Digital resiliency of high-profile individuals in the light of modern hybrid threats: To what extent is Cyber Hygiene enough to protect high-profile individuals against the hybrid risks they face?

Kooij, Kim van der

Universiteit Leiden
The Netherlands

Digital resiliency of high-profile individuals in the light of modern hybrid threats

To what extent is Cyber Hygiene enough to protect high-profile individuals against the hybrid risks they face?

Kim van der Kooij-Turk

January 2024

Thesis Supervisors
Dr Tommy van Steen, Universiteit Leiden
Dr Tanya Tropina, Universiteit Leiden

Intentionally left blank.

Abstract

The main question this thesis attempts to answer is: To what extent is Cyber Hygiene enough to protect high-profile individuals against the hybrid risks they face?

Based on our research, we have defined the following 8 categories of high-profile individuals: public safety personnel, port personnel, politicians and government officials, civil servants, legal professionals, media contributors, scientists and representatives of interest groups.

These high-profile individuals; 1) represent or symbolize an organisation or institution; *2)* have access to an organisation's 'crown jewels' (critical assets/targets); 3) or (access to) power; and are, therefore, specifically interesting to various threat actors. It is not about task-oriented threats, threats by acquaintances nor about indiscriminate victims of threats of violence.

There is an increase in individual threat levels, these threats increase in nature, severity and quantity. In this regard, there appears to be structural incidentalism. The threats high-profile individuals face nowadays are quite diverse. We have identified the most common threats we have encountered in our research into a model, distinguishing between expressive and instrumental threats and their manifestations, whether they are physical or digital. All our described threats are currently used against high-profile individuals, have (potential) physical or informational consequences, and are all intentional.

In the context of threats to high-risk individuals, we see the following threat actors: 1) angry citizens (with or without *underlying mental health issues), 2) hacktivists, 3) extremism and terrorism, 4) organised crime, 5) insider threats and 6) State (sponsored) actors.* If, in the future, threat actors would expand their TTPs, and, for example, make greater use of resources available to State (sponsored) actors. Then digital and hybrid threats could increase significantly in both severity and scale, with potentially very dangerous consequences. Not only for the high-profile individuals themselves, but also in maintaining our legal order.

Cyber hygiene encompasses the habits and precautions users or organisations can implement to ensure that sensitive data remains organised, secure, and protected against theft and external attacks. Cyber hygiene is frequently compared to personal hygiene. Just as individuals adopt specific personal hygiene routines to uphold good health and well-being, cyber hygiene practices safeguard and maintain data security. Our research concludes that Cyber Hygiene, particularly Vishwanath's (2020) Cyber Hygiene Inventory, does not provide sufficient measures to protect high-profile individuals from contemporary physical, digital and hybrid threats. Keeping high-profile individuals resilient in the future requires not only additional measures but also a different approach and more research.

Key words: High-profile individuals – Security Awareness – Cyber Hygiene – Digital threats – Hybrid threats

Acknowledgements

First of all, I would like to thank all the (guest) lecturers who provided our Executive Master Cybersecurity, for your expertise, inspiration and discussions. I really enjoyed going to the University every Friday, and the past two years have flown by.

In particular, I would like to thank my two supervisors. Thank you, Dr Tommy van Steen, for your trust, honesty, knowledge, pushback, support, brainstorming and humour during the thesis process. And Dr Tanya Tropina, the way you can convey (theoretical) knowledge about *'regulating security in cyberspace'* in a way that many students still think about weekly is a special talent. Thank you both for your feedback.

Thanks are also due to all experts interviewed. Without their input, this research would never have yielded such great insights.

I would also like to thank my employer, the House of Representatives, for the opportunity to follow this programme. In particular, I would like to thank our former CISO, Rik Driessen, for his encouragement and boundless faith in me.

Not only the lecturers gave colour and meaning to our programme, but also all my fellow students. In particular, I would like to thank Maarten, Maaike and Nynke. Thank you, for your 24/7 support, humour and care.

My parents and brother have always encouraged and supported me to follow my own path. Thank you!

Dear Eva and Fiene, may you be able to do everything you dream of later in life, in such a manner that safety, or the fact that you are a woman will not make any difference in succeeding.

And Marcel, I could never have done this without you. Thanks for your love and support and for making sure everything ran smoothly at home. You are always there for me.

Preface

In 2020, in the week of the national elections, I started working as Security Awareness Officer at The House of Representatives. As a-former- Information Security Officer I was used to working with excessive cybersecurity frameworks, that have clear requirements for security measures, are holistic and adaptable to organisation types and threat levels. So one of my first questions to colleagues and security partners was; 'What digital measures do Members of Parliament have to take to stay secure?"

However, there are many useful lists and methods to reduce human risk in the field of user awareness, but these are all quite general. And no, there seemed to be no all-inclusive list with digital security measures for our specific high-profile target group with above-average and diverse threats.

In the following years, Members of Parliament were threatened more and more, digitally, physically and hybrid. At the same time, I have noticed that in the last years more and more functionaries and occupational groups within society are being threatened digital, physical or hybrid. Because they represent an organisation or institution, they have access to (confidential or sensitive) information or access to power. At the same time, the whole surveillance and security system in the Netherlands focuses on someone's physical integrity.

More and more news articles appeared around certain occupational groups that have received more threats 'than ever before'. These individuals are threatened primarily because of their specific profession, but the threats are specifically directed at the individual. These threats can be digital, physical or hybrid and can violate an individual's personal privacy. Threat actors behind these threats vary from State (sponsored) actors, criminals, hacktivists, and terrorists. However, this phenomenon of growing hybrid threats towards broadening group of individuals is not really considered as a broader societal problem.

In this thesis, I will try to zoom out and understand which professional groups in society are increasingly threatened, by which actors, and in what ways. What are the common denominators between these 'high-profile individuals' and what do they need to better protect themselves sufficiently digitally? While many threats still have a physical nature, they often start digitally. A hate mail, a threatening post on social media or a threat actor using Open-Source Intelligence to find a potential victim's personal information online.

Is basic digital hygiene sufficient for these target group(s) to protect themselves from contemporary hybrid threats? Or does this group, or specific groups within, need additional measures to stay secure?

Table of Contents

Figures

Tables

1 Introduction

Last years, the media increasingly covered certain groups of professionals who have received more threats than before, or cases of threatened individuals were highlighted. These threatened individuals, seem to be threatened because of their specific position in an organisation. So far, the group 'high-profile individuals' is not a defined and described group within scientific literature concerning cybersecurity.

Unjustified, by focusing on either individuals or organisations, one almost denies that certain individuals – representing an organisation or institution, having access to an organisation's 'crown jewels' or power – are therefore specifically interesting to various threat actors.

1.1 The research problem

These threats often violate *high-profile individuals* in their personal privacy, and can be digital, physical or hybrid. Threat actors behind these threats vary from State (sponsored) actors to criminals, hacktivists, and terrorists. To illustrate this, we have a few examples:

- In 2019, a man was sentenced to 10 years in prison for preparing a terrorist attack on MP Geert Wilders. The defendant wanted to murder the politician for holding a controversial cartoon contest.[1]
- In 2021, Turkish hackers claimed the temporary take-down[2] of the websites of Dutch politician and European Parliament's former rapporteur on Turkey Kati Piri and the website of the Labour Party after Piri called on Turkey to release political prisoners.
  And during demonstrations the Dutch police works with incognito policemen to pick out instigators of riots, these policemen are called Romeos. However, on social media, they are accused of starting riots themselves to cast the demonstration in a bad light and justify a harsh intervention by the government. As a result, radical activists call for the unmasking of Romeos. Videos, names and even addresses of these Police officers were spread online[3].
- Minister of Finance Sigrid Kaag, was visited in 2022 at her home by a man with a burning torch.[4]
- In 2023 Employees of the Rutgers Sexuality Expertise Centre were threatened because of taking out of context and twisting their teaching materials for Spring Fling Week. Police had to monitor troublemakers on social media[5], safety measures were taken to protect employees working outside the headquarter.
  In the same year, the National Criminal Investigation Department director declared that corrupting public officials became a business model for criminals; "*It used to be that a criminal and a civil servant knew each other, for example from school or the neighbourhood. And that relationship would lead to corruption or information leaks. Now we see criminal intermediaries deliberately and actively searching for officials to corrupt.*"[6]

Sometimes (sub)problems that touch on this subject are referred to as "online hate" or "online thugs" (NL: online hufters), or some professional groups are bundled together. The latter happens, for example, around anti-institutional extremism (AIVD, 2023), or recently when the Senate voted for the first bill around criminalizing doxing. After the passage of this law the Minister of Justice and Security reacted: "*From our emergency workers, police officers and others who work in any way for our free society stay away! Spreading private information to frighten another is truly unacceptable. Journalists, scientists and politicians should always be able to speak freely. That families no longer feel safe at home is something we cannot and must not accept.*"[7]

But rarely does one zoom out and look at the bigger picture. What connects all these professional 'target groups'? Who are the threat actors, what motivates them, and how do they threaten these individuals? And what do these *high-profile individuals* have to do to adequately protect themselves from (future) threats at a digital level?

[1] https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2019:5877
[2] https://twitter.com/ankaofficialtr/status/1360611894785167366
[3] www.nrc.nl%2Fnieuws%2F2022%2F07%2F05%2Fcorona-activist-jan-b-opgepakt-wegens-bedreiging-van-agenten-a4135621
[4] https://nos.nl/artikel/2440772-man-die-met-brandende-fakkel-bij-huis-van-kaag-stond-opnieuw-opgepakt
[5] https://nos.nl/artikel/2469670-ondanks-onrust-meer-voorlichtingslessen-gegeven-in-week-van-de-lentekriebels
[6] https://www.nrc.nl/nieuws/2023/05/08/een-integere-overheid-is-geen-vanzelfsprekendheid-zegt-de-baas-van-de-rijksrecherche-a4164146
[7] https://www.rijksoverheid.nl/actueel/nieuws/2023/07/12/gebruik-van-persoonsgegevens-met-als-doel-intimidatie-wordt-strafbaar

1.2 Research questions

The main question of this thesis attempts to answer the following exploratory research question: ***To what extent is cyber hygiene enough to protect high-profile individuals against the hybrid risks they face?***

To answer this question, we break it up into demarcated sub-questions:

1. Who are high-profile individuals?
2. What are the threats & threat actors for this specific group?
3. What is Cyber Hygiene?
4. To what extent is there a gap between Cyber Hygiene-measures and the security measures needed to protect high-profile individuals against current threats?
5. Are additional measures needed to make these individuals more digitally resilient?

1.2.1 Research choices and limitations

In this thesis, we focus on threats that manifested in The Netherlands between 2000 and 2023. We start our research in 2000 because Dutch people started using the internet *en masse* after the introduction of ADSL[8]. And focuses on threats that are directed specifically towards individuals (in their private personal or business life) because of his or her function. These threats are not task-oriented nor part of another incident of violence (e.g. threats expressed during a robbery). In addition, we have strived to include only publicly available information in this thesis so that the thesis itself can be made public.

We do not aim to give exact numbers about threats. Nevertheless, we are trying to make meaningful statements about any increase or decrease, based on a literature review and qualitative research. Quantifying the phenomenon of threats proves problematic. Statistics regarding threats are often based on samples and surveys; these figures provide only feint accuracy, according to Bovenkerk (2005, p. 4).

1.3 Justification

Mapping the group of high-profile individuals and researching threats, threat actors and security measures needed to keep 'high-profile individuals' digitally resilient, has relevance for society, for science in the field of cyber security, and the industry.

1.3.1 Societal Relevance

Threats on *'high-profile individuals'* undermine our democratic legal order. The feelings of fear or anxiety that a threat may cause the functionary or those around him may cause one to experience societal limitations in thought, action, and movement (AIVD, 2023; Bovenkerk, 2005; Kuiper, 2018). To keep our country, and democratic legal order, resilient against current threats and threat actors it might be necessary for *'high-profile individuals'* to take additional security measures to get the degree of digital resilience at the appropriate level. A more widespread problem also requires a more comprehensive approach. In which the government, employers and individuals must take their responsibility. And for a long time, and for understandable reasons, focus has been on physical threats toward high-profile individuals. Anno 2023, it is time for widening this perspective.

1.3.2 Scientific and Industry Relevance

This thesis shows that the current approach to cybersecurity awareness, which (sometimes) distinguishes between roles within an organisation, should be more differentiated. How certain individuals within an organisation are viewed by the outside world, because of their role or function should be decisive in determining the right awareness approach and defining adequate security measures. Since functionaries are often affected in their private lives when they are threatened, the focus of security measures should perhaps be different than it has been in the past. Thereby, it will be interesting to find out whether the targeted group is targeted by other threat actors, with different Modus Operandi, and whether threats have a hybrid nature. And foremost, what do these individuals have to do to stay (digitally)resilient?

[8] https://www.kpn.com/zakelijk/blog/internet-wifi-nederland-geschiedenis.htm

2 Literature review

To answer our research question, '*To what extent is cyber hygiene enough to protect high-profile individuals against the hybrid risks they face?*' we must first further explain the key concepts that constitute the question, based on a literature review.

In 2.1 we will start by defining the group '*high-profile individuals*', and describe how threats towards them developed over time. Then we will outline in 2.2 what threats this specific group faces and which threat actors are behind. What Cyber Hygiene is, will be defined in 2.3. Based on this review, we assess whether we have enough information to answer to what extent there is a gap between Cyber Hygiene - measures and the needed measures to protect against current hybrid threats or whether additional measures are needed.

We try to approach these themes separately from each other as much as possible, but sometimes they intertwine.

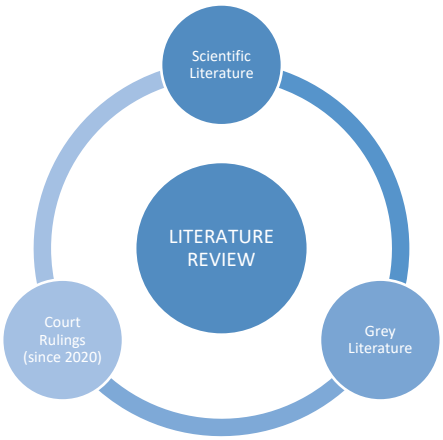


Figure 1 - Research Sources Target Group (Source: created by author)

2.1 High-profile individuals

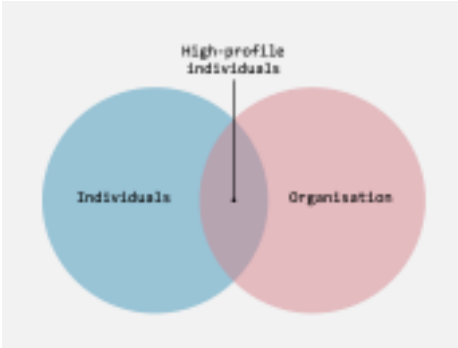


Figure 1 - High-profile individuals (Source: created by author)

The starting point of this literature review is the targeted group. Who are *high-profile individuals*? This group is-so far- not a defined and described group within scientific literature in relation to cybersecurity. Unjustified, because by focusing on either individuals or organisations, one almost denies that certain individuals – representing an organisation or institution, having access to an organisation's 'crown jewels' or power – are therefore specifically interesting to various threat actors.

The first step of our research is to get a better picture of the threatened *'high-profile individuals'*. In order to get the broadest possible picture of this group, we used scientific and grey literature, and various news articles or reports on threats in specific occupational groups. In addition, we reviewed the judgments of judges regarding threats after 2020. When a judgement revealed a new "target group," that was reason for further research in too news articles, and literature, and vice versa.

There is a body of previously conducted scientific research on threats in general or on specific occupational groups. Most of them focus on the development of threats and harassment, some on specific occupational groups or combinations of them (like 'public figures', and some articles dive deeper into specific aspects of threats, like psychological consequences, intervention opportunities, or offenders' 'willingness to take action'. We have focused on scientific literature that was written after the year 2000 and conducted our searches with Google Scholar and we have used the database of the University Leiden library.

We will start with the major overarching scientific studies about threats (towards individuals) in the Netherlands, then we will examine case law and news articles to verify that our overview of possible targeting is complete and current. Finally we will define who we see as 'high-profile individuals'.

2.1.1 Scientific research on threats to occupational groups and functionaries

One of the first extensive studies on threats to individuals in the Netherlands was conducted by Driessen and Middelhoven (2001), and was commissioned by the Dutch Ministry of the Interior and Kingdom Relations and the Ministry of Justice. At the start of this century, social concern about violence increased; however, there was uncertainty about the extent and development of violence. This also applies to violence against workers who work in public spaces or in areas freely accessible to the public, such as stores, hospitals or trains (Middelhoven &

Driessen, 2001). This study involved a very broad target group, which we have rarely seen again in similar studies since.

The study results showed that the extent of violence against employees in (semi-)public spaces is significant. On one hand, they observed verbal forms of violence, such as swearing and sexual and discriminatory remarks. On the other hand, these individuals experienced physical violence, such as spitting, physical hindering, hitting and so on. Notable was the finding that this is true for occupational groups for which dealing with violence is traditionally part of the job (task-oriented), such as police officers and prison employees, but it is equally true for occupational groups for which dealing with violence is not part of the job, such as train conductors and hospital employees. Digital threats, even threats via e-mail or social media were not yet part of this research.

After a broad inventory of professional groups, a list of selection criteria was used to make a selection of professional groups for which deeper research was conducted.

Table 1 - Inventoried occupational groups in the (semi-)public space (Middelhoven & Driessen, 2001)

Personnel whose task is (partly) to supervise compliance with rules and, if necessary, to enforce compliance.	***Healthcare & emergency personnel.***	***The third category concerns other service personnel (also commercial).***
Police officers Penitentiary Employees Public transport personnel Bailiffs Inspectors and auditors Social service employees	General practitioners Hospital employees Psychiatry employees Home care Addiction care workers Social workers Psycho-social workers, etc.	Housing corporation staff Sales staff Catering staff Teachers Bank employees Prostitutes Cab drivers Lawyers Postal workers, deliverers Fairground operators

Shortly after this study was published, in 2002, the phenomenon of threats on public figures suddenly grew significantly in the Netherlands. During this period, political party list leader Pim Fortuyn entered the political stage, and in his election campaign he strongly criticized the established order. This unleashed something within society. A broad spectrum of politicians were threatened and several politicians were forced to take drastic security measures in this period (Bovenkerk, 2005, p. 6).

In addition to politicians, other prominent figures were threatened during this period, some decided to withdraw from public life after this, others came (temporarily) under police surveillance, received bullet letters or had to shelter in safe houses. These threats, from various threat actors, were directed at mayors, aldermen, prosecutors, judges, lawyers, journalists and columnists. And even prominent sportsmen, scientists, artists and representatives of interest groups (Bovenkerk, 2005, p. 7). These 'public' persons received threats by e-mail, letters (some accompanied with suspicious 'powder' or bullets) or via phone. Some were harassed in public, by getting a pie smashed in their faces, for example. But most threats were anonymous and dismissed as a sign of "lack of civilization" (Bovenkerk, 2005).

That changed when Pim Fortuyn was assassinated on May 6, 2002 and more than two years later, the outspoken columnist and artist Theo van Gogh, was murdered. The view until then, in criminological science, was that '*barking dogs don't bite*'. Threats were rarely followed up by a physical act (Bovenkerk, 2005; Kuiper, 2018; Meloy et al., 2004) and although both in the murder of Fortuyn and van Gogh, it appears that the ultimate perpetrators themselves had not threatened before their violent act (Adviescommissie toekomstbestendig stelsel bewaken en beveiligen, 2021; Bovenkerk, 2005, p. 8). Yet the perception after these events in the Netherlands is a different one: violent threats can actually lead to extreme violence, whether by the same perpetrator or not (Bovenkerk, 2005, p. 8). Until this horrible event, there was little support in our country for setting up a system of personal security to which, in principle, any seriously threatened Dutch citizen could be entitled (Schuurman et al., 2021, p. 6)

In his study, Bovenkerk focussed on threats regarding (individuals working in) public administration, the police, lawyers, judges and prosecutors, journalists and notaries. Bovenkerk (2005, p. 28) shows in his research that threats on public figures, even with physical consequences and/or entering the private sphere, have existed for decades. He gives examples of various home visits to politicians, with diverse consequences. These consequences varied from digging up gardens to threats of extreme violence. There were, for example, bomb attacks on the official residence of the mayor of Amsterdam in 1985, the 1991 bombing of Secretary of State Kosto's home, or

the attack on the caucus of the Centre-Democrats with firebombs, in which the political party list leader's wife lost a leg (Adviescommissie toekomstbestendig stelsel bewaken en beveiligen (2021), p. 5).

Partly as a result of lessons learned after the assassination of Fortuyn, the National Surveillance and Protection System was thoroughly reformed in 2003. As a result of this reform, the Royal and Diplomatic Protection Service (DKDB) and the National Police Services Agency (KLPD) were significantly expanded. The basic principles formulated at the time are still being used (Schuurman et al., 2021, p. 7): 1) An individual's own responsibility for guarding and security is the starting point; 2) the emphasis on specific (diplomatic) persons and objects disappears; and 3) persons who personify the democratic constitutional state (ministers, party chairmen, magistrates) fall under the Surveillance and Protection System and specific functions, such as our Prime Minister, are provided with security as standard and others when threat assessments warrant it.

Since then, it seems that threats have further increased in popularity, partly explained by coarsening for manners, and a broader decrease in respect for authority and the rise of the Internet. However, this trend cannot be observed in other and surrounding countries, which is why Bovenkerk (2005) refers to this phenomenon as a "*Dutch Disease*". Van Buuren (2016) concludes in his dissertation "Target The Hague?" that there is an increase in conspiracy thinking and system hatred in the Netherlands. He also emphasizes the role of the Internet, which on the one hand; 1) plays an important role as a medium to provide access to digital communities in which ideas can be shared and sparked; 2) is a tool that can reinforce resentment, because the increase in opportunities to have your voice heard, does not actually mean that it is listened to, which can finally lead to more frustration. This is also underscored in 2009 by our national intelligence community (Algemene Inlichtingen- en Veiligheidsdienst, 2010, p. 13 and p.25), the Internet is proving to be an important medium for making threats. An increase in threats toward politicians, opinion makers and government targets (individuals representing the government) is seen.

Parallel to this plays another relevant development. Under the renewed administrative approach to organised crime (the BIBOB Act), local authorities were given more responsibilities. (Schuurman et al., 2021, p. 8). Because the (local) government is more prominent in fighting crime, the phenomenon of "undermining" arises parallel to this. The term "undermining" was initially used to describe criminal activities that have such an economic and social impact that they undermine the functioning of the rule of law (Boutellier et al., 2020).

In 2010, the National Coordinator for Counterterrorism (NCTb, nowadays NVTV) published a report about individual threateners of "public figures" in the Netherlands, defining this group as national politicians, judges, lawyers, mayors and aldermen (Nationaal Coördinator Terrorismebestrijding (NCTb), 2010). And the Prosecutor's Office also sees a further increase during this period in terms of threats toward politicians and local administrators (Schuurman et al., 2021, p. 10).

Until now, in most general scientific studies into the phenomenon of threats do not discuss digital threats, other than being threatened via social media, email or other digital messages. A more recent study was conducted by Schuurman et al (2021), constituted by the 'Advisory committee on future-proofing the Surveillance and Protection System (Adviescommissie toekomstbestendigheid stelsel bewaken en beveiligen, 2021). They looked at threats that have confronted the system since 2000 and the development of threats to politicians, office holders, civil servants, journalists, employees of the Public Prosecution Service, the Police, the Council of the Judiciary and members of diaspora communities in the Netherlands.

Regarding the upcoming reforms of the Surveillance and Protection system, a broad focus on threats has been selected, in which digital threats have also been included; *'if, for example, in addition to direct physical threats, safeguarding the undisturbed functioning of politicians and civil servants is also included in the responsibility of the system, then it could be argued that action against cyber espionage and digital disinformation campaigns is also part of this*.' (*Adviescommissie toekomstbestendig stelsel bewaken en beveiligen, 2021*, p. 4).

At the same time, our National Intelligence Service's 2020 annual report calls attention to unwanted foreign interference through disinformation campaigns with destabilising effects on the rule of law, misinformation and how the cyber domain can be used for (economic) espionage. These new threats should also be covered by the national Surveillance and Protection system (AIVD, 2021, p. 10). Influenced by U.S. elections, our own National elections, and a global COVID pandemic, the influence of disinformation campaigns continues to grow, with increasing support for anti-democratic and right-wing extremist sentiments (Schuurman et al., 2021, p. 16).

2.1.2 Threatened occupational groups in court rulings

To get the most up-to-date picture of the professions under threat, we conducted research based on recent case law.

Reviewing judgements in the database of jurisprudence (rechtspraak.nl) presented some constraints. Only statements emerge in this database where A) a report has been made, B) a perpetrator can be identified, so anonymous threats do not appear in the overview and C) threats have a certain subjectivity value, the recipient of the threat must perceive it as such and finally D) digital threats such as spearphishing or installing spyware will not appear in these results.

In addition, searching proved to be complex because if you search on "threat" in combination with some of the target groups; such as police officers or lawyers. Then these functionaries come up in almost all judgements in relation to all kinds of threats, because a police officer was involved when reporting the threat, and a lawyer is defending the accused. Broad search terms produce too many and, therefore, unusable results. At the same time, search terms such as "doxing" or "public figures" yielded practically no results. As a result, we used some guiding search terms. Such as all statements ***after Jan. 1, 2020*** combined with the search terms ***"threats employee"*** and ***"social media"*** within ***criminal law***. This search yielded 60 rulings[9]. This search helped to sharpen the criteria for the target group. We found a few rulings in which employees were verbally threatened during a criminal -physical- incident like a robbery. We have decided to exclude these cases because we focus on specifically targeted threats on specific individuals due to their specific functions or occupation. The expressed threat is not an addition to a criminal act, the threat is 'leading', and so it was not uttered because someone happened to be in the way. There are also examples in which threats can lead to physical incidents, these situations are part of this research. Thereby, we see that many of these threats touch the private sphere of the affected individual, while the reason to threaten is often business-related or ideological.

This analysis resulted in 21 threatened occupational groups and functionaries.

Table 2 - Threathened occupational groups and functionaries in case law since 01-01-2000

1. *Employees Youth Protection*	11. *Mayor (3x)*
2. *Elementary school teacher (2x)*	12. *Real estate agent*
3. *Police officer (8x)*	13. *Journalist*
4. *Probation officer*	14. *Photographers*
5. *Special investigating officer at State Forestry Commission*	15. *Employees GGD*
6. *Youth care workers*	16. *Employees nursing homes*
7. *Employees National Expertise Team Youth Protection (LET JB)*	17. *Prime Minister*
8. *National High Risk Team employees of the Child Protection Council*	18. *Employee arrestee care*
9. *Employees of a law firm (2x)*	19. *Housing association consultant*
10. *Lawyer*	20. *Cab driver*
	21. *University employee*

Analysing court rulings focused on groups of employees who are also regularly threatened but who, for whatever reason, have not received recent publicity nor attention in scientific literature. For example, we found a ruling (*ECLI NL RBROT 2021 7111.Pdf*, n.d.) in which an employee of the State Forestry was threatened by an angry citizen, then we searched "threats on employees State Forestry" via Google and found several articles about Forrest Guards who were threatened in 2018 due to a discussion about the supplementary feeding of animals in a specific Dutch nature reserve Oostvaardersplassen. The King's commissioner changed his decision about the supplementary feeding because Forrest Guards were doxed, and thereby threatened in their private sphere; *''Their home addresses were published, and their full names also appeared on Facebook* [10]".

2.1.3 Threatened occupational groups in news articles

We have succeeded in identifying many of the currently regularly threatened professions. Finally, we did another search for news articles surrounding this topic. The idea behind this is similar to our reason for reviewing case law.

[9]https://uitspraken.rechtspraak.nl/#!/resultaat?uitspraakdatuma=01-01-2020&uitspraakdatumrange=na&zoekterm='bedreiging%20medewerker','social%20media'&inhoudsindicatie=zt0,zt0&publicatiestatus=ps1&rechtsgebied=r3&sort=UitspraakDatumAsc

[10] https://www.ad.nl/binnenland/bedreigingen-aan-adres-boswachters-gaven-doorslag-bij-besluit-tot-bijvoeren~ad6dfb17/

Recent developments or trends are not yet part of most scholarly literature surrounding this topic. In our search, we focused on traditional media in the Netherlands since 2020.

For the most part, this search gave us similar results. Where we did notice that messages surrounding threatened politicians had headlines with a certain urgency that indicate an (extreme) increase; 'The ticking time bomb of political harassment[11]', 'Record number of reports of threatened politicians[12]', 'More reports than ever of threatening politicians[13]', 'Provincial and local government officials should be able to get more security[14]' and 'Political youth drop out due to keyboard heroes[15]'. We also see this around other professional groups, for example; 'Study: Journalists in the Netherlands increasingly threatened[16]', 'Doctors increasingly threatened or intimidated: 'It won't stop'[17]' and ''Scientists increasingly intimidated[18]'. In addition, the following professional groups were identified; scientists, diversity officers, Members of the Royal House, Civil Servants and port personnel.

In 2022, the Minister of Education, Culture and Science announced a hotline for threatened scientists, prompted by an appeal by the Human Rights Board stating that participation in public debate is becoming increasingly unsafe[19]. In addition, recent serious threats have led to this development, such as threats to the addresses of scientists and researchers such as the RIVM director and the deputy head of Analysis. In Belgium, virologist Marc van Ranst was met at home by someone with a rocket launcher[20].

In the same year, a news article refers to a study conducted by Dutch Universities and Colleges showing that Diversity Officers of these institutions are increasingly threatened. These employees have a role, for example, in '*making teaching materials inclusive, using more pronouns and changing men's or women's restrooms to gender-neutral restrooms*'[21].

In 2023, staff at Rutgers Expertise Centre have been under threat since the 'Week of Spring Fling' kicked off. During that week, elementary school children are taught about love, relationships and sexuality. In addition to threats, and name-calling, there was also a need for additional physical security. This was caused in part because a lot of disinformation was actively spread via social media, in which the teaching material was taken completely out of context and it was suggested, for example, that 4-year-old children were being taught about oral and anal sex[22].

In the same year, Princess Amalia moved out to study in Amsterdam, and shortly after moving, she faced extreme threats. After the Public Prosecutor's Office reported concerns surrounding her safety due to terror threats from organised crime, she moved back to her parent's because she could no longer move freely outside home[23].

The last professional group we came across are Civil Servants and Port personnel, both in the context of undermining. The director of the National Criminal Investigation Department indicated in 2023 that bribing officials has become a revenue model; "Previously, you would see that a criminal and an official knew each other, through school, for example, or from the neighbourhood. And that relationship then led to corruption or leaking information. Now we see middlemen, information brokers, deliberately looking for officials they can corrupt.[24]" Information brokers search for officials who are in money problems or struggling with addiction. Bribing and/or threatening officials is a relatively easy way to get information because of the access they have to various systems.

[11] https://www.bnnvara.nl/joop/artikelen/de-tikkende-tijdbom-van-politieke-intimidatie-hoe-bestuur-en-bevolking-zich-van-elkaar-vervreemden
[12] https://nos.nl/artikel/2456538-recordaantal-meldingen-bedreigde-politici
[13] https://www.volkskrant.nl/nieuws-achtergrond/meer-meldingen-dan-ooit-van-bedreiging-politici-zes-verdachten-maandag-voor-rechter~bb50c6c74/
[14] https://nos.nl/artikel/2467406-provinciale-en-lokale-bestuurders-moeten-meer-beveiliging-kunnen-krijgen
[15] https://www.rtlnieuws.nl/nieuws/politiek/artikel/5396076/politieke-jongerenorganisaties-zorgen-over-bedreigingen-en-haat
[16] https://nos.nl/artikel/2383721-onderzoek-journalisten-in-nederland-steeds-vaker-bedreigd
[17] https://nos.nl/artikel/2452748-artsen-steeds-vaker-bedreigd-of-geintimideerd-het-stopt-niet-meer
[18] https://nos.nl/artikel/2394575-wetenschappers-steeds-vaker-geintimideerd
[19] https://nos.nl/artikel/2401180-extra-hulp-voor-bedreigde-wetenschappers-collectief-achter-onze-mensen-staan
[20] https://nos.nl/artikel/2437959-dijkgraaf-vanaf-najaar-meldpunt-voor-bedreigde-wetenschappers
[21] https://nos.nl/artikel/2455216-medewerker-diversiteit-hoger-onderwijs-geintimideerd-en-bedreigd
[22] https://www.trouw.nl/onderwijs/hoe-de-week-van-de-lentekriebels-een-week-van-bedreigingen-werd~b7042dfa/
[23] https://nos.nl/artikel/2463179-amalia-over-bedreigingen-en-zware-beveiliging-ik-heb-het-nog-steeds-heel-moeilijk
[24] https://nos.nl/artikel/2474403-rijksrecherche-ziet-dat-omkopen-van-ambtenaren-verdienmodel-is-geworden

We see the same with port personnel, they pose great risk once corrupted. As soon as they stop cooperating with criminal groups, they become victims of threats, violence, extortion and even murder[25]. The mayor of Rotterdam said; '*Almost every day, police and customs remove people from containers in the port of Rotterdam. The drug traffickers can almost only get there with help from within. Because you have to know how to get to the premises and where the container is that contains drugs. There are always people in the port who lend themselves to this, with all the consequences. Because if you do it once then you hang. Then you are blackmailable and they get to your family, your children and you are threatened. It's life-threatening.*' [26]

2.1.4 Defining High-profile individuals

Systematic and overarching scientific studies have given us a good picture of occupational groups that have been threatened since the year 2000. We have supplemented this list with more recent cases based on case law and news articles.

The following overview shows all professional groups that emerged from our inventory. We are going to group these occupations into categories, then based on selection criteria we will make a selection of occupational groups to include in this study. Then we will make an attempt to include the selected occupational groups in a model. Considerations for this model are discussed in 2.1.4. In doing so, we will lay an important foundation for our research, because which target groups we focus on will also determine the threats and threat actors they face. Based on our inventory of occupational groups that have been threatened, we have categorised all occupational groups, our underlying classification can be found in Annex 1:

- Public Safety Personnel
- Health and Social Care Professionals
- Teachers
- Service employees
- Port staff
- Politicians and government officials
- Civil servants
- Members of the Royal House
- Legal professions
- Media contributors
- Famous Dutchmen
- Scientists
- Representatives of interest groups
- Members of diaspora communities

2.1.4.1 Selection Criteria

Are all these categories of occupational groups who we define as *high-profile individuals*? Therefore we need to define selection criteria. We have defined that *high-profile individuals;*

- represent or symbolize an organisation or institution;
- have access to an organisation's 'crown jewels' (critical assets/targets);
- or (access to) power;

and are, therefore, specifically interesting to various threat actors.

So, it is not about task-oriented threats, threats by acquaintances nor about indiscriminate victims of threats of violence. Therefore, we further exclude service employees in this study. These professionals usually have direct contact with citizens, and when they are threatened, it is often in the situation at the moment itself. The threats are directed less at the specific individual, but more at the person as the approachable face of an organisation.

Small professional groups or groups with relatively little exposure to threats also fall off such as Members of the Royal House, Teachers and Prominent sportsmen. And finally, Members of diaspora communities drop out because they represent a community rather than an institution or organisation. This does not mean that these professional groups do not face hybrid threats; the conclusions of this study may still be very relevant to them.

Because the group of Diversity Officers is quite small and the way they are threatened shows similarities with representatives of interest groups, they are also left out.

[25] https://www.nt.nl/havens/2023/04/26/bestrijden-van-ondermijning-in-de-haven-is-een-crime-voor-werkgevers
[26] https://www.rijnmond.nl/nieuws/1376017/aboutaleb-prive-omstandigheden-havenpersoneel-bespreekbaar-maken-om-weerbaarheid-tegen-drugsronselaars-te-vergroten

So from now on we will focus on the following 9 categories of high-profile individuals:

1. Public Safety Personnel
2. Health and Social Care Professionals
3. Port personnel
4. Politicians and government officials
5. Civil servants
6. Legal professions
7. Media contributors
8. Scientists
9. Representatives of interest groups

2.1.4.2 Modelling high-profile individuals

Like Schuurman et al (2012, p.31), we observe that there is a broad group of individuals at risk. These individuals play a role in maintaining the democratic rule of law. Either because they are part of the political system or within the open society. Both are conditional for maintaining our democratic rule of law (AIVD, 2004, p. 13). They point to journalists and lawyers who also face (very) serious threats and (lethal) violence and that both are indispensable for the proper functioning of the rule of law. Bovenkerk (2005) also focused on '*threats to prominent officials who play a role in upholding the rule of law in the Netherlands and threats that interfere with their private lives'*. And even when politicians, for example, quit because of threats, or keep opinions to themselves because of fear of threats, the democratic rule of law cannot function adequately.

The interactions between government and citizens should be shaped according to the principles, procedures and institutions of the democratic rule of law. These include the '*principle of legality, the separation of powers, a distribution of power, fundamental rights, the vesting of the monopoly of violence in the government, the openness of the independent rule of law, a restrained attitude on the part of the government where the private lives of citizens are concerned, the right to vote, the freedom to acquire political power, fundamental political rights, democratic say in and control over decision-making, open government, rights of political minorities and majority rule in political decision-making*' (AIVD, 2023, p. 14).

If both the vertical relations (the interactions between the government and the citizens) and the horizontal relations (the interactions between the citizens themselves) meet certain conditions, one can speak of a democratic legal (AIVD, 2023, p. 14). Does the threat undermine the vertical axis of society, the political system, or the horizontal axis, the open society? Indeed, a democratic legal order also requires a certain degree of social trust, social cohesion, solidarity, active citizenship and loyalty on the part of citizens. Values and norms are central to this, such as respect for the open character of society, respect for a plural and diverse society, the (desire to) promote social trust between citizens, respect for divergent interests and the will to cooperate as much as possible in harmonising interests, respect for the privacy of fellow citizens, respect for other moral and philosophical orientations, and so on (AIVD, 2023, p. 14). We will also use this horizontal and vertical axis in our mapping; visually plotting the professions on this axis will make it clear that threats towards high-profile individuals are dangerous to the democratic rule of law.

We will make the second distinction in this model based on the 'crown jewels' to which the individual has access. The "Guidance on positions of trust" issued by our national intelligence service (*Leidraad-Aanwijzing-Vertrouwensfuncties-September-2014.Pdf*, n.d., p. 8) provides guidance for determining whether individuals working in an organisation are likely to harm vital interests. In addition to the organisation's key position in guarding the democratic legal order, they apply two criteria:

---

1. 'The individual gives structural access to sensitive and/or state secret information and/or core interests that if compromised will cause damage to national security (information)

2. gives direct, uncontrolled access to potential targets or resources that facilitate an attack or espionage, in all cases causing damage to national security (access)'

Not all functionaries we have categorised so far have a fiduciary role. However, all of them seem to be vulnerable somehow. Think of civil servants who issue passports or port personnel with access to containers. This results in the following mapping (figure 2).

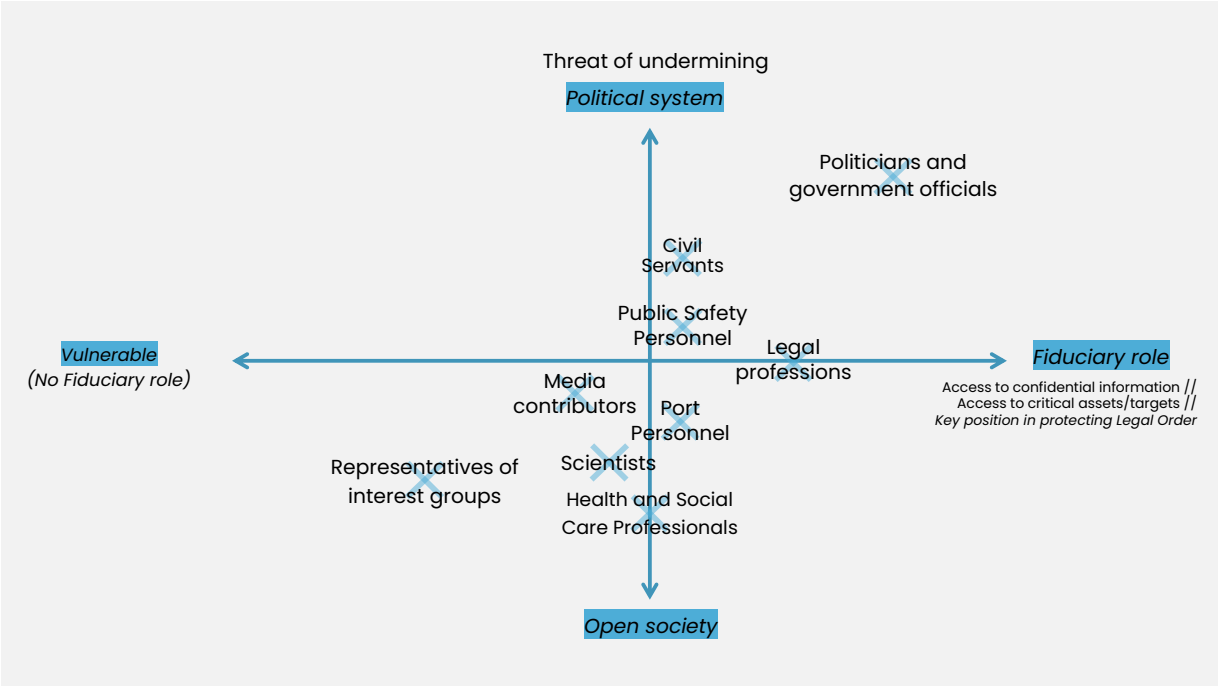


Figure 2 - Mapping of high-profile individuals (Version 0.9) (Source: created by author)

The degree and manner in which an individual is threatened in a high-risk function is represented by means of the vertical axis, this concerns the undermining of the democratic legal order. Within this, the individual may play a role primarily with respect to the vertical axis (the political system) or the horizontal axis (the open society). The extent to which the individual has access to confidential information, assets, or potential targets from his or her position determines his or her position with respect to the horizontal axis.

This mapping will help us later in this research to determine whether all high-profile individuals, based on the hybrid threats to which they are nowadays exposed, need the same protective measures or whether they may need to be differentiated.

2.2 Threats & Threat actors

In this section, we will provide an overview of hybrid threats that high-profile individuals could face.

The threats high-profile individuals face are described by Wallström et al. (2007, p.2) as 'unlawful influence'.

> *"The term **unlawful influence** refers to harassment and threats, and acts of violence directed at persons or property, which, besides constituting a major problem in relation to health and safety at work, may affect the individual official's exercise of authority, which therefore by extension constitutes a threat to democracy. The term unlawful influence also refers to corruption in the form of improper offers, which also affect the individual official.*
> *(Wallström et al., 2007, p.2)*

2.2.1 Instrumental and Expressive threat concepts

We will make use of the thinking of Bovenkerk (2005), who distinguishes instrumental and expressive threats. This distinction was previously made by Meloy (2004), who studied threat letters to American politicians. In doing so, he noticed that they can be classified in two ways.

We are well aware that the line between an instrumental and an expressive threat can be a tricky one, sometimes this line is also very thin (Torre, E.J. van der et al., 2013, p. 95). It is also not true that only instrumental threats can be vicious, indeed "*instrumental violence is rational and therefore ceases when the goal cannot be achieved or when the goal has been achieved. Expressive violence has its own dynamics and the link to an underlying goal is often unaware by the perpetrator. Serious expressive violence can be more dangerous for this reason.*" (Middelhoven & Driessen, 2001, p. 15). In this regard, a digital threat can also be of an instrumental nature, then we classify it under instrumental threats; e.g., when an individual's computer is hacked in order to gain access to their information, or with the aim of influencing that person (e.g., through blackmail).

2.2.1.1 Expressive threat concept

According to Meloy (2004), expressive threats articulate the emotions of the threatener, which can arise from frustrations or ideology. The threatener threatens or intimidates someone out of felt frustration or anger, with no plan of influence (Torre, E.J. van der et al., 2013, p. 92). The threatener makes no demand. Most current threats regarding high-profile individuals belong to this concept. Demonstrative actions by threat actors have primarily a symbolic purpose, and most threateners of Dutch public figures often 'just' want their political opinion or their ideological disapproval clear (Bovenkerk, 2005, p. 10)

2.2.1.2 Instrumental threat concept

Instrumental threats are "*intended to control or influence the behaviour of the threatened person*" (Bovenkerk, 2005, p. 10), there is no demonstration of emotion, and the threat actor sets a clear condition regarding the threatened person. Instrumental threats are '*a concrete expression to harm someone or their loved ones*' (van Miltenburg et al., 2022, p. 21). Many of these threats match the description of the Dutch Penal Code (Bovenkerk, 2005; Kuiper, 2018). Goals of the instrumental threatener include imposing his will, challenging authority, preventing an arrest or gaining prestige (Torre, E.J. van der et al., 2013, p. 24).

2.2.2 Threats according to the law

The Dutch Penal Code, article 285, describes what threats are in general. Their description corresponds to the concept of instrumental threats. The offence is aggravated if the threat is of a terrorist nature or if the person threatened belongs to a specific professional group or functionary: 'Minister, State Secretary, King's Commissioner, Member of Parliament, mayor, alderman, member of a general representative body, judicial officer, lawyer, journalist or publicist in connection with news gathering, police officer or special investigating officer'. This aggravating circumstance has been introduced for threats against these specific professions and officials. By virtue of their public function, they are considered to represent a public body that performs an essential function in the democratic legal order. Article 285a is an addition to this, but is specifically aimed at threats made to a person who is required to give evidence before a judge or a public official. So this threat is also conditional, as is Article 285b on stalking and harassment. Where the threats systematically invade the privacy of the threatened person.

> *Article 285*[27]
>
> 1. *Threat of openly committing violence in unison against persons or property, of violence against an internationally protected person or his protected property, of any crime causing danger to the general security of persons or property or common danger to the provision of services, of rape, of actual indecency assault, of any crime against life, of hostage-taking, of aggravated assault or of arson, shall be punishable by imprisonment of up to three years or a fine of the fourth category.*
> 2. *If this threat is made in writing and under a specific condition, it shall be punishable by imprisonment for a term not exceeding four years or a fine of the fourth category.*
> 3. *Threat of a terrorist crime shall be punishable by imprisonment of not more than six years or a fine of the fifth category.*
> 4. *If the offence described in the first, second or third paragraph is committed with the intent to prepare or facilitate a terrorist crime, the term of imprisonment imposed on the offence shall be increased by one third.*
> 5. *If the offense described in the first, second, or third paragraph is committed against a person in his capacity as a Minister, State Secretary, commissioner of the King, deputy, mayor, alderman, member of a generally representative body, judicial officer, lawyer, journalist or publicist in the context of news gathering, police officer, or special investigating officer, the penalty of imprisonment imposed on the offense shall be increased by one third.*
>
> *Article 285a*
>
> 1. *He who intentionally makes oral, gestural, written or pictorial statements towards a person, apparently with the aim of influencing that person's freedom to make a statement truthfully or conscientiously before a judge or civil servant, while knowing or having serious reason to suspect that such a statement will be made, shall be punished with imprisonment of not more than four years or a fine of the fourth category.*
> 2. *[…]*
>
> *Article 285b*
>
> 1. *He who unlawfully and systematically infringes upon another person's privacy with the intent to compel that other person to do something, not to do something, to tolerate something or to arouse fear shall, as guilty of stalking, be punished with imprisonment of not more than three years or a fine of the fourth category.*
> 2. *[…]*

July 2022, a bill was introduced to make 'doxing' a criminal offence. As of 2024, a paragraph has been added to article 285. Doxing is the act of publishing someone's personal information, such as their address and phone number. The reason for introducing this law is that it's not always a criminal offence to disclose someone's private information when it's not in the form of threats, insults or coercion. The explanatory memorandum to this bill shows that the proposed criminalisation of the use of personal data for intimidation purposes differs from the criminalisation of coercion in that criminal liability (in the case of doxing) already arises when the act of making data available is done with a specific purpose. The perpetrator intends to cause the victim fear, serious harassment or serious obstruction in the exercise of his or her duties or profession[28]. Criminal aggravation will also occur when the victim has a specific function, as also mentioned in the main article (285).

> *Article 285d*
>
> 1. *The person who obtains personal data of another person or a third party, distributes these data or otherwise makes them available with the intent to instigate fear of that other person or to have them instigate fear of that other person, to cause serious nuisance to him or to have him cause serious nuisance, or to seriously hinder him or have him seriously hindered in the exercise of his office or profession, shall be punished with imprisonment of not more than two years or a fine of the fourth category.*
> 2. *If the offence described in the first paragraph is committed against a person in his capacity as a Minister, State Secretary, commissioner of the King, member of a provincial executive, mayor, alderman, member of a generally representative body, judicial officer, lawyer, journalist or publicist in the context of news gathering, police officer or special investigating officer, the term of imprisonment imposed on the offence shall be increased by one third.*

What caught our eye about the wording of the added law article is that it may also have a broader role with respect to digital threats. An IP-adress can also be considered as personal data (NCSC, 2012, p. 96), so when someone is actively distributing someone's IP address, with a public call to perform a Distributed Denial of Service (DDOS) this article might be useful, because this specific section of the law seems to be worded just a bit more broadly than solely focusing on doxing.

[27] https://wetten.overheid.nl/BWBR0001854/2023-09-01/#BoekTweede_TiteldeelXVIII_Artikel285
[28] https://www.uitspraken.nl/uitspraak/gerechtshof-arnhem-leeuwarden/strafrecht/strafrecht-overig/hoger-beroep/ecli-nl-gharl-2023-10209

2.2.3 About digital threats

A digital threat is a threat, via or in cyberspace. Van den Berg (2022, p.2) defined cyberspace as an ecosystem (with a variety of actors and behaviours), made up of digital technologies and connected through networks, shaped and viewed by its use. '*Most importantly involving the creation, storage, modification, sharing and exploitation of information and in their use of cyberspace these actors treat this ecosystem as an operational space, that is, a space in which strategic activities take place*' (Van Den Berg & Kuipers, 2022, p.2). Some previously physical threats have now partly shifted to cyberspace, such as cybercrime or espionage.

In addition, technological developments have led to the development of new and digital tactics, techniques, and procedures (TTP's[29]) of (threat) actors. Actors can attempt to achieve goals through the use of these TTPs, these goals can be physical or informational (Van Den Berg & Kuipers, 2022, p. 9). All our described threats regarding high-profile individuals have (potential) physical or informational consequences and are all intentional.

As with cybercrime, digital threats cover all forms of threats where IT plays an essential role in execution. Since 2000, the digitalisation of our society has made it easier to send a threat via e-mail or via another digital medium (Bovenkerk, 2005; Kuiper, 2018; Leukfeldt et al., 2015). In this case, it is a digital threat, in a broad sense. A digital threat in the narrow sense exists when IT is both a tool and a target. Think, for instance, of a smartphone containing spyware, a hacker trying to access individuals' accounts or a malicious actor hijacking a social media account. Leukfeld et al (2015) compiled a handbook for the Dutch Police 'Everyday Policing in a digitalised world' in which he divides two types of digital threats that are relevant to our target group of 'high-profile individuals', they can be found in Table 3:

Hacking and other crimes targeting computers	Hacking Data theft (data, as well as photos and e-mail) Causing breakdown Destroying data Defacing Malware
Threats and other forms of person-oriented crime	Stalking or belaying Defamation or slander Insult Discrimination Threat Cyberbullying (not punishable in the first instance) Distribution of texts via the Internet without permission Distributing photographs via the Internet without permission

Table 3 - Overview digital threats: computer-/ and person-oriented (Leukfeld, 2015)

In their research, they described all individual threats, clearly explained what they entail and how to recognise these means, and designated all relevant (criminal law) legislation for each threat.

Therefore, the advice of the Advisory Committee on the Future-proof Surveillance and Protection system is not without reason that the system will have to be further tailored to digital threats. Given the focus of the NCTV's Surveillance and Protection System, where physical integrity is the focus, their main concern is a digital threat as a prelude to a physical threat (Adviescommissie toekomstbestendig stelsel bewaken en beveiligen, 2021). In our overview, we will categorize most of these threats as a hybrid because more traditional-physical- threats are combined with digital, often-informational- threats.

[29] https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

2.2.4 Overview threats

Based on the difference between the instrumental and expressive threat concept and an analysis of grey literature and news articles, we have compiled the following overview (figure 3) of threats towards high-profile individuals. The threats that high-profile individuals face nowadays are now quite diverse. We have tried to bring together the most common threats we have encountered in our research into a model, distinguishing between expressive and instrumental threats and their manifestations, are they physical or digital?

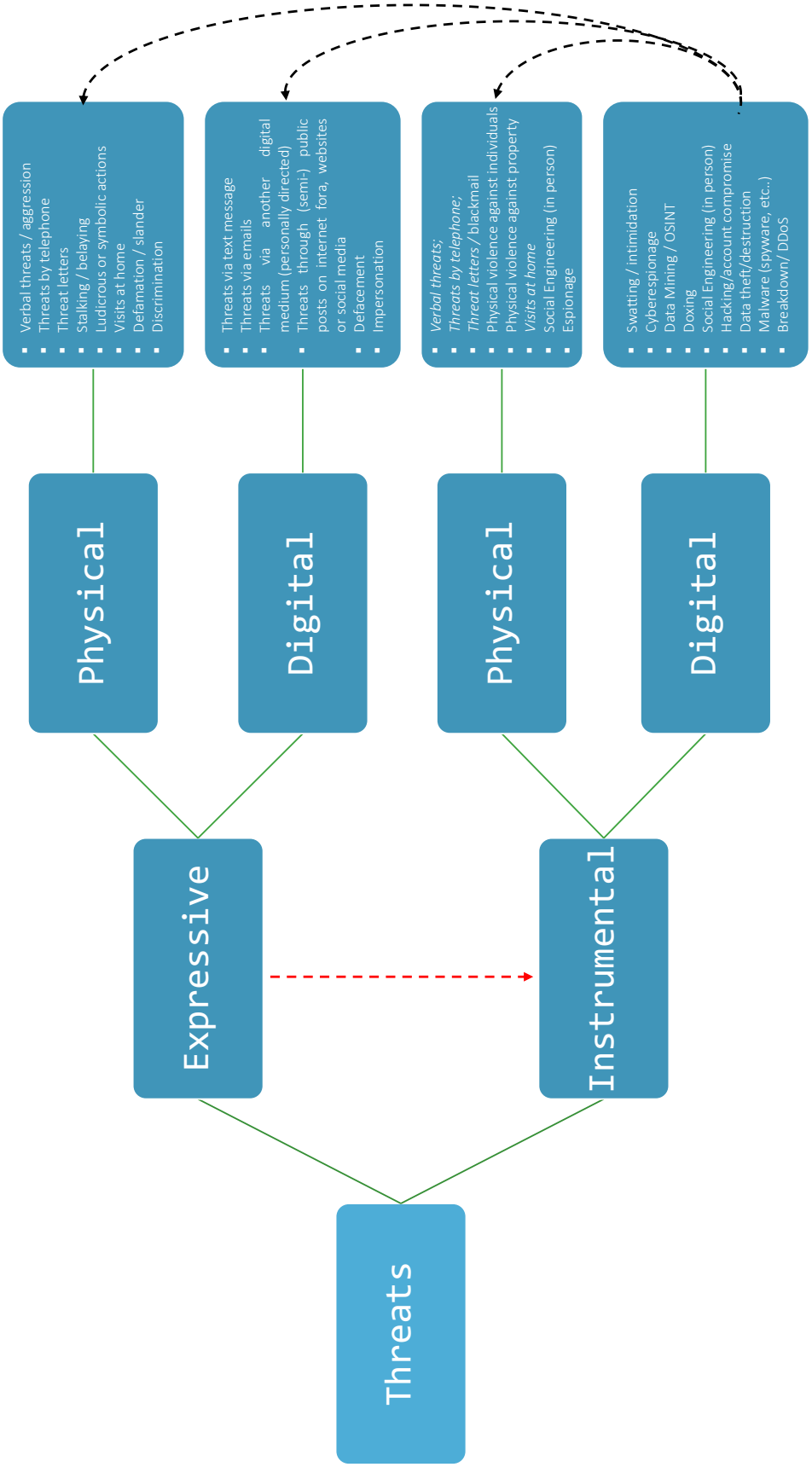
In some situations, this subdivision is quite clear. For example, if a threat actor decides to deploy spyware, then the spyware is the tool with which the threat actor obtains its (initial) objective. Thus, malware will be categorized as an instrumental digital threat. This is more difficult in the case of ludicrous or symbolic actions. For example, during the recent nitrogen protests, there was a situation where angry farmers hung a life-sized doll from a gallows at a viaduct to call for suicide among frustrated farmers[30]. Because similar protests earlier also involved driving around a coffin with an MP's name on it, this action created a very different impression and was actually threatening to some individuals. Consider also the situation where Minister Kaag was met at a debate by a group of angry protesters carrying torches. Shortly before this, the minister was visited at home by a man carrying a torch, a situation she and her family experienced as very threatening. The torches at the protest referenced this and were intimidating, but if the protesters are to be believed, they were meant '*to give her a warm welcome*' and were rather symbolically[31]. We have placed a (red) arrow in the overview for exactly this reason: a threat can be initially expressive but, due to interpretation, context or frequency, transition into an instrumental threat.

At the same time, threats are also combined, these are hybrid threats. When a threat actor actively searches for a journalist's home address based on public sources (OSINT), shares the address in a Telegram group (doxing) and then decides to make a 'home visit', it is a hybrid threat. For this reason, black arrows have been added to the right-hand side of the overview, in which case the prelude, or reconnaissance phase is digital and subsequent threats may be found elsewhere in the overview.

When we identified our target group, we focused on the Netherlands. Now we are assessing the threats, our view is broader. Due to the borderlessness of the internet, threats that occur elsewhere will very probably also be relevant here in the future (Schuurman et al., 2021).

[30] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5315517/boerenprotesten-stikstof-pop-strop-snelweg-a1-azelo-viaduct
[31] https://www.powned.tv/video/ophef-over-fakkels-tegen-kaag-boosheid-is-normaal~3169/

Figure 3 - Overview Physical and Digital threats regarding High-profile individuals (Version 0.9) (Source: created by author)



2.2.4.1 Expressive physical threats

The overview starts with the threat that is the biggest in the Netherlands, namely expressive threats. The category of expressive physical threats includes verbal threats/aggression, threats by telephone, threat letters, stalking/ belaying, ludicrous or symbolic actions, home visits, defamation and slander & discrimination.

2.2.4.1.1 Verbal threats/aggression, threats by telephone and threat letters ;

The most commonly used threats towards individuals are expressed in the form of verbal threats/aggression, threats by telephone and threat letters (Bovenkerk, 2005; Drs. I.N.J. de Groot Mr. drs. L.F. Drost Prof. dr. J.C.J. Boutellier, n.d.; Kuiper, 2018; Meloy et al., 2004; Wallström et al., 2007). Based on emotion(s) or ideology, the threatener wants to proclaim his message, which can be shouted on the street, during a telephone conversation or articulated in a physical letter.

2.2.4.1.2 Stalking/ belaying

When the threats are systematic in their character and touch on the private realm (Article 285b), then there is stalking/ belaying (Bovenkerk, 2005; Drs. I.N.J. de Groot Mr. drs. L.F. Drost Prof. dr. J.C.J. Boutellier, n.d.; Kuiper, 2018; Marijnissen et al., 2020; Meloy et al., 2004; Torre, E.J. van der et al., 2013; Wallström et al., 2007). In fact, the legislation in this area has been amended following a proposal by former MP Boris Dittrich, who himself was stalked for a long time, in his function as MP[32] [33].

2.2.4.1.3 Ludicrous or symbolic actions

We also regularly see, especially at the ideological level, ludicrous or symbolic actions. Such actions also have a long history, as can be read in Bovenkerk's (2005, p.27) study;

> *'In the 1980s, for instance, it was customary to change the minds of politicians outside by destroying material property. Especially the flora at politicians' homes had to suffer: 'Some front gardens were dug up. Louw de Graaf, CDA secretary of state for social affairs in the first Van Agt cabinet [...], lost all his plants.*
>
> *The year before, in 1981, the lawn of PvdA minister André van der Louw had been torn up by angry youths who had no appetite for his coercive youth task plan. [...] In the mid-1980s, CDA MP Ad Lansink discovered upon returning home to Nijmegen that his house had been wrapped in barbed wire by anti-nuclear protesters.'*

Another example are the stickers on doors of home addresses from outspoken individuals with the message 'Vizier op links'[34]. Or the package that was sent to Minister Hennis-Plasschaert with a plastic model of an embryo inside, along with an anti-abortion letter from a Bishop [35]. The minister has previously been open about her personal life and found this mailing intimidating. Coincidentally, these examples occurred at home addresses, which is not conditional to such symbolic actions.

2.2.4.1.4 Home visits

Examples of (angry) citizens coming to get redress from a member of parliament or alderman are also of all times. Yet such home visits can be quite threatening. We have already discussed the home visit to Minister Kaag[36] and the angry farmers at Minister Van Der Wal's house[37]. In some cases, such home visits have a clear requirement or condition, but often they are more symbolic or based on (personal) frustrations.

[32] https://www.rtlnieuws.nl/editienl/artikel/1558791/beetje-bner-heeft-een-stalker
[33] https://www.toniemudde.nl/Tonie_Mudde/Artikelen/Artikelen/2009/1/2_Dichterbij_dan_je_denkt_files/Confrontatie_stalking.pdf
[34] https://www.nrc.nl/nieuws/2023/01/27/om-na-2-jaar-onderzoek-geen-vervolging-wegens-bedreiging-van-stickeractie-vizier-op-links-a4155537
[35] https://www.rtlnieuws.nl/nieuws/artikel/3170651/kwetsende-passages-brief-niet-geschrapt
[36] https://nos.nl/artikel/2440772-man-die-met-brandende-fakkel-bij-huis-van-kaag-stond-opnieuw-opgepakt
[37] https://nos.nl/artikel/2445657-rellende-boeren-bij-huis-minister-van-der-wal-vandaag-voor-de-rechter

2.2.4.1.5 Defamation and slander

Individuals also regularly face defamation and slander. In which someone deliberately spreads negative (or false) messages about you so that others think badly of you (I&O Research, 2020; NCSC, 2012; van Buuren, 2016).

2.2.4.1.6 Discrimination

And then there is discrimination, defined under Article 90quater (Criminal Code) as follows: *'any distinction, exclusion, restriction or preference, which has as its purpose or may have as its effect the recognition, enjoyment or exercise on an equal on an equal footing of human rights and fundamental freedoms in the political, economic, social, cultural or other spheres of social life*.' Discriminatory threats are also of long-standing, whether they discriminate based on physical appearance, ethnicity, religion or gender (I&O Research, 2020; Meloy et al., 2004; PersVeilig, n.d.; Torre, E.J. van der et al., 2013; van Buuren, 2016; van Miltenburg et al., 2022). Of all discriminatory comments, 31% were related to gender, 27% to skin colour and 25% to ethnicity (Middelhoven & Driessen, 2001, p.69).

2.2.4.2 Expressive digital threats

Our overview of expressive digital threats starts with threats that are spread via cyberspace; think about threats via text messages, emails, via another digital medium (personally directed), or threats through (semi-) public posts on internet fora, websites or social media. In addition, we found two digital threats that are also only possible because of developments in Cyberspace; defacement and impersonation.

2.2.4.2.1 Threats via text messages/emails /another digital medium (personally directed) and threats through (semi-) public posts on internet fora, websites or social media

Since 2000, the majority of expressive threats have been sent over the internet, making it even easier for the threat actor to remain anonymous. Examples of this include threats via text messages (SMS, WhatsApp, etc.), via emails, via another digital medium (personally directed), for example, a Direct Message at X or LinkedIn or 4) threats through (semi-) public posts on internet fora, websites or social media (Bovenkerk, 2005; Drs. I.N.J. de Groot Mr. drs. L.F. Drost Prof. dr. J.C.J. Boutellier, n.d.; Kuiper, 2018; Meloy et al., 2004; Wallström et al., 2007). From a survey conducted by the Dutch Broadcasting Agency (NOS) Chamber members most often cite "social media" as a source of threats and harassment. An experienced MP says that because of social media, MPs get negativity all day long, from hate speech to death threats, where it used to be an angry letter or email once in a while [38]. This is also reflected in the various studies by I&O Research, which have conducted research on threats within public administration (various layers), on gown carriers and journalists. The graph below (figure 4) is from their survey on threats towards political office holders and illustrates the shift from threats into the digital domain.

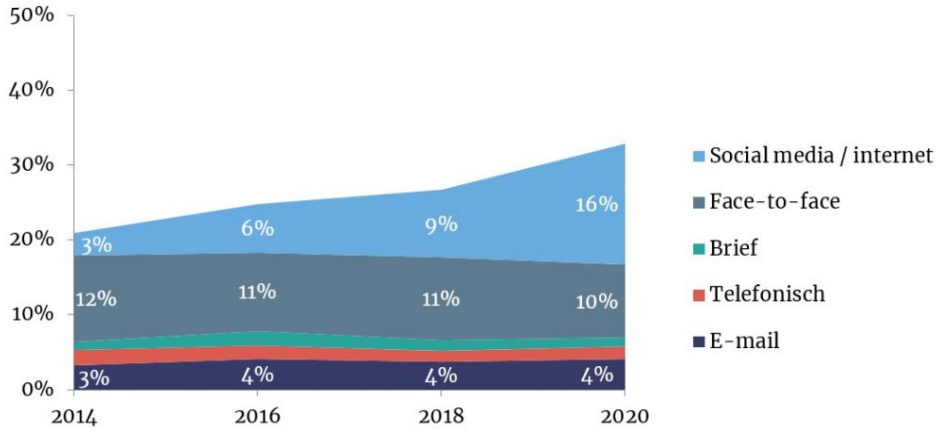


Figure 4 - Form of expression of most recent incident / political office holders (n=3,002) (I&O Research[39])

[38] https://nos.nl/artikel/2453170-onderzoek-nos-kamerleden-voelen-zich-geintimideerd-houden-mening-soms-voor-zich
[39] https://www.ioresearch.nl/actueel/toename-agressie-via-sociale-media-tegen-politieke-ambtsdragers/

2.2.4.2.2 Defacement

Defacement occurs when "*intentional and unlawful removal and modification of data from data stored, processed or transmitted*' (Leukfeldt et al., 2015, p. 25). Often, websites are targeted for this, and the threat actor gains access to the website and hijacks it. By proclaiming a (totally) different message on it, conceivably from emotions or an ideological basis of the threat actor. An example occurred during a Twitter hack, where a hacker accessed Wilders' Twitter-profile. By modifying login details, Wilders himself could no longer access his profile. While meanwhile, his profile pictures was replaced, and the hacker also tweeted, '*porn is being used as a weapon of the elite, we are engaged in a depopulation agenda, wake up the Netherlands*' [40].

Figure 5 - Screenshot defaced Twitter profile Geert Wilders (RTLnieuws.nl)

In 2013, hackers from Bangladesh attacked about 30 websites of Dutch individuals in response to the controversial anti-Islam film 'Innocence of Muslims', which caused worldwide controversy and was released in the Netherlands last year. Reports appeared on the hacked sites that the action was aimed at ridiculing the Prophet Mohammed[41].

2.2.4.2.3 Impersonation

Another example of an expressive digital threat regarding individuals is impersonation. In 2017, a user of the platform Reddit, placed faces of famous people on the bodies of porn actresses (Bart van der Sloot et al., 2021, p. 37). This phenomenon, since then, has also occurred in the Netherlands in recent years; presenter Welmoed Sijtsma, for example, has been duped by this[42] and even made a documentary[43] about sexfakes. In addition, deep-fake porn videos of members of our Royal House[44] and a small number of female MPs, including Lilian Marijnissen and Sylvana Simons, may be circulating[45]. Simons has perceived this as threatening and responded "*Someone takes your identity, your being, your body, your face and appearance and does what they want with it. That really feels like sexual assault*"[46].

While female politicians are regular victims of pornographic deepfakes, men often involve words put in their mouths (Bart van der Sloot et al., 2021, p. 37). A famous Dutch example-although not threatening- but showing future techniques was 'KlimaatRutte', in which the online news platform 'De Correspondent' showed what climate leadership from our Prime Minister could look like. While this video had no bad intentions, it illustrates how credibly a person can be personified and proclaim a message[47], with all its potential consequences.

In a joint report by our intelligence service (AIVD) and the Scientific Research and Data Centre, the knowledge institute for the Ministry of Justice and Security (WODC) we read an interesting passage about the risks of deepfakes: *'The democratisation of deep-fraud technology may result in so much fake content appearing on the internet that truth and fiction will become increasingly mixed up. This combined with the fact that over 90% of digital material could eventually be manipulated could have a very disruptive effect on society' (Bart van der Sloot et al., 2021).*

And consider, for example, the following incident in April 2021. Members of the House of Representatives' permanent foreign affairs committee had a digital conversation with someone posing as Leonid Volkov, a direct

[40] https://nos.nl/artikel/2340852-hacker-wilders-had-toegang-tot-priveberichten-het-was-een-grap
[41] https://www.parool.nl/nieuws/nederlandse-sites-gehackt-om-anti-islamfilm~b058ebf7/
[42] https://www.uitspraken.nl/uitspraak/rechtbank-amsterdam/strafrecht/strafrecht-overig/eerste-aanleg-meervoudig/ecli-nl-rbams-2023-6923
[43] https://npo.nl/start/serie/welmoed-en-de-sexfakes/seizoen-1/welmoed-en-de-sexfakes
[44] https://www.youtube.com/watch?v=pEtwSA9e5Gg
[45] https://npo.nl/npo3/welmoed-en-de-sexfakes/10-11-2022/POW_05416194
[46] https://panorama.nl/artikel/488062/ook-nepporno-gemaakt-van-sylvana-simons
[47] https://decorrespondent.nl/12847/beste-mark-rutte-zo-klink-je-als-je-klimaatleiderschap-toont/07e9cdc8-fc27-0bd6-0370-3533b3fc042d

associate of Russian opposition leader Alexei Navalny [48] [49]. First they thought it was a deepfake, then it seemed to be an actor, however, impersonation involves many risks. State Actors and also some anti-establishment extremists actively seek to increase tensions in society, according to the Dutch Intelligence Service (AIVD, 2023). Using disinformation (or, more specifically, deep fakes) based on personal online information (and personal image material) is another risk (Bart van der Sloot et al., 2021).

If we then talk about hybrid threats, it is conceivable that individuals will increasingly be blackmailed with deepfake technology[50]. Or that the -without consent- obtained sensitive information that could make an individual blackmailable comes from a hack, account compromise, or malware. It is known, for example, that Russia has an interest in having material with which it can beat up European Union countries at strategic moments, this is called 'kompromat'. This certainly includes a personalised approach, on the individual and his or her position[51]. When this is the case, the threat is conditional and thus becomes an instrumental, often physical, threat.

2.2.4.3 Instrumental physical threats

Instrumental threats are "*intended to control or influence the behaviour of the threatened person*" (Bovenkerk, 2005, p. 10). These entail verbal threats, threats by telephone and threat letters/ blackmail, visits at home, social engineering *(in person) and* espionage.

2.2.4.3.1 Verbal threats, threats by telephone and threat letters/ blackmail.

Traditionally, these threats involve verbal threats, threats by telephone and threat letters/ blackmail (Bovenkerk, 2005; Drs. I.N.J. de Groot Mr. drs. L.F. Drost Prof. dr. J.C.J. Boutellier, n.d.; Kuiper, 2018; Meloy et al., 2004; Wallström et al., 2007). There is no demonstration of emotion, and the threat actor sets a clear condition regarding the threatened person.

2.2.4.3.2 Physical violence against individuals or their property

Then we have physical violence against individuals and physical violence against property. Unfortunately, we have had a longer history of such violence in the Netherlands, with a number of extreme events. In the past 20 years, political list leader Pim Fortuyn has been murdered, columnist Theo van Gogh and lawyer Dirk Wiersma, and crime reporter Peter R. de Vries who was also confidant of a key witness in the Marengo trial[52]. There are, unfortunately, many more examples of violence against high-profile individuals; one can think of violence against journalists[53], policemen[54], gown wearers[55], and politicians[56].

2.2.4.3.3 Visits at home

Sometimes such threats are combined with visits at home[57] [58] [59]. These are home visits where there is not so much about frustration or ideology, but where there is a clear demand.

2.2.4.3.4 Social engineering *(in person)*

Exploiting human weaknesses and manipulating people into breaking normal security procedures is called social engineering (in person). From the available evidence, it is clear that the scale and sophistication of related attacks are increasing (ENISA, 2008). Social engineering varies in effectiveness and sophistication, from relatively simple digital attempts (through phishing or malware) to more sophisticated attempts that target individuals directly, for example, our target group of high-profile individuals. According to ENISA (2008), the success of such attacks depends on the pretext, conducted background research and the attacker's competence in then using these factors to change the perception of the target. Social engineering can involve both psychological and technological means

[48] https://www.volkskrant.nl/nieuws-achtergrond/kamerleden-vergaderen-met-deepfake-imitatie-van-stafchef-russische-oppositieleider-navalny~b04b5322/
[49] https://www.nu.nl/tech/6136120/medewerker-navalny-die-met-kamerleden-sprak-geen-deepfake-maar-acteur.html
[50] https://nos.nl/artikel/2300688-zorgen-om-over-deepfakes-risico-op-oplichting-en-afpersing
[51] https://eenvandaag.avrotros.nl/item/russische-inmenging-kompromat-dit-is-wat-we-weten-over-de-rus-die-de-partij-splinter-250000-euro-aanbood/
[52] https://nos.nl/artikel/2388971-zaak-wiersum-extra-beladen-na-aanslag-op-peter-r-de-vries
[53] https://www.wodc.nl/actueel/nieuws/2023/03/27/geweld-tegen-journalisten-is-onderdeel-van-breder-maatschappelijk-vraagstuk
[54] https://www.politie.nl/nieuws/2023/april/4/00-jaarcijfers-gtpa-2022.html
[55] https://nos.nl/artikel/2495939-tientallen-rechters-en-officieren-voelen-zich-bedreigd-weigeren-sommige-zaken
[56] https://nos.nl/artikel/2433952-minister-van-der-wal-doet-aangifte-na-doodsbedreiging-op-vrachtwagen
[57] https://www.parool.nl/nederland/minister-van-der-wal-over-bedreigingen-als-een-van-de-kinderen-wil-dat-ik-stop-dan-stop-ik~b3aa7f86f/
[58] https://www.parool.nl/nederland/man-vecht-zich-de-woning-van-wybren-van-haga-binnen-hij-riep-iets-over-een-mitrailleur~b5b571fb/
[59] https://www.nu.nl/politiek/6176936/de-jonge-eigenlijk-iedere-dag-bedreigd-of-geintimideerd-vaak-bij-zijn-huis.html

(like email spoofing, masking of fraudulent URLs, typosquating or a bogus web site, using faked images, etc..) to gain the target's trust (ENISA, 2008, p. 34). Consider, the use of, Cialdini's (2020) seduction techniques; *reciprocity, consistency, social proof, sympathy, authority, unity and scarcity*.

2.2.4.3.5 Espionage

But 'digital and physical espionage, in which actors focus on gathering intelligence, is also a significant problem for the Netherlands' (AIVD, MIVD & NCTV, 2022, p.18). Take for example, the recent expulsion of Russian diplomats in March 2022 on suspicion of espionage. Here, too, individuals in specific positions are the key to certain information or can be influenced, in a more or less friendly way. The fact that they target individuals in doing so is evident partly because state actors use (public procurement) documents, for example, to identify potential individual targets (AIVD, MIVD & NCTV, 2022, p. 34). There is scientific, military (Schuurman et al., 2021, p. 30) and commercial espionage, where companies try to enhance their competitive advantage by gathering information about their competitors' practices and future plans (Van Den Berg & Kuipers, 2022, p.5). Despite the development of cyber espionage, about which more can be read in the next section, spying in the physical world is still relevant in 2023.

2.2.4.4 Instrumental digital threats

Based on literature, we have seen the following instrumental digital threats; swatting & intimidation, cyber espionage, data mining / OSINT, doxing, social engineering (digital), hacking, account compromise, malware and data theft/destruction and breakdown/ Distributed Denial of Service attack.

2.2.4.4.1 Swatting and intimidation

Our first instrumental digital threat is swatting and intimidation. Swatting is 'the use of technology to deceptively cause a heightened emergency and la*w enforcement response*'[60]. The police assume after a false report that there is a seriously threatening (often armed) situation with all the potential consequences; feared victims and "*a volatile scenario that can result in property destruction, injury, and death*"[61]. Those consequences are in the physical world, thus this threat is also hybrid. In 2020, an unknown caller in the US claimed that hostages would be held at the home of a leader of the Black Lives Matter movement (Melina Abdullah) in Los Angeles. Police surrounded her home, live footage was streamed on Instagram. Fortunately, the confrontation ended without violence. The caller said afterwards, that he wanted to "send a message" about his aversion to Black Lives Matter[62]. In the Netherlands, we hardly have any examples of swatting, where the false reporting is targeted at an individual (as opposed to an institution). Nevertheless, several false bomb threats from China and Hong Kong have been made to Europe in the past year. This happens to Chinese dissidents, but also to former China reporter Marije Vlaskamp. Fake bomb threats were made under her name, including to the Chinese embassy in The Hague[63]. The prosecution says, following a criminal investigation, that the IP addresses could be traced back to China and Hong Kong. In these cases, the false reports are made supposedly on behalf of the threatened individual, with all consequences, and were not directed at the (location of the) individual. That's why we have combined swatting and intimidation.

2.2.4.4.2 Cyberespionage

Then we want to highlight cyberespionage. According to Van Den Berg (2022) two points are crucial to understand cyberespionage. The rise of networked, digital technologies changed the means and methods for gathering intelligence with enormous consequences for its scale, reach, and impact. And second, in cyberspace there is a multitude of different actors, with or without relationships to the state, that may conduct intelligence-gathering activities. The digital tools that can be used in cyberespionage can also be deployed by other actors and with other motives.

A more recent development is that of spyware, although such malware, with slightly different scopes, has been around a lot longer. Spyware is software that collects and sends information to someone else unnoticed. Examples include keystrokes, screenshots, e-mail addresses, surfing behaviour or personal information such as login details, a location or a credit card number[64]. In 2021, journalists' collective Forbidden Stories, Amnesty International and international media partners revealed an investigation claiming that several authoritarian governments are using spyware called Pegasus from Israeli company NSO Group to spy on the smartphones of journalists and human

[60] https://www.fbi.gov/audio-repository/news-podcasts-thisweek-the-evolution-of-swatting.mp3/view
[61] https://www.fbi.gov/audio-repository/news-podcasts-thisweek-the-evolution-of-swatting.mp3/view
[62] https://www.csoonline.com/article/569815/what-is-swatting-unleashing-armed-police-against-your-enemies.html
[63] https://nos.nl/artikel/2470611-oud-china-correspondent-volkskrant-geintimideerd-en-bedreigd
[64] https://www.cyberveilignederland.nl/woordenboek

rights activists. NSO Group claimed to have developed this tool to spy on smartphones of terrorists and criminals[65], but the investigation found that the spyware is being used against (180) journalists, (600) politicians and (85) human rights activists in numerous countries[66].

The most recent threat analysis by the Dutch government shows that abuse of spyware by foreign actors is also possible in the Netherlands; '*it is conceivable that foreign powers deploy spyware against Dutch journalists, activists, dissidents or even politicians. It is also conceivable that criminals deploy spyware against asset managers, for example, in order to benefit from their knowledge about sensitive transactions*' (NCTV, 2023, p. 16).

2.2.4.4.3 Data mining / OSINT

Actors may now gather (meta)data in bulk and use data analytics to go through the data for relevant patterns (van den Berg & Kuipers, 2022), this called data mining. This is in line with OSINT. Some people are very experienced or trained in putting all kinds of Digital Puzzle Pieces together. By combining personal information from different sources, complete profiles about persons can be made. When focused on Social Media sources, this expertise is called (OSINT) and Social Media Intelligence (SOCMINT). In the case of high-profile individuals, you can think about shared personal information, active or passive (see Text Box 1: *Personal information in cyberspace*).

Personal information in cyberspace

Active sharing of personal information on the internet refers to situations where individuals intentionally and willingly disclose personal details about themselves. Some examples of active sharing include Social media posts, blogging, online forums, online surveys or questionnaires, online dating profiles. Think about online personal exposure of: Address(es), temporary whereabouts, telephone number, e-mail address, private relationships, profession/organisation, pictures/videos and other personal information (hobbies, etc).

Information individuals expose can be direct and indirect. If you post your address on your blog intentionally, you actively and direct share information with others. If you willingly share a picture of your daughter with a flag for her graduation at the front door (as Dutch often do), you actively share indirect personal information about yourself. Individuals not only share information actively in their everyday lives, but they also share information passively. By using apps, or visiting websites individuals share data streams, metadata and telemetry. This is the reason why many governments, also the Dutch government, denies civil servants to use of the Chinese App 'TikTok' on their phones (AIVD, 2023). So many apps want access to your location data, and thereby your home address and whereabouts are easily traceable. And what if a threat actor gets access to information like this? The Cambridge Analytica Scandal showed us that psychometrics, based on the behaviour on social media and questionnaires can build quite specific profiles about an individual and its preferences (Prichard, 2021). And then there is publicly available information from data breaches (leaked databases) and third-party data collection (and data brokers).

Kröger et al. (2021) categorized eleven categories 'in which personal data can be used against people, by criminal, private, public and governmental organisations, or by other individuals' including quite specific examples (Kröger et al., 2021):

Categories	Examples
Consuming data for personal gratification	▪ Ridicule ▪ Voyeurism
Generating coercive	▪ Threats of physical violence. ▪ Personalized rewards / sanctions ▪ Blackmail
Compliance monitoring	▪ Political oppression ▪ Domestic abuse ▪ Workplace surveillance
Discrediting	▪ Publication of Kompromat ▪ Political discrediting tactics. ▪ Legal evidence
Assessment and discrimination	▪ Identification of political opponents. ▪ Discriminatory hiring practices ▪ Discriminatory provision of goods and services
Identification of personal weak spots	▪ Torture ▪ Bullying ▪ Legal vulnerabilities
Personalized persuasion	▪ Commercial advertising ▪ Political campaigns ▪ Social engineering attacks
Locating and physically accessing the data subject	▪ Fraudulent messages and unsolicited advertising ▪ Threat messages and letter bombs ▪ Online sexual predation

[65] https://www.knack.be/nieuws/wereld/europa/pegasus-project-onderzoek-naar-spyware-bekroond-met-europese-persprijs/
[66] https://www.knack.be/nieuws/von-der-leyen-pegasus-affaire-totaal-onaanvaardbaar-indien-bevestigd/

Contacting the data subject	▪ Sex crimes ▪ Religious, racist and political persecution. ▪ Organized crime
Accessing protected domains or assets	▪ Social media burglary ▪ Identity theft.
Reacting strategically to actions or plans of the data subject	▪ Stifling of political resistance ▪ Predictive policing ▪ Forestalling legal action

Table 4 - Categories of personal data misuses (Kröger et al., 2021)

We haven't found a better overview of the risks of misuse of personal data, although some examples are more realistic and others are a bit more far-fetched. It is interesting to see that most risks are hybrid. Based on the article of Chen (2019) we miss two examples in this overview, based on the way China collects information about US-citizens in the context of cyber espionage:

1) The "assessment" and "development" of potential informants by State Actors;
2) And the way some foreign governments actively scan the internet to fill databases with as much information about (specific) citizens, there are signs that China is even behind some extensive and very sensitive data leaks in the US (Chen, 2019).

Text box 1 - Personal information in cyberspace

In 2020, the "*overseas key people*" database of Chinese company Zhenhua leaked[67]. It contained information on 2.4 million people worldwide and about 700 Dutch nationals. Of children or relatives of politicians or Dutch celebrities, the database contained sometimes summary and sometimes more complete information on education or career received, often supplemented by links to profile photos. In addition, public registers of Rechtspraak.nl and Interpol appear to have been consulted. One column listed other high-profile cases such as alleged tax evasion or other high-profile information. Company documents of the company Zhenhua show that the company sees sifting through and integrating freely accessible data on social media as a "cost-effective weapon in an intelligence war", seemingly hinting at opportunities and threats in analysing and disseminating misinformation (Balding et al., 2020; *No One Cares about Your Baby Pictures. Except China. – POLITICO*, n.d.).

2.2.4.4.4 Doxing

It is called doxing when this personal information gets published or used with wrong intentions; like stalking, harassing or a house visit. In addition, doxing has become an increasing problem so that a new law article on this has also been added to the penal code with effect from 2024. There are numerous examples of MPs being doxed[68], police officers[69], journalists[70], etc.

2.2.4.4.5 Social engineering (digital), hacking, account compromise, malware and data theft/destruction

Other digital threats or means are social engineering (digital). Which, through digital means and the use of psychological techniques, the receiving individual is tricked into handing over (sensitive) information that makes it possible hacking something or someone, compromise accounts, or trick a person into downloading rogue software which is called malware, which could lead for example to data theft/destruction. According to the latest threat assessment of the Dutch government, prepared by the NCTV (NCTV, 2023, p. 42), stolen data is mainly used 1) as a stepping stone for a cyberattack or cybercrime, 2) to blackmail individual victims (kompromat), 3) to cause reputational damage or 4) by using stolen data to create credibility for disinformation to be spread.

Some examples to illustrate these terms. Star Blizzard, a Russia-based actor is recently targeting organisations and individuals in the UK, and other geographical areas of interest. Targeted sectors include academia, defence, governmental organisations, NGOs, think tanks and politicians. Using OSINT to conduct reconnaissance, they identify hooks to engage their targets by researching an individual's interests and identifying their real-world social or professional contacts[71]. Their next step was creating email and social media accounts impersonating known contacts of their targets, they even used alleged conference or event invitations as lures. To appear authentic, the actor also created malicious domains resembling legitimate organisations. Star Blizzard's goal was to harvest credentials and session cookies to successfully bypass the use of two-factor authentication, which makes an account compromise possible with all the informational and physical consequences. Such as data theft/destruction, installing malware for example or locating an individual.

[67] https://nos.nl/artikel/2348443-zhenhua-files-ruim-700-nederlanders-op-uitgelekte-lijst-chinees-databedrijf
[68] https://www.rtvdrenthe.nl/nieuws/15717674/delen-van-persoonsgegevens-om-te-intimideren-wordt-strafbaar
[69] https://nos.nl/video/2462248-politieman-rick-werd-slachtoffer-van-doxing-duizend-euro-voor-mijn-adres
[70] https://nos.nl/regio/overijssel/artikel/226771-edwin-wordt-thuis-bedreigd-vanwege-zijn-publicaties-kvk-gooit-privegegevens-op-straat
[71] https://www.ncsc.gov.uk/news/star-blizzard-continues-spear-phishing-campaigns

Another example of hacking, for example, is the iLeakage side-channel attack; the attack allowed a threat actor to retrieve sensitive information from a Safari user's browser after it displayed a malicious, random web page. This information included viewing a user's Gmail inbox, accessing a user's YouTube watch history and collecting login details. You will understand that this allows you to obtain valuable information about an individual.

A Belgian MP who has been critical of China's systematic repression of its Uighur Muslim minority has become the target of a digital attack in 2023. Investigations have revealed that the attack came from the Chinese hacking unit APT31. In all likelihood, the parliamentarian opened a spearphishing e-mail, containing tracking pixels. For example, these 'small images' are hidden in an e-mail to collect general data about a computer system. With that data, follow-up steps for a digital attack can be taken[72].

But don't forget what can happen, for example, if smart devices are hacked, certainly in relation to individuals. The programme of a thermostat could give insight into when someone is home, the software of security cameras is rarely up-to-date and there are even public sites that can be watched with poorly secured cameras, or what if your smart car is suddenly turned off while driving[73]? The most recent threat assessment of the Dutch government, prepared by the NCTV (NCTV, 2023, p.53), also outlined a hybrid threat scenario in which a notary's client is threatened by criminals based on information obtained from the notary himself, obtained by a hack. Through the notary's smart thermostat, criminals gain access to the company network (and perhaps even broader), through which criminals had access to confidential data and files.

2.2.4.4.6 Breakdown/ Distributed Denial of Service attack (DDoS).

Our last digital threat is that of a breakdown/ Distributed Denial of Service attack (DDoS). In 2021, Turkish hackers claimed the temporary take-down[74] of the websites of Dutch politician and European Parliament's former rapporteur on Turkey Kati Piri and the website of the Labour Party after Piri called on Turkey to release political prisoners. The attackers generated such heavy traffic towards Piri's website that it was no longer accessible. Such an attack is called a (Distributed) Denial of service attack.

2.2.5 Threat actors

All threats in the overview are intentional. Threat actors behind these threats are range, according to Veld Van Den Berg (2020, p.33), script kiddies, ethical and unethical attackers, organized criminals and various agents of nation-states. In the threat assessment of the Dutch Government the overview of threat actors developed through the years, for a long time the focus was on 1) State actors, 2) Criminals, 3) Terrorists, 4) Hacktivists and 5) Script kiddies (Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2019). The following overview is slightly more comprehensive and distinguishes between targets, although we may find our high-profile individuals at the interface of government/citizens or private organisations/citizens. Because the threatened are mostly threatened at the individual level, but with an aim on the organisation they represent or have access to. The most recent threat assessment of the Dutch Government (NCTV, 2023) only distinguishes between state, criminal, ransomware and hacktivist threat actors.

If we check our threats and threat actors behind, as we have compiled them in the overview, we come reasonably far with the standard list of threat actors. However, we see limited actions from the 'script kiddies' and, at the same time, we miss an important group that is frequently covered in the literature regarding the more traditional threats, namely; angry citizens, with or without psychological problems.

In the context of threats to high-risk individuals, we will use the following typology from now on:

- State (sponsored) actors, a- notably very large digital- threat that is expected to increase further in the future (Adviescommissie toekomstbestendig stelsel bewaken en beveiligen, 2021).
- Private organisations, in the context of commercial espionage, or all kinds of influence aimed at improving competitiveness or sabotaging competitors (van den Berg & Kuipers, 2022).
- Criminals. Due to the increase in serious criminal threats, it is plausible that the number of persons who need long-term surveillance and security will increase. In addition, cybercriminals today presumably have the capacity to disrupt our Dutch digital infrastructure (Adviescommissie toekomstbestendig stelsel bewaken en beveiligen, 2021, p.30).

[72] https://nos.nl/artikel/2465699-belgisch-parlementslid-doelwit-digitale-aanval-na-kritiek-op-china
[73] https://www.autoblog.nl/nieuws/hacker-kraakt-10-automerken-opent-en-start-auto-zonder-sleutel-3435618
[74] https://twitter.com/ankaofficialtr/status/1360611894785167366

- **Terrorists**. While the digital capabilities of terrorists are moderate for now, we have seen examples of serious and convicted threats on Wilders, for example[75].
- **Hacktivists**
- **Angry citizens**, a large proportion of the threats our target group faces are angry citizens, with or without multiple issues (Bovenkerk, 2005; Drs. I.N.J. de Groot Mr. drs. L.F. Drost Prof. dr. J.C.J. Boutellier, n.d.; I&O Research, 2020; Kuiper, 2018; Marijnissen et al., 2020; Torre, E.J. van der et al., 2013; van Buuren, 2016).

2.3 Cyber Hygiene

Cyber hygiene is frequently compared to personal hygiene. Just as individuals adopt specific personal hygiene routines to uphold good health and well-being, cyber hygiene practices safeguard and maintain data security. Cyber hygiene encompasses the habits and precautions users or organisations can implement to ensure that sensitive data remains organised, secure, and protected against theft and external attacks. By following good cyber hygiene practices, individuals and organisations can reduce the risk of falling victim to cyber threats like hacking, identity theft, and malware attacks, '*cybersecurity experts estimate that 90 percent of cyberattacks could be defeated by implementing basic cyber hygiene and sharing best practices*[76]'. In this chapter we will determine how we see cyber hygiene in relation to high-risk individuals.

In the field of Cyber Security, there are a lot of container terms or buzzwords, and one of them is cyber hygiene. When a hack becomes public, whether it is the hack on the Maastricht University or the hack into the servers of the Democratic National Committee at the 2016 Presidential elections in the US, improving cyber hygiene and raising awareness are always top recommendations (Universiteit Maastricht, 2020, p. 27; Vishwanath et al., 2020, p. 1). And also in the aftermath of the ransomware attack on the UK's National Healthcare System (NHS) in which data was wiped and ransomware was spread worldwide, better cyber hygiene would have prevented spreading (*Government under Pressure after NHS Crippled in Global Cyber Attack as Weekend of Chaos Looms*, n.d.). Improving cyber hygiene seems to be the panacea to prevent the most common cyber incidents. The term is often used by policy makers, scientists and field experts.

The search results on this topic in scientific literature are quite thin. A structured search into peer-reviewed-articles in the database of the library of University Leiden using the keyword string "cyber hygiene", since 2020 resulted in 35 search results. Some of these results focus on specific target groups, or focus on specific countries. Others focused on specific topics within cyber hygiene like password use, insider threat, compliance, resilience, network monitoring, smishing. This explains why we also used grey literature, from reputable institutions such as the European Union Agency for Network and Information Security (ENISA).

2.3.1 Defining Cyber Hygiene

In the NIS2 Directive, Cyber hygiene plays an essential role. In article 49 (*NIS DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, n.d.) it states that "*Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices, including: 1) software and hardware updates, 2) password changes, 3) the management of new installs, 4) the limitation of administrator-level access accounts, and 5) the backing-up of data"*

Researchers of Carnegie Mellon University defined a Baseline Set of eleven practices on Cybersecurity hygiene for handling the most common and pervasive cybersecurity risks organisations face nowadays, as a part of the CERT Resilience Management Model (CERT-RMM) (Trevors, 2017).

In the same year, ENISA formulated 10 action points for hygiene (European Union Agency for Network and Information Security., 2016, p. 15). In the following table we have compared both sets of measures. Broadly speaking, these are similar, with strikingly no action item on user awareness in ENISA's list, and the item '*perform cyber threat and vulnerability monitoring and remediation'* also seems to be secured to a lesser extent. Still, there is considerable overlap, and again, this shows that the focus of these measures is at the organizational level.

[75] https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2019:5877
[76] https://www.gao.gov/products/gao-20-241

Table 5 - Comparison of cyber hygiene practices (CERT-RMM and ENISA)

Baseline Set of Practices Cybersecurity hygiene (Trevors, 2017)	**Action points for Cyber hygiene** (Enisa, 2017, p.15)
1. Identify and prioritize key organizational services, products and their supporting assets.	1. Have a record of all hardware so you know what your estate looks like
2. Identify, prioritize, and respond to risks to the organization's key services and products.	2. Have a record of all software to ensure it is properly patched
3. Establish an incident response plan.	8. Establish an incident response plan
4. Conduct cybersecurity education and awareness activities.	
5. Establish network security and monitoring.	4. Manage data in and out of your network
6. Control access based on least privilege and maintain the user access accounts.	6. Minimise administrative accounts
7. Manage technology changes and use standardized secure configurations.	3. Utilise secure configuration / hardening guides for all devices
8. Implement controls to protect and recover data.	7. Regularly back up data and test it can be restored
9. Prevent and monitor malware exposures.	5. Scan all incoming emails
10. Manage cyber risks associated with suppliers and external dependencies.	9. Enforce similar levels of security across the supply chain 10. Ensure suitable security controls in any service agreements (including cloud services)
11. Perform cyber threat and vulnerability monitoring and remediation.	

Most Cyber hygiene measures have to be taken at the organizational level. Where the responsibility for having strong passwords and regularly updating software lies with the users themselves. In the following article (50) in the NIS2 Directive the emphasis lays on the responsibility of users; '*in light of the growing number of connected devices that are increasingly used in cyberattacks. Efforts should be made to enhance the overall awareness of risks related to such devices*'. And ENISA stated that '*cyber hygiene should be viewed in the same manner as personal hygiene and, once properly integrated into an organisation will be simple daily routines, good behaviours and occasional check-ups to make sure the organisations online health is in optimum condition.*' (ENISA, December 2016, pp. 4). Cyber hygiene is thus something that should be integrated into an organization.

Of course, a secure infrastructure of the organisation where a high-profile individual works is needed. However, the threats we discuss in this thesis mostly affect the individual and sometimes even their personal space. What cyber hygiene measures lie with the functionaries themselves? And where can they be relieved by the organisation they represent?

> *"Having such an important concept be so vaguely defined, broadly construed, and, for the most part, untested, does little to improve cyber resilience."* *Vishwanath et al. (2020, p. 2)*

We found our answer in the recent study of Vishwanath et al. (2020). In their study, they conceptualise cyber hygiene, operationalise the definition, identify its sub-dimensions, and develop an inventory for cyber hygiene. In doing so, they identify measures for which the responsibility lies with individuals, or in which they can be relieved by their organization. But to be adequately protected, it is important that the whole set of measures be taken. Table 7 shows the Cyber Hygiene Inventory and underlaying measures.

Table 6 - Cyber Hygiene Inventory (Vishwanath et al., 2020)

Storage and device hygiene	1. Enabling firewalls on your computing devices
	2. Running a virus scan on any new USB or external storage device
	3. Monitoring different processes such as CPU, power, or network usage on your device
	4. Keeping virus protection updated
Transmission hygiene	5. Checking the quality of the SSL certificate when doing online financial transactions
	6. Storing logins and passwords on all Internet enabled devices
	7. Placing online alerts for your name or personal information
Facebook and social media hygiene	8. Assessing the authenticity of social media friend/information requests
	9. Knowing who you are connected to on social media
	10. Reassessing social media friends/connections
	11. Ensuring the location information is not leaked in posts
Authentication and credential hygiene	12. Changing default username from administrator to something unique on all internet enabled devices

	13. Changing default passwords on all internet enabled devices
	14. Managing how your browser stores passwords
	15. Creating new/unique logins and passwords for all your online sign-ins
Email and messaging hygiene	16. Checking an incoming email's header
	17. Checking a sender's email domain name
	18. Checking to see if email requests have grammatical or typographical errors

To determine whether high-profile individuals are sufficiently resilient in the face of today's hybrid threats, we will use this inventory to assess their resiliency.

3 Methodology

Based on our literature review, we concluded that we need more data to answer our research question and sub-questions. One of the most common qualitative methods to study new uncharted phenomena is Grounded Theory. Glaser and Straus laid its foundations more than 50 years ago, when quantitative research was the norm (Charmaz, 2008, p. 2). This research method has proven itself when it comes to mapping uncharted, contingent and dynamic phenomena, proclaimed on emergent logic. As we are mapping contemporary hybrid threats, targeting a very specific group(s), this method is ideally suited. However, we have decided to use the derived variant of the traditional Grounded Theory, namely the Gioia Method, for collecting qualitative data through expert interviews and data analysis. More than with Grounded theory, the Gioia Method encourages us to also apply originality in our theorising and not to be limited by advances in knowledge (Gioia et al., 2013, p. 16).

We have started our qualitative research by formulating our research question and an extensive literature review into the subcomponents; high-profile individuals, threats, threat actors and the concept of cyber hygiene. Based on scientific literature, grey literature, news items and case law we have been able to form a current understanding of these subtopics. We established two models, the mapping of high-profile individuals and the overview of contemporary physical, digital & hybrid threats.

Figure 10 - Research Method

We want to conduct interviews with experts to get a comprehensive and current overview. According to Gioia, the advantage of interviews with people constructing (organisational) reality, or "*knowledgeable agents*", is that they are able to put into words thoughts, intentions & actions that cannot be captured on the basis of a literature review (Gioia et al., 2013, p. 17). In addition, we try to give the most up-to-date picture possible in this study, on the one hand, of the hybrid threats our target group faces and, on the other, of the cyber hygiene measures an individual can take. Like many cyber-related issues, developments are rapid, so it is also inevitable that the literature will lag behind practice. Therefore, we decided to conduct semi-structured interviews with two groups of experts:

General experts

These experts have up-to-date and above-average knowledge about threats regarding high-profile individuals in the Netherlands. They have this knowledge because they have a role in the field of protecting high-profile individuals in the Netherlands, researched the phenomenon of threats toward one or more groups of high-profile individuals or even teach highly educated students about these topics. These experts are more or less familiar with digital threats and measures one can take to mitigate the risks thereof.

Specific experts

These experts have up-to-date and above-average knowledge regarding digital threats, informational (and physical) risks and measures regarding high-profile individuals. These experts have experience working with high-profile individuals within a specific occupational group. In doing so, they can not only give us an insight into the digital threats and measures, but also share their experiences what is encountered when individuals have to implement measures. We also discussed our overview of threats (figure 5) with these experts to see if they recognised the threats in practice, had examples, comments or additions.

A share of the experts interviewed are part of our own network. When we invited the experts for the interviews, we made explicit agreements that we wanted our study to be public and therefore we were only looking for information that could be shared publicly. In addition, agreements were made about informed consent, the (temporary and encrypted) storage of the recordings and transcripts, and the situation in which the expert would accidentally share confidential information anyway. This was important because we benefit from experts who are comfortable at the time they cooperate in the interview.

The recommended sample size for semi-structured interviews is according to Lyon et al (Lyon et al., 2015) between 5 and 25. At first, we organized 8 interviews, but after our second interview with a specific expert, we decided to schedule another interview to achieve theoretical saturation. According to Gioia (2013, p. 20) ten interviews can already result in 50 to 100 first-order themes.

Almost all respondents that have been approached by mail, were eager to cooperate in this study. They recognise the gap in knowledge in this particular area. This is our overview of interview candidates; the last columns show whether they are General Exerts (*GE*) or Specific Experts (*SE*).

Table 7 - Interview candidates

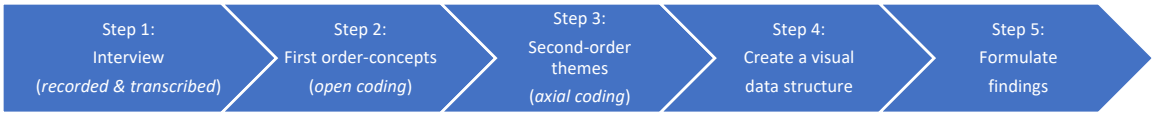
Interview Candidates			Nr.
1. Unit Head	Intelligence and Security Service	GE	1i
2. Senior Researcher	Research Agency	GE	2i
3. Professor	Vrije Universiteit, Amsterdam	GE	3i
4. Senior employee	Ministry of Justice and Security	GE	4i
5. Lecturer and researcher	Avans University of Applied Sciences	GE	5i
6. Head Lecturer	Leiden University	GE	6i
7. Security Expert	House of Representatives	SE	7i
8. Director	Rotterdam Port Cyber Resilience	SE	8i
9. Director	Persveilig (Press Safety)	SE	9i

3.1 Semi-structured interviews

We have conducted semi-structured interviews with our experts; they took 30-60 minutes each and most of them took place via video conferencing. They were a great opportunity to gain their extensive insights. We've prepared the interviews by formulating an interview protocol with quite broad and open questions. Depending on the progression of the interview, or interesting topics raised by an expert, either in-depth questions or additional questions were added. These relatively open-ended questions give the expert room to elaborate on topics that he perceives as worthy of mention or essential. The interview is less directive in nature and also keeps us as researchers on our toes to keep an open mind. The interview protocol of the General Experts differed from that of the Specific Experts and can be found in Annex 2.

3.2 Data analysis

The Gioia method is a suited method to develop new concepts from inductive research in a qualitatively rigorous way (Gioia et al., 2013, p. 15). After preparing, arranging and conducting the interview it is time for data analysis. According to the Gioia method there are five steps in this process (Gioia et al., 2013, p. 15), we explain them one by one.



We have recorded all interviews and transcribed them afterwards, this was our first step. We used the transcribe function in Teams[77] and also in Microsoft Word[78]. However, the reports turned out to contain a lot of linguistic errors. At first, we thoroughly edited two reports, which resulted in a considerable investment of time, but not necessarily more or better results. From there, we decided to work with the mediocre transcriptions and, where quotations were relevant enough to be used further, we edited these pieces using the recording. This method proved to be a lot more result-oriented.

Our next step is to analyse and code the transcripts into a set of first-order concepts (see figure 6 for an example). Our preference was to do our first coding step, perhaps a little old-fashioned, manually with the printed versions

[77] https://support.microsoft.com/en-au/office/view-live-transcription-in-microsoft-teams-meetings-dc1a8f23-2e20-4684-885e-2152e06a4a8b
[78] https://support.microsoft.com/en-us/office/transcribe-your-recordings-7fc2efec-245e-45f0-b053-2a97531ecf57

of the transcripts. This stroke resulted in 396 initial codes, which we then tabulated (in Apple's Freeform) and grouped based on the "open coding" concept. This resulted in 146 first-order concepts.

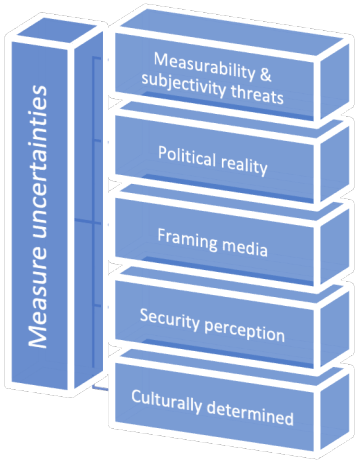


Figure 6 - Example second-order concept 'Measure uncertainties' and subjacent first-order concepts

In our third step, we will conduct a list of second-order themes by performing axial coding (Gioia et al., 2013, p. 6) and linking relationships between first-order concepts. This resulted in the following 15 second-order themes: high-profile individuals, social media, anti-institutionalist extremists, measure uncertainties, increase in individual threat level, threat actors, causes/ roots, digital threats, about digital threats, hybrid threats, physical threats, private sphere, undermining democratic rule of law, security measures and history. The overview with the first-order concepts and second-order concepts is in Annex 3.

In the fourth step a visual data structure is established, visualising the emerging concepts and themes. This visual representation should reflect both first and second-order concepts, their relationships and aggregate dimensions. As shown in the following data structure (figure 7).

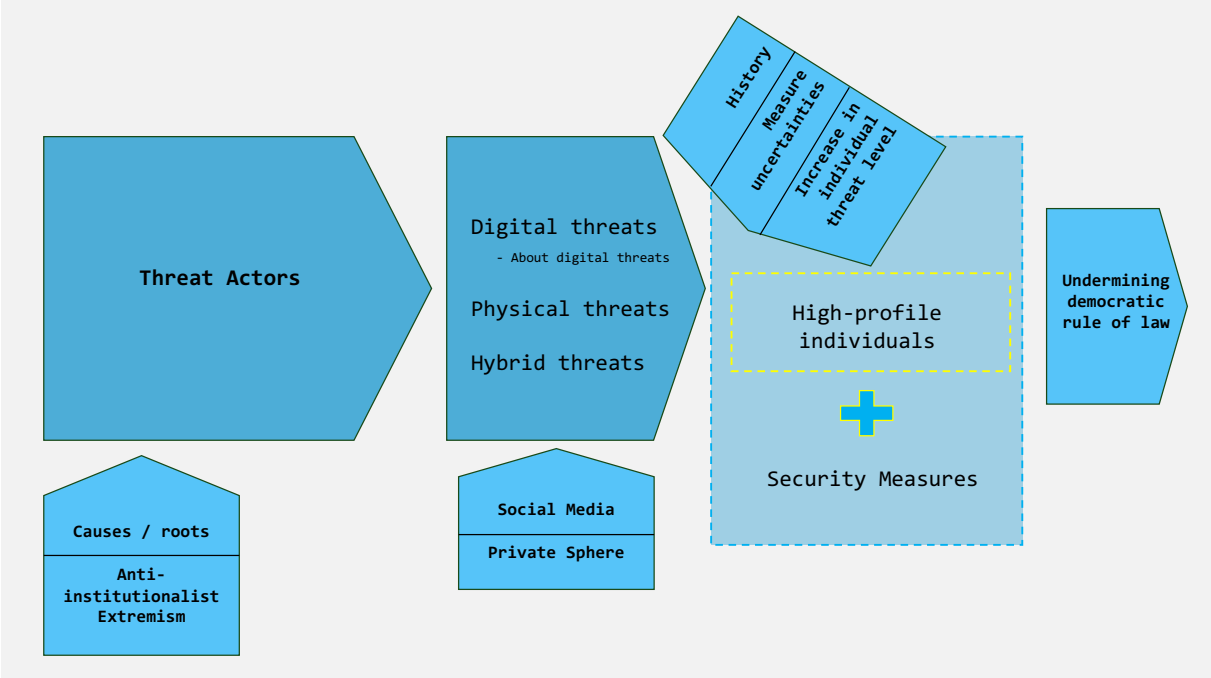


Figure 7 - Data structure (Source: created by author)

4 Results / Analysis

In this chapter, we present the results that emerged from the data analysis thematically and in order of our sub-questions.

4.1 High profile individuals

4.1.1 Group

According to our experts, the most threatened high-profile individuals belong to the following occupational groups: politicians and government officials, public safety personnel, legal professionals, media contributors, scientists, port personnel and civil servants. They recognize that the group of high-profile individuals is quite broad nowadays; *'Actually, anyone who says something that someone else does not like can become the object of threats'* (5i). This includes the opinions they represent and the institutions or organisations they represent; *'It concerns all kinds of people who represent the democratic rule of law*' (1i). Where work is done also matters *'working on the streets is by definition a threat*' (9i), and civil servants who have direct contact with citizens are also threatened above average (6i, 2i).

Threats faced by political officeholders have doubled since 2014. Some of these threats can be explained by the increased threats towards administrators at the local level. The introduction of the BIBOB Act has given local authorities more responsibilities. This has caused a shift of threats from organised crime towards local administrators (2i, 6i, 2i). At the same time, it also seems that local journalists reporting on sensitive cases in this context are also increasingly threatened (9i).

A group that falls outside the scope of this study but was also mentioned by experts (1i, 9i) are (former) citizens of other countries who have come to the Netherlands (diaspora), or more specific journalists belonging to diaspora (9i). The threats they face mostly come from state (sponsored) actors and aim, for instance, to silence dissidents or gain or maintain influence[79]. They, too, face above-average and hybrid threats, and the findings of this study could certainly be relevant to them.

Based on the interviews we have decided to remove 'health and social care professionals' from our mapping of high-profile individuals. Since some of the threats facing this group are more task-oriented, some are pointed at docters in their role as scientist (especially during COVID-19). Since individuals increasingly are being threatened for clearly speaking out opinions, we did leave the 'representatives of interest groups' in our final model (Figure 12).

4.1.2 Increase

Overall, our experts see an increase in individual threat levels, threats increase in both severity and quantity. *'The threat level, including the individual threat level, has increased in recent years. Incidents have always been there, but they are now more structural in character'* (3i). 'Structural incidentalism' is the phenomenon where apparently unrelated incidents are symptoms of a deeper cause (Helsloot et al., 2016, p. 5). '*The severity, nature and scale of the threats is new. But also how we as a risk society look at this phenomenon. How do we deal with risks and what risks are we willing to take?*' (5i).

At the same time, almost all interviewees acknowledge that threats towards individuals in office are of all times. In this respect, reference is made remarkably often to the research of Bovenkerk (2005). Whether they refer to the upturned front gardens of MPs and politicians, the ferocity of some serious incidents in the past or target groups he has researched and which have remained 'popular' ever since (2i, 3i, 5i, 6i). Therefore, the core of high-profile individuals seems to have roughly the same composition over the years. Although there have been some interesting shifts, towards, for example, civil servants with customer contact or government officials of Water Authorities (6i) or from lawyers to the judiciary (5i). The period of the political rise of Pim Fortuyn and his assassination is also a period in which politicians, administrators, and other prominent figures with a clear opinion (e.g. columnists) were threatened. In addition to threatening messages, bullet or powder letters were received regularly (2i). Several interview candidates mentioned that the events of this period have really done something to the way threats are experienced by those under threat, but perhaps also more widely in society (6i, 5i, 2i).

[79] https://www.aivd.nl/onderwerpen/ongewenste-buitenlandse-inmenging

The broadening of threats towards government representatives to institutions (including media, or science) has perhaps been the most striking in recent years. This can be explained by the development of anti-institutional extremism (1i, 3i, 5i). Parallel to this, threats from the criminal circuit have, in some cases, become a lot more violent. Although members of organised crime know remarkably well how to intimidate, while remaining within the confines of the law (2i, 3i, 6i).

4.1.3 Measuring security

When it comes to security statistics, interpretation is important. Our interview candidates rightly had some nuances to the statistics. What is the story behind the marked increase?

The increase in threats toward high-profile individuals is among others evidenced by the expansion of the Surveillance and Protection system, data coming from the Regional Information Organisation (RIO) of the Dutch Police (4i), figures from the Threatened Politicians Team (1i, 6i) and is evident from studies into threats within certain professional groups (3i, 2i) that threats have become increasingly structural in nature in recent years (4i, 3i, 2i). '*The increase in the threat level places such an incredible demand on the prosecution and the police that the police now hardly have time for neighbourhood policing. They don't do that for no reason'* (3i). Although some nuance seems appropriate, one of the experts indicates that the figures may represent a larger increase, than is actually going on (5i).

For instance, after the murder of lawyer Derk Wiersum, related to the Marengo trial, many gown carriers were given protection. Without this being preceded by individual threat assessments (5i), it is difficult to assess whether this measure is justified. Around 70% of the threats received by the Team Threatened Politicians are directed at Wilders. According to Wilders, the ministry of foreign affairs isn't doing enough to stand up for him; former minister Hoekstra said he finds these threats completely unacceptable and has raised this several times with Pakistani authorities and the embassy[80]. This could explain why every threat email or letter from Pakistan maybe gets different attention than other threat emails or letters, potentially creating a distorted picture (5i).

As Bovenkerk (2005, p.10) already noticed in his study, there is a difference between the objective level of threat (in acts of intimidation) and the subjectively perceived level of threat; '*the boundary between what is and is not meant and conceived as a threat varies across cultures, time periods, population groups and individuals, and moreover depends on the context*'. An expert gave examples of how threats towards prosecutors are perceived in Italy (4i). When such functionaries step into their role, they know it comes with strict security measures, such as living on a military base. Also, citizens react when an attack occurs differently; 'anger is directed against the perpetrators, not the government' (4i).

Discussing incidents has become much more normal in recent years (within the public domain), whereas only 30% did so a few years ago, today it is 70% (2i). This may mean, for example, that people are more likely to recognise threats as such, that there is a policy on this within organisations so that threat incidents are now reported centrally, and perhaps that feelings of insecurity are shared more widely. In parallel, the possibility is also that potential perpetrators may be inspired and copycat behaviour occurs (6i).

How we view threats is also related to the way threats to high-profile individuals are framed. '*The media lacks time, nuance or background knowledge to better interpret the figures on threats*' (5i). Incidents and research outcomes can be magnified as a result. Thus, the perception that the 2023 elections were the first in which politicians did not want to continue their careers because of threats is not a justified one (3i, 4i, 6i, 5i).

4.1.4 Undermining the democratic rule of law

All experts agree that threats against individuals in high-risk positions undermine our democratic rule of law to a greater or lesser extent (1i/9i). These threats create avoidance, cynicism/hardening, it can affect decision-making, some decide to perform another function or to no longer stand for election.

Avoidance of high-profile individuals can manifest itself in different ways; in some cases, functionaries will (physically avoid certain places or people), but this may just as well be substantive by preferring not to take

[80] https://www.ad.nl/politiek/ministerie-beklaagt-zich-in-pakistan-over-doodsbedreigingen-geert-wilders~aef5cbeb/

responsibility on specific files (6i). Cynicism and hardening occur particularly among individuals in high-risk positions where there is repeated victimisation or when the threats are spread over a longer period of time (6i).

Threats can actually affect decision-making. In the last annual survey on threats in the public domain by I&O research, 7% of officers admitted that they have sometimes made different decisions in their jobs because of threats or violence. But even more interestingly, 25% of respondents said they sometimes see this among their colleagues (2i). When threats or violence affect decision-making, it certainly touches on the foundations of our rule of law (2i, 6i).

When individuals retire from office for whatever reason, or no longer stand for election, it also affects our rule of law. According to an interviewed expert '*one in ten deputy politicians has considered resigning from his post due to threats of violence'* (2i).

4.2 What are the threats & threat actors for this specific group?

The experts interviewed gave various causes or explanations for an increase in threats towards individuals in high-risk positions. These are directly related to the threat factors and are therefore included in section. Where causes or explanations are related to a specific threat actor, we will include them in the description of the threat actor.

Something else that emerged clearly from the interviews is that threat actors also have their preferred threat agents. And that certainly the more advanced digital threats are -for now- primarily deployed by state (sponsored) actors (1i, 4i).

We begin this section with the threat actors, after which we discuss the digital, hybrid and physical threats that emerged in our interviews.

4.2.1 Threat actors

From the interviews with the experts, the following threat actors emerged; 1) angry citizens (with, or without *underlying mental health issues), 2) hacktivists, 3) extremism and terrorism, 4) organised crime, 5) insider threats and 6) State (sponsored) actors.*

4.2.1.1 Angry citizens

One of the most interesting findings of this study is that 'the angry citizen', '*with or without underlying mental health issues'* (2i), is behind a large proportion of the threats towards high-profile individuals. This threat actor appears frequently in studies on more traditional threats (threatening letters or threats via digital channels) (6i, 3i, 2i), but is certainly not a standard threat actor when talking about threats in cyberspace.

On the one hand, it involves citizens who do not feel heard (6i, 2i, 5i) and then start threatening them as a cry for attention. Generally, these citizens are threatened via the internet (e.g. by sending an e-mail, posting a message on social media, etc). In some cases, individuals have also been physically threatened or harassed after an angry citizen was informed, based on public information (e.g. the municipality's diary) (2i, 6i), where an officer was at what time. But increasingly, you also see examples of for example doxing, often involving issues where more citizens are dissatisfied (2i).

Extra vigilance around Potentially Violent Loners is in order here. Digital threat agents are becoming increasingly accessible to them too (6i).

A number of explanations were mentioned by our experts for the increase in threats overall. These also partly explain the increased threats from citizens. An important explanation is sought in our egalitarian and more individual society (3i, 1i). Individuals in certain positions, such as politicians or policemen, are expected to be approachable and accessible (1i). Parallel to this, respect in our society has decreased considerably, polarisation has increased significantly (6i, 3i), and violence (in case of threats) seems to be less eschewed (1i).

4.2.1.2 Hacktivists

Another threat actor that regularly emerges are citizens but organised around an ideological, but not a terrorist motive. Whether as a member of a group or not. International conflicts and socially controversial issues are triggers

for hacktivism (NCTV, 2023, p. 6). Hacktivists deploy multiple digital means to reinforce their message. Targeted threats to individuals in high-risk positions are also common, these can be quite traditional but often via digital channels. But more advanced digital means, like the use of more complex digital threats (such as compromising accounts, hacks, temporary outages, and information theft), are not inconceivable (7i). '*Hacktivists are mostly opportunistic, who often have potential and can really do something. But genuinely short-term (as opposed to state actors)*' (1i).

A number of experts referred to hybrid groups. On the one hand, there are activist interest groups where one branch is fighting an organisation in court, and where another branch is engaged in carrying out attacks on an organisation through in cyberspace (8i). On the other hand this referred to interest groups that, for example, first pursue common nitrogen goals out of anger but then agitate from the same composition when an asylum seekers centre in their region is announced. Or, for example, Extinction Rebellion, who primarily oppose climate change and biodiversity loss, speaks out about the Israeli–Palestinian conflict (6i). The latter can be explained by what Boutellier (2023) calls 'identity politics', which considerably strengthened over the past two decades. *'We come from a pillarized society, in which there were different collectives. The collective determined your identity and how you stood in society. Now you look for a community that suits you based on your identity. In the background of this, contradictions are sharpening. Because if your identity is very strong, it increases the chances of being harmed, causing the feeling that you are not being done justice or recognised*' (3i), something that commonly leads to threats (6i, 2i, 5i).

4.2.1.3 Extremism and terrorism

But where do we now place a phenomenon like anti-institutional extremism when looking at these threat actors? Is this an accumulation of individual angry citizens here? Or are these citizens, to a greater or lesser extent, organised around their ideals? High-profile individuals tend to represent a system against which, increasingly, hatred has developed; system hatred (5i, 3i, 6i). A major driver of this was the COVID-19 pandemic; during this period, *'social discontent seems to have turned into social unrest'* (6i). Until recently we spoke about 'anti-government thinking', but this has quickly broadened to 'anti-institutional extremism' (1i). '*A large part of the population is drawn to more or less extent by this narrative. And this is certainly not limited to certain regions or social classes. According to our estimate, it concerns more than 100,000 Dutch citizens, and this group seems to be growing rather than shrinking*' (1i).

We place this group of 'angry citizens' under the heading of extremists, and this is linked to the potential threat of violence according to our General Security Service. '*The spread of this narrative could also pose a threat of violence in the short term. Although instigators of anti-institutional extremism generally do not explicitly call for violence, the narrative provides a framework that there is an enemy - the 'evil elite' - with whom one is actually at war. Individual adherents may see this as a justification for violence and intimidation against representatives of institutions, such as politicians, judges, journalists and scientists'* (1i). This makes this threat actor of above-average relevance to our target group.

According to our Intelligence and Security Service (AIVD, 2019, p.10) '*jihadists in the Netherlands support an ideology of violence which they predominantly propagate in private online circles. Some jihadists threaten Dutch persons or objects and there are jihadists who genuinely wish to carry out violent terrorist ac*t'. Not eschewing violence is why terrorism and extremism are merged in our research. But given the threats our target group faces, terrorism is worth naming. Certainly, not every extremist is a terrorist, but a terrorist is an extremist.

4.2.1.4 Organised Crime

From organised crime, we see two main trends when it comes to threats to our target group. On the one hand, in recent years we see that the threat regarding gown-wearers and crime journalists has increased considerably, both in severity and scope. *'Organised crime has become much tougher'* (5i). These threats are mainly related to serious organised crime, such as around the Marengo trial. It is not inconceivable that such actors will eventually also use more sophisticated digital means in their threats (5i).

In addition, at a more local level, our target group is also considerably affected by organised crime, especially when financial interests are thwarted (5i, 3i, 2i). As described earlier, this is also related to the BIBOB Act introduced in 2003. This law regulates that local governments may '*refuse or revoke licences, subsidies, tenders and real estate*

transactions if there is a risk of criminals taking advantage of them'[81] *(2i, 3i, 5i)*. This also makes local government officials, or their representatives and administrators, more susceptible to undermining. But more often than not, members of organised crime know exactly what is punishable or not (6i), '*they proceed subtly, more often they 'just' intimidate instead of (punishable) threatening'* (2i).

Not only government officials are threatened by organised crime, such as motorbike gangs. Local journalists are also increasingly threatened; this development seems related to the responsibility shift to the local level as far as the Bibob Act is concerned.

Part of the threats from organised crime can be explained by the fact that the Netherlands offers a good opportunity structure for criminal activities. *'The drug economy has been able to establish itself so strongly in our society because they take advantage of the rule of law and the complexity of the system. That provides a great opportunity structure for foreign money flows. Criminal actors do not like to be stood in the way, for example, by judiciary judgments. It frustrates their use of the system*' (3i).

4.2.1.5 Insider Threats

Insider threat is -even in this context- a relevant threat actor, but especially in relation to the two other threat actors; organised crime and state (sponsored) actors.

Insiders are increasingly used as 'puppets' by criminals, where pressure will be exerted-by whatever means- on the internal employee (3i). In the port of Rotterdam, for example, this is a problem. Individuals, who may be blackmailable, are brought into contact with organised crime by information brokers. In doing so, information brokers take a very targeted approach, often using public digital sources.

It is notable that "*the Insider Threat is increasingly used deliberately as a tool. Where previously an internal employee was bribed, you now see that students from criminal networks are taking specific education with a view to specific future positions*'.

4.2.1.6 State (sponsored) actors

When it comes to digital threats in particular, we can still conclude that state (sponsored) actors are at the leading edge of this. Fuelled by geopolitical tensions, State (sponsored) actors are turning to cyberattacks as a means of pursuing their interests (NCTV, 2023, p. 6). With a wide arsenal of TTPs, access to public sources, and combined deployment of zero-day exploits, this group is perhaps the most exciting on the digital/hybrid front.

Roughly speaking, you have the opportunistic and the persistent state (sponsored) actors, and with so much power and hacking capabilities, as an individual, you can implement a huge number of security measures and make it hugely difficult for them, but then they still succeed' (1i). The most recent cyber threat assessment by the Dutch government also touched upon this '*the deployment of zero-days by state actors against Dutch targets is illustrative of the structural and sophisticated state digital threat against Dutch economic and political security interests*' (NCTV, 2023)

Fortunately, we do not see their- full palette of threat tools being used by other threat actors. But it is not inconceivable that, in the future, other threat actors may start using some of these TTPs (4i).

4.2.2 Threats

First of all, several experts acknowledge that the digital threats towards individuals in high-risk positions are not yet well crystallised (5i, 2i, 4i). '*Securing the safety of threatened individuals is in the portfolio of the NCTV and by nature focusses on the safety of their physical integrity. Shielding them from digital threats is something that needs further development over the next years.'* (1i). 'Digital threats are not yet integrated into our doing and working; by nature, the focus is on securing threatened individuals and keeping physical integrity safe' (1i). Several experts harshly question the extent to which digital threats can physically harm the individual (1i, 3i). Although the possibilities of sec digitally damaging someone physically are still very limited, think, for example, of hacking a driving smart car or aeroplane[82]. No examples of this yet known in the Netherlands (4i). At the same time, it is not

[81] https://www.amsterdam.nl/veelgevraagd/bibob-2255e#
[82] https://stories.kuleuven.be/nl/verhalen/eredoctor-karen-sandler-we-hebben-softwarevrijheid-nodig

inconceivable that a digital tool will be used to attack someone's physical integrity sooner or later. But, for now, the experts' main concern lies with hybrid and traditional physical threats.

Studies of threats within professions also focus more on traditional physical threats (2i), digital is really only included when the threat is sent over the internet. But even for a phenomenon like doxing, very few figures are known. Informational harm (van den Berg & Kuipers, 2022), or psychological consequences on individuals of digital threats has attention to a lesser extent (6I).

4.2.2.1 Digital threats

Our interviewed experts gave a wide range of examples of digital threats. In doing so, it remained a challenge to distinguish between digital threats aimed at the organisation and those aimed more at the individual. That boundary is not always very clear because the threats are mostly work-related.

So let's start with the most familiar digital threats, namely those sent through cyberspace. Think of a threat by e-mail, text message, through a digital channel or by a message posted on the internet. Since households started using the internet, some of the traditional threats have moved to cyberspace (HB, 6I). In addition, threats via the internet have increased significantly over the past decades (2i, 61, 3i). Here, it is important to keep the distinction between 'online hatred' or an actual death threat, it is a well-known phenomenon that people express hostile feelings more quickly via social media' (3i). In 99.9%, such a threat will not turn into an actual physical threat, but there is always the possibility of a 'lone wolf' (3i, 2i).

In general, attribution is difficult in digital attacks or threats (1i), this is also the case with threats via social media. It is easier for the threat actor to remain anonymous (HB). There is a difference between the nature of threats men and women receive. '*It is noticeable that when women are threatened it is more often on the person, and for men on the subject matter or profession. Threats on the person can be much harsher*' (2i).

Several experts describe risks that may arise for individuals from the digital theft or manipulation of data, or based on information obtainable from public sources (1i, 5i, 7i, 8i). These include harassment based on information obtained, or, for example, calling on others to do so as in the case of doxing. It is also possible to blackmail someone based on stolen or manipulated sensitive information. In addition, a threat actor can obtain -often sensitive- information about an individual that makes it easier to recruit them, either from a state actor or a criminal actor (or via his information broker) (8i, 1i).

That parties have an interest in spreading disinformation at this time - including about individuals in high-risk positions - may be clear. The motives behind this also differ for each underlying actor, whether from (anti-institutional) extremism or state actors. That this will also involve more frequent use of digital techniques enabling impersonation in the future, such as deepfakes or audio clips, is a real risk (7i).

Obtaining, manipulating or deleting sensitive or personal information requires access to a person's device, digital traffic or accounts. Private conversations for example, can be a good lever to pressure someone, the actors who engage in this are mostly criminal or state (sponsored), 'it's certainly not easy either, you have to have real recourses to get into someone's PC or phone' (1i). The possibilities for enabling this in this field are diverse; from social engineering (physical and digital), relatively simple compromises of poorly secured accounts (by guessing passwords or using previously captured passwords) to the more sophisticated hacks (e.g. use of zero-day exploits) (1i, 7i). In that context, several experts warn about malware, spyware, wipers and ransomware (8i, 7i, 9i). Spyware *'is a form of exploitation, which state actors could use when targeting individuals. Because they 1) want to use those individuals as agents or because they have interesting knowledge or 2) because they are a threat to the State's thinking. We see in the Netherlands that, for example, the Iranian regime is spying on its diaspora to keep an eye on (former) Iranian citizens*' (1i).

What should not be underestimated is the voluntary use of freeware by individuals. Where software is free, the individual, or in this case their personal data (active or passive), is often the payment (1i, 7i). For this reason, the Dutch intelligence service has also issued an advisory to ban the use of software originating from countries with offensive cyber programmes by central government officials (1i, 7i), examples include the banning of China's TikTok and AlieExpress and the Russian social network VKontakte[83]. Recently, the use of chatbots ChatGPT and Bard by

[83] https://nos.nl/artikel/2482736-ambtenaren-mogen-niet-meer-mobiel-shoppen-op-aliexpress-vanwege-spionagevrees

central government officials has also been banned for civil servants[84]. But consider also, the risks of listening in on (smart) devices and the sensitive information one can get from them. Recently, US media giant Cox Media Group (CMG) claimed that "*it is able to listen to ambient consumer conversations via built-in microphones in smartphones, smart TVs and other devices to collect data and use it to target ads'*[85].

Several experts know of situations where sites or social media accounts have been defaced (7i, 9i). However, they do recognise that this is more likely to happen at the organisational level than at the invidual level (fore example someones personal website, blog, social medium). The same goes for temporary breakdowns or Ddos attacks.
Where experts are at home in the modus operandi of State (sponsored) actors, they all warn against cyberespionage, and in relation; the insider threats (1i, 8i). What is striking in this respect is that more and more large organisations are taking the insider threat more and more seriously, by setting up internal programmes (1i).

Recent cases, which came to light during the interview period, again emphasise that espionage is highly relevant to part of our target group of individuals in high-risk positions.

In December 2023, the UK (and its allies) uncovered a series of attempts by Russian intelligence to target high-profile individuals and entities through cyber operations, with the intention of using the information gained to interfere in UK politics and democratic processes. The UK has identified the FSB (through the activities of Star Blizzard) as being involved in 1) the targeting, including spear phishing, of parliamentarians from various political parties from at least 2015 until this year, 2) the hacking of UK-US trade documents, 3) the hacking of the Institute for Statecraft, a UK think tank whose work includes initiatives to defend democracy against disinformation, and the more recent hacking of its founder, Christopher Donnelly, whose account was compromised from December 2021; in both cases documents were subsequently leaked. And 4) the targeting of universities, journalists, the public sector, NGOs and other civil society organisations, many of which play a key role in UK democracy"[86]

In the same month, the Belgian political party Vlaams Belang expelled an MP from the party for allegedly having been an informant for the Chinese spy agency for three years[87]. Among other things, the MP was said to have spread denials about China's crackdown on the Uighur minority, the Chinese origin of the Corona virus, and to have provided information about Belgian politician Charles Michel, who was soon after elected president of the EU government. This is the conclusion of the Financial Times, Le Monde and Der Spiegel[88].

It is also still the case that *'personal and physical contact really does have added value*' (1i) in the context of espionage. *'When our intelligence service caught Russians operating in the Dutch high-tech sector a few years ago, you also saw that Russian intelligence officers approached all kinds of individuals. And through those individuals, who by the way were not threatened themselves at all at the time, but manipulated, they did get information*' (1i).

Finally, several experts also see a major risk in all the personal information that can be found directly or indirectly about individuals online. Based on OSINT, or large-scale data mining, this personal (sensitive) information is processed, to then serve another objective. Experts recognise that individuals often do not have sufficient insight into the information that can be found about them within cyberspace and what-future- risks this may entail. As this threat is often combined with other threats, we will return to this under hybrid threats.

4.2.2.2 Hybrid threats

Several experts acknowledge that the number of hybrid threats is increasing (7i, 6i, 3i) and that this concern may be greater than solely the digital threat to individuals. *'There is still a real difference between digital threats and physical threats. There is a little bit of overlap. That's where it gets dangerous' (3i).* Precisely because the (traditional) focus in keeping an individual safe is on their physical and physical integrity (1i, 4i). Where digital overlaps with physical threats, digital preparatory acts may be involved (5i, 9i).

One expert points out that threat actors often follow the first steps of the (Lockheed Martin) Cyber Kill Chain[89], even in the case of an eventual physical threat; '*the scenario for ransomware is 95 % similar to that of "recruiting*'

[84] https://www.security.nl/posting/821754/Chatbots+ChatGPT+and+Bard+in+principle+prohibited+for+civil%20servants
[85] https://www.404media.co/cmg-cox-media-actually-listening-to-phones-smartspeakers-for-ads-marketing/
[86] https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes
[87] https://www.trouw.nl/buitenland/china-rekruteerde-belgische-politicus-frank-creyelman-voor-beinvloedingsoperaties~b757182d/
[88] https://www.ft.com/content/601df41f-8393-46ad-9f74-fe64f8ea1a3f
[89] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

an insider' (8i). Consider, for example, the deliberate distribution of someone's residential address (found through OSINT) with the call to harm someone, such as doxing. And so, in the Port of Rotterdam, for example, information brokers are used to target vulnerable key people working in the port. Public sources, such as social media, can give a good picture of someone's personal situation, loved ones, personal problems or someone's financial situation (8i). In 2022, in the port of Rotterdam, the following case occurred; *'Not only did the suspects target the computer systems of these companies (computer hacking), they also had and sought contact with corrupt employees of these companies in order to get into the relevant computer systems more easily with their help. [...] The use of (lethal) force, weapons, intimidation and threats is also an inseparable part of large-scale narcotics trafficking'*[90].

Also notable in this context was the recent news revelation that credit data companies are tacitly dealing in the personal data of millions of Dutch citizens. RTL News found (sometimes secret) home addresses of threatened ministers, journalists and lawyers in its databases. Credit information agencies create large databases in which they link consumers' personal data to information about their payment behaviour. They sell that information to other companies, including collection agencies and private investigation companies, which are looking for someone's address.[91] *'Through that search function, RTL News got hold of the current residential addresses of Dutch citizens who are being secured, partly because of serious threats from the criminal milieu. Think of crime journalist John van den Heuvel, the heavily threatened MP Ellian and also threatened ministers of state secretaries, who are not mentioned by name on request*.' This is against the law on several levels, yet it is currently happening. Earlier, the same news medium brought up that there is an active trade, for example, license plate data or home addresses, for example, through apps like Telegram[92].

4.2.2.3 Physical threats

Since a lot of research has already been done on physical threats, we returned to this to a lesser extent during the interviews. The most well-known types of physical threats were of course discussed, for example verbal aggression and threats on the street, accompanied by discrimination, racism and misogyny, bullet letters, home visits, office visits, as well as physical attacks on the person or their property (1i to 9i).

When it comes to physical threats, the phenomenon of 'target substitution' increasingly occurs (5i). This is '*when you can't get your intended target, you grab someone "right next door", for instance, an aunt, cousin or second cousin*'. That also makes guarding & securing a lot more complicated now. You see this now with those explosions in Amsterdam and Rotterdam neighbourhoods; they do not aim to kill people but to threaten them. [...] the whole family is taken as a target.'

If it is really about looting as far as espionage is concerned, it is also often not a threat to the individuals but much more focused on the information the person has. Incidentally, on average, they do it more on organisation than on persons' (1i). On the person anyway, it is often back in the Humint corner (1i, 7i) . This ties in with what we described within the Literature Review as Social engineering (in person).

4.3 What is Cyber Hygiene?

On the one hand, the term Cyber Hygiene is a panacea, but what measures it covers exactly and who takes care of which measures (individual, organisation, government) is far from always clear (6i, 7i). Of course, it is important that the organisations where the individuals in high-risk positions work take the necessary security measures to keep their digital infrastructure secure. Especially since threats-towards individuals in high-risk positions- are often work-related (4i).

Regarding organisations, basic principles from Cyber Hygiene and the Zero Trust concept are frequently mentioned. This holistic approach to cyber security, includes measures around authentication, authorisation, network segmentation (the use of implied trust zones based on policy enforcement) and monitoring to detect possible misuse (7i, 8i, 1i). This foundation should ensure that individuals can only access the information they need to work and that the necessary security measures are in place to keep this information safe. '*Through proper compliance, you can avoid putting individuals in a position where they are threatened because of the access they have. You*

[90] https://www.om.nl/actueel/nieuws/2022/09/12/strafeisen-tot-12-jaar-voor-grootschalige-handel-en-invoer-van-harddrugs-via-hacken-haventerminals
[91] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5425259/geheime-adressen-bedreigde-journalisten-politici-en-advocaten-te
[92] https://www.rtlnieuws.nl/tech/artikel/4789901/handel-rdw-kentekenregister-namen-woonadressen-nederlanders-lek

reduce the attack surface' (8i). A number of factors have been mentioned that make digital security of individuals complex.

Own responsibility & very personal

Whether it is the use of social media, someone's device, what someone does on the internet, or the apps someone uses, it has a personal and sensitive side (4i, 7i). Individuals certainly have their own responsibility in this. *'And how do we look at social media, for example? Is that someone's private sphere or rather the public domain?'* (4i). At the same time, individuals often have no idea what (personal) information about them can be found in public digital sources and what security risks they may pose. Whether it is a date of birth on LinkedIn, which matches 1-to-1 with the login code of someone's device, or photos that indirectly refer to someone's place of residence (9i).

Coercive measures

It is difficult to take coercive measures or enforce security measures regarding how individuals interact with their digital traffic, devices or online visibility (4i, 7i).

Awareness

Several experts express doubts about whether most individuals are uber capable of recognising a digital attack (1i, 5i, 6i). '*Everyone understands what a (physical) threat is, for example, if someone runs at you to attack you with a knife. In the digital domain, developments are going incredibly fast. There's an enormous amount of ease in what you can use digitally. Nice good browsers, cool new AI tools that can help you. But the downside of these developments is often just not visible*' (1i).

Psychological defensibility

Complementing all kinds of concrete measures to mitigate digital risks, it is important that individuals also learn how to deal with threats properly. "People need to become more resilient, you cannot build walls against online aggression" (2i). The psychological impact of threats can be enormous, especially when they occur over a long period of time or in the case of repeated victimisation (6i). It is important that (potentially) threatened individuals gain insight into their coping mechanisms and know when and how to ask for help (6i, 9i).

Gap between knowledge and behaviour

Experts acknowledge that there is a gap between knowing how to do something and actually turning this knowledge into desired behaviour. 'Even the most tech-savvy individuals sometimes take shortcuts' (1i). This can partly be explained by all kinds of theories in the context of behavioural economics: individuals do not always act rationally and in their own interests. There are several biases that cause people to make systematic mistakes in specific situations (Kahneman, 2016, p. 33). Kahnemann (2016), among others, describes this in his book 'Thinking, fast and slow'. His research shows that in 95% of cases individuals act based on their fast automated memory (*system 1*) and in only 5% of cases on their more rational and slow memory (*system 2*), see figure 8. So when a hacker sends a phishing email and uses various seduction techniques in it to get the recipient to quickly click on a rogue link, it will act on the recipient's fast memory (system 1). Partly for this reason, it is important that security in cyberspace is also offered to users increasingly easily and 'by default'; the use of a good password manager, automatic installation of updates, and the use of passkeys[93] instead of passwords, as well as Apple's lockdown mode[94], are good examples of this.

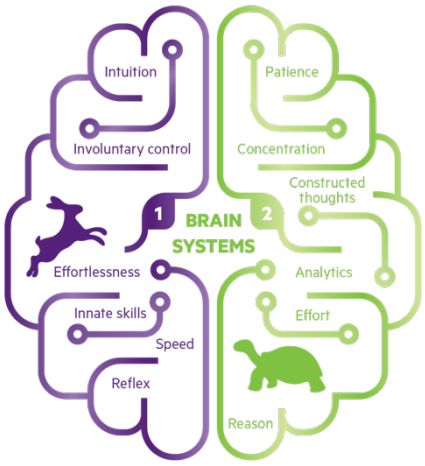


Figure 8 - Brain System 1 & 2
(source: https://mandarjoshi1595.medium.com/thinking-fast-and-slow-cf8634f30cae)

In addition, the advice can be as good and comprehensive as it is; if a state actor wants to gain access to an individual target there is little that can be done about it (1i), and there remains a gap between knowing what to do to stay safe and actually doing it, and enforcing security measures in the personal digital sphere is enormously difficult for employers or other security partners (4i, 7i).

[93] https://www.rtlnieuws.nl/nieuws/video/video/5415698/weg-met-je-wachtwoord-zo-werken-passkeys
[94] https://support.apple.com/nl-nl/105120

4.3.1 Recommended security measures

Part of our target group falls under the current Surveillance and Protection system or works elsewhere within the Central Government. Some of these functionaries receive a brochure from the NCTV or one of their security partners, containing measures around their digital security. This leaflet with 34 security measures was compiled by different security organisations within government[95] (7i, 4i, 1i).

The measures described are more extensive than, for example, basic awareness rules, like '*10 golden rules*' (7i) for working safely that are used in many organisations to share the most essential and basic tips on working safely, this basis is mostly aimed at the entire employee population, regardless of whether you are in a high-risk function or not.

Based on seven focus areas; general, software and apps, mobile devices, on the road and while travelling, private and home environment, contact Information and your environment, 34 measures are shared (4i, 7i). Interestingly, when we hold these measures alongside Vishwanath's Cyber Hygiene Inventory (2020), there is hardly any overlap. This is shown in Figure 9.

In part, this can be explained because the recommended measures in this brochure focus on what the individual can do themselves. They provide the individual with targeted action perspectives. Where some of the measures from the Cyber Hygiene Inventory are more at the organisational level than at the user's personal level, such as the measures around storage and device hygiene. Also, the advised measures are just of a different level of abstraction, but above all, they focus on measures a user can take to stay safe. An organisation will, for example, Management (MDM). MDM allows the organisation to manage end-user devices remotely. This will also happen, for instance, to a large proportion of individuals in high-risk positions working in central government.

Or consider measures in the area of securing email systems that an organisation can take, not often in practice will an individual check the header of an email upon receipt (Cyber Hygiene Inventory, no 17) or '*checking the quality of the SSL certificate when doing online financial transactions*' (Cyber Hygiene Inventory, no 5). In this area too, an organisation will prefer to take technical measures to mitigate risks in this regard.

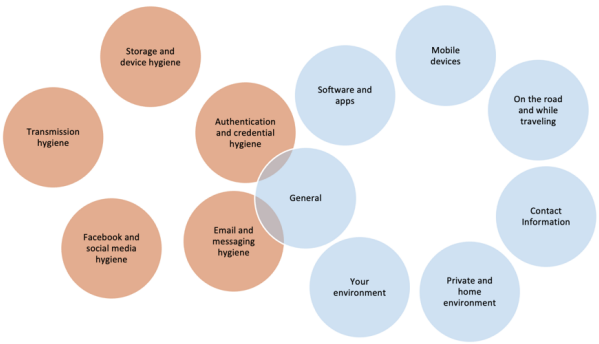


Figure 9 - Overlap between Cyber Hygiene Inventory & Measures "Your Digital Security" Brochure (AIVD and NCTV, April 2022) (Source: created by author)

Advice around the use of strong passwords, 2FA, a reputable password manager, VPN, privacy screens, antivirus, updates and smart devices were mentioned multiple times (3<) during the interviews. This advice is also reflected in the brochure. As such, these 34 measures, to a greater or lesser extent (e.g. regarding internal incident reporting procedures or the way to work with classified documents) also seem very applicable to our target group.

At the same time, experts recognize that providing good advice does not guarantee the actual implementation of all measures and safe behaviour. This responsibility for this lies predominantly with the individual.

[95] https://bio-overheid.nl/media/xmvhdbb0/brochure-digitale-veiligheid-tbv-rijksportaal.pdf

And again, *'if you are better protected than your "neighbour" they might threaten them instead of you*' remains true (1i). However, the latter is also still a major risk. When it comes to physical threats, the phenomenon of 'target substitution' increasingly occurs (5i). This is '*when you can't get your intended target, you grab someone "right next door", for instance, an aunt, cousin or second cousin*'. That also makes guarding & securing a lot more complicated now. You see this now with those explosions in Amsterdam and Rotterdam neighbourhoods; they do not aim to kill people but to threaten them. [...] the whole family is taken as a target.' (5i). That actors sometimes focus on the environment of those they want to influence is also something we see in espionage, '*if your immediate personal environment (through external influence) sees something as a problem (or not) then the influence is optimal*' (7i).

4.4 To what extent is a gap between Cyber Hygiene -measures and the security measures needed to protect against current threats?

Our experts saw the greatest danger in the hybrid threats, where, for example, digital preparation acts and then action is recorded. Partly, this is explained because many of our interview candidates know a lot about the more traditional threats where the physical integrity and physical security of individuals are the main concern.

If we then consider how much digital personal information about individuals can be found in cyberspace based on Open Sources and the fact that there is often still little focus on personal exposure, and subsequent safety risks this is certainly where experts' concerns lie (8i, 4i, 7i).

4.5 Are additional measures needed to make these individuals more digitally resilient?

Supplementary recommended security measures by our expert panel:

- In some organisations, **awareness talks** are held (4i), others offer **personal counselling sessions on digital security and hands-on help** (7i) and yet others offer, for example, **training on digital security** (9i). In the latter two examples, a brief OSINT survey precedes it to understand a person's online findability. Instead, other experts advise these individuals to undergo more general **resilience training**, in which they also learn to deal with the psychological effects of threats (2i, 6i). Apart from increasing one's resilience, it is also a good idea to *'make settlements around dealing with threats, sometimes it is better for a colleague to read them and act on them than for the threatened person to absorb them all themselves'* (6i).
- The **Internet Privacy tool** is being used within a number of professions today. With it, functionaries can check whether personal data is visible on the internet (with regard to specific sources such as the Land Registry, Chamber of Commerce, etc), **reduce the online visibility of personal data** and learn how to better protect personal data (9i).
- A **central registration** within an organisation where all threats, including individual threats, coming in through a variety of channels are registered can be an important tool. '*In my research, I found an civil servant who was threatened on a particular case and the alderman with that same case was also threatened, but so they didn't know about each other. And then you are so vulnerable on all fronts" (6i).* By **periodically reflecting** on the threats and the risks and taking **steps if necessary**. An angry citizen who moves on to a more concrete threat to an individual has often tried to express his or her dissatisfaction through other channels before that (6i, 2i). 'But just also those little situations, for example, when the civil servant(s) at the front desk have been subjected to emotional treatment by the same person several times. Then, an organisation has to act on that. You can't let these things happen' (6i).
- In extreme situations, a threatened individual may have to **leave his or her device behind** when they have to temporarily hide at a secure secret address (4i).

In addition, the advice can be as good and comprehensive as it is; if a state actor wants to gain access to an individual target there is little that can be done about it (1i), and there remains a gap between knowing what to do to stay safe and actually doing it, and enforcing security measures in the personal digital sphere is enormously difficult for employers or other security partners (4i, 7i).

5 Conclusion and discussion

5.1 Conclusion

The main question of this thesis attempts to answer the following exploratory research question: To what extent is Cyber Hygiene enough to protect high-profile individuals against the hybrid risks they face? Based on our research, we can conclude that Cyber Hygiene, particularly Vishwanath's (2020) Cyber Hygiene Inventory, does not provide sufficient measures to protect high-profile individuals from contemporary physical, digital and hybrid threats. We reached this conclusion after answering all sub-questions.

5.1.1 Who are high-profile individuals?

Based on our literature review, interviews and selection criteria we have defined the following 8 categories of high-profile individuals: public safety personnel, port personnel, politicians and government officials, civil servants, legal professions, media contributors, scientists and representatives of interest groups. These high-profile individuals; 1) represent or symbolize an organisation or institution; 2) have access to an organisation's 'crown jewels' (critical assets/targets); 3) or (access to) power; and are, therefore, specifically interesting to various threat actors. It is not about task-oriented threats, threats by acquaintances nor about indiscriminate victims of threats of violence.

Like Schuurman et al (2021, p. 31), we observe that there is a broad group of individuals at risk. These individuals play a role in maintaining the democratic rule of law. Either because they are part of the political system or within the open society (the vertical axes of our model, figure 10). Both are conditional for maintaining our democratic rule of law. Our second distinction in the model is based on the 'crown jewels' to which the individual has access. Not all functionaries we have categorised so far have a fiduciary role (access to confidential information/critical assets/targets), however, all of them seem to be vulnerable somehow. Think of civil servants who issue passports or port personnel with access to containers. This resulted in our mapping of high-profile individuals (figure 10).

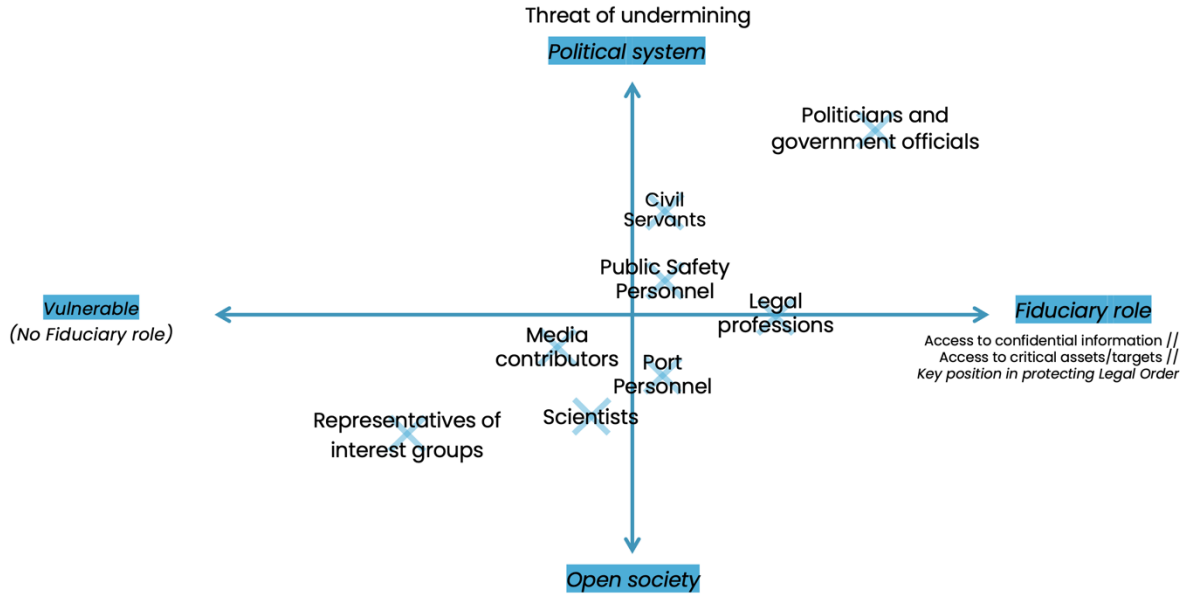


Figure 10 - Mapping of high-profile individuals (Version 1.0) (Source: created by author)

The core of high-profile individuals seems to have roughly the same composition over the years. Although there have been some interesting broadenings, for example towards civil servants with customer contact, government officials of Water Authorities or from lawyers to the judiciary. The broadening of threats towards government representatives to institutions (including media, or science) has perhaps been the most striking in recent years. This can be explained by the development of anti-institutional extremism. Parallel to this, threats from organised crime have, in some cases, become a lot more violent and partly shifted to threats on the local level. Increased international tensions, on the other hand, are, in turn, encouraging state (sponsored) and extremist actors.

Threats against individuals in high-risk positions undermine our democratic rule of law to a greater or lesser extent. They lead to avoidance, cynicism/hardening, which can affect decision-making, and some high-profile individuals decide to no longer stand for election or switch to another function.

Individual threats in perspective

Overall, our experts see an increase in individual threat levels. Threats increase in nature, severity and quantity. In this regard, there appears to be structural incidentalism; *'Incidents have always been there, but they are now more structural in character'* (3i). Thereby, almost all interviewees acknowledge that threats towards individuals in office are of all times, even with physical consequences and/or entering the private sphere.

The assassination of Fortuyn in 2002 and 2004 of the outspoken columnist and artist Theo van Gogh changed the perception of the public according to threats toward individuals; violent threats can actually lead to extreme violence, whether by the same perpetrator or not (Bovenkerk, 2005, p. 8). Partly as a result of lessons learned after the assassination of Fortuyn, the National Surveillance and Protection System was thoroughly reformed in 2003. Since then, it seems that threats have further increased in popularity, partly explained by coarsening for manners, a broader decrease in respect for authority, the rise (and role) of the Internet, an increase in conspiracy thinking and system hatred or what Boutellier (2023) refers to as 'identity politics'.

How we view threats is also related to the way threats to high-profile individuals are framed. *'The media lacks time, nuance or background knowledge to better interpret the figures on threats*' (5i). The perception that the 2023 elections were the first in which politicians did not want to continue their careers because of threats is not a justified one. There also is a difference between the objective level of threat and the subjectively perceived level of threat; '*the boundary between what is and is not meant and conceived as a threat varies across cultures, time periods, population groups and individuals, and moreover depends on the context*'. High-profile individuals tend to share their experiences with threats more widely nowadays. On one side, this may affect the subjective way individuals perceive their security. In addition, this may also lead to copycat behaviour. In addition, today's risk society also looks at (accepted) risk differently.

5.1.2 What are the threats & threat actors for this specific group?

Threats

The threats that high-profile individuals face nowadays are now quite diverse. Based on literature and our interviews, we have identified the most common threats we have encountered in our research into a model, distinguishing between expressive and instrumental threats and their manifestations, whether they are physical or digital. All our described threats are used against high-profile individuals, have (potential) physical or informational consequences, and are all intentional.

Our overview (figure 11) starts with the biggest threat in the Netherlands, namely expressive threats. According to Meloy (2004), expressive threats articulate the emotions of the threatener, which can arise from frustrations or ideology. The threatener threatens or intimidates someone out of frustration or anger, with no plan to influence (Torre, E.J. van der et al., 2013, p. 92). The category of expressive physical threats includes verbal threats/aggression, threats by telephone, threat letters, stalking/ belaying, ludicrous or symbolic actions, home and office visits, defamation and slander & discrimination.

Our list of expressive digital threats entails threats that are spread via cyberspace; threats via text messages, emails, via another digital medium (personally directed), or threats through (semi-) public posts on internet fora, websites or social media. In addition, we found two digital threats that are also only possible because of developments in Cyberspace; defacement and impersonation/ deepfakes.

Instrumental threats are "*intended to control or influence the behaviour of the threatened person*" (Bovenkerk, 2005, p. 10), there is no demonstration of emotion, and the threat actor sets a clear condition regarding the threatened person. Physically, these include verbal threats, threats by telephone and threat letters/ blackmail, visits at home or office, social engineering*/ HUMINT and* espionage.

We have inventoried the following instrumental digital threats; swatting & intimidation, cyber espionage, data mining / OSINT, doxing, social engineering (digital), hacking, account compromise, malware, freeware and data theft/destruction and breakdown/ Distributed Denial of Service attack.

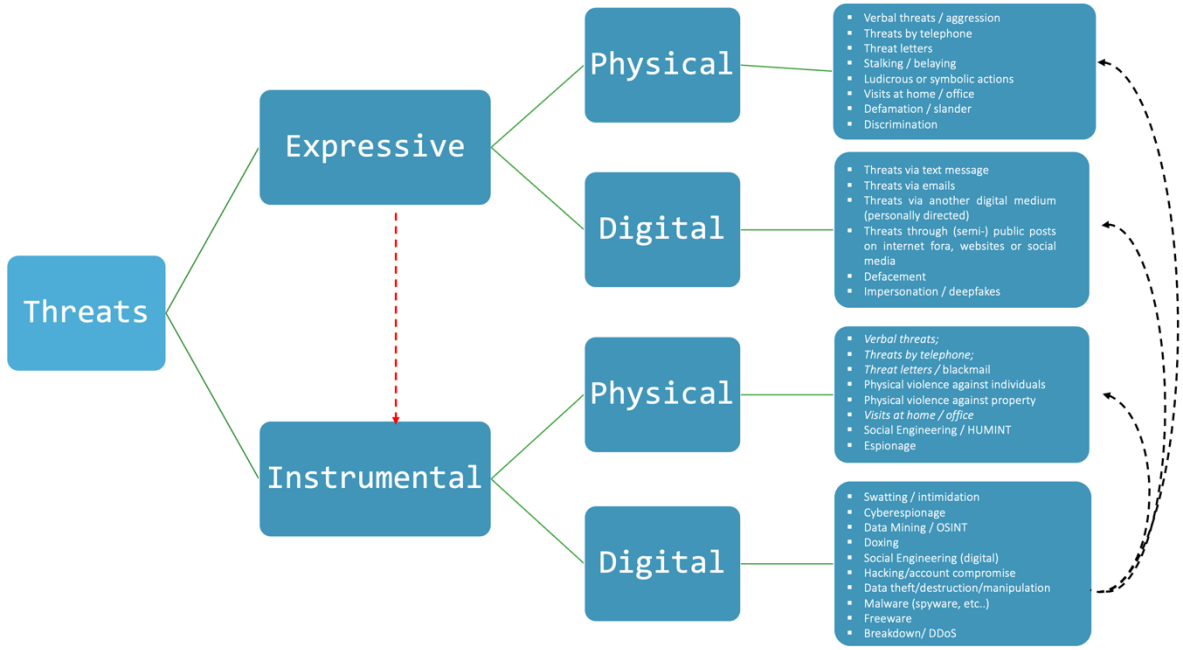


Figure 11 – Overview of physical, digital & hybrid threats regarding high-profile individuals (Version 1.0) (Source: created by author)

We have placed a few arrows in the overview (figure 11). A threat can be initially expressive but, due to interpretation, context or frequency, transition into an instrumental threat, visualised with a (red) arrow in the overview. At the same time, threats are also combined, these are hybrid threats. Black dotted lines arrows been added to the overview, in which case the prelude, or reconnaissance phase is digital and subsequent threats manifest in a another form.

Finally, we would like to reflect on the phenomenon of target substitution. Situations are conceivable where the threat is made against a family member, or loved one, with the ultimate aim of indirectly threatening a high-profile target. Target substitution is not shown in the overview, but could become increasingly relevant in the coming years, for both physical, hybrid and digital threats. When a threat actor accesses information of a high-profile individual through a colleague or acquaintance, there could be digital target substitution.

Threat actors

In the context of threats to high-risk individuals we see the following threat actors: 1) angry citizens (with, or without *underlying mental health issues), 2) hacktivists, 3) extremism and terrorism, 4) organised crime, 5) insider threats and 6) State (sponsored) actors.*

Angry citizens (with, or without underlying mental health issues)	One of the most interesting findings of this study is that 'the angry citizen' is behind a large proportion of the threats towards high-profile individuals. This threat actor appears frequently in studies on more traditional threats (threatening letters or threats via digital channels), but is certainly not a standard threat actor when talking about threats in cyberspace. We see this group in particular when it comes to (more traditional) threats via the internet. Most of the threats are expressive. Extra vigilance around 'angry citizens' with underlying mental health issues, the so-called Potentially Violent Loners is in order here. An important explanation is sought in our egalitarian and more individual society , the decrease of respect in our society, the increase polarisation and violence (in case of threats) seems to be less eschewed.
Hacktivists	Hacktivists deploy multiple digital means to reinforce their (ideological) message. Targeted threats to individuals in high-risk positions are also common, these can be quite traditional, but often digital channels are used. But more advanced digital means, like the use of more complex digital threats (such as compromising accounts, hacks, temporary outages, and information theft), are not inconceivable.

	Explanations for an increase in hacktivism can be found in Boutellier's (2023) '*identity politics', if your identity is very strong, it increases the chances of being harmed, causing the feeling that you are not being done justice or recognised, which* could lead to threats. In addition international conflicts and socially controversial issues are triggers for hacktivism (NCTV, 2023, p. 6).
Extremism and terrorism	Extremism, whether with a terrorist or more ideological motive, is another relevant threat actor. A characteristic of both is the fact that violence is not eschewed. We place anti-institutional extremism under the heading of extremists, and this is linked to the potential threat of violence according to our General Security Service. '*The spread of this narrative could also pose a threat of violence in the short term. Although instigators of anti-institutional extremism generally do not explicitly call for violence, the narrative provides a framework that there is an enemy - the 'evil elite' - with whom one is actually at war. Individual adherents may see this as a justification for violence and intimidation against representatives of institutions, such as politicians, judges, journalists and scientists*'[96]. This makes this threat actor of above-average relevance to our target group.
Organised Crime	Organised crime regarding gown-wearers and crime journalists has become much tougher last years. These threats are mainly related to serious organised crime, such as around the Marengo trial. It is not inconceivable that such actors will eventually also use more sophisticated digital means in their threats. In addition, at a more local level, our target group is also considerably affected by organised crime, especially when financial interests are thwarted due to the implementation of the BIBOB Act. This also makes local government officials, or their representatives and administrators, and local journalists more susceptible to undermining and thereby threats. But more often than not, organised crime knows exactly what is punishable or not, resulting in subtle -not punishable- threats. Part of the threats from organised crime can be explained by the fact that the Netherlands offers a good opportunity structure for foreign money flows and criminal activities.
Insider threat	is -even in this context- a relevant threat actor, but especially in relation to the two other threat actors; organised crime and state (sponsored) actors. Insiders are increasingly used as 'puppets' by criminals, where pressure will be exerted-by whatever means- on the internal employee (3i). In the port of Rotterdam, for example, this is a problem. Individuals, who may be blackmailable, are brought into contact with organised crime by information brokers. In doing so, information brokers take a very targeted approach, often using public digital sources. It is notable that "the Insider Threat is increasingly used deliberately as a tool. Where previously an internal employee was bribed, you now see that students from criminal networks are taking specific education with a view to specific future positions' (8i).
State (sponsored) actors	When it comes to digital threats in particular, we can still conclude that State (sponsored) actors are at the leading edge of this. Fuelled by geopolitical tensions, State (sponsored) actors are turning to cyberattacks as a means of pursuing their interests (NCTV, 2023, p. 6). With a wide arsenal of TTPs, access to public sources, and combined deployment of zero-day exploits, they are the most advanced threat actor on the digital/hybrid front. The most recent cyber threat assessment by the Dutch government also touched upon this 'the deployment of zero-days by state actors against Dutch targets is illustrative of the structural and sophisticated state digital threat against Dutch economic and political security interests' (NCTV, 2023) Fortunately, we do not see their- full palette of threat tools being used by other threat actors. But it is not inconceivable that, in the future, other threat actors may start using some of these TTPs.

Table 8 – Prominent threat actors regarding threats toward high-profile individuals

Something else that emerged clearly from the interviews is that threat actors also have their preferred threat agents. And that certainly the more advanced digital threats are -for now- primarily deployed by state (sponsored) actors, in which it is not inconceivable that criminal, extremist or maybe other threat actors will also use them in the future.

5.1.3 What is Cyber Hygiene?

Cyber hygiene is frequently compared to personal hygiene. Just as individuals adopt specific personal hygiene routines to uphold good health and well-being, cyber hygiene practices safeguard and maintain data security. Cyber hygiene encompasses the habits and precautions users or organisations can implement to ensure that sensitive data remains organised, secure, and protected against theft and external attacks. By following good cyber hygiene practices, individuals and organisations can reduce the risk of falling victim to cyber threats like hacking, identity theft, and malware attacks. On the one hand, the term Cyber hygiene is a panacea, but what measures it covers exactly and who takes care of which measures (individual, organisation, government) is far from always clear.

We found our answer in the recent study of Vishwanath et al. (2020). Their study conceptualises cyber hygiene, operationalises the definition, identifies its sub-dimensions, and develops an inventory for cyber hygiene. In doing

[96] https://www.aivd.nl/onderwerpen/extremisme/anti-institutioneel-extremisme

so, they identify measures for which the responsibility lies with individuals, or in which they can be relieved by their organization. But to be adequately protected, it is important that the whole set of measures be taken. Table 6 shows the Cyber Hygiene Inventory and underlying measures. To determine whether high-profile individuals are sufficiently resilient in the face of today's hybrid threats, we have used this inventory to assess their resiliency.

5.1.4 To what extent is there a gap between Cyber Hygiene measures and the needed security measures to protect against current threats?

Based on our 'Mapping of high-profile individuals' (figure 10), we asked ourselves whether, in terms of required security measures, it matters where you are classified in the overview. Based on the mapping and the threats perceived by occupations within it, we concluded that it hardly matters.

For instance, reducing an individual's online findability turns out to be a good measure, whether you work in the port and run the risk of coming into the picture of an information broker or if, as a member of government, you risk a home visit from a frustrated citizen. Setting 2FA, on all accounts, makes finding out someone's personal data a lot harder, apart from the fact that by doing so you also reduce the chances of account compromise, hacking or defacement. And that, at the same time, is the great thing about all these measures, and the corresponding desired behaviour. To reduce or mitigate human risk, all kinds of measures and secure behaviour can help. At the same time, the successful implementation of measures and secure behaviour(s) also reduces the likelihood of other risks.

Within the security community, the MITRE ATT&CK knowledge base[97] is widely used. Behind this knowledge base, there is a taxonomy that relates tactics/ techniques to defence measures. This knowledge base is based on real-world observations and focusses on the private sector, government, the cybersecurity product and service community. In addition, commonly used TTPs are described for each threat actor. This basis makes it possible to identify the most important threat actors and their preferred TTPs for a specific sector. Which mitigating measures (defences) are needed to protect yourself properly as an organisation can easily be identified using MITRE ATT&CK.

In the area of human cyber risk, the UK SEBdb[98] database is a very good example. The underlying taxonomy of this cyber security behaviour database relates the greatest human (cyber) risks to behaviours (a combination of practical measures and concrete behaviours). The behaviours are prioritised, from the most important (tier1) to the least important (tier4). This can help an individual decide which measures to prioritise first and have the greatest mitigating effects. In this way, during this research we did not look at the underlying target groups, threat actors, their TTPs and all appropriate measures and behaviours. That was beyond the scope of our study.

The interviews revealed that a large part of the (traditionally) endangered target group receives (advice based on) a brochure (‘Your digital security’, see annex 4) with advice and measures to increase their individual digital security. Based on seven focus areas; general, software and apps, mobile devices, on the road and while travelling, private and home environment, contact Information and your environment, 34 measures are described. Interestingly, when we hold these measures alongside Vishwanath's Cyber Hygiene Inventory (2020), there is hardly any overlap (Figure 9).

In part, this can be explained because the recommended measures focus on what the individual can do themselves. They provide the individual with targeted action perspectives. Where some of the measures from the Cyber Hygiene Inventory are more at the organisational level than at an individual’s level, such as the measures regarding storage and device hygiene. Also, the advised measures are just of a different level of abstraction. As such, these 34 measures, to a greater or lesser extent also seem very applicable to our target group of high-profile individuals and the contemporary threats they face nowadays.

At the same time, experts recognize that providing good advice does not guarantee the actual implementation of all measures and safe behaviour. A number of factors have been mentioned that make digital security of individuals tricky. Whether it is the use of social media, someone's device, what someone does on the internet, or the apps someone uses, it has a personal and sensitive side. Individuals certainly have their own responsibility in this. It is difficult to take coercive measures as an employer to enforce security measures regarding how individuals interact with their digital traffic, devices or personal online visibility. Several experts express doubts

[97] https://attack.mitre.org/
[98] https://www.cybsafe.com/research/security-behaviour-database/about/

about whether most individuals can recognise a digital attack or understand the downside of digital developments. High-profile individuals need to learn how to deal with threats properly. It is important that (potentially) threatened individuals gain insight into their coping mechanisms and know when and how to ask for help. And finally, experts acknowledge that there is a gap between knowing how to do something and actually turning this knowledge into desired behaviour and implementing security measures.

What can influence the extent to which someone is threatened is, for instance, their symbolic value (Bovenkerk, 2005, p. 11), the extent to which they have power (Bovenkerk, 2005, p. 11) or access to confidential information, and whether they are (already) a publicly known person. However, these factors do not appear to be dependent on one's position in the overview, but can be identified within individual target groups.

5.1.5 Are additional measures needed to make these individuals more digitally resilient?

Yes, shielding high-profile individuals from contemporary physical, digital and hybrid threats requires additional measures to Vishwanath's (2020) Cyber Hygiene Inventory. Overall, the breadth of our target audience of high-profile individuals has seen an increase in threats (nature and scope), but also in digital and, then especially, hybrid threats.

On the one hand, an expansion of measures will be needed. It would be good to understand the level at which the measures lie: with the individual themselves, the employer, the IT vendor, the government or, more specifically, within the Surveillance and Protection system of the NCTV.

Looking at the digital and hybrid threats we have now identified (figure 11), the measures in the brochure will be able to reduce or mitigate part of the risks. However, we miss for example;

- measures that increase privacy, such as a privacy screen and using privacy-safe browser;
- measures with regard to personal websites (to prevent defacement or breakdowns);
- shielding personal information in public sources e.g. the land registry (Kadaster), Chamber of Commerce, Municipal Personal Records Database, etc.;
- guidelines regarding the use of apps from countries with offensive cyber programmes;
- updating and securing personal devices, home computer(s), smart devices and other ICT assets (such as routers, etc) and making personal backups.

Supplementary security measures recommended by our expert panel:

1. Awareness activities take place within several organisations to educate high-profile individuals about digital risks and security, such as digital security training or resilience training. Some organisations use an even more personalised approach, where high-profile individuals receive personal advice in consultation and hands-on help.
2. It is important to reduce the online discoverability of high-profile individuals. Give individuals insight into the personal digital puzzle pieces that can be found about them online (based on an OSINT survey or the Internet Privacy Tool), and inform them about the risks of actively and passively sharing personal data and how a malicious person can act upon it. Give concrete tips on how to reduce online findability and, if necessary, offer help in this regard as an employer.
3. Regarding organisations, basic principles from Cyber Hygiene and the Zero Trust concept are frequently mentioned. This holistic approach to cyber security includes measures around authentication, authorisation, network segmentation and continuous monitoring to detect possible misuse. Under the motto 'never trust, always verify', this foundation should ensure that employees only have access to the information they need to work and that the necessary security measures are in place to keep this information secure. '*Through proper compliance, you can avoid putting individuals in a position where they are threatened because of the access they have. You reduce the attack surface*' (8i).
4. Apart from setting up a secure ICT infrastructure, organisations also have a role in making employees (psychologically) resilient. Address threats holistically within an organisation, also with regard to high-risk individuals. Record threats centrally, discuss them periodically and take steps if necessary. In addition, it can help an endangered individual if there is a working method around incoming threats, where the threatened individual does not face all the threats himself.

At the same time, the experts recognise that our target group is still insufficiently capable of recognising the severity and potential consequences of e.g. hybrid and digital threats. Meanwhile, we expect this target group to take personal responsibility and knowledge to take the measures needed to mitigate digital risks.

The biggest risk in terms of digital and hybrid risk is in terms of online findability among high-profile individuals.

If, in the future, threat actors were to expand a their TTPs, and, for example, make greater use of resources available to State (sponsored) actors, digital and hybrid threats could increase significantly in both severity and scale. With potentially very dangerous consequences. But think also, for instance, of hacking smart devices and the physical consequences that could have. In addition to the hybrid threat, this could also lead to affecting someone's physical integrity.

5.2 Limitations.

During our research, we aimed to explore a quite broad research question. We described many subthemes on the surface but did not dig deeper into them due to the scope of our research. During our research, we did not aim to:

- Give a complete and comprehensive overview of all threats regarding *high-profile individuals* in a specific period.
- Give exact numbers about threats. Nevertheless, we have tried to make meaningful statements about any increase or decrease. Quantifying the phenomenon of threats has proven to be problematic. Statistics regarding threats are often based on samples and surveys; these figures provide only feint accuracy, according to Bovenkerk (2005, p. 4).
- Modify a comprehensive and detailed list with digital security measures for all target groups. Most recommendations are formulated at a higher level of abstraction.
- Give criminological or forensic descriptions of threat actors, threat actors are contrasted with the most common threat actors referred to in the field of cybersecurity.
- Indicate the extent to which the threat is an incitement to violent action.
- Create a comprehensive taxonomy with all threatened occupational groups in relation to: threat actors; TTPs; motives; measures; and desired secure human behaviours.

Furthermore, high-profile individuals in the military, high-tech sector and more generally, private organisations may have received less attention in this study. According to van den Berg and Kuipers (2022), private organisations are adept at economic espionage or all kinds of influence to improve competitiveness or sabotage competitors via cyberspace. The bias towards high-profile public figures can be explained in part by the fact that many of the studies on threatened individuals were commissioned by governments and therefore had a specific public sector focus. The choice of interviewees will also have influenced our focus.

We also decided not to speak to the CISO's of organisations where many threatened high-profile individuals work, in addition to the general and specific experts. Although these conversations could certainly have given us interesting and deepening insights.

5.3 Areas for future research

Although in this study, we have made an attempt to zoom out and look at the bigger picture, whether it concerns the target group of high-profile individuals, the combination of threats they face or threat actors behind, the reality is a lot more obstinate. We have to be careful of pigeonholing.

In this respect, we also think it is a very good development that the Surveillance and Protection system of the NCTV is expanding in terms of the targeted high-profile individuals they support. And, in addition to focusing on threats to physical integrity, they are slowly broadening their focus. Overall, hybrid and digital threats towards high-profile individuals are likely to increase further in the coming years. Target groups, threats and threat actors will develop and new ones may emerge We see this thesis as a starting point for further research, on all sub-components, for example;

- ***threat actors***: TTPs, motives, what drives them?

- ***threats***; Does the subdivision work for the combination of physical and digital threats? Are there threats missing or new threats/TTPs emerging? Indicate the extent to which the threat is an incitement to a violent action.
- ***high-profile individuals;*** Research within the target group/CISOs on threats (/TTPs) (nature, quantity and perception, recognition). Comparison threats regarding high-profile individuals in other countries, is this a broader phenomenon? Deeper research into the role of employers and their responsibilities.
- ***Cyber Hygiene for high-profile individuals****:* Comprehensive research into needed measures (regarding current threats), behaviours, and other factors contributing to successful implementation/mitigation and thereby their resilience.

Not only do we need to think better about how to better reach this target group and what they need to do to adequately protect themselves from contemporary threats. There is also a role for policymakers, IT vendors, Big Tech, and employers to take the security of high-profile individuals seriously. How can an individual's online safety and privacy be better and easier to ensure in the future? In addition, a study of the effects of informational harm with regard to individuals would also be particularly interesting given the traditional focus on bodily integrity of the Surveillance and Protection system.

5.4 Discussion

Today's times call for a different and improved approach towards the current risks high-profile individuals are facing. We do not only need more or different measures, but also more research into the phenomenon of digital and hybrid threats regarding high-profile individuals, and we need an approach that considers behavioural aspects.

After all, it is well known that there is a gap between desired digitally secure behaviour and actual behaviour, which is partly why people are often dismissed as the weakest link[99]. But if we are aware of this, it will take more than a good brochure and a single explanation to make high-profile individuals aware of the risks they face nowadays and the measures and desired secure behaviour to minimise these risks.

One of the best pieces about the core problem of security awareness is '*152 Simple Steps to Stay Safe Online*' (Reeder et al., 2017). In this study 200 security experts were asked to give their top 3 advice for non-tech-savvy users. This outreach resulted in 152 unique and simple steps to stay safe online. Implementing this advice seriously takes at least several days of work for non-tech-savvy users, not even in a high-profile position. And perhaps therein lies the heart of the problem of Security Awareness. Technological developments in the past decades have been tremendous; never before have we been so dependent on technology, and so much of our personal data was online. Or as Pullitzer Price Winner Wilsons once beautifully put it in 2009[100];

'The real problem of humanity is the following:

We have Paleolithic emotions, medieval institutions and godlike technology.'

The (digital) threat surface has increased enormously (NCTV, 2023), for all individuals and especially for high-profile individuals. And there is sufficient reason to also take hybrid and digital threats more seriously in the coming years, especially given their consequential undermining effects on democracy. In the coming years, we will have to invest within our society to keep high-profile individuals resilient. The topic of digital security, therefore, deserves serious attention. From high-profile individuals themselves, the security expert community, employers, the government, IT suppliers, and policy-makers. For example when designing a future-proof Surveillance and Protection system.

In the case of digital and hybrid threats, structural incidents now predominate. However, the general increase in threats towards high-profile individuals that has started in recent years influenced factors such as social developments, technological developments (e.g. developments in the use of TTPs by threat actors), geographical

[99] https://www.schneier.com/blog/archives/2020/12/cellebrite-can-break-signal.html

[100] https://www.oxfordreference.com/display/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00016553

tensions and legislative developments. Is it not inconceivable that the threats faced by high-profile individuals will increase further in the future.

We cannot, therefore, wait any longer to make high-profile individuals more (digitally) resilient. By taking action now, we can make and keep high-profile individuals future-proof (digitally) resilient. Or how about potential future high-profile individuals, by taking measures now (for example as a student) and exhibiting digitally secure behaviour, they can be more resilient in the future. Ultimately, and hopefully, strengthening our Rule of Law.

But digital and hybrid threats also deserve serious attention broader within our society. By 2022, 99% of the Dutch population has used the internet[101], and '*4% of Dutch people (aged 15 years or older) said they had been victims of online threats and harassment in the past 12 months. That's 600 thousand people. Most of them, 2 per cent, were victims of online threats*'[102]. This makes it essential that everybody within our society becomes much more security aware in the coming years.

Right now, as we are more digitally active than ever, it seems that the lack of security awareness (not only regarding high-profile individuals) is a generally implicitly accepted risk. And with a view to future threats, this cannot be accepted any longer.

[101] https://www.cbs.nl/nl-nl/longread/rapportages/2023/online-veiligheid-en-criminaliteit-2022/2-internetgebruik

[102] https://www.cbs.nl/nl-nl/longread/rapportages/2023/online-veiligheid-en-criminaliteit-2022/6-online-bedreiging-en-intimidatie

6. References

References to research & articles, scientific or otherwise, can be found here.

In addition, footnotes have been used in this thesis, mostly referring to news articles, or other articles on cases, case law, or facts (other than scientific definitions).

Adviescommissie toekomstbestendig stelsel bewaken en beveiligen. (2021). *Adviescommissie toekomstbestendig stelsel bewaken en beveiligen*.

AIVD. (2004). *Van dawa tot jihad—De diverse dreigingen van de radicale islam tegen de democratische rechtsorde*.

AIVD. (2010). *Jaarverslag AIVD 2019.*

AIVD. (2014). *Leidraad aanwijzing vertrouwensfuncties.*

AIVD. (2019). *AIVD Annual Report 2019*. https://english.aivd.nl/binaries/aivd-en/documenten/annual-report/2020/09/03/aivd-annual-report-2019/AIVD+Annual+Report+2019.pdf

AIVD. (2021). *Jaarverslag AIVD 2020*.

AIVD. (2023, February 23). *Beschouwing risico's gebruik applicaties uit landen met een offensief cyberprogramma gericht tegen Nederland* [2023]. https://open.overheid.nl/documenten/ronl-71c4f5e2a1ae61e65fd9b8983d8860887651c9a0/pdf

AIVD, MIVD & NCTV. (2022). *Dreigingsbeeld Statelijke Actoren —November 2022*.

AIVD (2023). *Anti-institutioneel-extremisme in Nederland*

Balding, C., Potter, R., & et al. (2020). *Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua*. https://dx.doi.org/10.2139/ssrn.3691999

Bart van der Sloot, Yvette Wagensveld, & Bert-Jaap Koops. (2021). *Deepfakes; de juridische uitdagingen van een synthetische samenleving*. Tilburg Institute for Law, Technology, and Society.

Boutellier, H., Steden, R., Eski, Y., & Boelens, M. (2020). Een einde aan ondermijning: Over de opkomst en werking van een nieuwe veiligheidsstrategie. *Tijdschrift voor Veiligheid*, *19*(1), 3–16. https://doi.org/10.5553/TvV/187279482020019001001

Bovenkerk, F. (Ed.). (2005). *Bedreigingen in Nederland*. Augustus.

Charmaz, K. (2008). *Grounded Theory as an Emergent Method*.

Chen, M. S. (2019). *China's Data Collection on US Citizens: Implications, Risks, and Solutions*.

Cialdini, R. (2020). *Invloed de zes geheimen van het overtuigen* (Zesde editie). Boom.

Drs. I.N.J. de Groot Mr. drs. L.F. Drost Prof. dr. J.C.J. Boutellier. (2010). *Bedreigers van politici: Risico's en interventiemogelijkheden*.

ECLI NL RBROT 2021 7111.pdf. (2021).

ENISA. (2008). *Social Engineering – Exploiting the Weakest Links*.

European Union Agency for Network and Information Security. (2016). *Review of cyber hygiene practices.* Publications Office. https://data.europa.eu/doi/10.2824/352617

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms. (n.d.). Retrieved 3 November 2023, from https://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/

Helsloot, I., Scholtens, A., & Vlagsma, J. (2016). *Toeval of structureel incidentalisme?* https://crisislab.nl/wordpress/wp-content/uploads/Rapportage-Kijfhoek-def-mei2019-gecomprimeerd.pdf

I&O Research. (2020). *Bedreigingen en intimidaties van burgemeesters in relatie tot de bestuurlijke aanpak*. https://repository.wodc.nl/handle/20.500.12832/2486

Kahneman, D. (2016). *Ons feilbare denken Thinking, fast and slow*. Business Contact.

Kröger, J. L., Miceli, M., & Müller, F. (2021). How Data Can Be Used Against People: A Classification of Personal Data Misuses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3887097

Kuiper, M. L. (2018). *Het woord en de daad: Kenmerken van dreigbrieven en de intenties waarmee ze geschreven werden*. Boom

criminologie.

Leukfeldt, R., Kentgens, A., Prins, E., & Stol, W. (2015). Alledaags politiewerk in een gedigitaliseerde wereld. *bovenkerk*.

Lyon, F., Möllering, G., & Saunders, M. N. K. (Eds.). (2015). *Handbook of research methods on trust: Second edition* (Second edition). Edward Elgar Pub.

Marijnissen, D., Kolthoff, E., & Huberts, L. (2020). Coping With Threats and Harassment in Politics. *Public Integrity*, *22*(5), 485–506. https://doi.org/10.1080/10999922.2020.1714410

Meloy, J. R., James, D. V., Farnham, F. R., Mullen, P. E., Pathe, M., Darnley, B., & Preston, L. (2004). A Research Review of Public Figure Threats, Approaches, Attacks, and Assassinations in the United States. *Journal of Forensic Sciences*, *49*(5), 1–8. https://doi.org/10.1520/JFS2004102

Middelhoven, L. K., & Driessen, F. M. H. M. (2001). *Geweld tegen werknemers in de (semi-)openbare ruimte*. Bureau Driessen, Sociaal Wetenschappelijk Onderzoek.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2019). *Cybersecuritybeeld Nederland—CSBN 2019*.

Nationaal Coördinator Terrorismebestrijding (NCTb). (2010). *Individuele bedreigers van publieke personen in Nederland.pdf*.

NCSC. (2012). *Van herkenning tot aangifte*.

NCTV. (2023). *Cybersecuritybeeld Nederland—CSBN 2023*.

NIS DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. (2022). https://eur-lex.europa.eu/eli/dir/2022/2555

No one cares about your baby pictures. Except China. – POLITICO. (n.d.). Retrieved 21 April 2023, from https://www.politico.eu/article/china-baby-pictures-cares/

PersVeilig. (n.d.). *Onderzoek veiligheid journalisten*. PersVeilig. Retrieved 26 May 2023, from https://www.persveilig.nl/over-persveilig/onderzoek

Prichard, E. C. (2021). Is the Use of Personality Based Psychometrics by Cambridge Analytical Psychological Science's "Nuclear Bomb" Moment? *Frontiers in Psychology*, *12*, 581448. https://doi.org/10.3389/fpsyg.2021.581448

Reeder, R. W., Ion, I., & Consolvo, S. (2017). *152 Simple Steps to Stay Safe Online:*

Schuurman, B., van Buuren, J., & Bakker, E. (2021). *Dreigingsontwikkelingen relevant voor het stelsel bewaken en beveiligen: Een blik op verleden en mogelijke toekomst*. ISGA Rapport.

Adviescommissie toekomstbestendig stelsel bewaken en beveiligen. (2021). Adviescommissie toekomstbestendig stelsel bewaken en beveiligen.

Torre, E.J. van der, Gieling, M., Bruinsma, M.Y., Jans, M., & Linden, M. van der. (2013). *Bedreigen en intimideren van OM- en politiemedewerkers*. WODC Rapport 2231.

Trevors, M. (2017). *Cyber Hygiene: A Baseline Set of Practices*.

Universiteit Maastricht. (2020). *Cyberaanval Universiteit Maastricht*.

van Buuren, J. (2016). *Doelwit Den Haag? : Complotconstructies en systeemhaat in Nederland 2000-2014*.

Van Den Berg, B., & Kuipers, S. (2022). Vulnerabilities and Cyberspace: A New Kind of Crises. In B. Van Den Berg & S. Kuipers, *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1604

van Miltenburg, C., van Straaten, G., & Bouwmeester, J. (2022). *Agressie, bedreiging en intimidatie bij advocaten*.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Wallström, K., Korsell, L., & Skinnari, J. (2007). Unlawful Influence Directed at Public Servants: From Harassment, Threats and Violence to Corruption. *European Journal of Crime, Criminal Law and Criminal Justice*, *15*(3–4), 335–358. https://doi.org/10.1163/092895607X231198

Annex 1- Categorised threatened occupational groups based on inventory

Public Safety Personnel	• Police officers • Penitentiary Employees / Security personnel prisons • Public transport personnel • Inspectors and auditors • Probation officer • Special investigating officer at the State Forestry Commission • Youth care workers • Employees National Expertise Team Youth Protection (LET JB) • National High-Risk Team employees of the Child Protection Council
Health and Social Care Professionals	• Social service employees • General practitioners • Hospital employees • Psychiatry employees • Home care employees • Addiction care workers • Social workers • Psycho-social workers, etc. • Employees Youth Protection • Employees GGD • Employees nursing homes
Teachers	• Teachers
Service employees	• Bank employees • Prostitutes • Cab drivers • Postal workers, deliverers • Fairground operators • Housing corporation staff Sales staff / Real estate agent • Catering staff
Port personnel	• Port Personnel
High-Tech Industry Personnel	• Director/employee high-tech company
Politicians & Government officials	• Mayors • Aldermen • Prime Minister / Ministers • Politicians
Civil servants	• Civil servants
Royal House	• Members of the Royal House
Legal professions	• Prosecutors • Employees of the Public Prosecution Service • Judges • Employees of a law firm (2x) • Lawyers • Notaries • Employees of the Council of the Judiciary • Bailiffs
Media contributors	• Journalists • Columnists • Photographers • *Artists*
Prominent sportsmen	• Prominent sportsmen
Scientists	• Scientists
	• University employees
Representatives of interest groups	• Representatives of interest groups
Members of diaspora communities	• Members of diaspora communities

Table 9 - Categorised threatened occupational groups based on inventory

Annex 2- Interview Protocols

A2.1 Interview Protocol General Experts

1) You know a lot about threats in the Netherlands, which functionaries/professional groups are mostly threatened in your view and from your expertise?
    i. ***In-depth:*** What connects these groups? / Where are the differences/ similarities? / Is this group new or has it always been threatened?
2) What kind of (threats) does this target group/ these target groups face?
    i. ***In-depth:*** Physical/digital/hybrid? Do you see any developments regarding these threats? Decrease/increase? Private realm? Man/woman.
3) Which threat actors are behind these threats?
    i. ***In-depth***: Developments? New? Changed over time? Motives? Tangled loners/ Lone wolfs VS. script kiddies/ hacktivists?
4) Do you have explanations for the developments regarding threats?
5) To what extent do the outlined threats affect the democratic rule of law? And why?

A2.2 Interview Protocol Specific Experts

1) What digital and hybrid threats do (specific) employees in your organisation face?
2) Which threats have existed for some time, which are relatively new?
3) What measures do you recommend to the target group to mitigate the risks of these threats?
4) To what extent do these measures actually mitigate the risk of these threats?
5) Who is responsible for implementing these measures?
6) What is needed to make this target group more digitally resilient?

Annex 3- First and second order concepts

First order concepts	Second order concepts
1. Politicians & government officials 2. Civil Cervants 3. Scientists 4. Media Contributors 5. Legal professions 6. Public Safety Personnel 7. Diaspora	1. High-profile individuals
8. Chance lone wolf 9. 99.9% actual threat 10. Ressentiment 11. Faster 12. More subjective 13. Anonymous 14. 'Child's play' 15. Alternative sources of knowledge 16. Male/female	2. Social media
17. They represent the government 18. They represent institutions 19. Symbolic value	3. Anti-institutionalist extremists
20. Measurability & subjectivity threats 21. Political reality 22. Framing media 23. Security perception 24. Culturally determined	4. Measure uncertainties
25. Increase 26. Severity of threats increases	5. Increase in individual threat level
27. Insider threat 28. Hacktivism 29. Extremism 30. Criminals 31. Angry citizens (individual) 32. Angry citizens (grouped) 33. Tangled loners / PGE 34. Script kiddies 35. Terrorist/ extremist 36. Conspiracy thinkers 37. Extreme right/left 38. Port staff	6. Threat actors
39. Egalitarian society 40. Opportunity structure (NL & getting in the way) 41. Approachability/accessibility 42. Decreased respect 43. System hatred 44. Identity politics 45. COVID Pandemic 46. Violence less shunned 47. Conspiracy theories	7. Causes/ Roots
48. Cybercrime 49. Medical data 50. Spyware 51. Compromised phone 52. Doxing 53. Kompromat 54. Malware 55. Obtaining information 56. Disinformation, misinformation 57. Cyberespionage 58. Recruit 59. Freeware 60. Manipulation 61. Digital preparatory acts 62. OSINT 63. Hacking 64. Social engineering 65. Insider Risk 66. Threats VIA Social Media / Apps	8. Digital threats

67. Harassment 68. Blackmail 69. Compromised accounts (socmed, not org) 70. Defacement 71. Impersonation 72. Swatting 73. Ransomware 74. Wipers 75. Ddos	
76. Preparatory acts 77. Increasingly hybrid threats 78. Information brokers 79. Kill chain	9. Hybrid threats
80. Target protein substitution 81. Bullet letters 82. Spy 83. Physical contact* / Humint* 84. physical physical integrity 85. Structural incidents 86. Extreme violence 87. Destruction 88. Verbal aggression 89. Misogyny 90. Discrimination 91. Threatening phone calls/letters 92. Break-in 93. Home visits 94. Office visits	10. Physical (threats)
95. Cannot physically harm individual 96. Responsibility 97. Digital as a 'new' tool 98. Not crystallised 99. Attribution (Tricky) 100. Recognise digital attack/threat? 101. Dealing with digital threats 102. Digital as a means of attacking bodily integrity 103. Influencing/ threatening **via** loved ones, etc..	11. About digital threats
104. Achilles' heel 105. Of all times 106. Delineate (concept) 107. Work-life mixing	12. Private atmosphere
108. Avoidance drive 109. Cynicism/hardening 110. Influence on decision-making 111. Office unattractive/ not eligible (again)	13. Undermining democratic rule of law
112. Physical measures (at home) 113. Coping mechanisms 114. Basic Awareness 115. Basic hygiene 116. Policy threats @ organisation / Central registration 117. Enforce digital measures (Strong password, updates, etc) 118. Resilience training 119. Change router password 120. VPN 121. Antivirus 122. Better measures (ease of use as well as safety/security) 123. Step extra towards 'neighbour' 124. Never 100% safe 125. Shortcuts 126. Coercive measures difficult 127. Stick to tips and advice 128. Digital has a personal/sensitive side 129. Own responsibility 130. Employer responsibility 131. Online findability 132. Taking down equipment (extreme situations) 133. Folder on social media (for online findability) 134. Leaving all devices 135. Digital security leaflet 136. Awareness talk 137. Golden Rules	14. Security Measures

138. Zero trust 139. Enforce measures 140. Password manager 141. 2FA 142. Privacy Screens 143. Updates 144. Do not use public wifi	
145. Of all times 146. Period Fortuyn	15. History

Table 10 - First and second order concepts

Annex 4 – Measures "Your Digital Security" Brochure

General	Software and apps	Mobile devices	On the road and while traveling
1. Use a unique password for each account. Use a strong password of at least 16 characters. A reputable password manager is a convenient way to generate and securely store passwords. 2. Enable Multifactor Authentication (MFA) whenever possible. Preferably, do not use MFA via text message. Rather, opt for an authentication app or e-mail. 3. Check that contact information of your contacts is still correct and still in use if you have not been in contact for an extended period of time. Preferably verify that via another means of communication. 4. Be aware of risks such as social engineering and phishing. 5. Don't just open unknown files or files from strangers. Don't just click on forwarded links. 6. When in doubt or if you suspect you are the victim of a digital attack, seek advice from your Security Authority (BVA) and/or your Chief Information Security Officer (CISO).	7. Be cautious about installing apps. Only install apps from trusted sources (App stores). 8. Choose a chat app that applies end-to-end encryption by default and activate the option to (re)register via PIN or MFA. 9. (Re)consider app permissions, such as access to location data, are actually needed to use the app. 10. Make sure your software (apps and operating system) is always up-to-date and enable automatic updating. 11. Don't simply click away security warnings and notifications, act upon them. 12. Do not send error reports, usage statistics, etc. to the manufacturer. Where possible, disable these options.	13. Do not make state secret calls through your mobile device(s). 14. Do not make calls about state secret or company confidential information with mobile devices in the same room. Turning off devices is not enough. It does not guarantee that eavesdropping through the device is not being done. 15. Turn off Bluetooth, Wi-Fi and location service by default when not in use. 16. Delete (irrelevant) Wi-Fi networks stored on your mobile devices. 17. Set a lock on your mobile devices. Unlock your device with a password or biometrics (fingerprint or facial recognition). 18. Reboot your mobile devices daily and use only a manufacturer-provided charger and charging cable.	19. Do not take your mobile devices to travel destinations with an increased risk of digital espionage. 20. Are you visiting a country with an increased risk of digital espionage and need to be reachable? Choose temporary mobile devices that you use only at this destination and then destroy. 21. Never hand over or leave your equipment unattended. 22. Never use open Wi-Fi connections. Always use your mobile (data) plan. 23. When abroad, always use a Virtual Private Network (VPN). When doing so, choose only reputable VPN providers.
Private and home environment	**Contact Information**	**Your environment**	
24. Give your wireless network a non-traceable name and do not use identifying terms when naming your mobile devices. 25. Change the default password of your router and modem to a strong password. 26. If you want to allow guests to access your home network, set up a guest network for this purpose. Shield your guest network from your own devices. 27. Do not process business data on your private devices and vice versa. 28. Do not connect your business mobile devices to your home network and do not use your private email for business purposes.	29. Be cautious about providing your contact information. Preferably provide general contact information. 30. Use your full name online as little as possible. 31. Consider using a prepaid phone number and an alternative, non-traceable e-mail address for registration on social media accounts and websites. 32. Keep your private and business contact information separate.	33. Realize that people close to you may also (unintentionally) reveal your information. 34. Smart devices (such as speakers, cameras, doorbells, smoke detectors) are equipped with microphones and other sensors that can be used to eavesdrop. Do not place these devices in your work environment	

Table 11 - Measures "Your Digital Security" Brochure (AIVD and NCTV, April 2022)