1 Introduction

1.1 Introduction

I start this dissertation by providing an overview of the context and the relevance of this research (Section 1.2), which, at its core, concerns the intrinsically dynamic intelligence domain. Within that domain, intelligence and security services use their investigatory powers to counter constantly evolving cyber threats. This section ultimately leads to the main research question and a presentation of the (sub-)research questions needed to provide an answer to the main research question (Section 1.3). I then elaborate on the research scope and limitations (Section 1.4). In Section 1.5, I set out the methodological approach of this research and how this approach contributes to answering the main research question. At the end of this chapter, I provide background on fundamental concepts of the research (Section 1.6): economic cyber espionage (1.6.1), counterintelligence in the cyber domain (1.6.2), and the right to privacy and personal data protection (1.6.3). This chapter concludes with an overview of the research outline (Section 1.7).

1.2 Research context and relevance

In this section, I set out the context and the relevance of this research. I outline recent developments in the threat landscape and within the intelligence domain to provide context for the research questions presented in Section 1.3. I also address the (societal) relevance of this research.

1.2.1 Research context

In October 2023, the intelligence heads of the Five Eyes alliance warned the private sector about the rise in economic espionage. They specifically warned about the threat of intellectual property theft in the context of emerging technologies.[1] In

1. See Emma Woollacott, 'Global Intelligence Chiefs Warn of "Unprecedented" Chinese Spy Threat' *Forbes* (18 October 2023) <https://www.forbes.com/sites/emmawoollacott/2023/10/18/global-intelligence-chiefs-warn-of-unprecedented-chinese-spy-threat/> accessed 02 March 2025. The Five Eyes alliance is an intelligence partnership between the United States, the United

2024, the Federal Bureau of Investigation and the Infrastructure Security Agency confirmed that the Chinese hacking group "Salt Typhoon" had successfully targeted telecom companies in the United States, thereby accessing texts and calls in real time on a large scale.[2] This is one of numerous examples of cyber operations attributable to state actors, directed at states. In January 2025, Russian cyberattacks on Ukraine were reported to have increased by 69.8%, mainly targeting telecommunications, governmental organisations, and the Ukrainian defence sector.[3] At the same time, in spring 2025, a Russian ex-employee of the leading Dutch chip-making equipment manufacturer ASML was arrested on suspicion of passing sensitive company information to the Russian Foreign Intelligence Service, SVR. Cyber threats are ever-present and increasing.

As a response to increasing cyber threats, states are seeking ways to arm themselves against those threats. In 2024, the Dutch parliament passed a bill specifically designed to facilitate more dynamic cyber operations and provide greater leeway for Dutch intelligence and security services against offensive cyber programs of state actors.[4] In the 21st century, these state-sponsored offensive cyber programmes are more prominent than ever.[5] The mitigation of and response to these national security threats – and, notably, the initiation of those threats – fall within the scope of intelligence operations.[6] Although offensive cyber programmes involve a wide range of cyber activities, ranging from information campaigns to

---

Kingdom, Australia, Canada, and New Zealand. This partnership also amounts to sharing signals intelligence, see John Michael Weaver and Tom Røseth, *The 'Five Eyes' Intelligence Sharing Relationship: A Contemporary Perspective* (Palgrave Macmillan 2024) 3.

2. R Wyden & E S Schmitt, Letter to Department of Defense Inspector R.P. Storch, 4 December 2024; A. Greenberg, 'China's Salt Typhoon spies are still hacking telecoms: Now by exploiting Cisco routers', *WIRED* 13 February 2025; L. Hay Newman, 'Brass Typhoon: The Chinese hacking group lurking in the shadows', *WIRED* 14 April 2025.
3. Ukraine CERT-UA, State Service of Special Communications and Information Protection of Ukraine, 'CERT-UA recorded 4315 cyber incidents in 2024', 8 January 2025.
4. Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen 2024 [Staatsblad 2024, 88]; Jan Jaap Oerlemans, 'The necessity of a new cyberlaw for dutch intelligence and security services' (*jjoerlemans.com*, 26 June 2023) <https://jjoerlemans.com/2023/06/26/the-necessity-of-a-new-cyberlaw-for-dutch-intelligence-and-security-services/> accessed 15 April 2025; Rowin HT Jansen, 'Van accentverschuiving naar stelselwijziging: Toezicht in het conceptvoorstel Tijdelijke cyberwet voor de AIVD en de MIVD' (2022) 97 Nederlands Juristenblad 2406; Sophie AM Harleman, 'Een tijdelijke Cyberwet maakt nog geen sleepwet' (2022) 2695 Nederlands Juristenblad 3120.
5. AIVD, 'Jaarverslag 2023' (Algemene Inlichtingen- en Veiligheidsdienst 2024) 32; AIVD, 'Offensive Cyber-Programmes: An Ideal Business Model for States' (AIVD 2020); Winnona Desombre and others, 'A Primer on the Proliferation of Offensive Cyber Capabilities' (Atlantic Council 2021) Issue Brief.
6. See Paul AL Ducheine and Peter BMJ Pijpers, 'The Notion of Cyber Operations' (Amsterdam Center for International Law, 14 April 2020).

sabotage, cyber *espionage* is often an essential element, or even a precursor to further escalation.[7]

Espionage is an established state practice, and states are the main actors concerned with espionage.[8] When they conduct espionage to acquire information held by states, this can be characterised as political espionage.[9] In this research, I use *economic cyber espionage* as a central theme. Economic cyber espionage is conducted by states, but directed against information held by non-state actors. Espionage is a valuable tool for intelligence collection. Intelligence and security services are concerned with such intelligence collection in the state's interests. I want to note that while this research centres on Euro-Atlantic[10] intelligence and security services and their efforts to counter and prevent cyber espionage, this does not necessarily preclude that these states also conduct – and are accused of conducting – espionage.[11]

Intelligence can be used to prevent and counter espionage. There is no uniform definition of what intelligence constitutes, neither as a practice nor as an "end product."[12] Intelligence can be regarded as a foreign-focused process which requires elements of deception and operates in the interests of the state,[13] or, more

7. Dominik Herrmann, 'Cyber Espionage and Cyber Defence' in Christian Reuter (ed), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (Springer Fachmedien 2019) 85–86 <https://doi.org/10.1007/978-3-658-25652-4_5> accessed 14 April 2025.
8. Russell Buchan, *Cyber Espionage and International Law* (Hart Publishing 2018) 45–50.
9. ibid; Seumas Miller, 'On National Security Intelligence: Concepts and Contexts', *The Ethics of National Security Intelligence Institutions* (Routledge 2024) 38–39.
10. I have opted for the use of the term "Euro-Atlantic" as I mainly use examples of legal frameworks for intelligence and intelligence activities from European as well as British and American intelligence and security services. In Chapter 5, I use the legal framework governing the Dutch intelligence and security services as an example, thereby placing even more emphasis on the Euro-Atlantic context. I have opted for "Euro-Atlantic" instead of "Western", as I find it more geopolitically accurate and less normatively laden.
11. See, for instance, Laurie Chen and others, 'China Accuses US of Launching "advanced" Cyberattacks, Names Alleged NSA Agents' *Reuters* (15 April 2025) <https://www.reuters.com/technology/cybersecurity/chinas-harbin-says-us-launched-advanced-cyber-attacks-winter-games-2025-04-15/v> accessed 17 April 2025.
12. Seumas Miller, 'National Security Intelligence Activity: A Philosophical Analysis' (2022) 37 Intelligence and National Security 791, 791. The Dutch General Intelligence and Security Service (AIVD) does not explicitly provide a definition of intelligence, but defines an intelligence *service* as follows: "An intelligence service maps out international political developments and determines what affects the interests of its own country. This concerns developments that take place outside diplomatic channels, or in other words, the hidden agenda of certain countries. As part of our intelligence task, we inform the government about what is important for foreign policy", see <https://www.aivd.nl/onderwerpen/over-de-aivd/inlichtingenwoordenboek>.
13. Michael Warner, 'Wanted: A Definition of "Intelligence": Understanding Our Craft' (2002) 46 Studies in Intelligence 15.

broadly, to be "knowledge and foreknowledge of the world around us."[14] It can also be seen as the achievement of improving "the quality of decision making by reducing ignorance."[15] Although there is thus no uniform definition of intelligence, I use the following definition of intelligence in this research:

> Intelligence is the organisation of covert activities aimed at achieving an information advantage for better decision-making, either by reducing uncertainty for one's own party or by increasing it for the counterparty, in an environment that consciously tries to frustrate the achievement of such an information advantage.[16]

When intelligence is seen as an end-product, intelligence and security services are the "producers" of intelligence, in order to counter (espionage) threats. Intelligence is valuable because it provides information about the intentions and capabilities of actors that are not otherwise openly available.[17] The way in which this information is sought after and obtained, has evolved. Similar to many processes which have undergone digitalisation in the past decades, threats to national security increasingly emerge in the cyber domain, targeting digital infrastructure and exploiting digital systems.[18] Espionage in the cyber domain, by use of digital infrastructure, creates advantages compared to traditional espionage: it provides more options for anonymity and can be conducted on a larger scale.[19]

The quick growth of the cyber threat landscape means greater state vulnerability to cyber threats. Moreover, an open economy with greater dependency on digital infrastructure, global supply chains and foreign investments is more exposed to cyber threats impacting economic security.[20] Economic security is an essential pillar of national security.[21] In this research, I argue that the substantial threat that economic cyber espionage poses to economic security thus affects national security, albeit more indirectly than a threat that is directed towards the physical integrity of individuals residing in the state.

---

14. Central Intelligence Agency Office of Public Affairs, *A Consumer's Guide to Intelligence*, 1999.
15. David Omand, 'Securing the State: National Security and Secret Intelligence' (2013) 4 PRISM 14, 21.
16. Mark M Lowenthal, *The Future of Intelligence* (1st edn, Polity Press 2017) 13; Bob De Graaff, *Data en Dreiging: Stap in de wereld van intelligence* (Boom Geschiedenis 2019) 23.
17. Angela Gendron, 'Just War, Just Intelligence: An Ethical Framework for Foreign Espionage' [2005] International Journal of Intelligence and CounterIntelligence 411.
18. For an in-depth analysis of the cyber domain, see J van Haaster, 'On Cyber: The Utility of Military Cyber Operations during Armed Conflict' (PhD Thesis, University of Amsterdam 2019).
19. Buchan (n 8) 45–50.
20. Gatra Priyandita, Bart Hogeveen and Ben Stevens, 'State-Sponsored Economic Cyber Espionage for Commercial Purposes' (Australian Strategic Policy Institute 2022) 67 <https://www.aspistrategist.org.au/state-sponsored-economic-cyber-espionage-for-commercial-purposes-on-the-rise/> accessed 14 April 2025.
21. AIVD, 'Jaarverslag 2022' (Algemene Inlichtingen- en Veiligheidsdienst 2023) 35–36.

One of the first significant (and discovered) cyber espionage incidents was "Operation Aurora", which constituted a series of cyberattacks from China that targeted American companies.[22] Following the discovery of the espionage operation, Google made a public statement in which it accused China of stealing source code for spying and penetrating companies' networks.[23] This event propelled a discussion on economic cyber espionage as a harmful state practice. States are particularly vulnerable to this kind of espionage when their economy depends on the stability and profitability of so-called "key" sectors or industries,[24] such as the semiconductor industry and the agricultural or new generation information technology industries.[25] The Netherlands is an example of a state with a large high-tech sector. It strives to retain and expand its "knowledge economy",[26] which is built on knowledge security.[27] As a consequence of hosting companies in key sectors, the Netherlands is highly vulnerable to economic cyber espionage. Therefore, it is not surprising that economic cyber espionage has been classified as one of the biggest threats to Dutch national security for more than five years.[28] In 2020, espionage by Chinese state actors targeted the Dutch semiconductor industry, the telecom sector, and the bio-pharmaceutical sector.[29] In 2024, the Dutch Ministry of Defence published a report in cooperation with the Dutch National Cyber Security Centre, stating that an (independent and unclassified) network of the Ministry had been compromised by Chinese malware.[30] Russian state actors have reportedly been involved in spying on tech companies in the Netherlands, too.[31]

22. Kim Zetter, 'Google Hack Attack Was Ultra Sophisticated, New Details Show' [2010] *Wired*.
23. Andrew Jacobs, Miguel Helft and John Markoff, 'Google, Citing Attack, Threatens to Exit China' *The New York Times* (12 January 2010) <https://www.nytimes.com/2010/01/13/world/asia/13beijing.html> accessed 14 April 2025.
24. The Made in China 2025 strategy identifies ten key sectors: new information technology; high-end computerised machines and robots; space and aviation; high-tech ships and maritime equipment; railway equipment; new energy and energy saving; new materials; biopharma and high-tech medical devices; agricultural machinery; and power/energy equipment.
25. MIVD, 'Jaarverslag 2024' (Militaire Inlichtingen- en Veiligheidsdienst 2025) Jaarverslag 20.
26. See *generally* Walter W Powell and Kaisa Snellman, 'The Knowledge Economy' (2004) 30 Annual Review of Sociology 199.
27. 'Digitalisering en kenniseconomie 2024' (Centraal Bureau voor de Statistiek 2025).
28. See National Cyber Security Centre, 'Cyber Security Assessment Netherlands 2016' (2016) 12, 19; 'Netherlands Cybersecurity Strategy 2022-2028' (National Coordinator for Security and Counterterrorism 2022) 12; AIVD, 'Jaarverslag 2024' (Algemene Inlichtingen- en Veiligheidsdienst 2025) 29–32; AIVD, 'Jaarverslag 2018' (Algemene Inlichtingen- en Veiligheidsdienst 2019) 9; National Cyber Security Centre, 'Cyber Security Assessment Netherlands 2019' (2019) 7; Kamerbrief over jaarplan AIVD 2021, *Kamerstukken II* 2020/21 (Dutch House of Representatives, Parliamentary Document), 30977, no 158.
29. AIVD, 'Jaarverslag 2020' (Algemene Inlichtingen- en Veiligheidsdienst 2021) 9.
30. AIVD & MIVD, 'Ministry of Defence of the Netherlands Uncovers COATHANGER, a Stealthy Chinese FortiGate RAT' (2024) Cybersecurity Advisory.
31. M. Hijink, 'Bij ASML en NXP vermoedde niemand dat "einzelgänger" German een spion was', *NRC* 1 April 2025; 'Kamerbrief verstoring Russische economische spionageactiviteiten