1 Introduction

"Police data breach: hackers seize contact details of all police employees."

"Police hack of 62,000 employees is dangerous: officers names bought and sold."

"Disquiet over police hack extends to employees of Public Prosecutor's Office."

These are just a few of newspaper headlines that appeared in October 2024 after what has become known as the 'police hack'.[1,2,3] The data breach in question,[4,5] which took place in September 2024, is believed to involved the capture of contact details of nearly 65,000 police officers, and possibly also of a number of chain partners. According to intelligence services, a state actor – an entity representing a country or state – was responsible. At the time of writing, not all the details around the data breach are known. A 'root-cause analysis' – a method focused on identifying (and tackling) the underlying causes of the problem – is still underway. What is clear is that the impact of this incident is significant.[6] Although its long-term consequences are not yet precisely known, the assumption is that the data will be misused to conduct phishing attacks and commit identity fraud.

1 https://nos.nl/artikel/2538710-datalek-bij-politie-hackers-bemachtigen-contactgegevens-alle-politiemedewerkers

2 https://www.ad.nl/politiek/politiehack-van-62-000-medewerkers-is-gevaarlijk-naam-agent-is-handelswaar

3 https://nos.nl/artikel/2539487-ook-onrust-bij-medewerkers-openbaar-ministerie-om-politiehack

4 A data breach is a security incident (or near incident) in which access is (or may have been) obtained to information without authorization. See https://autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/wat-is-een-datalek.

5 Earlier in 2024, there was a data breach at CEPOL, the European Union's agency dedicated to law enforcement training. See https://www.cepol.europa.eu/newsroom/news/notification-data-breach-related-leed-platform.

6 https://www.politie.nl/informatie/datalek---veelgestelde-vragen.html

The short-term impact is undeniable. The hack has caused a great deal of disquiet among police officers. There are various reasons for that disquiet. An important one is that it is hard for them to know which other data may have been captured and what the impact will be on them personally. Take for example the phenomenon of doxing, which involves confidential information about a person being made public, generally via the internet, with the aim of blackmailing, shaming or intimidating people. Regardless of how realistic this scenario may actually be, the possibility naturally plays on people's minds.[7]

Another reason for the disquiet is probably related to the communication about the data breach. This is a complex issue. After all, at what point is it appropriate to communicate what, internally and externally, how quickly does the organization itself have an adequate picture of what has happened and when have sufficient measures been taken in response? The Dutch police force had to strike a complex balance between security on the one hand and transparency on the other. This tempted some journalists to resort to sensational headlines. For example: *Error by police volunteer opened door to hackers: "Russia behind attack"*.[8] This headline reveals a reflex that is no longer appropriate to the current zeitgeist. Asking who is to blame does not help achieve resilient and learning organizations. It should be noted that the police leadership immediately distanced itself from this 'who is to blame' approach in its internal communication.

It is important to establish the cause of an incident, but the blame never lies with the employee if the organization suffers damage as a result of their actions (Spithoven et al., 2024). It only highlights the fact that a new risk has emerged or that the existing measures were not yet sufficient. Although an article in the Dutch newspaper NRC offered some counterweight to the impulse to blame an individual employee, even that article continued to focus on the issue of blame, only in this case directed towards 'management'.[9] This reflex is understandable, but

7 The reporting also focused on specific police roles, such as officers assigned to riot police mobile units, arrest teams, and those who carry out secret work. The suggestion that the personal data of such officers had been captured was quickly refuted by the Netherlands Minister of Security and Justice, David van Weel. He stated that their data were not on the list of addresses captured. See https://www.ad.nl/binnenland/inlichtingendiensten-politiehack-uitgevoerd-door-ander-land~a09ea492/

8 https://www.telegraaf.nl/nieuws/23538070/fout-van-politievrijwilliger-zette-deur-open-voor-hackers-rusland-zit-achter-aanval

9 https://www.nrc.nl/nieuws/2024/10/11/politiehack-als-een-vrijwilliger-of-de-stagiair-de-schuld-krijgt-is-er-echt-iets-mis-met-de-it-a4869054

it does not contribute to digital resilience. Completely preventing and avoiding incidents is impossible. For this reason, it is more important and more useful to establish the actual reasons why the incident was able to take place and have the impact that it did, and to take measures in response in order to improve systems and procedures.

We need to change our perspective on digital resilience and the role of human beings, from *human-as-problem* to *human-as-solution*, and in doing so let go of old patterns. I will touch on this later on in my lecture. First I would like to sketch the context in which my professorship operates. I will start with the security challenges we currently face and will be facing in the near future (section 1.1). I will then briefly describe what I understand by digital resilience (section 1.2), before discussing the core themes around policing and digitalization (section 1.3).

1.1 Digitalization and security challenges

Society is digitalizing at a rapid pace.[10] Digital processes play an ever greater role in our daily lives, and they are often regarded as being the 'nerve system' of our society (NCTV, 2022; Van Dijk, 2012). This is because society can no longer function properly without digital technologies. Our increasing dependence on digital processes (including products, services, and networks) makes us vulnerable and offers opportunities to malicious actors at all kinds of levels to take advantage of it. Security is a basic condition for a society of vitality and resilience, in which people are able to live and develop as they should. However, security is a 'delicate interplay of forces', because too much security can restrict initiative and freedom, while too little security can lead to chaos (Ducheine, 2018). Therefore, a good balance is needed.

According to the National Coordinator for Security and Counterterrorism (NCTV, 2024), digital threats loom as large as ever. Digital threats come in various kinds and sizes. Alongside data breaches, as discussed above, they mainly comprise crime[11] that already has a significant

10 Digitalization is "the development characterized by automated processes that play a role at more and more points in daily lives and in more and more different ways" (Stol & Strikwerda 2017, p. 304, translated from the Dutch).

11 By crime I mean any behavior that has been made a criminal offence.

digital component.[12] For example, phishing attempts, ransomware attacks,[13] DDoS attacks[14,15] and the hacking of systems.[16] These can result in the victimization of citizens, the failure of businesses, and general disruption to society. Digital threats therefore also have an impact on our national security. Geopolitical tensions, such as the wars that are currently being fought, also play a role in this (NCTV, 2024).

In addition, there are numerous other developments going on around the digitalization of society. These developments are more and more far reaching and bring new security challenges with them. For example, generative AI (artificial intelligence), which can be used to optimize the commission of online crime – from writing text for phishing messages[17] to video calls in which deep fakes are used to commit CEO fraud[18,19] but also developments such as robotics, nanotechnology, and quantum computing. We should note that these developments can also be harnessed for police work, for example using AI to help overcome language barriers, improve knowledge management, provide support for policing and contribute to data-driven working.[20]

Virtual worlds, including the metaverse,[21] and the further integration of digital technologies in and on the body[22] can also lead to new and/

12 The internet has various properties that increase the risk of crime (Leukfeldt, 2016; Yar, 2005). It goes beyond the scope of this lecture to explore this in more depth.

13 Attacks that involve attempts to fraudulently elicit personal data, such as passwords or credit card information using e-mail, messages, or fake websites, by posing as a reliable entity.

14 Attacks that involve malicious actors using software to encrypt a computer or network and block access until a ransom is paid (e.g., in Bitcoin).

15 Attacks that involve overwhelming a system in order to disable it.

16 Attacks that involve penetrating computers or networks in an unauthorized manner in order to steal data, cause damage and/or obtain control over the system.

17 https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models

18 A deepfake is "content (video, audio or otherwise) that is wholly or partially fabricated or existing content (video, audio or otherwise) that has been manipulated" (Van der Sloot & Wagensveld, 2022, p. 1).

19 https://www.bloomberg.com/opinion/articles/2024-02-05/a-25-million-hong-kong-deepfake-scam-on-zoom-shows-new-ai-risks

20 Generative AI can also be deployed to enhance digital resilience (NCTV, 2024).

21 The metaverse is a virtual world in which people can interact and engage in activities via digital avatars. The metaverse uses various technologies, such as virtual reality, augmented reality, and mixed reality. Taken together, these technologies are also known as extended reality. See https://forwork.meta.com/nl/blog/difference-between-vr-ar-and-mr/.

22 Verbeek (2011, p. 14) emphasizes that humans and technology are becoming ever more interwoven, "even to the extent that it is becoming harder and harder to define the boundary between the two". (Translated from the Dutch). Van Mensvoort (2019) recognizes this,

or modified forms of crime (Borwell et al., 2021a; Stol & Jansen, 2024; Van der Wagen, 2018).[23,24,25] In addition, there are issues such as data sovereignty[26] (and our dependence on technology and software from, for example, the United States and China), online espionage and cyber warfare (NCTV, 2024), and phenomena such as polarization, incitement of hatred, and disinformation, which can lead to tensions within society and public order disturbances (Bantema, 2023). Finally, there are harmful and immoral behaviors facing society, such as cyber bullying and doxing, as referred to previously (Van Huijstee et al., 2021).

In short
Today, digital safety and security are crucially important for a digital and connected Netherlands, Europe and globe. Prosperity and progress have become more and more dependent on digitalization. To the extent that that dependence grows, the potential impact if something goes wrong also increases. This means that as a society, we need to be resilient in order to deal with those digital challenges.

1.2 Digital resilience in outline

I have already used the term digital resilience several times. But what exactly do I mean by it? Digital resilience refers to "the capacity to reduce risks to an acceptable level by means of a collection of measures to prevent cyber incidents and, when cyber incidents do occur, to discover

and states that technology is not only changing our environment but also human beings themselves. We are already seeing this with mobile phones that, in a relatively short time, have made the transition "from unknown to familiar to indispensable" (Van Mensvoort, 2019, p. 63, translated from the Dutch). He observes that although these devices are not incorporated into our bodies, they have become an extension of our brains and experience.

23 https://www.bbc.com/news/technology-44697788

24 https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta

25 https://www.upi.com/Health_News/2022/06/01/medical-devices-pacemakers-cybersecurity/7041653656330/

26 https://www.computable.nl/2024/10/21/overheid-herziet-cloudbeleid-wegens-zorgen-over-leveranciers-vs/