams for its information position and is unable to pursue its own strategic objectives without crippling financial sanctions. The above measures would allow us to avoid turning our backs to the world, yet manage flow securities to maximize the benefits to the Netherlands and the global community, while seeking to minimize or mitigate the risks that come with over-dependence. To this end, various strategies can be utilized, which can be categorized into four different approaches elaborated below:

1. securitizing flow dependencies;
2. creating flow redundancies;
3. obtaining flow autonomy; and
4. offensive leveraging of flow dependencies.

5.3 Securitizing flow dependencies

In some instances, there is no viable alternative for accepting potential flow security concerns in the short term. The logical approach then is to set strong standards and requirements to mitigate and minimize these security concerns. Such approaches include trying to limit the risks to non-vital sectors, but also the setting of specific considerations in the procurement process of technology.

The clearest example of this is the discussion about distinguishing between the core and the edge of communication networks when making use of 5G equipment made by Huawei. The 2020 5G toolkit developed by the EU, while not specifically naming Huawei, sets various requirements for telecom providers to properly assess risks and take appropriate security measures.[96] In addition, it also encourages member states to not award procurement contracts based solely on the lowest price, but to also take into consideration security, quality, labor, and environmental standards. It also highlights various certification schemes including under the 2019 Cybersecurity Act, as well as naming the NIS Directive for security measures. These measures are all broadly aimed at creating restrictions on the implementation of 5G infrastructure by high-risk suppliers and avoiding dependencies.

In the broader sense, the 5G toolkit serves to define regulatory powers to the European Commission on high-risk technology. This is part of longer-term trend with multiple anti-trust lawsuits aimed primarily at US based tech giants including Google and Facebook. More recently the passage of the General Data Protection Regulation (GDPR) has unified the regulatory landscape within the European Union and conferred

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

a considerably greater level of control for individuals over personalized data.[97] Because foreign tech businesses must conform to GDPR regulation while operating on any European citizen's data, various countries have already adjusted their data protection legislation to conform to the GDPR. South Korea has recently amended its Personal Information Protection Act (PIPA)[98] to reflect GDPR standards, and the California Consumer Privacy Act (CCPA)[99] of 2018 set stringent privacy requirements on the use of data for the State of California that are similar, albeit smaller in scope, to the GDPR.[100] As such, while the EU might be largely dependent on foreign parties for the procurement of technology, it is very well suited to set rules and regulations globally when it comes to the use of data.

5.4 Creating flow redundancies

The primary problem in flow security is not that there is some level of dependence, which is inherent to flows, but rather that there is an over-dependence. Indeed, the F-35 and 5G cases illustrate where the Netherlands is largely dependent on the goodwill of a single partner to ensure the technology will remain functional and secure. One possible solution to this problem is to diversify these dependencies and spread the risk across different parties. This would serve to reduce the impact that a breakdown of relations with a single party would have. Note that the goal of this approach is *not* to create a direct replacement for existing cooperation structures (such as the trans-Atlantic bond in the F-35 case), but rather to create secondary or redundant capacity.

Within the policy objective of spreading risk, two different avenues may be pursued. The first is that the Netherlands should attempt to create redundancies in its flows to ensure that, when a flow becomes compromised, there is a suitable replacement. Examples would be to use Ericson and/or Nokia as 5G solution providers next to Huawei; and have European UAV suppliers next to an American manned fighter provider. While this may come with (possibly considerable) logistical and financial burdens, it would guarantee Dutch telecom providers and the RNLAF respectively a greater share of operational integrity.

The second approach is to create small networks of flow dependencies which are more likely to remain strategically aligned with the Netherlands and have comparable geostrategic objectives. This could include alternative collaboration structures, which revolve around creating mutual dependencies with likeminded parties. In fact, the F-35 case already exhibits some of these mutual dependencies, in which the USAF and the

97 https://gdpr.eu/
98 https://www.legal500.com/developments/thought-leadership/major-amendment-to-the-personal-information-protection-act-passed-by-national-assembly/
99 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121
100 https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

American OEM draw considerable profit from foreign partners in the F-35 development program. Another example in the military realm of such a (nascent) collaboration is the Permanent Structured Cooperation (PESCO). While still limited in scope, the PESCO collaboration is a good example of stronger policy and security integration within the EU, also beyond the defense and security sector. By itself, the Netherlands is simply too small to be able to strategically compete with the US or China. However, working in tandem with other EU member countries, it is much more able to defend its strategic interests. Another example has been the creating of the Instrument in Support of Trade Exchanges (INSTEX), which was aimed at circumventing secondary sanctions for trading with Iran. INSTEX was never meant to be a complete replacement for the SWIFT banking system, but rather served as a specialized financial vehicle in cases where financial flows might otherwise be obstructed.

5.5 Obtaining flow autonomy

Whereas creating flow redundancies is about securing 'back-up' possibilities in the event of a flow security failure, the purpose of flow autonomy is to remove the possibility of flow interruptions entirely. The goal here is to limit flow dependencies to a set of likewise nations that have largely convergent political interests. For the Netherlands this primarily means looking at European partners. An example of flow autonomy are efforts towards European industrial policy.

One major difference between innovation policies of the US and China on the one hand and Europe on the other, is that the EU has long resisted to designated some of the new high-tech sectors as strategic sectors. Only as recent as 2020, the European Commission has formally called for the sustainability and digital transition sectors to be strengthened.[101] The report not only named these sectors critical for Europe's sovereignty, but also calls for the leveraging of the impact, size, and integration of its market to set global standards. Notably, the EU competition framework, which historically has been centered on preventing the emergence of national champions, is under review.

The 5G case features in a broader discussion on advanced technologies such as quantum computing, artificial intelligence, and advanced data analytics. Flow security concerns occur when Europe becomes dependent on such technologies from parties that are not fully trusted. In the case of 5G, there is a lack of trust in the intentions of China. But there is also a contemporary discussion on trust in large American tech giants such as Facebook and Google. The creating and economic support mechanisms for national European based tech giants would go a long way towards strengthening

101 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0102&from=EN

not only trust in technology, but also the ability of the EU to regulate such industries on its own terms. If successfully implemented, the EU would be able to have a trusted domestic supplier for high-tech industry and thereby avoid the geopolitically tricky waters of the US-China tech war.

5.6 Offensive leveraging of flow dependencies

A final policy tool is to actively create and offensively leverage flow dependencies that other countries might have. This would thus entail a more active and aggressive policy towards countries such as China and, in some instances, the US and attempt to leverage flow dependencies that they might have on us. We illustrate this approach with an actual example regarding the semiconductor industry.[102]

China has considerable flow dependencies within its nascent high-tech sector that it is looking to consolidate. This is particularly true in the developing Chinese semiconductor industry, which has been a long-term strategic priority. As for 2019, China made up nearly a quarter of global demand for semiconductors, while domestic production in China accounts for only 14% of that amount.[103] As a result, US led sanctions and export control on semiconductors have considerable impact on the Chinese tech industry. Being aware of this, the Chinese government has directed efforts towards securing non-American sources of semiconductors, most notably in Taiwan. Together with South Korea and the US, Taiwanese semiconductor developers are some of the most advanced in the world. The Taiwanese corporation TSMC produces almost half of the world's annual supply of chips.[104]

This has led to concerted efforts by Chinese parties to invest in Taiwanese semiconductor firms, most notably through the Tsinghua Unigroup. These deals have been repeatedly blocked by the Taiwanese government for fear of losing a competitive and technological advantage. Successful efforts by the Chinese to acquire Taiwanese semiconductor corporations would have significant strategic consequences, as it would allow for the absorption of manufacturing knowledge as well as reduce US ability to curtail Chinese semiconductor imports. While the Chinese domestic semiconductor industry complex is vast, it is still lagging in innovation. Estimates from experts indicate that China is 5-10 years behind Taiwan, South Korea, and the US.[105] The

102 This case is based on work performed by Datenna (https://www.datenna.com/), as commissioned by HCSS in the context of this research. Annex A gives a more detailed elaboration of the case.

103 Jacky Wong and Dan Gallagher, "Real Winner in U.S.-China Chip War Won't Be Either Side," *The Wall Street Journal*, June 4, 2020, https://www.wsj.com/articles/real-winner-in-u-s-china-chip-war-wont-be-either-side-11591265619.

104 Kate Sullivan Walker, "The Semiconductor Industry Is Where Politics Gets Real for Taiwan," *The Inerpreter*, September 10, 2020.

105 "China Needs 'Five to 10 Years' to Catch up in Semiconductors, Peking University Professor Zhou Zhiping Says," *South China Morning Post*, September 3, 2019, https://www.scmp.com/tech/tech-leaders-and-founders/article/3024315/china-needs-five-10-years-catch-semiconductors.

competitive advantage is still with the Taiwanese firms, but capital and investment will be needed to maintain this edge.

With the Chinese not being a viable strategic source of investment, there is an opportunity for Europe to step into this gap. This would serve two important strategic purposes for Europe. The first is that it slows down China's ability to leverage flow dependencies and dominate the global tech competition. The second is that collaboration and investment in the Taiwanese semiconductor industry could allow for knowledge transfer to European corporations which give rise to the possibility of domestic European semiconductor industry.

Strategic investment and long-term partnerships with amenable partners would allow for Europe to remain competitive in the global semiconductor industry. Domestic parties such as ASML and NXP Semiconductors are both internationally recognized manufacturers of semiconductors. NXP Semiconductors had previously been in negotiations with Qualcomm to be acquired, a move that was later blocked by the Chinese. Similarly, ASML acquired Taiwan's Hermes Microvision for $3.1 billion in 2016. However, TSMC reached a peak market capitalization of $410 billion in June of 2020, giving an indication of the scale needed to be globally competitive. More ambitious long-term plans and the ability to provide larger amounts of investment would be necessary to keep Europe a factor in the global tech competition.

This example illustrates that Europe indeed has opportunities to leverage flow dependencies against global competitors but may need to step up its game to actually seize these opportunities.

6. Final remarks

Flow dependency is not inherently a risk and should not be formulated as such. In fact, virtually all flows come with at least some form of mutual dependency. Furthermore, international dependency and collaboration have generated a large net positive for the Netherlands and Europe. Therefore, the interwoven nature of the modern globalized community should not be discarded out of hand, despite populist political rhetoric to do so. A retrenchment of the Netherlands vis-a-vis many of the international flow dependencies would cripple our country socially, militarily, and economically. But that does not mean that dependency is beyond reproach. The Netherlands and Europe must adapt to the new geopolitical reality, with its multi-polar constellation of powers and increased competition and rivalry.

The specter of economic nationalism and backlash against globalization has accentuated the urgency for Europe to proactively think about its dependencies and manage them appropriately where and when needed. Interwoven financial dependencies have forced Europe into accepting the de-facto collapse of the Joint Comprehensive Plan of Action with Iran. The prospect of technological dependency on Chinese built 5G has made explicit the contrasting economic and security incentives within the continent. The possibility, far-fetched or not, of a US departure from the NATO alliance has led to consternation and alarm within the European defense community. In each of these cases, the conclusion is inexorable: regardless of what form of strategic autonomy Europe seeks to pursue, it requires the proactive management of dependencies, and as such entails a holistic understanding of flow security.

Technological flows especially represent both a seminal challenge and opportunity for the Netherlands and Europe. Various options are viable to pursue, but all emanate from a paradigmatic shift from previous policy. That is the decision to designate sectors within Europe that are deemed vital to its strategic interests and as such merit tailored treatment. The subsequent policy menu ranges from traditional securitization of flow dependencies (such as keep out high-risk vendors of 5G equipment) to the offensive leveraging of flow dependencies towards strategic rivals. An associated shift is to move from looking at flows in purely economic and financial terms towards a more comprehensive – and in policy terms, a whole of government – approach. The age of unfettered global capitalism and the underlying assumption that free trade automatically entails (democratic) liberalization appears to be over and a new reality

of innovation mercantilism[106] has dawned. Europe has the tools that it needs to shake off its geostrategic impediments and to do so in a fashion that does not endanger the trans-Atlantic relation or alienates potential new friends and allies elsewhere. All that remains is a proactive vision and the political will to pursue that goal. Whichever policy direction we choose, we must be cognizant of the flows that tie the world together, but also bind us to each other's strategic imperatives.

106 Defined broadly as policies that seek to grow nations' innovation-based firms and industries through policies such as local production requirements, export subsidies, weak intellectual property (IP) protection, discrimination against foreign firms, economy-specific technical requirements, and data localization requirements. See the forthcoming strategic monitor report for a broader description of this phenomenon.

Annex A: PRC-Taiwan semiconductor case[107]

In mainland China the government has a large influence in key industries such as the semiconductor industry. Taiwan on the other hand is more oriented on capitalism and a free market and has less influence of the state. This supposedly provides a more investor friendly climate. In this case we show that the Chinese national government also has an influence in Taiwanese businesses through investments in their Chinese subsidiaries.

Taiwan's national policy does not allow investments from mainland China in its local semiconductor industry. In 2018 however, Taiwan based ASE Technology Holding Co., the world's number one company in the semiconductor packaging and test market, agreed to sell a 30% stake in its Suzhou (China mainland) subsidiary to Beijing Ziguang Capital Management. This investment company is ultimately controlled by Tsinghua Unigroup (through their investment vehicle Tsinghua Holdings. Tsinghua Holdings Co Ltd has investments of over 350 million euros and is the largest investment vehicle of Tsinghua Unigroup. The second largest investment vehicle is Beijing Tsinghua University Enterprise Group which invested another 234 million euros. Tsinghua Holdings Co Ltd owns the majority share (51%) in Ziguang Group, which in turn fully owns Beijing Ziguang Capital Management Co Ltd. The other 49% in Ziguang Group is held by Beijing Jiankun Investment Group which is owned by three individuals. With 70% of the shares Zhao Weiguo is the controlling shareholder. He is also chief executive of Tsingua Unigroup, and legal representative of Ziguang Group as well as Beijing Ziguang Capital Management Co. Ltd.

Suzhou ASEN Semiconductors Co. was founded in 2007 as a joint venture between Taiwan based ASE and Netherlands based NXP Semiconductors, to provide IC packaging and testing services in China. ASE had a 60 percent stake in Suzhou ASEN and NXP 40 per cent, but in March 2018 ASE bought back NXP's stake and subsequently sold 30% to Beijing Ziguang Capital Management Co Ltd (controlled by Tsinghua Unigroup). This deal was remarkable, because Tsinghua Unigroup had tried to buy into Taiwanese semiconductor companies before, but those deals were repeatedly blocked by the Taiwan government.

107 Research performed by Datenna, as commissioned by HCSS in the context of this research.

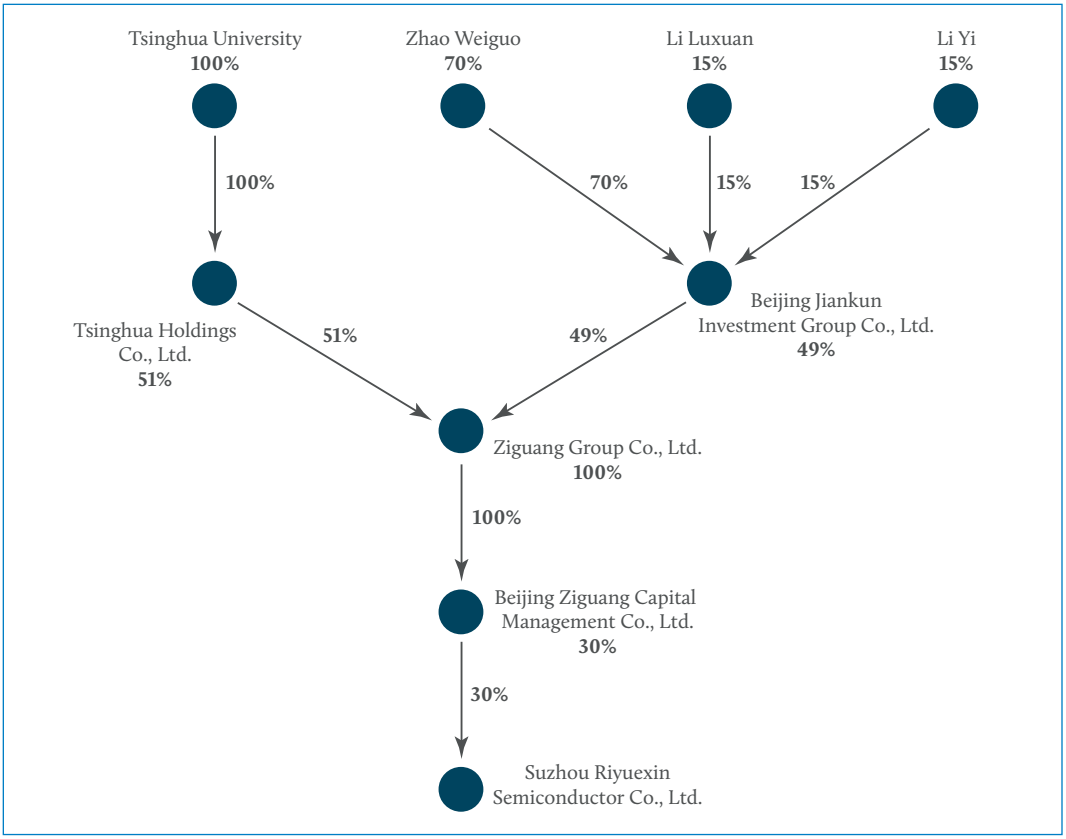

Figure 1: Ownership structure Suzhou subsidiary ASE Technology Holding Co

Two years before, in 2016, Tsinghua Unigroup attempted to buy into Suzhou ASEN, but that deal failed due to regulatory scrutiny. Another deal that took some time to proceed was the merger between ASE and Silicon Precision Industries (SPIL), another big IC packaging and testing service provider from Taiwan. This merger was first announced in mid-2016, but the deal had to be reviewed by anti-trust regulators in several jurisdictions. The Ministry of Commerce of the People's Republic of China had its concerns that the deal could have the impact of eliminating or restricting competition in the market. However, right after the sale of 30% shares in Suzhou ASEN to (indirectly) Tsinghua Unigroup, China approved the proposed merger between ASE and SPIL. This caused speculation on whether China's approval came with the condition of the sale of ASE subsidiary's share in Suzhou ASEN to Tsinghua Unigroup.

ASE Technology said that the sale of the 30 percent stake in Suzhou ASEN was aimed at building a strategic partnership with Tsinghua Unigroup to help it to penetrate China's semiconductor market. Interestingly, Taiwan's Central News Agency notes that the merger between ASE and SPIL, which was thus only approved after ASE sold the 30 per cent stake of Suzhou ASEN to Tsinghua Unigroup, "was made to strengthen the new company's global competitive edge through larger economies of

scale and *fend off investment overtures by Chinese companies such as Tsinghua*."[108] The Economist writes that mainland China's chip firms mostly lag far behind global leaders in invention.[109] Tien Wu, chief operating officer of ASE, explains that Taiwanese firms were entering the chip market at a time when it was enjoying heady expansion, which makes it harder for Chinese firms to succeed during times of slower growth.[110] The Taipei Times writes that according to SPIL, the transaction is expected to help the company tap the fast-growing Chinese market, and that the proceeds will be used to expand its production capacity in Taiwan.[111] The partnership is expected to help ASE secure orders from the Chinese group's units.[112]

108 "ASE Technology to sell Suzhou unit stake to Tsinghua Unigroup - Focus Taiwan," accessed September 24, 2020, https://focustaiwan.tw/business/201808110005.

109 "Chips on Their Shoulders," *The Economist*, January 23, 2016, https://www.economist.com/business/2016/01/23/chips-on-their-shoulders.

110 Ibid.

111 Lisa Wang, "ASE Gets Chinese Regulatory Approval for SPIL Merger," *Taipei Times*, November 25, 2017, https://www.taipeitimes.com/News/front/archives/2017/11/25/2003682877.

112 "ASE Technology to sell Suzhou unit stake to Tsinghua Unigroup - Focus Taiwan," accessed September 24, 2020, https://focustaiwan.tw/business/201808110005.

The Hague Centre for Strategic Studies

info@hcss.nl

hcss.nl

Address:
Lange Voorhout 1
2514EA
The Hague
The Netherlands