To trust or to restrict?–mapping professional perspectives on intelligence powers and oversight in the Netherlands using Q-methodology

Oomens, E. C.; van Wegberg, R. S.; Klievink, A. J.; van Eeten, M. J.G.

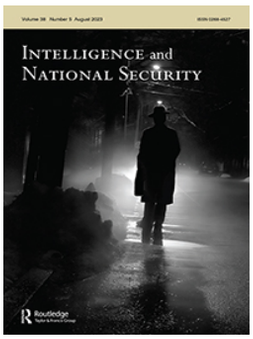
DOI
10.1080/02684527.2023.2239037

Publication date
2023

Document Version
Final published version

Published in
Intelligence and National Security

Citation (APA)
Oomens, E. C., van Wegberg, R. S., Klievink, A. J., & van Eeten, M. J. G. (2023). To trust or to restrict?–mapping professional perspectives on intelligence powers and oversight in the Netherlands using Q-methodology. *Intelligence and National Security*, *39*(1), 40-63. https://doi.org/10.1080/02684527.2023.2239037



Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

To trust or to restrict? – mapping professional perspectives on intelligence powers and oversight in the Netherlands using Q-methodology

E.C. Oomens, R.S. van Wegberg, A.J. Klievink & M.J.G. van Eeten

To cite this article: E.C. Oomens, R.S. van Wegberg, A.J. Klievink & M.J.G. van Eeten (2023): To trust or to restrict? – mapping professional perspectives on intelligence powers and oversight in the Netherlands using Q-methodology, Intelligence and National Security, DOI: 10.1080/02684527.2023.2239037

To link to this article: https://doi.org/10.1080/02684527.2023.2239037

Published online: 02 Aug 2023.

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2023.2239037

Routledge
Taylor & Francis Group

ARTICLE

OPEN ACCESS Check for updates

To trust or to restrict? – mapping professional perspectives on intelligence powers and oversight in the Netherlands using Q-methodology

E.C. Oomens, R.S. van Wegberg, A.J. Klievink and M.J.G. van Eeten

ABSTRACT

In recent years, the intelligence domain has transformed and become more cyber-oriented. This has been accompanied by governance reforms of intelligence agencies' powers and oversight mechanisms. However, opinions on key points of these reforms diverge and diverging professional opinions may affect how reforms achieve intended goals. Using Q-methodology, this article identifies and analyses four distinct viewpoints that professionals in the Dutch intelligence community hold regarding intelligence powers and oversight thereof. This study was done in the context of recent reforms in the Netherlands and also considers how views on trust, privacy, and effectiveness play a role.

ARTICLE HISTORY
Received 06 April 2023
Accepted 14 July 2023

KEYWORDS
National security; intelligence oversight; checks-and-balances; intelligence resources; intelligence powers; intelligence accountability; perspectives; q-methodology

1. Introduction

Cyber brings new challenges for national security and the intelligence community, as digitalization and globalisation have induced new and increasingly cyber-oriented threats.[1] At the same time, social, political, economic, and technological developments have transformed the ways through which intelligence is gathered. As a result, intelligence services are increasingly using large datasets and digital methods to mitigate both cyber and traditional threats.[2] This transformation has been accompanied by a wave of reforms in governance systems of intelligence in various countries.[3] Generally, such reforms have aimed to increase the effectiveness of intelligence services in the new cyber-oriented reality, while striving to maintain and improve checks-and-balances.

However, for reasons of e.g., complexity and unintended consequences, the governance reforms and policies on paper (i.e., regulations) can be quite different from how they work out in practice. Studies on policy implementation highlight how formal regulations almost by necessity cannot cater for all variations and complexities the real world presents to implementers.[4] The intelligence domain is no different. Hence, the actors and stakeholders involved in the implementation and execution of these reforms, play a significant role in shaping what these reforms end up looking like. The actors involved may interpret laws, rules, regulations, and criteria differently in that process. This can create tensions between these stakeholders, which may even stem from fundamental disagreements about how far a state may go. These divergent perspectives impact how regulations are applied, and the resulting tensions can permeate the daily practices of intelligence agencies and overseers, potentially even causing system paralysis due to excessive conflict.[5]

Ultimately, we see the underlying tension as one between the permitted powers, their balance with other public values (e.g., privacy), and the mechanisms that need to be put in place for balancing this in a just and accountable way. As stakeholders implement reforms, their core perspectives on crucial themes

CONTACT E.C. Oomens e.c.oomens@tudelft.nl

like privacy and trust shape the implementation. These core ideas underlie disagreements on the design of checks-and-balances, regarding for instance the focal point of oversight (prior to power usage or afterward), the scope of overseers' mandates, and the binding nature of their rulings. The assumption underlying this paper is that decisions are initially guided by policy, but the practicalities are ultimately shaped during implementation by actors who may hold fundamentally divergent viewpoints on the significance of specific values, the legitimacy of government powers, and the necessary checks-and-balances.

Though there is a body of research that has investigated the impacts of reforms on intelligence communities,[6] less attention has been paid to the perspectives of professionals that shape those reforms in practice. Furthermore, while studies have investigated the impact of privacy attitudes and trust on the acceptance of surveillance and intelligence by governments for citizens,[7] there is a dearth of research on attitudes of stakeholders who play a crucial role in defining the boundaries of intelligence activities in practice. This gap could be attributed to the reluctance of many intelligence professionals to participate in academic research due to the secretive and sensitive nature of their work. Traditionally, intelligence studies have had a predominantly historical focus, with limited empirical social scientific studies. However, there has been a recent shift towards embracing more methodological variety.[8]

This paper contributes by empirically examining the perspectives of intelligence professionals as well as other important stakeholders, including overseers, privacy watchdogs, and researchers. Their views are studied on the design of checks-and-balances in relationship to the powers of an intelligence community that has become more cyber-oriented. We also examine how elements like trust, privacy, and effectiveness play a role in their reasoning. Insight into their views is important as they ultimately make the choices that determine the actual work of intelligence agencies and their overseers.

This study is done in the context of the Dutch intelligence community. It is a particularly current case of a re-evaluation of powers and checks-and-balances due to the introduction of a new law for the Dutch intelligence and security services in 2017 (the WIV 2017) and an ongoing regulatory debate on an update of this recent law.[9] The law extended the powers of the intelligence agencies and included reforms to the accountability and oversight mechanisms.[10] However, the WIV 2017 faced significant criticism, specifically regarding concerns for bulk data collection, privacy, and inadequate oversight mechanisms.[11] Further background is provided in section 2.

Noteworthy in this case are the disagreements among professionals on these topics, which have led to impasses and friction between the Dutch intelligence services and the oversight bodies as they interpreted parts of the law differently.[12] The reforms have been reviewed by two separate evaluation committees that both concluded there were issues that needed resolving, such as decreased efficiency of the services resulting from extensive oversight burdens.[13] This set actions in motion to again reform the law on the intelligence services. In the meantime, a temporary law on cyber operations (Cyber Act) has been proposed.[14] The Cyber Act includes a shift in oversight mechanisms for some powers, with less focus on prior authorisation (ex-ante oversight), and more emphasis on assessing legality during and after power use (ex-durante and ex-post oversight).[15] The Cyber Act too has been criticized, with critics warning against erosion of ex-ante oversight mechanisms.[16]

While countries encounter specific challenges in intelligence reform, there are also common challenges for oversight that have been discussed in previous literature on reforms.[17] One such challenge is striking a balance between ineffective and symbolic oversight on one hand and an overwhelming amount of oversight that hinders efficiency on the other. Additionally, addressing information asymmetry and managing secrecy poses significant difficulties. Moreover, overseers ideally need to assess legality/proportionality, effectiveness, and (cost) efficiency, but it remains a challenge for them to effectively focus on all these aspects simultaneously. This is also known as the trilemma. These challenges are similarly present in the Dutch reform process. Therefore, this case can inform others grappling with the same issues.

Our aim is to provide an in-depth analysis of the various positions that professionals take in the discussion on powers and oversight of the Dutch intelligence and security services in the digital

domain. The stakeholders include a diverse group of intelligence practitioners, overseers, researchers, private sector professionals, policymakers, law enforcement practitioners, and professionals in civil society. We use Q-methodology to identify four distinct perspectives. The main research question we answer is: What are the prevalent perspectives of Dutch intelligence professionals on oversight, digital intelligence powers, trust, privacy, and effectiveness in the context of recent intelligence reforms in the Netherlands?

The paper is structured as follows. Having introduced the research problem, question, domain, and case in this section, the next section briefly discusses some background on the Dutch context. The Q-methodology applied in this study is outlined in section 3. Section four presents the results, followed by a discussion in section 5.

2. Background

2.1. Oversight in the Netherlands

The Netherlands has two intelligence services, namely the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). Since 2002, they have been checked by an independent oversight body, named the Security Services Review Committee (CTIVD), which is concerned with legality ex-post. The CTIVD itself determines what it investigates and reports on its findings and conclusions in public reports. It also informs parliament and the relevant ministers. Recommendations by the CTIVD are not binding, meaning that a minister can choose to not follow-up on them. Other parties that oversee the services are parliament, court judges, and the Algemene Rekenkamer (Netherlands Court of Audit), which occasionally evaluates the intelligence services on (cost) efficiency.[18]

2.2. WIV 2017 & oversight

The WIV 2017 was developed because its predecessor, the WIV 2002, was deemed outdated as it did not allow for the services to use newer technologies, such as bulk cable interception. The WIV 2017 was met with criticism, which largely focused on the new cyber powers for collecting bulk data and concerns for citizens' privacy.[19] Remarkably, a nationwide consultative referendum was held on 21 March 2018, in which a small majority (49,44 per cent against, 46,53 per cent for) of the Dutch public voted against the law.[20] Despite this result, the law was passed with some alterations.

The WIV 2017 provides the legal framework within which the AIVD and MIVD can operate. It introduced a new oversight body: the Review Board for the Use of Powers (TIB). The TIB is, like the CTIVD, concerned with legality. However, the primary task of the TIB is to assess proportionality and authorise the use of powers before operational use (ex-ante). It provides a binding Go/No Go decision, meaning that the use of a power is either approved or rejected. Only 'special investigatory powers' (e.g., hacking, wiretapping, cable interception) must be authorised before use by the TIB. Other powers, that are seen as generally less intrusive (e.g., OSINT, informants), require only internal prior authorisation, and in some cases ministerial approval. While the CTIVD has access to all information of the services, the TIB only has access to information that is provided to them in requests for power use by the services.

2.3. Temporary Cyber Act

An evaluation committee concluded that some norms in the WIV 2017 were left open for interpretation. Overseers interpreted these norms strictly, leading to difficulties in obtaining authorisation for the use of some powers by the services.[21] The Algemene Rekenkamer concluded that that no proper estimate had been made of the amount of work required to implement the WIV 2017 beforehand

and that the extensive administrative burdens take up too much time and capacity, impeding the efficiency of the services.[22]

In an effort to resolve these issues, the temporary Cyber Act contains amendments to the ex-ante review of power use by the TIB. The prior authorisation process is made less probing for some cyber powers, and oversight ex-durante and ex-post by the CTIVD is strengthened. Thus, oversight is transferred partly from front-end to real-time and back-end.[23] The CTIVD will receive binding decision-making powers, meaning that it can follow operations and terminate them if unlawful practices are identified. The intelligence services get the possibility to appeal decisions made by the CTIVD via the Council of State.

Like the WIV 2017 before, the Cyber Act has been met with criticism and doubts. Some question whether this temporary law will succeed where the WIV 2017 has failed, and others criticise the transformation of the oversight system.[24] This research was conducted while the Cyber Act was still in development.

3. Methodology

3.1. Q-methodology

Q-methodology has been used in political science and policy analysis to identify complex perspectives on policy issues, including national security.[25] Here, we use it to identify the viewpoints of professionals around the issues of oversight and intelligence powers. Q-methodology is designed to identify the population of perspectives on an issue by combining qualitative and quantitative features. Respondents construct their viewpoint on the topic at hand by sorting cards printed with statements (the Q-set) onto a quasi-normal distributed grid that runs along a scale of 'most disagree' to 'most agree' (Figure 1). The sorting process is accompanied by an interview about why statements are ranked in a certain way, thereby capturing the underlying narratives of the participants. The resulting Q-sorts are statistically analysed to reveal clusters – or perspectives – where participants ranked certain statements in a similar way. The idea of enforcing a structure on the sorting of statements, is to get participants to rank the statements in relation to each other. The structure also requires participants to prioritize, revealing information about how much they care about certain issues.

Q-methodology stands in contrast to a survey approach, where a respondent can freely take a position on any question or issue, irrespective of their other positions. The requirement of making choices is why Q-sorts are less susceptible to many response biases that are often present in Likert-type survey questions, such as midpoint responding and acquiescence.[26] Compared to semi-structured interviews, Q-sorts are more effective in identifying relationships across respondents' perspectives, since all respondents rank the same set of statements. Also, the identification of the underlying perspectives is guided by the statistical analysis and thus less prone to biases of the researchers.

	Most disagree					Neutral					Most agree
Statement scores	-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
No. of statements	1	2	5	7	9	12	9	7	5	2	1

Figure 1. Forced-choice frequency distribution for Q-sorts.

3.2. Q-set design

The statements in a Q-set should be 'representative of the breadth of debate on an issue',[27] so that participants are able to fully express their individual perspective. Each statement is evaluated and ranked by a participant in relation to the other statements that are already on the table. The final arrangement of statements (the Q-sort) each participant makes becomes a 'model of their viewpoint on the issue under study'.[28]

In the accompanying interview, participants can explain and elaborate on their positions. Contrary to survey questions, statements do not need to be unbiased or unambiguous. In fact, statements should elicit a response and contain all the ingredients for participants to fully express themselves. Therefore, Q-sets can also contain controversial statements. How participants interpret specific statements, emerges from the conversation.

The Q-set statements in this study were generated through document review. Initially a newspaper database (LexisNexis) was searched using various Dutch search terms regarding the Dutch intelligence apparatus (e.g., 'inlichtingen', 'privacy', 'WIV 2017', 'AIVD' etc.). The newspaper articles from this search were used as a source for snowball sampling as the articles referenced other news articles, podcasts, policy reports, and TV clips that were not included in the LexisNexis database.

From these sources, 198 statements were selected on the basis that they mentioned specific intelligence resources (hacking, wiretapping, cable interception, open-source intelligence (OSINT) or malware) in combination with a value judgment (effectiveness, usability, acceptability, accuracy, risk). Statements were also selected if they contained views on specific issues surrounding data processing (automated data-analysis, bulk data, sharing, storage) and oversight. Statements on privacy and trust were also included.

The initial set was then reduced to a set of 80 statements, by discarding statements that were similar to other statements, unclear, or deemed less relevant. We conducted four pilot interviews. These demonstrated that the set of 80 statements was too large to sort and discuss within an hour, so the set was further reduced to 60 statements. This is within the accepted standard range of 40–80 statements, as described by Watts & Stenner.[29] A second pilot study ($N = 10$) was held with the set of 60 statements. After the pilot, some statements were altered to make them more understandable and shorter. There were no indications from participants that important issues were missing from the statements. Pilot participants indicated they were able to sufficiently express their views, which led the research team to believe the Q-set had sufficient coverage. The final Q-set is presented in Table A1, Appendix A.

The statements were kept as close to their original source as possible, to represent organic views from practice. This also meant that some statements consisted of multiple sentences, e.g., because they contained an argument. Because of the complexity of the intelligence domain and the discussion surrounding it, the research team felt it appropriate to include longer statements and reduce only where necessary. During the final study, participants indicated they liked the complexity and variance of the statements and agreed the debate on Dutch national security and intelligence was well represented. They also thought the statements came from good sources, as the content was sufficiently detailed. This reassured the research team that they were correct in altering the statements as little as possible.

3.3. Participants

The core idea in building a sample of participants is that they represent the range of perspectives that need to be identified. Q-methodology does not generalize to a population of respondents but to the population of views. We recruited respondents from stakeholder groups that play a significant role in the Dutch intelligence and security debate, namely intelligence practitioners ($N = 4$), overseers ($N = 6$), civil society ($N = 3$), private sector ($N = 3$), researchers ($N = 5$), policymakers ($N = 2$), and law enforcement ($N = 3$). Within these stakeholder groups, participants with diverse roles and

backgrounds (e.g., technical, operational, legal) were asked to take part. The diversity and expertise of professionals was a priority during selection to ensure the representation of as many perspectives as possible. About half of the approached individuals agreed to participate. Some stakeholder groups were less willing to participate than other groups, most notably digital rights and privacy activists were concerned that the research would be biased in favour of the intelligence agencies. Policymakers were also reluctant to go on the record with their views, stating reasons like time constraints. Therefore, the number of policymakers and civil society professionals in the sample is smaller than the research team preferred. The final sample consisted of $N = 26$ participants, which is in line with Watts and Stenner's suggestion for participant numbers in Q-methodological research.[30]

3.4. Procedure

The Q-sorts were conducted in person with printed cards containing numbered statements. Participants made forced sorts, meaning that they are instructed to position the statements on a quasi-normal grid. Figure 1 shows the forced-choice frequency distribution, which is a quasi-normal distribution of the 60 statements. Participants could rank only a single statement on the extremes (−5, most disagree to + 5, most agree), and more statements in each column the closer it came to the neutral position. All statements thus receive a ranking between −5 and + 5 for each participant. A few participants ($N = 5$) deviated somewhat from the forced categories, due to time constraints or because they felt an unforced sort best represented their viewpoint. This has only a negligible impact on the subsequent factor analysis.[31] The deviating participants still ranked statements and tried to stick to the frequency distribution to the best of their abilities.

Conversations with participants were recorded. They were asked to comment briefly on each statement during the sorting and were asked for clarification if needed. Afterwards participants were asked whether they could summarize their viewpoints, whether they had any remarks or observations to add, and whether they missed any aspect of the issue they believed was relevant for their perspective.

3.5. Analysis and interpretation

The 26 Q-sorts were intercorrelated and subjected to by-person factor analysis.[32] KADE software version 1.2.1[33] was used for the analysis. First a correlation matrix was calculated. Eight factors were extracted using Principal Components Analysis (PCA). To determine the final solution of factors, various options were closely examined, ranging from 2 to 7 factors. The research team settled for a final solution of three factors, with one factor being bi-polar, so capturing two perspectives. The researchers found that this solution provided the clearest factor interpretation, while still being detailed and offering a range of nuanced views. A solution of three factors was also in line with the scree test criterium, which suggests that the final number of factors to extract is indicated by the point at which the line in the scree plot changes slope.[34] All three factors had an eigenvalue of greater than 1 and together explained 50 per cent of the study variance, which can be considered a 'sound solution on the basis of common factors'.[35] See Table A2, appendix B.

The three factors were varimax rotated to maximize factor loadings. Participants loaded significantly on a factor at $p < 0.005$. Majority of common variance was required. At this level all participants loaded significantly on one factor. One participant had a significant negative loading on Factor 1, which means that this participant expressed an opposing perspective to the positive loaders on Factor 1.[36] Factor 1 was therefore split into Factor 1a (representing the positive loadings) and Factor 1b (representing the negative loading). This was done to enhance interpretability and because the researchers thought this participant had a relevant minority viewpoint that was worth explaining. The researchers know from the public debate that the perspective of Factor 1b is not uncommon. Rather, this viewpoint is underrepresented in the participant sample for this study, because other individuals with similar professional backgrounds

to the Factor 1b participant were unwilling to participate. Table A3, Appendix C shows the loadings of every participant for each factor.

Participants with significant loadings on a factor sorted the statements in a similar way. They agreed or disagreed with the same statements and were similarly neutral about other statements, which suggests they share similar positions in the discussion on reforms. Participants with significant loadings are factor exemplars and can be seen as representative for the thought pattern present in the factor on which they load. The factor exemplars were used to calculate a composite Q-sort for each factor, which is called a factor array. 'Higher loading factor exemplars are given more weight' in the calculation of the factor arrays because they 'better exemplify the factor'.[37] The subsequent factor array is the ideal Q-sort for a factor, based on the weighted averaging of all the factor exemplars for that factor. The factor arrays are presented in Table A1, Appendix A.

Lastly, the factors were interpreted using the factor arrays. The qualitative interview data were also used to clarify and help understand the underlying perspective. The aim was to uncover and holistically explain a viewpoint captured by a factor, that is shared among the significantly loading participants.[38] The next section will describe the final factor interpretations.

4. Results

We identified four factors representing distinct perspectives. The factors were labelled and are presented in Table 1. In the next section, a more detailed in-depth analysis of the perspectives is discussed. Statements and their corresponding scores are included in-text as '(statement: score)'. Tables with important statements for a factor are also included. For the complete set of statement scores, we refer to Table A1, Appendix A.

Table 1. Factor labels and descriptions.

Factor	Label	Description
Factor 1a	To trust and relieve	Trusts intelligence services, favours more operational scope and relieving services of burdens that impede effectiveness.
Factor 1b	To distrust and restrict	Distrusts intelligence services, favours restricting services by removing powers and opposes adding new powers.
Factor 2	To check and improve	Trusts in the overall functioning of the intelligence system, 'trust but verify', favours improving checks on powers just enough to fit intelligence practice.
Factor 3	To control and protect	Neither trusts nor distrusts intelligence services, favours controlling services (that already have extensive powers) to protect citizens against risks.

4.1. Factor 1a: to trust and relieve

Nine participants scored significant loadings on Factor 1a. This included intelligence practitioners ($N = 4$), law enforcement ($N = 2$), a researcher ($N = 1$), overseer ($N = 1$), and private sector professional ($N = 1$). Participants in this factor have a high level of trust in the Dutch intelligence services and emphasize the importance of trust. They highlight some undesired effects of oversight mechanisms introduced in the WIV 2017. The current ex-ante authorisation for some cyber powers is perceived as burdensome and micromanagement. The factor wishes for oversight mechanisms that are sufficiently flexible and give the intelligence services more scope and room to operate, thus relieving them of mechanisms that impede effectiveness. This includes a shift to more ex-post centred oversight for some powers.

As shown in Table 2, Factor 1a regards trust as very important for the services, as they have no democratic legitimacy without societal trust. Participants in this factor strongly disagree with characterizations of the services that undermine trust, because those are seen as harmful and often unjustified and incorrect. They emphasize that intelligence services work carefully and meticulously, as they must always be able to motivate why certain actions are necessary and lack the capacity to monitor people willy-nilly.

Table 2. Factor arrays on trust.

	F1a	F1b	F2	F3
03. One can safely trust the Dutch intelligence and security services. I believe that they work purposeful, self-critically, and with integrity.	+2	−2	+2	−2
05. The Dutch intelligence and security services prefer to go about their business without oversight. They want more power, and this goes against the will of the Dutch people.	−5	+5	−5	0
20. Even if one is not doing anything wrong, one is being watched and spied on.	−4	+2	−3	+1
54. The Dutch intelligence services will regularly break the law if they deem it necessary.	−4	+2	−4	−2

In the past years, there has been discussion about collecting large amounts of data and how these data should be processed (e.g., how long should they be stored? When should data be filtered and assessed for relevancy?). In this factor, participants argue that the collecting and storing of information are inherently part of intelligence services' task to identify threats to national security at an early stage (Table 3).

Table 3. Factor arrays on bulk data.

	F1a	F1b	F2	F3
12. Bulk data prove their value for research over a longer period. It is also not always known which data will be relevant. This must be included in the determination and review of retention periods and relevance assessments.	+3	−1	+3	−3
27. Stricter limits must be set on the data hunger of the secret services, which are now not limited by regulations. They collect more data than they can handle and keep the data longer than allowed.	−3	+3	−2	+1
49. Big data does not prevent attacks, because intelligence services do not have the capacity to analyse it and such data has rarely revealed anything that they could not have known otherwise.	−3	−1	−2	0

To assess the nature of a threat, they need a lot of data, and they need to gather those data sooner rather than later. As a result, intelligence services have 'passive' information in their systems, i.e., data that are not actively looked at. In the view of Factor 1a, passive information does not constitute a serious infringement on people's privacy, mainly because it is not used or looked at.

The sensitivity of datasets and the time that they remain relevant for investigations varies. Participants suggest that some leniency in assessing what is relevant is required because intelligence services must go through data of which they cannot immediately demonstrate whether the data are relevant or not (12: +3). Intelligence work is described as a puzzle. A puzzle piece that has been collected may seem irrelevant at first but can become crucial information in combination with pieces that are found later (40: −1). Intelligence services' task is objective truth-finding and informing policymakers, even if they do not want to hear it. To do this, services need flexibility, independence, and the ability to make fast decisions and adapt to their target's movements (32: +2).

While Factor 1a does assert that administrative burdens are necessary because intelligence services must motivate their considerations and methods (29: +1), it also worries about their impact on the effectiveness of intelligence services (44: +3) (Table 4). Participants describe that currently the burdens of oversight are considered high and seen as an obstacle for investigations. Some requests for prior authorisations are dropped because of the workload they entail, while the chance of approval is unclear.

Table 4. Factor arrays on administrative burdens.

	F1a	F1b	F2	F3
44. Administrative burdens resulting from oversight should not hinder the efficiency and effectiveness of the services. Paperwork should not be an obstacle to conducting research in the interest of national security.	+3	−4	+1	−1

In this factor, ex-ante oversight is therefore met with mixed feelings. The ex-ante test of proportionality proves difficult because it does not fit with the operational reality where not everything can be predicted in advance (33: 0). Respondents of Factor 1a prefer a system of ex-durante and ex-post oversight, in which overseers observe the operations in real-time and engage in discussion during the process, instead of making assessments from written text beforehand. One reason is that overseers are likely to experience information asymmetry since intelligence officers are unable to perfectly write down all the details of operational processes. This is partly because operations are complex and partly because written words are subject to the interpretation of the reader. Additionally, participants think current ex-ante overseers are too convinced of their own interpretation of the law and accept little debate.

The Cyber Act introduces a focus shift from ex-ante to ex-post oversight for some intelligence powers, mainly for cyber operations that can't be fully mapped out in advance. The proposal also includes the plan to provide the CTIVD with ex-durante oversight and binding powers, meaning that their rulings must be followed. Participants in Factor 1a were relatively neutral about making rulings by oversight binding (55: −1). Nonetheless, some participants commented that this makes them uneasy, because an undemocratically chosen oversight body receives the power to overrule the decisions of the minister of a democratically elected government.

Factor 1a has stronger views on statements about intelligence resources than other factors (Table 5). The factor is positive about the effectiveness and possibilities of most powers (9: +5, 10: +2, 49: −3). Resources are seen as especially useful in combination with other resources, as part of an all-source intelligence mix. The frame sees a major role for intelligence services in mitigating digital threats, since they are one of few parties that have insight and can act on a certain scale (25: −2). Resources such as cable interception and strategic hacking are useful because they help detect digital attacks earlier, which is needed to prevent them from being successful (26: −3, 48: +2). Factor 1a considers it justified for services to have wide access to open sources for lead generation (4: +4, 34: +2, 17: 0). Regarding automated data-analysis, the frame believes intelligence services are aware of risks like bias and are therefore careful in making sure models are accurate (7: 0, 28: 0, 35: 0). Accuracy has the highest priority. Additionally, it is seen as a useful method to save time on data processing, such as filtering and searching.

Table 5. Factor arrays on intelligence resources.

	F1a	F1b	F2	F3
04. Nosing around on social media by the Dutch intelligence and security services is almost always justified.	+4	−2	−1	−1
09. Hacking is a wonderful resource for Dutch services because it is very effective.	+5	−2	+3	+2
15. The services must be able to circumvent strong security, for example by hacking people who are in contact with a target to gain entry to the target.	+3	0	+2	0
53. It is good that Dutch communication services are obliged to supply data and to cooperate if our intelligence services want to wiretap or hack targets.	+4	0	+1	0

Regarding organisation effectiveness, one participant mentioned that re-evaluation and reprioritisation of certain matters at the organisational level should be considered, such as the need for the number of contra terrorism teams within intelligence services. According to the participant 'this is not being discussed'. For example, the participant wondered whether terrorism is as threatening as is supposed or if policymakers are just afraid to downscale contra terrorism teams because of possible political consequences.

4.2. Factor 1b: to distrust and restrict

As mentioned, only one participant from civil society scored significant on this factor. Factor 1b reasons from a position of suspicion and distrust. Because intelligence services cannot be trusted to operate carefully, it is better to limit the amount of power they have and to prevent them from

getting new powers. The argument here is that limiting their power is the best way to avoid power abuse and diminish the chance of function creep – that is, the possibility that powers are ultimately used for ends other than initially intended when the power was granted.

In contrast to the previous factor, Factor 1b is more distrusting towards the Dutch intelligence services. A reason for this, is that this factor does not perceive the services to be self-critical (3: −2). In discussions with oversight, the participant observes that they reject feedback. They prefer not to hear critical opinions. Factor 1b supposes the services break the law if they deem it necessary (54: +2) and prefer as little oversight as possible, so that 'they can just do their own thing' (5: +5). An example given is the discussion relating to retention periods; Factor 1b believes the services want more and more power and would rather have no limits on storing data at all. Instead, they would rather save all the data (27: +3) and collect information on everyone (20: +2, 52: +1).

The services are looked at with distrust because they threaten people's privacy (56: −4) (Table 6). The participant in Factor 1b does not perceive the intelligence services as careful with sensitive data (59: +5). Accordingly, the intelligence services have themselves to blame for distrust, as scandals and law-breaking have damaged people's trust, says the participant.

Table 6. Factor arrays on privacy.

	F1a	F1b	F2	F3
56. Our privacy is not really threatened. Details are lost in the huge pile of data that is brought in.	−1	−4	−2	−5
59. One can assume that when collecting intelligence, the intelligence services are careful with the privacy of people who have no intention of harm.	+1	−5	−1	−1

Since intelligence services have extensive powers that threaten privacy and other fundamental rights, oversight mechanisms are needed to restrict and discipline them, according to this factor. Thus, ex-ante oversight should not be loosened and must have the ability to make comprehensive assessments, both on intelligence collection and processing, before authorising the use of powers (33: +3) (Table 7). Additionally, both ex-ante and ex-post oversight should have binding decision-making powers so that the services cannot ignore their conclusions (55: +2). While most factors argue that the intelligence services should work independently from politics because they are tasked with objective truth-finding and should not be used for political purposes, Factor 1b sees independence as problematic and autonomous services as dangerous (32: −2). Lastly, the participant finds it harmful that intelligence services speak of administrative burdens. Demonstrating proportionality is an essential requirement and framing it as a burden undermines the rule of law. It is fair that paperwork provides an obstacle because it is intended as a mechanism to discourage using powers that cannot be adequately justified, thereby preventing abuse of powers (44: −4).

Table 7. Factor arrays on oversight.

	F1a	F1b	F2	F3
24. It is worrying if the Dutch intelligence services can exchange unevaluated data with foreign services without permission from oversight.	0	+4	+3	+2
32. The Dutch intelligence and security services and oversight should operate completely independent from politics. Political colour has no place in intelligence gathering.	+3	−2	+2	+2
33. To be able to test proportionality, the TIB must be able to take everything into account. The TIB cannot do its job if it can only look at the collection of data and not at how the data is subsequently processed.	0	+3	−1	+2
55. Quantity of oversight is not the same as quality. Good oversight is binding and effective. The TIB and CTIVD should have binding powers that they can use on their own initiative.	−1	+2	−2	+2

Factor 1b questions the effectiveness of various intelligence resources (36: +2, 60: +1, 10: −3) (Table 8). It is thought that the services exaggerate effectiveness to legitimize having and using powers. Factor 1b would prefer them to not have certain powers, such as cable interception and

strategic hacking (26: +2, 48: −2). The participant prefers access to open sources to be restricted (4: −2, 34: −3), because open sources also contain sensitive information (17: +2). Factor 1b is critical of automated data-analysis (7: −3). The risk of bias is seen as too great, and the results are generally not accurate (28: +3, 35: −3).

Table 8. Factor arrays on intelligence resources.

	F1a	F1b	F2	F3
26. There is much criticism of cable interception, and the intelligence services hardly make use of this far-reaching power. There is no need for them to have this resource.	−3	+2	−3	−1
36. Hacking isn't all that precise and effective. In addition, large data files are gathered, and a hack can lead to unacceptable collateral damage.	−1	+2	−1	0

Lastly, Factor 1b notes that the secrecy of intelligence services is problematic in a democracy. There are only a few ways citizens can understand what these services are doing: through regulatory reports or through the law, which are complicated and important information is kept secret. The constant changes in laws and regulation lead to a 'policy spaghetti', making the work of the services opaque for citizens. Little effort is put into informing and explaining. Intelligence services even sow confusion, which borders on power abuse. Therefore, citizens cannot form well-informed or realistic opinions, which is undesirable in a democratic state.

4.3. Factor 2: to check and improve

Nine participants had significant loadings on Factor 2, which included overseers ($N = 2$), researchers ($N = 3$), private sector professionals ($N = 2$), a policy maker ($N = 1$) and one civil society professional ($N = 1$). Participants in this factor believe that the Dutch intelligence services operate from good intentions and with propriety, though this is partly spurred by oversight mechanisms. 'Trust but verify' is a prominent sentiment in this factor. For certain powers, like OSINT and data sharing with foreign agencies, it is argued oversight could be strengthened. For other powers that are generally seen as more intrusive, like hacking and cable interception, oversight is already seen as quite strict or even too strict in some cases. However, overall, the intelligence apparatus works well. In this view, oversight should be thorough and aimed at improving intelligence practices, but also sufficiently fitted to the operational reality of intelligence services.

Like Factor 1a, this factor generally expresses high trust in the Dutch intelligence services, though this trust is more influenced by the overall strength of the system than the inherent trustworthiness of the services (54: −4, 5: −5). Some participants argue that intelligence services value oversight because positive feedback legitimizes their work and negative feedback can help them improve their performance. Furthermore, intelligence services might not always be intrinsically motivated to be self-critical, but they are forced to be critical of their own work by accountability and oversight mechanisms (3: +2). Participants do emphasize that one can never just assume intelligence services are trustworthy and do not make mistakes. Oversight mechanisms are needed to verify, as 'trust is good, but checks are better'.

A notable difference with Factor 1a is the stance regarding various intelligence resources (Table 9). Unlike Factor 1a, participants in this factor indicate they have little knowledge on effectiveness, accuracy, and technical risks of different methods (10: 0, 11: −1, 25: 0, 36: −1, 47: 0, 60: −1, 35: 0, 28: 0, 7: 0). Nonetheless, they think certain resources are necessary for the services to have, such as hacking (9: +3, 38: +2, 26: −3, 42: −2). A key viewpoint here is that oversight on general resources, such as OSINT, can be improved. Participants argue that the definition of open sources has been stretched and that there is a difference between the sensitivity of various open sources (S17, +3). It is deemed logical that intelligence services search newspapers, but OSINT is considered more severe when it involves

targeted research on social media or the dark web. Therefore, intelligence services should have restricted access to open sources (34: −3, 4: −1). Similarly, participants show some concerns when it comes to oversight mechanisms around data sharing between intelligence services (24: +3).

Table 9. Factor arrays on OSINT and data sharing.

	F1a	F1b	F2	F3
24. It is worrying if the Dutch intelligence services can exchange unevaluated data with foreign services without permission from oversight.	0	+4	+3	+2
34. The Dutch intelligence and security services may have unlimited access to open sources, as ordinary citizens and journalists also have unlimited access.	+2	−3	−3	0

Factor 2 rejects the notion that intelligence services are watching everyone and that they should only spy on suspects (52: −4) (Table 10). According to participants, 'suspects' is law enforcement terminology. They notice that law enforcement and intelligence are often mixed up and confused, even by overseers. Participants emphasize targets do not have to be suspected of a crime, because in many cases a crime has not yet occurred. Intelligence services are not 'catching criminals' but trying to 'predict probability'. To identify unknown threats and to assess whether a target might become a threat, intelligence services need a certain amount of freedom. It is therefore valid that intelligence services store a large amount of data (40: −3). This is further justified by the fact that the Dutch intelligence services have no police powers; they only inform others and cannot take direct action, like arresting individuals, themselves. Of course, there are limits to how much data should be stored and for how long. Yet, so participants say, overseers are often strict on these limits as they predominantly argue from a law enforcement perspective and forget the nature of intelligence. Overseers could show more leniency and flexibility regarding bulk data collection and processing (12: +3). Consequently, Factor 2 argues that mere possession of data by intelligence services does not equal a major privacy violation (14: +2).

Table 10. Factor arrays on bulk data.

	F1a	F1b	F2	F3
40. Bulk data should only be kept when necessary. No data should be kept just because it might be useful later.	−1	+3	−3	+3
52. Intelligence agencies can wiretap and hack entire neighbourhoods. In this way, every innocent citizen is potentially 'suspicious' without concrete reason to follow that citizen. The services should only spy on suspects.	−3	+1	−4	0

Holding intelligence services accountable is the cornerstone of democratic governance, according to Factor 2. Oversight is seen as incredibly valuable for this end but should also match the intelligence practice. Oversight mechanisms do not have to be made continuously stricter (27: −2). Intelligence services should still be able to function effectively with checks-and-balances (44: +1). Overall, the factor thinks the system of checks-and-balances functions well, even though there are imperfections that can be improved upon. There is no perfect model of oversight. Intelligence services are differently organized in every country and a good system of checks-and-balances is fitted to its oversight subject.

Within Factor 2, opinions are somewhat divided on whether decisions made by oversight should be binding (55: −2). Several participants are strongly against this, others more neutral. It is argued that binding oversight can be counterproductive and ineffective in this domain, as it can lead to friction between stakeholders. As opposed to other domains where an oversight body oversees many actors, in this domain oversight and the services have a much closer, nearly one-on-one relation. Friction hinders the functioning of the system. Additionally, overseers have their own

interests and opinions on specific issues. With binding powers, they can make their will into law, even though they can also make mistakes and be wrong. Moreover, binding rulings result in a shift in responsibility. Binding approval or rejection would make overseers jointly responsible for actions from the intelligence services, which could affect their independence.

Lastly, participants add that perceptions of the intelligence services are subject to change and dominated by emotions. Incidents and reporting in the media influence the level of trust people have. Factor 2 thinks the public debate is often oversimplified and contains misconceptions. One reason given is that some stakeholders thwart a nuanced discussion by making statements that damage trust and unjustly question other stakeholders' legitimacy, because they are preoccupied with their own interests.

4.4. Factor 3: to control and protect

Seven participants had significant loadings on the last factor, which included overseers ($N = 3$), law enforcement ($N = 1$), a policymaker ($N = 1$), researcher ($N = 1$), and civil society professional ($N = 1$). Factor 3 emphasizes the importance of privacy for citizens. Though participants agree that most intelligence resources are very effective, this effectiveness is also what makes these technologies risky in terms of both the technical risks and the impact on privacy. Therefore, participants want oversight mechanisms that prioritise the protection of citizens' rights and controlling the services. While participants trust that the Dutch intelligence services adhere to the law in the current situation, they fear transgressions in the future if certain regulations are altered, such as a decrease of ex-ante oversight. Such changes are seen as a slippery slope.

Of all the factors, Factor 3 is the most outspoken on privacy issues (Table 11). The participants emphasize the need to protect people's privacy, since most people are not equipped to properly protect their own and generally have little control over their information (58: −3). Individuals often do not voluntarily share information, instead they share unwittingly, out of convenience, or because they are required (1: −3). It is argued that the trade-off between privacy and security follows the *law of diminishing returns*. A lot of security can be gained by giving up a little privacy. But as people give up more privacy, after a certain point, the rate of returned security decreases. Privacy violations therefore quickly become disproportional (30: −2). Factor 3 believes that privacy is violated from the moment intelligence services collect and store data, even if it is 'uninteresting' data (14: −1). Information that is not interesting now may still become so later. Additionally, the data that services collect are almost always interesting and sensitive, since they are not allowed to collect data if they cannot justify their importance (22: −4). The participants argue that storing data is risky, since intelligence services too can be hacked. Also, details are never lost, because all information remains findable in the systems if it is not explicitly deleted (56: −5). Factor 3 thinks there should be more attention in policymaking for *reasonable expectations of privacy* and *chilling effects*. Because, generally, people can feel uneasy about services collecting their data and not knowing what happens with that information, and therefore might alter their behaviour if they suspect they are being watched.

Table 11. Factor arrays on privacy.

	F1a	F1b	F2	F3
01. Sharing information is your own choice and responsibility. People voluntarily give up some privacy for the convenience of a safe society.	0	−1	+1	−3
22. The fact that intelligence services have sufficient freedom of movement to function properly is more important to me than that they have some information about me that is otherwise of little interest.	+1	−1	0	−4
42. The fact that targets of the services generally secure their computers well can never justify the privacy risks of hacking civilians that are connected to a target.	−2	−1	−2	+1
56. Our privacy is not really threatened. Details are lost in the huge pile of data that is brought in.	−1	−4	−2	−5
58. People should inform themselves and take steps to protect their privacy if they do not want the government to use their data.	0	0	−1	−3

Though quite focused on privacy issues and risks, Factor 3 is neither explicitly distrusting nor trusting towards the Dutch intelligence services. According to this factor, one should always remain critical of the intelligence services because they make mistakes, and they can see margins of discretion in the law where there are no margins. Participants emphasize how precarious intelligence work can be and that mistakes can have grave consequences. Furthermore, the services are not perceived as self-critical (3: −2). It is described that intelligence practitioners generally have integrity but are also part of a subset of the population that values security over privacy. Therefore, the view of what is reasonable in terms of privacy is not representative of what the average citizen thinks. Nonetheless, Factor 3 does not believe the services would break the law intentionally (54: −2). Participants do think that the services sometimes perceive oversight as difficult, as they are convinced that they are right and that their work is hindered by restrictions set by oversight. Although the factor does not think the services want more power, it does believe they would prefer less oversight and that they often want more than the law allows (5: 0).

Factor 3 emphasizes the role of oversight in mitigating risks and stresses that weakening oversight would lead to hazards in the future. *Subsidiarity* is considered a vital element of the system (18: +4) (Table 12). It is a principle within the Dutch law that intelligence services should first consider the use of less intrusive powers before deploying powers that are regarded as more intrusive. This factor explicitly stresses that 'without the principle of subsidiarity, the end would be near'. Participants believe the intelligence services are 'rather lazy than tired' and that without specific safeguards they would get out of control. An example given is that the intelligence services frequently complain about their administrative burdens, while in fact 'everyone has administrative burdens' and 'such burdens are just part of it'. Checks-and-balances are time consuming, but necessary to allow their far-reaching powers (29: +3, 44: −1).

Table 12. Factor arrays on oversight.

	F1a	F1b	F2	F3
18. The intelligence services must always have tried all less intrusive resources before they start deploying more intrusive resources.	+1	0	+5	+4
29. Oversight creates an administrative burden for the intelligence services, but this is necessary to check the government. While it is a burden now, it ultimately leads to better work and efficiency in the future.	+1	+1	+1	+3

Participants think that oversight and intelligence services should be as independent from politics as possible since services are excellent tools to spy on and suppress opposition and dissenters (32: +2). This might not be a problem currently but can become a problem when there are shifts in the political climate. In contrast to Factor 2, this factor would like oversight to have binding decision powers (55: +2). If oversight deems something unlawful, it should be able to enforce it. Moreover, ex-ante overseers are seen as vital in preventing wrongdoing and mistakes, and therefore should be informed about both acquisition and processing of data to be able to properly assess proportionality (33: +2, 16: −2). According to participants, ex-ante oversight cannot simply be replaced by ex-post oversight, as checking afterwards costs more time and effort, and does not have the same preventative power.

Intelligence services must have good arguments to store bulk datasets. 'You never know whether information might become important' is not a good enough reason, according to Factor 3 (40: +3, 12: −3) (Table 13). The same goes for sharing data with other intelligence services. The services are not in the best position to make decisions about sharing information, because they have significant interests in this. The actual pain of sharing information lies not with the services, but with the people whose data are part of the transaction (6: +1, 24: +1, 45: +3).

Table 13. Factor arrays on bulk data.

	F1a	F1b	F2	F3
12. Bulk data prove their value for research over a longer period. It is also not always known which data will be relevant. This must be included in the determination and review of retention periods and relevance assessments.	+3	−1	+3	−3
45. When data are shared with foreign countries, the services no longer have control over what happens to the data. That is why the Netherlands should not share intelligence with countries that engage in targeted killing.	−1	+1	−3	+3

Factor 3 is neutral on whether certain powers are necessary for intelligence services to have (37: 0, 38: 0). It is reasonable if they can argue why deployment of resources is necessary. Participants agree that resources such as hacking can be very effective (9: +2) (Table 14). This is also what makes the use of powers sensitive and perilous. The participants have reservations about resources that are less targeted, such as strategic hacking and cable interception (48: −3, 47: +1). Moreover, they deem automated data-analysis hazardous, mostly due to the risks of bias and inaccurate results, since AI and algorithms often draw wrong conclusions (7: −4, 28: +3, 35: −2). Lastly, open-source intelligence is considered much more intrusive than people generally think (17: +5). Public data are usually seen as less sensitive, but many people are not aware that public datasets can contain sensitive information. OSINT is deemed justified in trend-based research, but more sensitive for research on targets (34: 0).

Table 14. Factor arrays on intelligence resources.

	F1a	F1b	F2	F3
07. Intelligence services should use automated data analysis (including Artificial Intelligence) as much as possible, as this saves a lot of time and costs and produces accurate results.	0	−3	0	−4
09. Hacking is a wonderful resource for Dutch services because it is very effective.	+5	−2	+3	+2
17. Systematically collecting information from open sources goes far beyond snooping around on Twitter and is more drastic than it seems. This power should also be checked, as the internet is full of sensitive information.	0	+2	+3	+5
28. Automated data analysis is harmful because certain citizens are more likely to be on the radar of the services due to data bias. The chance of errors is high, and people are harmed by this.	0	+3	0	+3
48. The services must also be able to hack strategically to increase knowledge and possibilities, and to acquire a better information position.	+2	−2	+2	−3

5. Discussion

In this study, we used Q-methodology to investigate the various perspectives of professionals in the Dutch intelligence community on the powers of intelligence services and oversight. We examined how their views on trust, privacy, and effectiveness support their perspective. In the previous section, we discussed four factors that represent unique viewpoints on this matter. In this section, we first discuss these findings and then reflect on their implications. Lastly, we include some limitations and conclusions.

5.1. Trust, privacy & effectiveness

First, we observe varying levels of trust between factors that seemingly correspond with different notions of oversight. Factors that display more trust in the intelligence services emphasize checking for mistakes and improving intelligence practices as primary goals. They support giving the services some leeway. Meanwhile, the most distrusting factor, Factor 1b, sees oversight mainly as a gatekeeper to prevent power abuse and as a mechanism to restrict and discipline. Here, extensive regulation is favoured.

Second, we identify contrasting understandings of privacy. While all factors agree on the importance of privacy, they differ in views on what privacy entails and precisely when it is violated. Two main views on privacy are discerned that relate to the debate on privacy as access versus privacy as control.[39] The terminology 'privacy as access' refers to the idea that no invasion of privacy occurs unless information is in fact accessed.[40] Conversely, people who take the 'privacy as control' approach maintain that privacy is invaded when control over information is lost and taken by another party. Thus, while there is agreement that intelligence services are allowed and justified to intrude upon privacy *if* it is proportional, there is disagreement on *when* this is proportional, because people understand privacy and infringement thereupon differently.

Third, the four factors diverge in their views on effectiveness. Effectiveness was mainly addressed in relation to specific intelligence resources, such as hacking and cable interception, and does not seem to align with levels of trust. Factors that found most resources effective, did not share the same level of trust that resources are used properly. Likewise, showing trust did not equal having knowledge about resource effectiveness.

5.2. Implications

As mentioned, we understand trust as impacting the perspectives participants have on oversight and how strict it should be. It relates to the challenge for oversight to strike a balance between oversight that is ineffective and more of a legitimizing 'ritual dance' on the one hand and oversight that is too extensive on the other.[41] In the Dutch case, viewpoints vary on the degree of detail or abstraction ex-ante oversight should have and whether rulings should be binding or not.

In the proposed temporary Cyber Act, the CTIVD is to receive binding decision-making powers. Proponents of this proposal mention that conclusions on legality cannot be disregarded, and if overseers determine that certain datasets must be destroyed, then the services should comply. Opponents consider it undesirable that undemocratically chosen overseers get the ability to overrule a minister from the democratically elected government. They argue that binding decision-making powers affect the independence of oversight bodies, as they would bear partial responsibility for potential consequences. Additionally, binding rulings can exacerbate tensions between intelligence services and oversight bodies, hampering cooperation between stakeholders.

Furthermore, ideas vary on where the weight of oversight should be, ex-ante or ex-post, and on the approach that oversight should take; a more reactive and hands-off or a more 'proactive "police patrol" approach'.[42] Ex-ante oversight is valued for its ability to prevent mistakes and wrongdoing. However, some participants believe that current ex-ante overseers focus excessively on details and adopt a law enforcement perspective that fails to adequately consider the operational reality of intelligence services that lack police powers. Others counterargue that implementation issues are the responsibility of the intelligence services, who prioritize wrongly, do not employ enough manpower, or are 'rather lazy than tired'. Here, information asymmetry between the TIB and services also plays a role.[43] Ex-ante overseers regularly indicate they need more information to properly assess legality, whereas intelligence practitioners feel they cannot always know all the details in advance and provide all nuances in written authorisation requests.[44] Therefore, some participants prefer ex-durante and ex-post oversight by the CTIVD, which can access all information.

Regarding the contrasting understandings of privacy, this fundamental difference in views has been at the root of various disagreements in the implementation of the WIV 2017. Most notable, overseers, taking the 'privacy as control' approach, have denied authorisation for the collection of bulk data through cable interception on multiple occasions. Consequently, use of that power, which inherently involves untargeted bulk data collection, has been permitted only once since it was granted by law.[45] In all other instances, power use was deemed disproportional, insufficiently targeted, and the privacy invasion was considered too great. Coming from a 'privacy as access' viewpoint, the intelligence services disagreed with these decisions, asserting that privacy intrusion depends more on data usage and examination than collection and storage. In another situation, the

services were compelled by the CTIVD and a civil rights organisation to delete various datasets that they had labelled relevant, thereby overruling the minister who had agreed with the services. The CTIVD contended that storing these datasets violated the privacy of the included non-targets, whereas the services insisted that the complete datasets were valuable because they were frequently used as reference work to search for target characteristics.[46]

Much of the discussion revolves around the issues of data collection, storage, and use and its impact on privacy. Interestingly, the WIV 2017 is a power-centred law, meaning that oversight mechanisms are primarily tied to powers. Powers that are generally perceived as more intrusive are subject to stricter oversight. However, participants note that the privacy impact depends on a number of factors, including the content and sensitivity of the information, the purpose of its collection, and how it is used. The underlying assumption in the law is that certain powers, such as hacking and wiretaps, automatically produce the most intrusive intelligence. But other powers, like OSINT, can yield sensitive information too. Therefore, sensitive datasets obtained through 'less intrusive' powers may receive less scrutiny.

As mentioned, effectiveness was mostly discussed in relation to technology. Additionally, the efficiency of the organisation has been a topic of discussion. This discussion mostly pertains to the impact of administrative burdens from oversight on the efficiency of the services. However, we notice that overall effectiveness is left mostly implicit or undiscussed. Organisation effectiveness relates to the question: are intelligence agencies focusing on the rights threats and are they effective in mitigating those threats and/or increasing security? Also undiscussed was the question of who is responsible for reviewing organisation effectiveness. On the one hand, we had not included many statements on organisation effectiveness in the Q-set. This might point to the absence of this topic in the public debate in the Netherlands, since statements were collected from a wide range of open sources. Of course, it might also mean that we missed relevant statements. On the other hand, almost no participants brought up the subject, even when asked whether they missed certain topics in the Q-set. One participant did speak on organisation effectiveness in relation to reprioritisation of threats and other matters. This person also stated that the discussion is not taking place.

Considering the trilemma, as described by Gill,[47] we find this an interesting observation. Gill describes that oversight should address three elements: effectiveness, cost (efficiency), and legality/proportionality.-[48] A difficulty facing oversight is that oversight bodies usually have mandate to look at just one of these elements or, if the mandate includes two or more elements, do not focus on more than one.[49] It seem to be almost impossible to successfully address all three elements. In the Netherlands, external ex-ante and ex-post oversight bodies are mainly concerned with legality and proportionality. The Court of Audit (Algemene Rekenkamer), an independent high council of the state, intermittently reviews the (cost) efficiency of the Dutch intelligence services. Though there has been some attention for organisation effectiveness within parliamentary oversight, this element seems relatively absent otherwise within the Dutch oversight system.[50] Furthermore, parliamentary oversight comes with its own defects, such as a lack of time, expertise, or political will.[51] Additionally, evaluating effectiveness is complicated, as it is difficult to empirically measure to what extent intelligence activities succeed in increasing security.[52]

5.3. Limitations

Our research contains some limitations. First, the sample size of policymakers and professionals from civil society is smaller than preferred. Therefore, we suspect the viewpoints expressed in Factor 1b are underrepresented in our study. Second, it is possible that we have missed certain relevant topics in our Q-set, e.g., statements that more explicitly mentioned organisation effectiveness or topics such as zero-days, public-private cooperation, and intelligence services' role in economic security and mitigating cybercrime. Future work could pay more attention to these subjects. Lastly, it is important to recognize that our study is cross-sectional and that viewpoints are influenced by participants' professional experiences and interests at one point in time. It would be valuable for future studies to also examine the perspectives of non-experts on the balance of oversight and proportionality, perhaps on a more case-specific level.

6. Conclusion

This paper contributes by empirically examining the perspectives of important stakeholders on recent reforms in the Dutch intelligence community and their fundamental views regarding trust, privacy, and effectiveness. It provides insight into how diverging views can be challenging for and affect the implementation of reforms. Furthermore, the paper helps to better understand the difficulties intelligence communities can encounter in their attempts to enhance effectiveness in the cyber domain while maintaining and improving checks-and-balances and privacy compliance.

In conclusion, while the WIV 2017 has expanded and introduced substantial improvements to intelligence oversight, there are still challenges to be addressed. Accommodating the various viewpoints remains a challenge for the reforms, as they are intertwined with issues of trust and diverging fundamental viewpoints. A key focus point should be deciding on a privacy interpretation and the evaluation of data since these topics cause significant disagreements between stakeholders. Similarly, choices must be made on the roles of ex-ante and ex-post oversight bodies, particularly in the unpredictable and ever-changing digital domain. Shifting the focus towards data and reducing emphasis on powers in oversight would be one step forward. Lastly, still more attention can be paid to questions of whether intelligence services are indeed looking at the right threats and are effective in mitigating them, and who is responsible for overseeing this.

Notes

1. Horlings, "Dealing with data".
2. Jaffel and Larsson, *Problematising Intelligence Studies*.
3. Defty, "From Committees of Parliamentarians to Parliamentary Committees"; Dietrich, "Of Toothless Windbags, Blind Guardians and Blunt Swords"; Gee & Patnam, "Small State or Minor Power?"; Walsh, "Australian Intelligence Oversight and Accountability".
4. Howlett, "Moving policy implementation theory forward".
5. Gill, "Of Intelligence Oversight".
6. Defty, "From Committees of Parliamentarians to Parliamentary Committees"; Dietrich, "Of Toothless Windbags, Blind Guardians and Blunt Swords"; Gee & Patnam, "Small State or Minor Power?"; Walsh, "Australian Intelligence Oversight and Accountability".
7. Kininmonth et al., "Privacy Concerns and Acceptance of Government Surveillance in Australia"; Trüdinger and Steckermeier, "Trusting and Controlling?"; Pavone and Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies".
8. Hoffman et al., "Rethinking Intelligence Practices and Processes"; Jaffel and Larsson, *Problematising Intelligence Studies*
9. AIVD, "The Intelligence and Security Services Act 2017".
10. Eijkman et al., *Dutch National Security Reform Under Review*.
11. Winterman, "Sleepwet".
12. Derix and Wassens, "Rekenkamer".
13. Algemene Rekenkamer, *Slagkracht AIVD En MIVD*; Jones-Bos et al., *Evaluatie 2020*.
14. AIVD, "Tijdelijke Wet Cyberoperaties".
15. "Cybersecurity Act Gives AIVD and MIVD More Scope to Act"; Derix and Berkhout, "Een Cyberaanval Is Nu Niet Te Stoppen".
16. Wassens, "Liever Weglakken Dan Anders Opschrijven".
17. Gill, "Of Intelligence Oversight"; Defty, "From Committees of Parliamentarians to Parliamentary Committees"; Dietrich, "Of Toothless Windbags, Blind Guardians and Blunt Swords"; Gee & Patnam, "Small State or Minor Power?"; Walsh, "Australian Intelligence Oversight and Accountability".
18. Aerdts, "Diensten met geheimen".
19. Winterman, "Sleepwet".
20. Kiesraad, "Uitslag Referendum over WIV".
21. Aerdts, "Diensten met geheimen," 185.
22. Ibid.
23. "Cybersecurity Act Gives AIVD and MIVD More Scope to Act".
24. Ibid.
25. For example, Koçak, "Threat Assessment of Terrorist Organizations"; Nederhand et al., "The Governance of Self-Organization"; Norval and Prasopoulou, "Seeing like a Citizen'; Van Eeten, 'Recasting Intractable Policy Issues".

26. Block, "The Q-Sort Method"; Serfass and Sherman, "A Methodological Note".
27. Norval and Prasopoulou, "Seeing like a Citizen," 371.
28. Stenner et al., "Putting the Q into Quality of Life," 2162.
29. Watts and Stenner, Doing Q Methodological Research, 61.
30. Ibid., 72.
31. Ibid., 77.
32. Ibid., 180.
33. Banasick, 'Kade'.
34. Watts and Stenner, Doing Q Methodological Research.
35. Ibid., 105.
36. Ibid.
37. Ibid., 181.
38. Ibid.
39. Macnish, "Government Surveillance"; Königs, "Government Surveillance, Privacy, and Legitimacy".
40. Macnish, "Government Surveillance".
41. Gill, "Of Intelligence Oversight"; Hijzen "More than a Ritual Dance".
42. Gill and Phythian, Intelligence in an Insecure World, 278.
43. Gill, "Of Intelligence Oversight".
44. Derix and Wassens, "Directeuren AIVD En MIVD".
45. AIVD, "jaarverslag 2022".
46. Versteegh and Wassens, "Meeste verzamelde data zijn niet relevant".
47. Gill, "Of Intelligence Oversight".
48. Ibid.
49. Ibid., 974.
50. Dessens et al., Evaluatie.
51. Gill, "Of Intelligence Oversight".
52. Cayford et al., "Plots, Murders, and Money".

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Ministry of the Interior and Kingdom Relations of the Netherlands and Delft University of Technology under Grant M75B07.

Notes on contributors

E.C. Oomens is a PhD candidate at Delft University of Technology, whose research is primarily focused on the perceptions of citizens on the proportionality of intelligence powers. She studied Sociology at Utrecht University.

R.S. van Wegberg is an assistant professor at the Faculty of Technology, Policy and Management of Delft University of Technology, in the Organisation & Governance section.

A.J. Klievink is a Professor of Public Administration at Leiden University, with a special focus on Digitalisation and Public Policy.

M.J.G. van Eeten is a Professor of Public Administration in the Organisation & Governance research group at Delft University of Technology, and a specialist in Internet security.

Ethics statement

This study includes human research participants and has been approved by Delft University of Technology's Human Research Ethics Committee (HREC) prior to the start of the study. All participants have provided written informed consent.

Bibliography

Aerdts, W. *Diensten met Geheimen: Hoe de AIVD en MIVD Nederland veilig houden*. Ambo|Anthos, 2023.

AIVD. "The Intelligence and Security Services Act 2017." Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, October 11, 2019. https://english.aivd.nl/about-aivd/the-intelligence-and-security-services-act-2017.

AIVD. "Tijdelijke Wet Cyberoperaties." Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, December 9, 2022. https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten/tijdelijke-wet-cyberoperaties.

AIVD. "Jaarverslag 2022." Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, April 17, 2023. https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022.

Austin, G., and R. G. Patman. "Small State or Minor Power? New Zealand's Five Eyes Membership, Intelligence Reforms, and Wellington's Response to China's Growing Pacific Role." *Intelligence & National Security* 36, no. 1 (2020): 34–50. doi:10.1080/02684527.2020.1812876.

Banasick, S. "Kade: A Desktop Application for Q Methodology." *Journal of Open Source Software* 4, no. 36 (2019): 1360. doi:10.21105/joss.01360.

Block, J. "The Q-Sort Method in Personality Assessment and Psychiatric Research." (1961). doi:10.1037/13141-000.

Cayford, M., W. Pieters, and C. Hijzen. "Plots, Murders, and Money: Oversight Bodies Evaluating the Effectiveness of Surveillance Technology." *Intelligence & National Security* 33, no. 7 (2018): 999–1021. doi:10.1080/02684527.2018.1487159.

"Cybersecurity Act Gives AIVD and MIVD More Scope to Act, Increases Supervision." Radboud University, September 28, 2022. https://www.ru.nl/en/research/research-news/cybersecurity-act-gives-aivd-and-mivd-more-scope-to-act-increases-supervision.

Defty, A. "From Committees of Parliamentarians to Parliamentary Committees: Comparing Intelligence Oversight Reform in Australia, Canada, New Zealand and the UK." *Intelligence & National Security* 35, no. 3 (2020): 367–384. doi:10.1080/02684527.2020.1732646.

Derix, S., and K. Berkhout. "Een Cyberaanval Is Nu Niet Te Stoppen, Waarschuwt Defensieminister Kamp." *NRC*, January 3, 2022. https://www.nrc.nl/nieuws/2022/01/03/cyberaanval-is-nu-niet-te-stoppen-a4075544.

Derix, S., and R. Wassens. "Directeuren AIVD En MIVD: 'Bij Inlichtingenwerk Weet Je Vaak Niet Waar Je Naar Op Zoek Bent'." May 2, 2021. https://www.nrc.nl/nieuws/2021/05/02/wij-zijn-niet-de-vijand-van-de-burger-a4042138.

Derix, S., and R. Wassens. "Rekenkamer: Geef Aivd En Mivd Meer Geld of Beperk Het Toezicht." April 22, 2021. https://www.nrc.nl/nieuws/2021/04/22/wet-belemmert-werk-diensten-te-veel-a4040999.

Dessens, C. W. M., M. A. Beuving, E. R. Muller, W. Nagtegaal, H. J. I. M. de Rooij, W. M. E. Thomassen, and W. J. M. Voermans Rep. *Evaluatie Wet Op De Inlichtingen- En Veiligheidsdiensten 2002: Naar Een Nieuwe Balans Tussen Bevoegdheden En Waarborgen*, 2013. https://www.aivd.nl/documenten/rapporten/2013/12/02/rapport-commissie-dessens-met-evaluatie-wiv-2002.

Dietrich, J.-H. "Of Toothless Windbags, Blind Guardians and Blunt Swords: The Ongoing Controversy About the Reform of Intelligence Services Oversight in Germany." *Intelligence & National Security* 31, no. 3 (2015): 397–415. doi:10.1080/02684527.2015.1017246.

Eijkman, Q., N. van Eijk, and R. van Schaik. 2018. *Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?* https://www.ivir.nl/publicaties/download/Wiv_2017.pdf.

Gill, P. "Of Intelligence Oversight and the Challenge of Surveillance Corporatism." *Intelligence & National Security* 35, no. 7 (2020): 970–989. doi:10.1080/02684527.2020.1783875.

Gill, P., and M. Phythian. *Intelligence in an Insecure World*. Cambridge, UK: Polity Press, 2020.

Hijzen, C. "More Than a Ritual Dance. the Dutch Practice of Parliamentary Oversight and Control of the Intelligence Community." *Security and Human Rights* 24, no. 3–4 (2014): 227–238. doi:10.1163/18750230-02404002.

Hoffmann, S., N. Chalati, and A. Dogan. "Rethinking Intelligence Practices and Processes: Three Sociological Concepts for the Study of Intelligence." *Intelligence & National Security* 38, no. 3 (2022): 319–338. doi:10.1080/02684527.2022.2113679.

Horlings, T. "Dealing with Data: Coming to Grips with the Information Age in Intelligence Studies Journals." *Intelligence & National Security* 38, no. 3 (2022): 447–469. doi:10.1080/02684527.2022.2104932.

Howlett, M. "Moving Policy Implementation Theory Forward: A Multiple Streams/Critical Juncture Approach." *Public Policy and Administration* 34, no. 4 (2018): 405–430. doi:10.1177/0952076718775791.

Jaffel, H. B., and S. Larsson. *Problematising Intelligence Studies: Towards a New Research Agenda*. Abingdon, Oxon: Routledge, 2022.

Jones-Bos, R. V. M., T. P. L. Bot, E. J. Dommering, L. J. van den Herik, B. P. F. Jacobs, W. Nagtegaal, and S. E. Zijlstra Rep. *Evaluatie 2020 Wet Op De Inlichtingen- En Veiligheidsdiensten 2017*. Evaluatiecommissie 2017, 2021. https://www.rijksoverheid.nl/documenten/rapporten/2021/01/20/rapport-evaluatie-2020-wet-op-de-inlichtingen-en-veiligheidsdiensten-2017.

Kiesraad. "Uitslag Referendum over WIV: Meerderheid Tegen." Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, April 3, 2018. https://www.kiesraad.nl/actueel/nieuws/2018/03/29/uitslag-referendum-over-wiv-meerderheid-tegen.

Kininmonth, J., N. Thompson, T. McGill, and A. Bunn. "Privacy Concerns and Acceptance of Government Surveillance in Australia." *Australasian Conference on Information Systems 2018*, 2018. 10.5130/acis2018.cn.

Koçak, M. "Threat Assessment of Terrorist Organizations: The Application of Q Methodology." *Journal of Risk Research* 15, no. 1 (2012): 85–105. doi:10.1080/13669877.2011.601323.

Königs, P. "Government Surveillance, Privacy, and Legitimacy." *Philosophy & Technology* 35, no. 1 (2022). doi:10.1007/s13347-022-00503-9.

Macnish, K. "Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World." *Journal of Applied Philosophy* 35, no. 2 (2016): 417–432. doi:10.1111/japp.12219.

Nederhand, J., E.-H. Klijn, M. van der Steen, and M. van Twist. "The Governance of Self-Organization: Which Governance Strategy Do Policy Officials and Citizens Prefer?" *Policy Sciences* 52, no. 2 (2018): 233–253. doi:10.1007/s11077-018-9342-4.

Norval, A., and E. Prasopoulou. "Seeing Like a Citizen: Exploring Public Views of Biometrics." *Political Studies* 67, no. 2 (2018): 367–387. doi:10.1177/0032321718766736.

Pavone, V., and S. Degli Esposti. "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off Between Privacy and Security." *Public Understanding of Science* 21, no. 5 (2010): 556–572. doi:10.1177/0963662510376886.

Rekenkamer, A., Rep. *Slagkracht AIVD En MIVD: De Wet Dwingt, De Tijd Dringt*, *De Praktijk Wringt*, 2021. https://www.rekenkamer.nl/publicaties/rapporten/2021/04/22/slagkracht-aivd-en-mivd.

Serfass, D. G., and R. A. Sherman. "A Methodological Note on Ordered Q-Sort Ratings." *Journal of Research in Personality* 47, no. 6 (2013): 853–858. doi:10.1016/j.jrp.2013.08.013.

Stenner, P. H. D., D. Cooper, and S. M. Skevington. "Putting the Q into Quality of Life; the Identification of Subjective Constructions of Health-Related Quality of Life Using Q Methodology." *Social Science & Medicine* 57, no. 11 (2003): 2161–2172. doi:10.1016/s0277-9536(03)00070-4.

Trüdinger, E.-M., and L. C. Steckermeier. "Trusting and Controlling? Political Trust, Information and Acceptance of Surveillance Policies: The Case of Germany." *Government Information Quarterly* 34, no. 3 (2017): 421–433. doi:10.1016/j.giq.2017.07.003.

van Eeten, M. J. G. "Recasting Intractable Policy Issues: The Wider Implications of the Netherlands Civil Aviation Controversy." *Journal of Policy Analysis and Management* 20, no. 3 (2001): 391–414. doi:10.1002/pam.1000.

Versteegh, K., and R. Wassens. "Toezichthouder inlichtingendiensten: 'Meeste verzamelde data zijn niet relevant'." *NRC*, June 14, 2022. https://www.nrc.nl/nieuws/2022/06/14/meeste-verzamelde-data-zijn-niet-relevant-a4133462.

Walsh, P. F. "Australian Intelligence Oversight and Accountability: Efficacy and Contemporary Challenges." *Intelligence & National Security* 37, no. 7 (2022): 968–984. doi:10.1080/02684527.2022.2095602.

Wassens, R. "Liever Weglakken Dan Anders Opschrijven." *NRC*, April 15, 2022. https://www.nrc.nl/nieuws/2022/04/15/liever-weglakken-dan-anders-opschrijven-2-a4113891.

Watts, S., and P. Stenner. *Doing Q Methodological Research: Theory, Method and Interpretation*. Los Angeles, California: Sage, 2012. doi:10.4135/9781446251911.

Winterman, P. "Sleepwet: Vijf Voor- En Tegenstanders." Algemeen Dagblad, March 21, 2018. https://www.ad.nl/politiek/sleepwet-vijf-voor-en-tegenstanders~a0ea061b/.

Appendix A

Table A1. Factor array for each factor.

	Factor arrays			
Item number and wording	F1a	F1b	F2	F3
01. Sharing information is your own choice and responsibility. People voluntarily give up some privacy for the convenience of a safe society.	0	−1	+1	−3
02. Privacy online does not exist. The government has been collecting data for years. If one wants to maintain complete privacy, the only option is to get off the internet.	0	0	−1	+2
03. One can safely trust the Dutch intelligence and security services. I believe that they work purposeful, self-critically, and with integrity.	+2	−2	+2	−2
04. Nosing around on social media by the Dutch intelligence and security services is almost always justified.	+4	−2	−1	−1
05. The Dutch intelligence and security services prefer to go about their business without oversight. They want more power, and this goes against the will of the Dutch people.	−5	+5	−5	0
06. Oversight should know in advance if data are shared with foreign countries. In retrospect they can say: 'You shouldn't have done that'. But then the damage is already done.	−2	+1	+1	+1
07. Intelligence services should use automated data analysis (including Artificial Intelligence) as much as possible, as this saves a lot of time and costs and produces accurate results.	0	−3	0	−4
08. Installing backdoors in the encryption of WhatsApp, for example, leads to a general weakening of security and makes users vulnerable to damage by hackers and criminals.	+3	+4	+4	+4
09. Hacking is a wonderful resource for Dutch services because it is very effective.	+5	−2	+3	+2
10. Intelligence services can do a lot with malware; from stealthily infiltrating networks and stealing data to active sabotage. This makes placing malware an effective means that should be used as much as possible.	+2	−3	0	−2
11. Wiretapping is an expensive, invasive, and labour-intensive resource and should be used as little as possible. Eavesdropping on someone 24/7 produces a mountain of data, which all must be analysed with the chance that there is nothing useful in the data.	−2	0	−1	0
12. Bulk data prove their value for research over a longer period. It is also not always known which data will be relevant. This must be included in the determination and review of retention periods and relevance assessments.	+3	−1	+3	−3
13. The legal distinction between metadata and content must be abandoned, for metadata can also seriously infringe privacy.	−2	+1	+3	+1
14. Most communications are of no interest to intelligence services. Collecting some communication data from large groups of people therefore does not mean that intelligence services actively monitor all those people.	+1	0	+2	−1
15. The services must be able to circumvent strong security, for example by hacking people who are in contact with a target to gain entry to the target.	+3	0	+2	0
16. In intelligence work it is often unclear what people are looking for, which is why the services cannot assess in advance and declare to oversight how data will be used, and which data will prove useful.	−1	0	0	−2
17. Systematically collecting information from open sources goes far beyond snooping around on Twitter and is more drastic than it seems. This power should also be checked, as the internet is full of sensitive information.	0	+2	+3	+5
18. The intelligence services must always have tried all less intrusive resources before they start deploying more intrusive resources.	+1	0	+5	+4
19. It is better to achieve a result with as few resources as possible, because this saves time and money. The financial costs and efficiency of deploying a resource must also be included in the TIB's assessment.	−3	−1	−2	−3
20. Even if one is not doing anything wrong, one is being watched and spied on.	−4	+2	−3	+1
21. People just shouldn't be on an extreme web forum, and they certainly shouldn't think they're not being watched there.	0	0	−2	−1
22. The fact that intelligence services have sufficient freedom of movement to function properly is more important to me than that they have some information about me that is otherwise of little interest.	+1	−1	0	−4
23. All bulk data sets should meet the same requirements in terms of retention periods and relevance assessments, regardless of the type of data the set contains and with what authority the data was collected.	−2	+1	0	−1
24. It is worrying if the Dutch intelligence services can exchange unevaluated data with foreign services without permission from oversight.	0	+4	+3	+2
25. Disruption and sabotage by intelligence services is harmful because they actively launch the attack and thereby invite hostile parties to do the same.	−2	+2	0	−1
26. There is much criticism of cable interception, and the intelligence services hardly make use of this far-reaching power. There is no need for them to have this resource.	−3	+2	−3	−1
27. Stricter limits must be set on the data hunger of the secret services, which are now not limited by regulations. They collect more data than they can handle and keep the data longer than allowed.	−3	+3	−2	+1
28. Automated data analysis is harmful because certain citizens are more likely to be on the radar of the services due to data bias. The chance of errors is high, and people are harmed by this.	0	+3	0	+3

(*Continued*)

Table A1. (Continued).

	Factor arrays			
Item number and wording	F1a	F1b	F2	F3
29. Oversight creates an administrative burden for the intelligence services, but this is necessary to check the government. While it is a burden now, it ultimately leads to better work and efficiency in the future.	+1	+1	+1	+3
30. Security is the most important condition for freedom. There is no option but to sacrifice a small amount of personal privacy for the safety of society. The end justifies the means.	+1	−2	+1	−2
31. There should be more safeguards for a dataset retrieved with a more intrusive intelligence resource than for a dataset with more sensitive content retrieved with a less intrusive intelligence resource.	−1	−2	−1	−2
32. The Dutch intelligence and security services and oversight should operate completely independent from politics. Political colour has no place in intelligence gathering.	+3	−2	+2	+2
33. To be able to test proportionality, the TIB must be able to take everything into account. The TIB cannot do its job if it can only look at the collection of data and not at how the data is subsequently processed.	0	+3	−1	+2
34. The Dutch intelligence and security services may have unlimited access to open sources, as ordinary citizens and journalists also have unlimited access.	+2	−3	−3	0
35. Automated data analysis is a non-intrusive and targeted means, because it allows intelligence agencies to extract accurately and quickly the information they are looking for from data they already possess.	0	−3	0	−2
36. Hacking isn't all that precise and effective. In addition, large data files are gathered, and a hack can lead to unacceptable collateral damage.	−1	+2	−1	0
37. Placing malware is necessary in many cyber operations to be able to spy unnoticed and obtain information from a target.	+2	0	+1	0
38. The wiretap resource is extremely suitable for monitoring individuals in a targeted manner.	0	0	+2	0
39. Via informants, the services can gain access to large data sets (such as passenger lists of the Marechaussee) without prior authorisation from oversight. There should be more checks.	+1	+3	+2	+2
40. Bulk data should only be kept when necessary. No data should be kept just because it might be useful later.	−1	+3	−3	+3
41. Protecting citizens' privacy is at least as important as protecting national security.	+2	+1	+4	+3
42. The fact that targets of the services generally secure their computers well can never justify the privacy risks of hacking civilians that are connected to a target.	−2	−1	−2	+1
43. Hacking a web forum where state-undermining activities take place, whereby the intelligence service obtains the data of all users, is sufficiently targeted and within the law.	+2	−1	0	0
44. Administrative burdens resulting from oversight should not hinder the efficiency and effectiveness of the services. Paperwork should not be an obstacle to conducting research in the interest of national security.	+3	−4	+1	−1
45. When data are shared with foreign countries, the services no longer have control over what happens to the data. That is why the Netherlands should not share intelligence with countries that engage in targeted killing.	−1	+1	−3	+3
46. Intelligence services must be able to perform a bulk hack to not be noticed if the use of a less intrusive resource would be noticed, even though this constitutes a greater invasion of privacy.	0	−3	0	0
47. Cable interception is a less effective resource than thought, because the amount of data traffic is increasing and much communication is encrypted.	−1	−1	0	+1
48. The services must also be able to hack strategically to increase knowledge and possibilities, and to acquire a better information position.	+2	−2	+2	−3
49. Big data does not prevent attacks, because intelligence services do not have the capacity to analyse it and such data has rarely revealed anything that they could not have known otherwise.	−3	−1	−2	0
50. The problem of cable interception: One is going to find a lot. But in there might be half a terrorist.	−1	+1	+1	−1
51. Data that is not related to targets of the services are not and will not be relevant to their job duties. A relevance assessment should therefore be detailed, and irrelevant data should be discarded immediately.	−2	−1	0	+1
52. Intelligence agencies can wiretap and hack entire neighbourhoods. In this way, every innocent citizen is potentially 'suspicious' without concrete reason to follow that citizen. The services should only spy on suspects.	−3	+1	−4	0
53. It is good that Dutch communication services are obliged to supply data and to cooperate if our intelligence services want to wiretap or hack targets.	+4	0	+1	0
54. The Dutch intelligence services will regularly break the law if they deem it necessary.	−4	+2	−4	−2
55. Quantity of oversight is not the same as quality. Good oversight is binding and effective. The TIB and CTIVD should have binding powers that they can use on their own initiative.	−1	+2	−2	+2
56. Our privacy is not really threatened. Details are lost in the huge pile of data that is brought in.	−1	−4	−2	−5
57. The AIVD and MIVD must cooperate more and better, both with each other and internationally. Intelligence services could also talk to countries with which they are cold politically or diplomatically.	+1	0	+1	+1
58. People should inform themselves and take steps to protect their privacy if they do not want the government to use their data.	0	0	−1	−3
59. One can assume that when collecting intelligence, the intelligence services are careful with the privacy of people who have no intention of harm.	+1	−5	−1	−1
60. Wiretapping is not that effective at all. Malicious persons know that they can be wiretapped and adjust their behaviour accordingly.	−1	+1	−1	+1

Appendix B

Table A2. Factor correlations.

Factor	1a	1b	2	3	Variance explained (%)	Number of coefficients > 0.35
1a	1.000	−0.4763	0.6510	0.0363	30	9
1b		1.000	−0.0925	0.5638		1
2			1.000	0.2458	14	9
3				1.000	6	7

Appendix C

Table A3. Factor loadings per participant.

	F1a	F1b	F2	F3		F1a	F1b	F2	F3
P1	0,63*	−0,63	0,47	−0,01	*P14*	0,02	−0,02	−0,02	0,62*
P2	0,61*	−0,61	0,36	−0,22	*P15*	0,07	−0,07	0,11	0,69*
P3	0,68*	−0,68	0,46	−0,03	*P16*	0,05	−0,05	0,10	0,63*
P4	0,56*	−0,56	0,47	0,06	*P17*	0,52	−0,52	0,55*	0,10
P5	0,05	−0,05	0,60*	0,23	*P18*	−0,29	0,29	0,41	0,53*
P6	0,12	−0,12	0,45*	0,06	*P19*	0,25	−0,25	−0,11	0,56*
P7	0,15	−0,15	0,60*	0,26	*P20*	0,84*	−0,84	0,18	0,04
P8	−0,63	0,63*	0,11	0,59	*P21*	0,72*	−0,72	0,08	0,43
P9	0,19	−0,19	0,52*	0,19	*P22*	0,25	−0,25	0,68*	−0,04
P10	0,49	−0,49	0,54*	−0,08	*P23*	0,46*	−0,46	0,12	0,02
P11	−0,07	0,07	0,20	0,42*	*P24*	0,73*	−0,73	0,18	−0,07
P12	0,67*	−0,67	0,26	0,04	*P25*	−0,46	0,46	0,22	0,59*
P13	0,19	−0,19	0,72*	0,02	*P26*	0,44	−0,44	0,51*	0,06

P1-P26 = participants; F1a-F3 = factors; loadings marked with an asterisk (*) are significant at $p < 0.005$ with majority of common variance required.