



UvA-DARE (Digital Academic Repository)

The New F-word: The case of fragmentation in Dutch cybersecurity governance

Mirzaei, P.; De Busser, E.

DOI

[10.1016/j.clsr.2024.106032](https://doi.org/10.1016/j.clsr.2024.106032)

Publication date

2024

Document Version

Final published version

Published in

Computer Law & Security Review

License

CC BY-NC-ND

[Link to publication](#)

Citation for published version (APA):

Mirzaei, P., & De Busser, E. (2024). The New F-word: The case of fragmentation in Dutch cybersecurity governance. *Computer Law & Security Review*, 55, Article 106032. <https://doi.org/10.1016/j.clsr.2024.106032>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.



The New F-word: The case of fragmentation in Dutch cybersecurity governance

Parto Mirzaei^{a,*}, Els De Busser^b

^a Institute of Security and Global Affairs (ISGA), Leiden University, the Netherlands

^b Institute for Information Law (IViR), University of Amsterdam, the Netherlands

ARTICLE INFO

Keywords:

Fragmentation
Cybersecurity
Governance
Policy
Institutional design
The Netherlands

ABSTRACT

The fragmentation of the Dutch cybersecurity government landscape is a widely discussed phenomenon among politicians, policy makers, and cybersecurity specialists. Remarkably though, a negative narrative is underlying the idea of fragmentation, suggesting that we are dealing with a serious problem. A problem that has the potential of impeding cybersecurity governance in the Netherlands. This research zooms in on how cybersecurity governance is organised within the central government, and which organisations are concerned with the creation, implementation, and oversight of cybersecurity policies vis à vis Dutch society. This article provides an overview of all central government organisations (de Rijksoverheid) that are involved in cybersecurity governance on a strategic level. This research provides the first step in doctoral research into the possible implications of the fragmentation of cybersecurity governance in the Dutch central government, and how this fragmentation could potentially impact policy creation, implementation, and oversight. Based on the mapping of this governance landscape, it set out to measure fragmentation based on the number of units or organisations that are concerned with cybersecurity governance in the central government on a strategic level. This study has found that based on Boyne's (1992) notion of fragmentation and the Dutch governments' definition of tiers, the Dutch cybersecurity governance landscape could indeed, when meticulously following Boyne's counting procedure, be regarded as fragmented.

1. Introduction

The fragmentation of the Dutch cybersecurity government landscape is a widely discussed phenomenon among politicians, policy makers, and cybersecurity specialists. Remarkably though, a negative narrative is underlying the idea of fragmentation, suggesting that we are dealing with a serious problem. A problem that has the potential of impeding cybersecurity governance in the Netherlands. An example where the fragmentation of responsibilities and information sharing has been mentioned as a potential culprit for failure, was during the Citrix-software hack in 2020 [59]. This research zooms in on how cybersecurity governance is organised within the central government, and which organisations are concerned with the creation, implementation, and oversight of cybersecurity policies vis à vis Dutch society. This article provides an overview of all central government organisations (de Rijksoverheid) that are involved in cybersecurity governance on a strategic level.

This research provides the first step in doctoral research into the possible implications of the fragmentation of cybersecurity governance in the Dutch central government, and how this fragmentation could potentially impact policy creation, implementation, and oversight. More context to this research will be provided through the outcomes of interviews conducted with the organisations of the central government that are concerned with cybersecurity governance. Geographically this research is restricted to the institutional architecture of organisations within the central government that are concerned with cybersecurity governance on a national level in the Netherlands. The outcomes may therefore prove insightful for better understanding the potential impact and relevance of national institutional architectures on the governance of cybersecurity.

All figures and tables should be print in colour.

* Corresponding author at: Leiden University - Institute of Security and Global Affairs P.O. Box 13228, 2501 EE The Hague, the Netherlands.

E-mail addresses: p.mirzaei@fgga.leidenuniv.nl (P. Mirzaei), e.debusser@uva.nl (E. De Busser).

<https://doi.org/10.1016/j.clsr.2024.106032>

Available online 23 August 2024

0267-3649/© 2024 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

2. Case study

2.1. Fragmentation claim

In Dutch cybersecurity governance, fragmentation is predominantly described as an obstacle which has to be overcome. A negative narrative around the concept of fragmentation in the Dutch cybersecurity governance landscape is noticeable. Politicians, policy makers, cybersecurity experts, in both the private and public sector, and academic experts perceive the Dutch cybersecurity governance landscape as being fragmented. Fragmentation in this context refers to the fact that ministries are considered too compartmentalised, there is a lack of information sharing, and little clarity about roles and task divisions. These are only some of the grievances posed by the above-mentioned group with regards to government fragmentation in the Dutch cybersecurity governance landscape ([12–14], 2021, 2021, [16,24,36,40–42,55,59,65,71–74]). Due to these expressed grievances, we initiated a study into the conceptualisation of fragmentation and how it was measured in existing academic literature. The negative narrative around fragmentation in the Dutch cybersecurity governance landscape raised the question of how one could potentially measure fragmentation.

3. Theory

3.1. Fragmentation

Fragmentation in governance is anything but a new phenomenon. It occurs in other transboundary policy fields, such as water management, climate-, international- and environmental governance, the construction and procurement industry, academia, child welfare, (im)migration, integration, and the international governance of artificial intelligence [1,4,11,18,21,33,35,63,83,84]. In the context of international law, fragmentation is described as: “the increased proliferation of international regulatory institutions with overlapping jurisdictions and ambiguous boundaries” ([2], p. 596). Institutional fragmentation is defined as “a situation and a process whereby different institutions pursue governance objectives in often overlapping jurisdictional terms” ([28], p. 315). The overlap of jurisdictions and ambiguous boundaries also corresponds with some of the concerns expressed about the Dutch cybersecurity governance landscape [15,58,65]. The existence of too many agencies is coined as one of the causes for fragmentation [10]. Side effects thereof are the lack of an overarching vision, the absence of coordination among agencies, and conflicting practices and goals which lead to various challenges [10].

3.2. Cybersecurity governance

This study focuses on fragmentation in cybersecurity governance in the Netherlands. Cybersecurity is a transboundary policy field which is vested with multiple ministries and organisations. Because of its transboundary character, multidimensionality and interconnectedness, cybersecurity has been referred to as a wicked problem [8]. Fragmentation impairs the ability of governments to tackle wicked problems [19,27,34,35].

Cybersecurity, or: “keeping the networked digital technologies connected to that network, safe and secure” (B. [76], p. 188) requires far more than just technological remedies. It requires interventions from a broad spectrum of actors: from governments to end-users (B. [76]). Cybersecurity is considered a dimension of national security [9,37,39,57,75]. Given that governments have the highest political authority within a state, it is the government who should be in charge of cybersecurity [82]. Yet securing cyberspace poses some challenges for governments. Although cyberspace is not confined by political or geographical borders [22], it is bounded by under-water and -ground cables and servers [6]. In spite of the absence of a central government in or over cyberspace, plenty of organisations and states do have ideas

about norm frameworks and rules in cyberspace, which subsequently leads to governance fragmentation [38]. Even though only states can enforce rules in cyberspace [31], cyberspace is mostly privately owned, which, control-wise, poses significant challenges for states [30]. Given that cybersecurity threats and risks have the potential of tarnishing national security, governments are considered responsible for protecting cyberspace (B. [77]). The definition of cybersecurity which has been retained for this paper is the one as suggested by van den Berg & Keymolen [[76], p. 188].

Governance is defined as “the processes and interactions through which very diverse social interests and actors create policy and procedures” “[...] with a focus on formal government institutions” ([3], pp. 4–5). Schmitter [70] places more emphasis on the processes required for solving a conflict or problem. He refers to governance as: “a method for solving conflicts and problems in which actors – usually a mix of public and private ones – regularly arrive at mutually satisfactory and binding decisions by negotiating with each other and cooperating in the implementation of these decisions” ([70], p. 552), and emphasises how governance is also concerned with the *implementation of policies*, and not just the negotiations and decision-making process ([70], p. 553).

Where governance usually refers to the content of the actions deployed, the government refers to the body that executes the actions. In the past few decades, the concept of governance has gone beyond the government as a single actor. Other actors such as the private sector, supranational organs, and societal stakeholders have gained more influence in governance [3,64].¹

Brown [7] offers a definition of government which also entails governance tasks:

“the key activity of a state and identified with a centralised body of institutions which has a monopoly over aspects of making, monitoring, and enforcing a dense complex of rules, regulations and norms covering a specified range of activities across the territory of a state” ([7], p. 2).

The key activities mentioned by Brown [7] correspond with the three core governance activities as recognised by the Dutch central government. Namely, policy creation, policy implementation and policy oversight [68]. This triumvirate, which is defined as governance by Brown [7] and the Dutch central government, is what we will move forward with as a definition of governance in the mapping exercise of the Dutch cybersecurity governance landscape. An overview of the core governance activities as recognised by the Dutch central government can be found in Fig. 1.

3.3. Fragmentation as a concept

Fragmentation is anything but a new phenomenon and has been discussed in a plethora of studies. Being a concept that is widely applied in various studies, it is often accompanied with measuring instruments and spectra suggestions. Boyne [5] defines fragmentation as the number of separate units in a local government system or structure ([5], p. 334).

Nonetheless, fragmentation remains a relative term, no number of units was ever assigned to the concept. It therefore remains ambiguous what ‘many units’ exactly entail. The only clarification granted by Boyne [5] is that the number of units is relative to the population size that is being served by the distinct units, or the geographical area that is covered by these units [5]. For the aim of this paper, which is to find out whether the Dutch cybersecurity governance landscape is indeed fragmented, Boyne’s definition of fragmentation will be applied in this context. In spite of its – at first sight – rather superficial nature, Boyne’s [5] conceptualisation of fragmentation allows us to say something about

¹ The core focus of this paper is the Dutch cybersecurity governance landscape, and the definitions mentioned here will therefore be limited to national governance only.

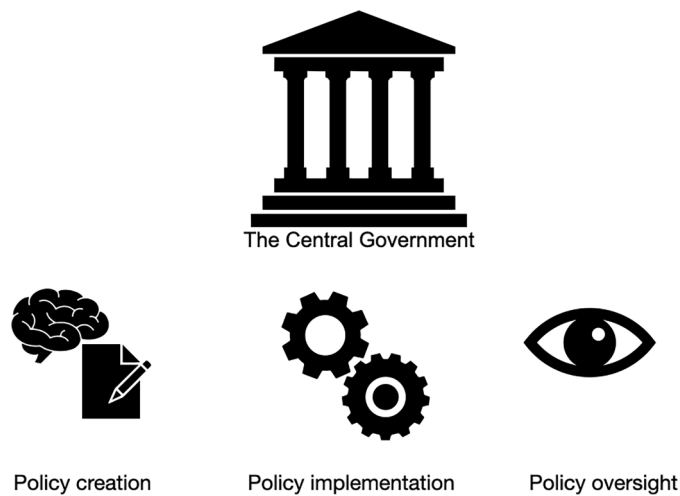


Fig. 1. The core governance activities as recognised by the Dutch central government.

the dispersion of the organisations concerned with cybersecurity governance within the Dutch central government, as is already being suggested in the Dutch policy documents.

3.4. Vertical and horizontal fragmentation

A distinction is made between horizontal and vertical fragmentation [5,23]. Whereas vertical fragmentation refers to the number of vertical tiers of an institutional structure, horizontal fragmentation refers to the number of organisations within a single tier [5]. It does however remain opaque what is exactly meant when we speak of tiers. The single tier within horizontal fragmentation could imply equivalent organisations. Boyne [5] has created an overview which displays in which instances horizontal fragmentation was studied. When it comes to horizontal fragmentation, it concerned the assessment of the spending of municipalities, counties, or pupils, in which all units were regarded as equal ([5], p. 344). In one study, vertical and horizontal structures refer to power relations and the distribution of power and interactions [26], whereas another study uses these concepts for measuring budgetary spending [29]. Horizontal fragmentation is associated with an increase in competition because the existence of organisations is dependent upon their performance [5]. The Dutch government identifies four tiers in Dutch public administration. Namely: the central government, the provinces, the municipalities and the water authorities [25]. This study will evaluate fragmentation based on the definition granted by Boyne [5] and the definition of tiers that has been established by the Dutch government.

3.5. Concentration

Another angle for looking at institutional structures is through the concepts of horizontal and vertical concentration. In this context, concentration implies the division of responsibilities and funding [5,23,29], or their relative market share [32].

4. Methodology

The first aim of this article is to provide a representation of the current strategic cybersecurity governance landscape of the Netherlands, focused on the Dutch central government, or *Rijksoverheid*. The second aim is to test whether and to what extent the Dutch cybersecurity governance landscape is indeed fragmented according to Boyne's [5] definition of fragmentation. The Dutch central government consists of 12 ministries [67]. Firstly, all the ministries and organisations

that fall within the central government have been collected and put together in a table overview. The information about these ministries and organisations and their conducts are derived from the website of the Dutch government with information about the ministries and organisations, the tasks allocated and services provided by these organisations: *Overheid.nl* [61]. The websites and webpages of each organisation have been consulted as well. Many organisations have their own website or webpage, such as: the National Coordinator for Security and Counterterrorism and the Digital Trust Center [17,56]. An overview has also been made based on all the official statements of the government (*Officiële bekendmakingen*), with the official statements and announcements coming forth from the government's journals and policy papers: *Staatscourant, het Staatsblad, Kamerstukken, Agenda's en Handelingen* [60], filtered on the words 'cyber security' and the types of organisations matching the scope of this research: ministry, office and agency '*dienst en agentschap*', *quango*² '*zelfstandig bestuursorgaan*'. The timeframe of this separate overview spans from 2011 to 2023. The table overview with organisations has also been supplemented with the organisations mentioned in the most recent cybersecurity policy documents available at the time, in which their role before, during or after a cybersecurity incident or attack was described ([54,55]a). The organisational charts of the ministries have been evaluated as well [43–51]. Although regional water authorities, municipalities, provinces, and security regions also have a(n) (in)formal responsibility for cybersecurity, they are omitted from the scope of this research since the focus is only on cybersecurity governance practices of the central government.

The collected organisations were labelled based on a number of categories: the type of organisation or agency (*agentschap, zelfstandig bestuursorgaan, organisatieonderdeel*), in some way concerned with cybersecurity or not through 'yes' or 'no', the type of task(s) they conduct: policy creation/implementation/oversight. Organisations concerned with advice were given the same label as implementation because the Dutch central government only recognises three core tasks and advice falls under implementation.³ The allocation to one or more of these tasks also indicated their concern with cybersecurity governance, as governance is defined by the central government as being policy creation/implementation/oversight [68]. Another requirement was the strategic dimension of governance. Organisations concerned with the tactical or operational tasks of governance were not included. The other categories were the domestic/international orientation of the organisation, and whether the organisation was concerned with cybersecurity within or with the central government, such as the Standardisation Forum, who deals with the provision of standards for the exchange of digital data (*Forum Standaardisatie*), and/or with cybersecurity vis à vis society. If the latter criterium was met, they were marked as external, even if both criteria suited the organisation. When an organisation qualifies as both an internal and external organisation, we will count it as an internal or external organisation based on what the majority of its practices is concerned with, or based on what the essence of their practices is. To illustrate an example, we will look at an organisation which shares significant resemblances with an internal government organisation, but which has nonetheless been counted as an external one: Logius. Logius is an agency which falls under the Ministry of Interior and Kingdom Relations. It is an organisation which is responsible for the provision of ICT-infrastructure to public service providers, so that citizens and (private) organisations can securely organise their personal affairs online, for instance through DigiD [62]. In order to make this distinction, one of the key questions which has been posed with every organisation that is listed is: do the practices of this organisation have an (indirect) effect on the cybersecurity of Dutch society? Because Logius is, among other things, concerned with facilitating a secure digital gateway for Dutch society, it has been categorised under

² See: [80].

³ This has been confirmed by our sources at the central government.

policy implementation. Since the focus of this research is cybersecurity governance towards society, we have decided to only display the so-called external organisations in the overview (Fig. 2).⁴ In the overview that resulted from this exercise, colour codes and fonts were allocated to the overview.

4.1. Quasi ngo's (Zelfstandige bestuursorganen)

Zelfstandige bestuursorganen (zbo's) or 'quangos' [79,80], are independent organisations that conduct a government task. Usually this concerns a commanding/authoritative (gezagvoerende) task. The minister under which the zbo falls, is responsible for overseeing the outcome of the policies conducted by these zbo's [69]. In total there are 141 zbo's in the Netherlands, of which three are concerned with cybersecurity governance:

- The Authority for Nuclear Safety and Radiation Protection (*Autoriteit Nucleaire Veiligheid en Stralingsbescherming, ANVS*);
- The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*);
- The Central Bank of the Netherlands (De Nederlandsche Bank).

4.2. Agencies (agentschappen)

Agencies or *agentschappen*, are part of a ministry but work on an independent basis, and are reimbursed by the central government for their products and/or services. Currently there are 28 agencies within the central government [66]. Five of the 28 agencies are concerned with cybersecurity governance:

- Rijkswaterstaat;
- The Dutch Authority for Digital Infrastructure (*Rijksinspectie Digitale Infrastructuur*);
- Shared Service Center ICT (SSC-ICT);
- Logius;
- DICTU.

The exercises described above have ultimately led to a total of 36 organisations over the following seven ministries:

- The Ministry of Interior and Kingdom Relations;
- The Ministry of Foreign Affairs;
- The Ministry of Justice and Security;
- The Ministry of Defence;
- The Ministry of Economic Affairs and Climate Policy;
- The Ministry of Finance;
- The Ministry of Infrastructure and Water Management;

Fig. 2 provides an overview of The Dutch Cybersecurity Governance Landscape. If an organisation is concerned with more than one task, the contour of the cell in the overview is coloured accordingly. An example is *De Nederlandsche Bank*, the first organisation shown under the Ministry of Finance, which besides policy oversight (blue) is also concerned with policy implementation (purple frame).

In 2024, the Network and Information Systems 2 (NIS 2) Directive [20] will lead to significant changes in the cybersecurity governance landscape as it is concerned with a broad scala and number of

organisations. This landscape should therefore in no way be treated as conclusive and should rather be considered a snapshot.

4.3. Verification

This landscape has been discussed at length with well-placed sources of the Dutch central government who have pointed out and clarified the errors and shortcomings of the overview, and have recommended additional policy documents which had not evolved from our search criteria. Based on this advice, some actors and organisations have been added or omitted from the landscape, or there has been a shift or addition in the type of tasks performed by these organisations. Some advice has not been adopted. An example is the suggestion for including all Policy Directorates or equivalents thereof. Although the scope of this research indeed is cybersecurity governance policy, and such directorates within ministries are indeed responsible for policy matters in general for the entire ministry, it would seem more than logical to add these by default. However, some policy directorates are so minimally involved in cybersecurity governance policy under the current Network Information Systems (NIS) framework, that inclusion in this cybersecurity governance overview seemed too far-fetched. The purpose of this overview is to demonstrate organisations and actors that have a prominent role in the creation, implementation, and oversight of cybersecurity governance policies, and that are also part of the central government. It is self-evident that a greater number of organisations and actors is also concerned with information security. Yet the two should not be confused or put under the same denominator, as cybersecurity goes beyond information security (cf. J. [78]; cf. [81]). Nonetheless, some roles may significantly change or be added after the implementation of the NIS 2 Directive.

5. Analysis

The following section includes the cybersecurity governance landscape that has derived from the mapping exercise as per described in the methodology. Subsequently, this section will touch upon the ministries and their corresponding organisations that are part of the Dutch cybersecurity governance landscape, and that are displayed in Fig. 2.⁵

5.1. The Ministry of Interior and Kingdom Relations

Within the Ministry of IKR, eleven organisations are concerned with cybersecurity governance. Seven out of eleven are engaged with cybersecurity governance within the central government: Chief Information Office, CIO-Rijk, SSC-ICT (Shared Service Center ICT), the Standardisation Forum (Forum Standaardisatie), the Advisory Board for ICT Review (*Adviescollege ICT-toetsing*), the Security Authority of the Central Government (BVA Rijk), and the Chief Information Security Officer (CISO). The other three organisations are concerned with cybersecurity governance as per the definition followed in this research paper: policy creation, implementation, and oversight vis à vis society. These organisations are: The General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst, AIVD*), Logius, and the National Office for Identity Data (*Rijksdienst voor Identiteitsgegevens*).

5.2. The Ministry of Foreign Affairs

The Ministry of Foreign Affairs has two organisations concerned with cybersecurity governance: Security Policy Directorate (*Directie Veiligheidsbeleid*) and the Crisis Coördinator.

⁴ The following internal organisations have been omitted from the scope because they were predominantly concerned with internal cybersecurity governance practices, i.e. within the central Dutch government: the CISO's of each ministry; CIO (Interior and Kingdom Relations); CIO-Rijk (Interior and Kingdom Relations), SSC-ICT (Interior and Kingdom Relations); Forum Standaardisatie (Interior and Kingdom Relations); Adviescollege ICT-toetsing (Interior and Kingdom Relations), and lastly BVA Rijk (Interior and Kingdom Relations).

⁵ Feel free to contact the researchers for the full dataset of organisations.

| The Ministry of Interior and Kingdom Relations | The Ministry of Foreign Affairs | The Ministry of Justice and Security | The Ministry of Defence | The Ministry of Economic Affairs and Climate Policy | The Ministry of Finance | The Ministry of Infrastructure and Water Management |
|--|----------------------------------|--|---|--|------------------------------------|--|
| <u>Logius</u> | Directie Veiligheidsbeleid (DVB) | Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) | Defensie Cyber Security Centrum (DCSC) | <u>Rijksinspectie Digitale Infrastructuur (RDI)</u> | <u>De Nederlandsche Bank (DNB)</u> | Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) |
| Algemene Inlichtingen- en Veiligheidsdienst (AIVD) | Crisis Coördinator | Nationaal Cyber Security Centrum (NCSC) | Defensie Cyber Commando (DCC) | <u>Dienst ICT Uitvoering (DICTU)</u> | Belastingdienst | Rijkswaterstaat (RWS) |
| Rijksdienst voor Identiteitsgegevens (RvIG) | | Ministeriële Commissie Crisisbeheersing (MCCb) | Koninklijke Marechaussee (KMar) | Dcypher | | Inspectie Leefomgeving en Transport (ILT) |
| | | Interdepartementale Commissie Crisisbeheersing (ICCb) | Militaire Inlichtingen- en Veiligheidsdienst (MIVD) | Digital Trust Center (DTC) | | Departementaal Coördinatie Centrum Crisisbeheersing (DCC) |
| | | Nationaal Kernteam Crisiscommunicatie (NKC) | Directie Generaal Beleid (DGB) | Computer Security Incident Response Team for Digital Service Providers (CSIRT-DSP) | | |
| | | Openbaar Ministerie (OM) | | | | |
| | | Autoriteit Persoonsgegevens (AP) | | | | |
| | | Nationale Politie | | | | |

| | |
|-------------------|---|
| Green | Policy creation |
| Purple | Policy implementation |
| Blue | Policy oversight |
| Underlined | agency, 'agentschap' |
| Italics | quango, 'zelfstandig bestuursorgaan' |

Fig. 2. Overview of the Dutch cybersecurity governance landscape.

5.3. The Ministry of Justice and Security

Eight organisations that belong to the Ministry of Justice and Security are concerned with cybersecurity governance: The National Coordinator for Security and Counterterrorism (*Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV*), The National Cyber Security Center (*NCSC*), of which the NCTV is the cybersecurity policy employer [52,53], the Ministerial Crisis Management Committee (*Ministeriële Commissie Crisisbeheersing, MCCb*), the Interdepartmental Crisis Management Committee (*Interdepartementale Commissie Crisisbeheersing, ICCb*), The National Core Crisis Communication Team (*Nationale Kernteam Crisiscommunicatie, NKC*), the Public Prosecution Service (*Openbaar Ministerie, OM*), The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens, AP*), and the National Police (*Nationale Politie*).

5.4. The Ministry of Defence

The Ministry of Defence has five organisations concerned with cybersecurity governance: The Defence Cyber Security Center (*DCSC*), the Defence Cyber Commando (*DCC*), The Royal Marechaussee (*KMar*), the Military Intelligence and Security Service (*MIVD*), and two organisations that fall under the Directorate General Policy (*DGB*), including the DGP itself.

5.5. The Ministry of Economic Affairs and Climate Policy

The Ministry of Economic Affairs and Climate Policy has five

organizations that are concerned with cybersecurity governance: The Dutch Authority for Digital Infrastructure (*Rijksinspectie Digitale Infrastructuur, RDI*), The ICT Implementation Office (*Dienst ICT Uitvoering, DICTU*), the Digital Trust Center, Dcypher, and lastly the Computer Security Incident Response Team for Digital Service Providers (*CSIRT DSP*).

5.6. The Ministry of Finance

The Ministry of Finance hosts two organisations that are concerned with cybersecurity governance. The Nederlandsche Bank (*DNB*) and two organisations that are categorised under The Dutch Tax Services (*Belastingdienst*): Team Security, Continuity and Privacy (*TSCP*), and the Fiscal Information and Investigation Service (*Fiscale Inlichtingen- en Opsporingsdienst, FIOD*).

5.7. The Ministry of Infrastructure and Water Management

In this ministry, four organisations are concerned with cybersecurity governance: The Authority for Nuclear Safety and Radiation Protection (*Autoriteit Nucleaire Veiligheid en Stralingsbescherming, ANVS*), Rijkswaterstaat (the executive agency of the ministry), The Human Environment and Transport Inspectorate (*Inspectie Leefomgeving en Transport, ILT*) and the Departmental Coordination Centre for Crisismanagement (*Departementaal Coördinatiecentrum Crisisbeheersing, DCC-IenW*).

6. Findings

6.1. Horizontal fragmentation

The Dutch cybersecurity governance landscape allows us to evaluate both horizontal and vertical fragmentation as per the definitions provided by Boyne [5] and the Dutch government.

Given that horizontal fragmentation entails the number of organisations within a single tier, we can establish that when taking the Dutch governments' definition of a tier into account, the central government can be considered one tier. The horizontal fragmentation of the Dutch central government therefore entails all the organisations that are part of the Dutch cybersecurity governance landscape. This allows us to derive the following observations from the overview in Fig. 2. The organisations concerned with the governance of cybersecurity are divided over seven ministries. When looking at each ministry individually, the number of organisations that fall under each ministry would also account for the horizontal fragmentation of the cybersecurity governance landscape, as this corresponds with the Dutch governments' definition of a tier. The 29 organisations and ministries depicted in the overview belong to the same central government tier. Therefore, the total of organisations that can be categorised as horizontally fragmented can be achieved through adding the ministries to the number of organisations that fall under each individual ministry, as can be seen in Table 1.

From the count in Table 1. and based on Boyne's definition of fragmentation explained above, and the definition of a tier as provided by the Dutch government, we can conclude that the Dutch cybersecurity governance landscape is horizontally fragmented.

6.2. Vertical fragmentation

According to Boyne [5] vertical fragmentation entails the number of vertical tiers of an institutional structure [5]. Because of the Dutch Government's definition of a tier, vertical tiers in the Dutch case would imply the inclusion of organisations in the provinces, municipalities, and water authorities. The organisations that would concern cybersecurity governance on a provincial, municipal, and water authority level

Table 1
Fragmentation of the Dutch cybersecurity governance landscape measured.

| Central Government level | |
|---|----------------|
| Horizontally | 7 (ministries) |
| Vertically | 0 |
| Ministry level | |
| The Ministry of Interior and Kingdom Relations | |
| Horizontally | 3 |
| Vertically | 0 |
| The Ministry of Foreign Affairs | |
| Horizontally | 2 |
| Vertically | 0 |
| The Ministry of Justice and Security | |
| Horizontally | 8 |
| Vertically | 0 |
| The Ministry of Defence | |
| Horizontally | 5 |
| Vertically | 0 |
| The Ministry of Economic Affairs and Climate Policy | |
| Horizontally | 5 |
| Vertically | 0 |
| The Ministry of Finance | |
| Horizontally | 2 |
| Vertically | 0 |
| The Ministry of Infrastructure and Water Management | |
| Horizontally | 4 |
| Vertically | 0 |
| Total fragmentation | |
| Horizontally | 29 |
| Vertically | 0 |
| General fragmentation | 29 |

have been omitted from the scope of this research, and therefore the Dutch cybersecurity governance landscape is not vertically fragmented. This claim does however hold the caveat that this inference is based on the strict definition of the Dutch government which has been used as a lens for this research. In terms of general fragmentation, which is the sum of the horizontal and vertical fragmentation, we can state that the landscape is generally fragmented. In the case of cybersecurity governance on a strategic level, this number accounts for 29 units or organisations. We can therefore conclude that the Dutch cybersecurity governance landscape is significantly horizontally fragmented, and not vertically fragmented. In terms of general fragmentation, the landscape can be considered fragmented.

6.3. Horizontal concentration

The cybersecurity governance tasks have been divided over three categories: policy creation, implementation and oversight. Table 2 displays the inferences that can be made about the horizontal concentration of the Dutch cybersecurity governance landscape.

When looking at horizontal concentration per policy section or type of organisation, the concentration of the number of organisations that are concerned with policy implementation (24) among ministries is significantly higher than policy creation and oversight, which account for 3 and 6 organisations respectively. Organisations concerned with internal cybersecurity governance are relatively fragmented (13), yet the majority falls under the Ministry of Interior and Kingdom Relations (7), and the other 6 internal organisations are the CISOs which are spread over the other ministries.

From this overview it can be concluded that the horizontal concentration of policy creation is rather high as it is divided over three organisations. Whereas the horizontal concentration of policy implementation is significantly low, as it is divided over 24 organisations. Policy implementation is therefore, in contrast to policy creation, rather dispersed. Policy oversight on the other hand is quite horizontally concentrated as this governance task is prevalent in 6 organisations. The numbers that are accompanied by an asterisk indicate that this number includes an organisation which is, besides being categorised as policy creation-, implementation, or oversight, also accompanied by a different frame colour which implies that it cannot be categorised under just one governance task. The overviews and the conclusions that can be derived from Tables 1 and 2 are not intended for making a value judgment about the quality of concentration, and merely serve as observations that can be made based on the Dutch cybersecurity governance landscape in Fig. 2. Given the absence of vertical fragmentation when following the definitions as given by Boyne [5] and the Dutch government, we are not reflecting on the vertical concentration of the Dutch cybersecurity governance landscape.

7. Conclusion

In this research, the aim was to assess whether the Dutch cybersecurity governance landscape is indeed fragmented as per Boyne's theoretical lens and methodology for assessing fragmentation (1992). Based on the mapping of this governance landscape, it set out to measure fragmentation based on the number of units or organisations that are concerned with cybersecurity governance in the central government on a strategic level. This study has found that based on Boyne's [5] notion of fragmentation and the Dutch governments' definition of tiers, the Dutch cybersecurity governance landscape of the central government can indeed be regarded as (horizontally) fragmented.

Based on the total count of 29 organisations in the central government that are concerned with cybersecurity governance on a strategic level, we can conclude that the Dutch cybersecurity governance landscape is indeed fragmented. Due to the focus of the research on one of the tiers of the Dutch government, namely the central government, the Dutch cybersecurity governance landscape is considered horizontally

Table 2

Fragmentation based on policy section or type of organisation.

| Ministry | Policy creation | Policy implementation | Policy oversight | Agencies | Quangos |
|---|-----------------|-----------------------|------------------|----------|---------|
| The Ministry of Interior and Kingdom Relations | 0 | 3 | 1* | 1 | 0 |
| The Ministry of Foreign Affairs | 1 | 1 | 0 | 0 | 0 |
| The Ministry of Justice and Security | 1 | 6 | 1 | 0 | 1 |
| The Ministry of Defence | 0 | 5 | 0 | 0 | 0 |
| The Ministry of Economic Affairs and Climate Policy | 1* | 5* | 1 | 2 | 0 |
| The Ministry of Finance | 0 | 2* | 1 | 0 | 1 |
| The Ministry of Infrastructure and Water Management | 0 | 2 | 2 | 1 | 1 |
| Total | 3 | 24 | 6 | 4 | 3 |

fragmented, and not vertically fragmented.

When looking at horizontal concentration per policy section or type of organisation, the concentration of the number of organisations that are concerned with policy implementation (24) among ministries is significantly higher than policy creation and oversight, which account for 3 and 6 organisations respectively.

When it comes to governance tasks, the horizontal concentration of policy creation is rather high as it is divided over three organisations. Whereas the horizontal concentration of policy implementation is significantly low, as it is divided over 24 organisations. Policy implementation is therefore, in contrast to policy creation, rather dispersed. Policy oversight on the other hand is quite horizontally concentrated as this governance task is prevalent in 6 organisations. This implies that policy implementation is a more fragmented feature of governance than policy creation and oversight are.

The findings of this research suggest that the statements mentioned earlier about the Dutch cybersecurity governance landscape being fragmented are legitimate, albeit on a central government level when it concerns cybersecurity governance practices on a strategic level vis à vis society, and when strictly following Boyne's [5] and the Dutch governments definitions of fragmentation and tiers respectively.

These findings do however not necessarily accord with the grievances as expressed by experts, politicians, or policy makers about the fragmentation of cybersecurity governance in the Netherlands. To find out more about how fragmentation potentially impacts the organisational cultures and collaborations in cybersecurity governance practices of the central government on a strategic level, additional research is required. Additional research is also necessary because it would allow for a deeper understanding of the relationships and interactions among the organisations that make up the Dutch cybersecurity governance landscape.

Furthermore, these findings offer a deeper understanding of the legal frameworks and their implementation as policy creation, implementation and oversight are flowing from the applicable legal frameworks and should be in accordance therewith. An in-depth understanding of the mapping exercise therefore allows for a better scrutiny of the frameworks of the Dutch legislation concerned with cybersecurity governance. To illustrate this with a concrete example, we take the oversight component of the NIS 2 directive. When more organisations within the Dutch cybersecurity governance landscape are required to introduce (additional) standards and practices, including e.g., pro-active reporting on cybersecurity threats, this will involve several agencies, quangos and government organisations. The landscape provides clarity, overview, and insight in how cybersecurity governance is administered and distributed over a variety of organisations within the Dutch central government.

7.1. Limitations and future research

This article deals with a measurable conceptualisation of fragmentation. Namely, the number of organisations within the ministries of the Dutch government which are concerned with cybersecurity governance. This does not allow us to provide value laden statements on how fragmentation is experienced by members of these organisations, or whether

the current state of the institutional architecture should be altered. To carefully assess the character of intergovernmental relations and the possible implications of fragmentation in cybersecurity governance, the next step would be to test the fragmentation claims through conducting interviews with public officials in the organisations that are displayed in the Dutch Cybersecurity Governance landscape in Fig. 2, to find out how they experience the fragmentation of this landscape.

Funding

This work was funded by NWO (The Dutch Research Council) (grant numer NWA.1215.18.008) and is part of the Dutch Research Agenda 2018: Cyber security - towards a secure and reliable digital domain.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

- [1] Bakker K, Cook C. Water Governance in Canada: innovation and fragmentation. *Int J Water Resour Dev* 2011;27(2):275–89. <https://doi.org/10.1080/07900627.2011.564969>.
- [2] Benvenisti E, Downs GW. The empire's new clothes: political economy and the fragmentation of international law. *Stanford Law Rev* 2007;60(2):595–631.
- [3] Bevir M. *Governance: a very short introduction*. Oxford University Press; 2012.
- [4] Biermann F, Pattberg P, Van Asselt H, Zelli F. The fragmentation of global governance architectures: a framework for analysis. *Glob Environ Polit* 2009;9(4):14–40. <https://doi.org/10.1162/glep.2009.9.4.14>.
- [5] Boyne GA. Local government structure and performance: lessons from America? *Public Adm* 1992;70(3):333–57. <https://doi.org/10.1111/j.1467-9299.1992.tb00942.x>.
- [6] Broeders D. *The public core of the internet: an international agenda for internet governance*. Amsterdam University Press; 2016. https://doi.org/10.26530/OAPEN_610631.
- [7] Brown MA. Global governance and national governance. In: Farazmand A, editor. *Global encyclopedia of public administration, public policy, and governance*. Springer International Publishing; 2017. p. 1–9. https://doi.org/10.1007/978-3-319-31816-5_1159-1.
- [8] Carr M, Lesniewska F. Internet of things, cybersecurity and governing wicked problems: learning from climate change governance. *Int Relations* 2020;34(3):391–412. <https://doi.org/10.1177/0047117820948247>.
- [9] Choucri N. *Cyberpolitics in international relations*. MIT Press; 2012.
- [10] Christensen, & Laegreid. Still fragmented government or reassertion of the centre?. *Transcending new public management*. Routledge; 2007. p. 17–41.
- [11] Cihon P, Maas MM, Kemp L. Fragmentation and the future: investigating architectures for international AI governance. *Glob Policy* 2020;11(5):545–56. <https://doi.org/10.1111/1758-5899.12890>.
- [12] Cyber Security Raad. *CSR jaaroverzicht 2019*. a. 2020. p. 1–13. <https://www.cybersecurityraad.nl/documenten/verslagen/2020/04/01/csr-jaaroverzicht-2019>.
- [13] Cyber Security Raad. *CSR werkprogramma 2020-2021*. b. 2020. <https://www.cybersecurityraad.nl/overige-publicaties/documenten/jaarplannen/2020/07/01/csr-werkprogramma-2020-2021>.
- [14] Cyber Security Raad. *CSR urgentieverklaring*. c. 2020. <https://www.cybersecurityraad.nl/documenten/adviezen/2020/03/31/csr-urgentieverklaring>.

- [15] Cyber Security Raad. CSR adviesrapport: integrale aanpak cyberweerbaarheid. Cyber Security Raad; 2021. p. 3–72. <https://www.cybersecurityraad.nl/documenten/n/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid>.
- [16] Cyber Security Raad. Urgentieverklaring: extra inzet op cyberweerbaarheid noodzakelijk voor een digitaal veilige samenleving en het benutten van economische kansen. 2023. <https://www.cybersecurityraad.nl/documenten/adviezen/2023/08/07/csr-urgentieverklaring-2023>.
- [17] Digital Trust Center. Over het digital trust center. 2024. <https://www.digitaltrustcenter.nl/over-het-digital-trust-center>.
- [18] Doremus H. CALFED and the quest for optimal institutional fragmentation. *Environ Sci Policy* 2009;12(6):729–32. <https://doi.org/10.1016/j.envsci.2009.06.004>.
- [19] Elliott IC, Bottom KA, Carmichael P, Liddle J, Martin S, Pyper R. The fragmentation of public administration: differentiated and decentered governance in the (dis) United Kingdom. *Public Adm* 2022;100(1):98–115. <https://doi.org/10.1111/padm.12803>.
- [20] European Commission. Directive on measures for a high common level of cybersecurity across the union (NIS2 directive). n.d.. 2024. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
- [21] Payazi M, Arefian FF, Gharaati M, Johnson C, Lizarralde G, Davidson C. Managing institutional fragmentation and time compression in post-disaster reconstruction – the case of Bam. *Int J Disaster Risk Reduct* 2017;21:340–9. <https://doi.org/10.1016/j.ijdrr.2017.01.012>.
- [22] Finnemore M, Hollis DB. Constructing norms for global cybersecurity. *Am J Int Law* 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843913.
- [23] Goodman CB. Local government fragmentation: what do we know? *State Local Government Review* 2019;51(2):134–44. <https://doi.org/10.1177/0160323x19856933>.
- [24] GovCERT. Cybersecuritybeeld nederland december 2011. 2011. p. 1–60. <https://www.tweedekamer.nl/kamerstukken/detail?id=2011D64639&did=2011D64639>.
- [25] Government of the Netherlands. Public administration. n.d. Government.Nl; 2024. <https://www.government.nl/topics/public-administration>.
- [26] Hamilton DK, Miller DY, Paytas J. Exploring the horizontal and vertical dimensions of the governing of metropolitan regions. *Urban Affairs Review* 2004;40(2):147–82. <https://doi.org/10.1177/1078087404268077>.
- [27] Head BW. Wicked problems in public policy: understanding and responding to complex challenges. Springer International Publishing; 2022. <https://doi.org/10.1007/978-3-030-94580-0>.
- [28] Held D, Young K. Global governance in crisis? Fragmentation, risk and world order. *International Politics* 2013;50(3):309–32. <https://doi.org/10.1057/ip.2013.9>.
- [29] Hendrick RM, Jimenez BS, Lal K. Does local government fragmentation reduce local spending? *Urban Affairs Review* 2011;47(4):467–510. <https://doi.org/10.1177/1078087411400379>.
- [30] Hoffman W, Nyikos S. Governing private sector self-help in cyberspace: analogies from the physical world. December 6. Carnegie Endowment; 2018. <https://carnegieendowment.org/2018/12/06/governing-private-sector-self-help-in-cyberspace-analogies-from-physical-world-pub-77832>.
- [31] Jayawardane S, Larik J, Jackson E. Cyber governance: challenges, solutions, and lessons for effective global governance, policy brief nr. 17. The Hague Institute for Global Justice; 2015. <https://scholarlypublications.universiteitiden.nl/access/item%3A2869007/view>.
- [32] Jimenez BS. The fiscal performance of overlapping local governments. *Public Finance Review* 2015;43(5):606–35. <https://doi.org/10.1177/1091142114535836>.
- [33] Jones GA. The horizontal and vertical fragmentation of academic work and the challenge for academic governance and leadership. *Asia Pacific Education Review* 2013;14(1):75–83. <https://doi.org/10.1007/s12564-013-9251-3>.
- [34] Karré PM, Alford J, Van Der Steen M. Whole of government in theory and practice: an exploratory account of how Australian and Dutch governments deal with wicked problems in an integrated way. Beyond fragmentation and interconnectivity: public governance and the search for connective capacity. Ios Press; 2012.
- [35] Karré PM, Van der Steen M, Van Twist M. Joined-Up Government in The Netherlands: experiences with Program Ministries. *Int J Public Adm* 2013;36(1):63–73. <https://doi.org/10.1080/01900692.2012.713295>.
- [36] KPMG. SWOT-analyse strategische waardeketens. 2020. <https://www.rijksoverheid.nl/documenten/rapporten/2020/10/30/swot-analyse-strategische-waardeketens>.
- [37] Lewallen J. Emerging technologies and problem definition uncertainty: the case of cybersecurity. *Regul Gov* 2021;15(4):1035–52. <https://doi.org/10.1111/rego.12341>.
- [38] Liaropoulos AN. Cyberspace governance and state sovereignty. In: Bitros GC, Kyriazis NC, editors. Democracy and an open-economy world order. Springer International Publishing; 2017. p. 25–35. https://doi.org/10.1007/978-3-319-52168-8_2.
- [39] Mata DC. Cybersecurity dimensions of national security. 2015. p. 132–42.
- [40] Ministerie van Binnenlandse Zaken. Conceptverslag openbare kennisbijeenkoms—Tijdelijke commissie digitale zaken. 2019. p. 1–84. <https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=2019D39722&did=2019D39722>.
- [41] Ministerie van Binnenlandse Zaken. Meer parlementaire grip op digitalisering. a. 2020. p. 1–16. <https://www.tweedekamer.nl/kamerstukken/detail?id=2021D00178&did=2021D00178>.
- [42] Ministerie van Binnenlandse Zaken. Parlementair onderzoek digitale toekomst. b. 2020. p. 1–45. <https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z9430&did=2020D20305>.
- [43] Ministerie van Binnenlandse Zaken. Organogram ministerie van bzk. 2023. <https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijksrelaties/organisatie/organogram>.
- [44] Ministerie van Buitenlandse Zaken. Organogram bzk - december 2021. 2021. <https://www.rijksoverheid.nl/ministeries/ministerie-van-buitenlandse-zaken/documenten/brochures/2021/12/06/organogram-bzk-december-2021>.
- [45] Ministerie van Defensie. Organogram ministerie van defensie. n.d.. 2024. <https://www.rijksoverheid.nl/ministeries/ministerie-van-defensie/organisatie/organogram>.
- [46] Ministerie van Economische Zaken. Organogram ministerie van economische zaken en klimaat. 2023. <https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/organisatie/organogram>.
- [47] Ministerie van Financiën. Organogram ministerie van financiën. 2022. <https://www.rijksoverheid.nl/ministeries/ministerie-van-financien/organisatie/organogram>.
- [48] Ministerie van Justitie en Veiligheid. Organogram ministerie van justitie en veiligheid. 2023. <https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/organisatie/organogram>.
- [49] Ministerie van Landbouw, Natuur en Voedselkwaliteit. Organogram ministerie van LNV. 2023. <https://www.rijksoverheid.nl/ministeries/ministerie-van-landbouw-natuur-en-voedselkwaliteit/organisatie/organogram>.
- [50] Ministerie van Onderwijs, Cultuur en Wetenschap. Organogram ministerie van OCW. 2023. <https://www.rijksoverheid.nl/ministeries/ministerie-van-onderwijs-cultuur-en-wetenschap/organisatie/organogram>.
- [51] Ministerie van Volksgezondheid, Welzijn en Sport. Organogram ministerie van VWS. 2023. <https://www.rijksoverheid.nl/ministeries/ministerie-van-volksgezondheid-welzijn-en-sport/organisatie/organogram>.
- [52] NCSC. Partners van het NCSC. n.d.-a. NCSC; 2024. <https://www.ncsc.nl/onderwerpen/partners-van-het-ncsc>.
- [53] NCSC. Samenwerking in een ISAC. n.d.-b. 2024. <https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten/samenwerking-sector>.
- [54] NCTV. Nationaal digitaal crisisplan. 2020. <https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal>.
- [55] NCTV. Nederlandse cybersecuritystrategie 2022–2028. a. 2022. <https://www.ncsc.nl/onderwerpen/nederlandse-cybersecuritystrategie>.
- [56] NCTV. Organisatie. b. NCTV; 2022. <https://www.nctv.nl/organisatie>.
- [57] Nissenbaum H. Where computer security meets national security1. *Ethics Inf Technol* 2005;7(2):61–73. <https://doi.org/10.1007/s10676-005-4582-3>.
- [58] Oldenarm P, Mooy L. CYCLOTRON Gezamenlijk sneller en gericht delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband. 2022. https://www.onderzoeksraad.nl/media/inline/2022/12/13/bijlage_reactie_ka_binet_cyclotron.pdf.
- [59] Onderzoeksraad voor Veiligheid. (2021). *Kwetsbaar door software—Lessen naar aanleiding van beveiligingslekken door software van citrix*. <https://www.onderzoeksraad.nl/page/17171/kwetsbaar-door-software-lessen-naar-aanleiding-van>.
- [60] Overheid.nl. Officiële bekendmakingen. n.d.-a. 2024. <https://www.officielebekendmakingen.nl>.
- [61] Overheid.nl. Wegwijzer naar informatie en diensten van alle overheden. n.d.-b. 2024. <https://www.overheid.nl>.
- [62] Overheid.nl. Logius. May 4. 2022. <https://organisaties.overheid.nl/71428/Logius>.
- [63] Pahl-Wostl C, Knieper C. Pathways towards improved water governance: the role of polycentric governance systems and vertical and horizontal coordination. *Environ Sci Policy* 2023;144:151–61. <https://doi.org/10.1016/j.envsci.2023.03.011>.
- [64] Peters BG, Pierre J. Governance without Government? Rethinking Public Administration. *Journal of Public Administration Research and Theory: J-PART* 1998;8(2):223–43. JSTOR.
- [65] Rathenau Instituut. Opwaarderen Borgen van publieke waarden in de digitale samenleving. 2017. p. 1–213. <https://www.tweedekamer.nl/kamerstukken/detail?id=2017D04400&did=2017D04400>.
- [66] Rijksoverheid. Agentschappen Rijksoverheid. n.d.-a. 2024. <https://www.rijksoverheid.nl/onderwerpen/rijkschappen/agentschappen>.
- [67] Rijksoverheid. Ministeries. n.d.-b. 2024. <https://www.rijksoverheid.nl/ministeries>.
- [68] Rijksoverheid. Taken van de Rijksoverheid. n.d.-c. 2024. <https://www.rijksoverheid.nl/onderwerpen/rijkschappen/taken-van-de-rijkschappen>.
- [69] Rijksoverheid. Zelfstandige bestuursorganen (zbo's). n.d.-d. 2024. <https://www.rijksoverheid.nl/onderwerpen/rijkschappen/zelfstandige-bestuursorganen>.
- [70] Schmitter PC. Defining, explaining and, then, exploiting the elusive concept of “governance”. *Fudan J Human Soc Sci* 2019;12(4):547–67. <https://doi.org/10.1007/s40647-018-0236-9>.
- [71] Schram J, den Uijl H, van Twist M. Actuele kwestie, klassieke afweging. Nederlandse School voor Openbaar Bestuur (NSOB); 2021. <https://www.nsob.nl/over-nsob/actualiteiten/nieuwe-publicatie-actuele-kwestie-klassieke-afweging>.
- [72] Timmers P, Dezeure F. Nederlandse strategische autonomie en cybersecurity. 2020. p. 1–72. <https://www.cybersecurityraad.nl/documenten/rapporten/2021/02/18/onderzoeksrapport-digitale-autonomie>.
- [73] Tweede Kamer. Regels ter uitvoering van verordening (EU) 2019/881 (Uitvoeringswet cyberbeveiligingsverordening). 2021. p. 1–10. <https://www.tweedekamer.nl/kamerstukken/detail?id=2021Z08205&did=2021D23776>.
- [74] Tweede Kamer. Debat op hoofdlijnen over digitale zaken (ongecorrigeerd stenogram). Tweede Kamer Der Staten-Generaal; 2022. <https://www.tweedekamer.nl/kamerstukken/detail?id=2022D28327&did=2022D28327>.

- [75] Vakulyk O, Petrenko P, Kuzmenko I, Pochtovyi M, Orlovskiy R. Cybersecurity as a component of the national security of the state. *J Secur Sustain Issues* 2020;9(3): 775–84. [https://doi.org/10.9770/jssi.2020.9.3\(4\)](https://doi.org/10.9770/jssi.2020.9.3(4)).
- [76] van den Berg B, Keymolen E. Regulating security on the Internet: control versus trust. *Int Rev Law, Comput Technol* 2017;31(2):188–205. <https://doi.org/10.1080/13600869.2017.1298504>.
- [77] van den Berg B, Kuipers S. Vulnerabilities and cyberspace: a new kind of crises. *Oxford research encyclopedia of politics*. Oxford University Press; 2022. <https://doi.org/10.1093/acrefore/9780190228637.013.1604>.
- [78] van den Berg J. A basic set of mental models for understanding and dealing with the cybersecurity challenges of today. *J Inf Warfare* 2020;19(1):24.
- [79] van Thiel S. Quangocratization: trends, causes and consequences = Verzelfstandiging. *Interuniv. Center Soc Sci Theory Methodol* 2000.
- [80] Van Thiel S. Trends in the public sector: why politicians prefer quasi-autonomous organizations. *J Theor Polit* 2004;16(2):175–201. <https://doi.org/10.1177/0951629804041120>.
- [81] von Solms R, van Niekerk J. From information security to cyber security. *Comput Secur* 2013;38:97–102. <https://doi.org/10.1016/j.cose.2013.04.004>.
- [82] Weiss M, Jankauskas V. Securing cyberspace: how states design governance arrangements. *Governance* 2019;32(2):259–75. <https://doi.org/10.1111/gove.12368>.
- [83] Zelli F. The fragmentation of the global climate governance architecture. *WIREs Climate Change* 2011;2(2):255–70. <https://doi.org/10.1002/wcc.104>.
- [84] Zelli F, van Asselt H. Introduction: the institutional fragmentation of global environmental governance: causes, consequences, and responses. *Glob Environ Polit* 2013;13(3):1–13. https://doi.org/10.1162/GLEP_a_00180.