Social Inclusion
2025 • Volume 13 • Article 8876
https://doi.org/10.17645/si.8876

cogitatio

ARTICLE

Open Access Journal

From Criminal to Crucial Participation: The Case of Dutch Volunteer Hackers

Anne Marte Gardenier

Department of Industrial Engineering and Innovation Sciences, Eindhoven University of Technology, The Netherlands

Correspondence: Anne Marte Gardenier (a.m.gardenier@tue.nl)

Submitted: 25 June 2024 **Accepted:** 13 January 2025 **Published:** 11 March 2025

Issue: This article is part of the issue "Public Participation Amidst Hostility: When the Uninvited Shape Matters of Collective Concern" edited by Olga Zvonareva (Maastricht University) and Claudia Egher (Utrecht University), fully open access at https://doi.org/10.17645/si.i419

Abstract

Since the 1980s, Dutch volunteer hackers have been identifying and disclosing vulnerabilities in computer systems. Initially criminalized, these hackers now play a crucial role in Dutch cybersecurity governance. This article explores the transformation of hackers from criminals to crucial participants and examines what this case reveals about citizen participation in the digital age. The case study demonstrates that citizens can play a pivotal role in addressing challenges posed by digitization, although their contributions can remain unrecognized and constrained by hostile institutions. This article aims to deepen the understanding of various forms of citizen participation in digital society, how institutions can support or constrain them, and how citizens play a central role in shaping these institutions to legitimize their participation.

Keywords

cybersecurity; digitization; material participation; technological citizenship; uninvited participation; volunteer hackers

1. Introduction

Digital technology permeates almost all aspects of contemporary life and is bringing a plenitude of opportunities, but also just as many risks. For instance, the information and communications technologies (ICT) that underlie today's digitized society contain vulnerabilities. These vulnerabilities include small technical errors in systems that can be exploited to make the system work differently than intended. Such vulnerabilities make it possible to carry out cyberattacks, such as ransomware, theft, stalking, and spying. Unattended vulnerabilities have the potential to disrupt the lives of individuals and essential societal processes. For example, human rights defenders, lawyers, and journalists around the world have fallen victim

to spyware like Pegasus (Benjakob, 2022), and hospitals, pharmacies, and universities have faced ransomware attacks, disrupting the continuation of their services. Vulnerabilities must be discovered as quickly as possible so that they can be patched and no longer be exploited, which is a key tenet of cybersecurity research.

An important principle of cybersecurity research is to enhance the cyber hygiene of ICT users. Ordinary ICT users are widely recognized as the "weakest link" in cybersecurity (Yan et al., 2018), indicating an alleged lack of knowledge and skills to avert cyberattacks. For that reason, cybersecurity research and governmental policy strategies often focus on improving user awareness of cybersecurity practices, viewing user behavior as one of the biggest challenges to maintaining cybersecurity (European Union Agency for Cybersecurity, 2022; Kävrestad et al., 2024). Such approaches pinpoint the "deficient user" as the security risk (Klimburg-Witjes & Wentland, 2021).

While the lack of knowledge and skills of ordinary users to avert cyberattacks is certainly an important problem, portraying the ordinary user or citizen, in general, as the deficient user does not fully do justice to their role in cybersecurity. In fact, this article demonstrates that citizens can play a central role in cybersecurity governance. In the case of Dutch volunteer hackers, which will be described in this article, citizens have independently and voluntarily contributed to establishing a cybersecurity governance system in which they now play a crucial and central role. Since the 1980s, these hackers have aimed to make the internet safer by exposing vulnerabilities. Initially, the Dutch government viewed hacking as illegal and criminalized it. However, over time, the perspectives of the government and other cybersecurity stakeholders shifted, and today the contributions of volunteer hackers to cybersecurity governance are recognized and encouraged, albeit with certain limits. Common terms used to describe well-meaning hackers who aim to improve cybersecurity through hacking or other means are "white hat" or "ethical" hackers. These terms have been associated with hackers affiliated with corporations (Goerzen & Coleman, 2022). In this article, "volunteer hackers" is used to describe and analyze the case study, as it focuses on hackers who voluntarily and independently contribute to improving cybersecurity governance.

The disclosure of vulnerabilities by these hackers and others around the world has been crucial for the development and security of the internet (Goerzen & Coleman, 2022). This demonstrates that viewing citizens as the "weakest link" overlooks their potential role in cybersecurity governance. Citizens can significantly contribute to the governance of cybersecurity, and digitization in general, but their potential for participation can remain unrecognized and unsupported by institutions. This indicates an institutional mismatch (Marres, 2012) regarding citizen participation in the digital domain. An institutional mismatch arises when existing structures fail to recognize or support emerging forms of citizen participation, such as ethical hacking. While cybersecurity campaigns assume a lack of citizen engagement and aim to foster participation where it is allegedly absent, in reality, citizen participation does occur but is not always acknowledged by institutions.

This case study shows that citizens can play a central role in addressing digitization challenges, such as raising awareness about insecure computer systems. However, there is limited research on how institutions support or constrain citizen participation in digitization, partly due to a narrow view of what constitutes "participation" in the digital society. This article aims to enhance understanding of various forms of citizen participation with regards to digital technologies, how institutions can support or constrain the participation of citizens on the

one hand, and how citizens can play a central role in shaping these institutions on the other (cf. Giddens, 1984). By applying the framework of technological citizenship (Gardenier et al., 2024) to a case study analysis of Dutch volunteer hackers (Gardenier, 2024), this article explores hacking to disclose vulnerabilities as a form of citizen participation. It clarifies how institutions can support or constrain this type of participation, and highlights how hackers have "legitimized their craft" (Goerzen & Coleman, 2022, p. 7) and shifted from being seen as threats to security to being recognized as valuable contributors to it.

This article is structured as follows. Section 2 reviews literature that explores emerging forms of participation in the digital society, connects these ideas to the framework of technological citizenship, and discusses the role of institutions in supporting or constraining these new forms of citizen participation. Section 3 describes the case study, demonstrating the transition of volunteer hackers from perceived criminals to crucial participants in Dutch cybersecurity governance over three distinct periods. In Section 4, the framework of technological citizenship is applied to the case study, and further discussion is provided on what this case reveals about citizen participation in the digital society. The article concludes with recommendations for further supporting volunteer hackers and a summary of the key findings.

2. The Diversity of Citizen Participation in the Digital Society

Literature on the relationship between participation and digitization has often focused on how digital devices facilitate particular types of political engagement and citizen participation. For instance, scholars have investigated how social media might affect citizens' participation in civic and political life (Boulianne, 2015), the role of digital technology in enabling and enhancing democratic practices and forms of governance (Fischli & Muldoon, 2024), and the use of digital tools to promote so-called e-participation (Hovik & Giannoumis, 2022).

While these approaches offer valuable insights into the impact of digitization on political participation and engagement, they demonstrate a narrow understanding of "participation" in the digital society. Chilvers and Kearnes (2015) have shown that dominant theories about participation have mainly focused on criticizing and improving top-down organized participation methods. This perspective views "the public" as an already existing, well-defined group that should be invited to participate to make their concerns about clear and specific issues heard.

In contrast, Chilvers and Kearnes (2015) argue that public participation should be seen as emergent and "in the making" (p. 4). They understand publics as being actively formed in the process of citizens articulating and addressing their shared matters of concern. For Chilvers and Kearnes, the goals of participation, the groups of people involved, and what is considered "political" are never given but always co-emerge. Therefore, for Chilvers and Kearnes, what is understood as "participation" should also encompass citizen practices beyond formal, top-down, organized public deliberation, such as "uninvited, informal, citizen-led, material, digital, mundane, private, [and] everyday" (Chilvers & Kearnes, 2020, p. 355) activities.

This links to Dewey's (2016) and, more recently, Marres' (2007, 2023) pragmatist view of "the public" as forming around collectively articulated and addressed issues. In this view, when citizens encounter a problem—which may be catalyzed by the rise of new technological applications in society—that requires government action, they emerge as a public by collectively framing and attempting to address the issue.

What publics become concerned with is not predetermined but emerges through this collective process of defining and responding to the issue. As citizens engage in this process, they gradually form a public. In this view, public participation naturally arises from the bottom up based on citizens' shared efforts to articulate and address concerns. Therefore, participation does not occur in predefined places, by predefined groups, or over predefined issues. Instead, publics emerge through the ongoing process of collectively identifying and attempting to address the issues they define as important.

Moreover, citizen participation is not limited to traditional forms of political engagement such as voting or protesting. Researchers in science and technology studies have expanded the understanding of participation in relation to technology. For instance, Marres (2012) has demonstrated that citizens' material interactions with technology in the private sphere may also constitute participation. Traditional political philosophers like Aristotle and Hannah Arendt emphasize that public activity is a key aspect of participation (Arendt, 1958), while material involvement is linked to private, domestic life (Marres, 2012). However, Marres argues that interactions with technology in private settings can also sometimes be understood as participation. She demonstrates this with the example of publicity campaigns that promote actions such as heating, cooking, and washing at home as ways to engage with issues like climate change and resource depletion. This was particularly evident in the Netherlands in 2022 when the government launched a campaign urging citizens to lower their heating to 19 degrees due to the gas shortage caused by the sanctions imposed on Russia after the invasion of Ukraine. These campaigns demonstrate how citizens' everyday interactions with material objects can facilitate public action on environmental issues.

This material perspective on participation broadens the concept to include engagement with technology in private settings. It can be effectively used to explore practices like hacking to disclose vulnerabilities as a form of participation where citizens address their shared concerns through a material practice that may be performed from their homes.

2.1. Technological Citizenship: A Framework for Understanding Citizen Participation in the Digital Society

The framework of technological citizenship (Gardenier et al., 2024) captures this perspective on citizen participation as emergent and taking place in multiple life spheres as described above, all within a single framework, and specifically related to digital technology. This framework can be used to scrutinize and assess the roles of citizens in shaping the digital society. It recognizes a broad range of citizen actions as forms of participation. Based on liberal, communitarian, and republican perspectives on citizenship, it conceptualizes citizen participation in relation to digital technologies in three distinct but overlapping spheres: private, social, and public. Citizens may deal with the impact of digitization within their private lives, for instance, by using e-health devices to keep better track of their health or by rejecting the use of WhatsApp out of privacy concerns. Citizens may also deal with the impact of digitization within their social sphere. For instance, by contributing to an online community such as Wikipedia or using apps to help members of their local neighborhood. Finally, citizens may deal with the impact of digitization within the public sphere by, for instance, protesting for net neutrality or voting for a politician who strives for better Big Tech regulations. By acting from within these three spheres, citizens can impact the role of digital technology in society and contribute to its governance (Gardenier et al., 2024).

The goal of distinguishing these different spheres of technological citizenship is to move beyond a single, normative vision of participation—the idea that only one form is "good." Instead, this framework highlights the diverse ways citizens contribute to shaping the digital society, whether in their private lives, social communities, or the public sphere, recognizing each as different, but equally valuable. This allows for investigating the roles of citizens in shaping the digital society while not being confined exclusively to formal ways of citizen participation such as voting or top-down organized public engagement initiatives.

Like "scientific citizenship" (Davies, 2015), technological citizenship is widespread and not confined to specific participatory spaces. Davies' concept of scientific citizenship accounts for moments when citizens negotiate the role of science and technology in society, which may materialize at science fairs and maker spaces. Similarly, technological citizenship includes material interactions with technology at home, work, and with friends and family. These interactions across private, social, and public spheres constitute moments of technological citizenship. This idea aligns with Ruha Benjamin's "viral justice" (Benjamin, 2022), where small, everyday actions collectively lead to significant social change. Similarly, every interaction of citizens with technology has its effect, and taken together may effectuate broader change. In sum, citizens' interactions in their private, social, and public lives contribute to shaping the role of digital technology in contemporary democratic society.

The goal of this approach is to understand the broader context of the challenges of digitization and strengthen citizens' ability to address them. In the case of hackers, it does not focus on creating new or better forms of citizen participation in cybersecurity but rather enables understanding the existing cybersecurity system and recognizing where citizen participation already takes place, and how citizens' constructive roles can be strengthened.

2.2. Institutions Supporting or Constraining Citizen Participation

The hackers discussed in this article currently make an important contribution to maintaining security in the digital society. However, they were initially not welcome to do so as they were regarded as criminals. In this case, participation by the hackers was uninvited (Wynne, 2007), and the government's hostile stance meant that hackers would face prison sentences when they tried to address the public issue of vulnerabilities.

This case highlights that participation always takes place within social systems of inclusion, validation, and exclusion across various fora in society, such as politics, the judiciary, and the media. Institutions, and the organizations that constitute them, can constrain citizens in their ability to address issues of public concern (Giddens, 1984). Here, institutions are considered as human-made, social systems that govern the behavior of individuals within a specific domain in society, enabling certain behaviors while restricting others (Greif, 2006). Relevant institutions in this case are legislation, the judiciary, science, corporations, and the Dutch government. Participation that diverts from the norms or rules within such institutions tends to be ignored or even persecuted. For instance, individuals who expose corruption, human rights abuses, or other illegal activities within organizations or governments often face severe retaliation. Whistleblowers like Edward Snowden have faced legal action and exile for their actions.

The case highlights the necessity of recognizing forms of technological citizenship as participation, as institutions play a crucial role in enabling or constraining participation. The goal of this article is to

demonstrate vulnerability disclosure as a form of uninvited participation, to assess the role of institutions in supporting or constraining citizen participation, and to highlight the role of citizens in shaping these institutions to legitimize their participation.

3. Case Study: Volunteer Hackers in the Netherlands

The description of the case study aims to represent the events that occurred between 1980 and 2022 that impacted and shaped the current practice and norms regarding vulnerability disclosure in the Netherlands. Four books have been written about volunteer hackers in the Netherlands (Jacobs, 1985; Reijnders, 2023; van 't Hof, 2015, 2021), which are referred to as secondary resources. The events and other sources discussed in these books, such as court hearings, governmental debates, and parliamentary papers were analyzed in their original form.

Moreover, a systematic analysis of newspaper articles, court hearings, and parliamentary papers available online was conducted by searching for relevant terms (e.g.: hacking, hacker, vulnerability disclosure, computer) within various databases (https://www.delpher.nl, https://www.rechtspraak.nl, https://www.tweedekamer.nl). From the retrieved information, sources that contain information about hackers in the Netherlands who disclose vulnerabilities intending to improve cybersecurity were analyzed. Additionally, international scientific papers and reports describing events relevant to the case were reviewed. Then, based on the conducted analysis, a timeline was created composed of the events that significantly impacted the development of the practice and norms regarding vulnerability disclosure in the Netherlands. Most relevant events from this timeline were written out and divided into three periods:

- Period 1: Hackers as uninvited participants;
- Period 2: Hackers as tolerated participants;
- Period 3: Hackers recognized as crucial participants.

While there are excellent accounts of the development of vulnerability disclosure in other countries, such as the United States (Ellis & Stevens, 2022; Goerzen & Coleman, 2022), and multiple books on hacker culture and practice in the Netherlands (e.g., Jacobs, 1985; Reijnders, 2023; van 't Hof, 2015, 2021), there is no comprehensive overview of the developments that led to the current vulnerability disclosure policy in the Netherlands, and this article fills that gap.

While this case study is situated in the Netherlands, the developments are naturally embedded within a global context. Similar developments have occurred in other countries, like the United States, which have influenced the development of vulnerability disclosure in the Netherlands. These influences will be highlighted as necessary. The description of this case is, however, focused on the evolving cybersecurity context of the Netherlands—how related laws, regulations, policies, and jurisprudence came into being—and the role volunteer hackers played in these developments.

3.1. Period 1 (1980–1993): Hackers as Uninvited Participants

In the 1980s, the hacker sub-culture emerged in the Netherlands, consisting of young individuals who hacked computers for fun or out of curiosity. Internet access was very expensive at the time, so hackers hacked into

networks of institutions like universities to get online (Stolwijk, 1990). During their online explorations, they discovered that many computer systems were poorly secured. On online fora and bulletin boards they shared methods to access these systems and tricks to exploit functions, allowing them to, for example, make free phone calls. Later, the "techno-anarchist magazine" Hack-Tic was founded, reporting on successful break-ins into poorly secured computer systems and offering a platform to share tricks with others in the community (Gonggrijp et al., 1989).

While some hackers were motivated by fun, others had more ideological reasons. Inspired by hacker communities in the United States (Levy, 1984) and West Germany, some saw how computers and the internet could benefit democracy by providing freedom of information and communication (Groenteman, 2006). For example, in the Netherlands, it was emphasized that the emerging internet was a public space that users were expected to take a part in shaping (Reijnders, 2023; Rustema, 2001; Stikker, 2019). Consequently, a Dutch hacker criticized the high costs that made the internet inaccessible to the general public: "Many of these large networks were set up with government funds and then made inaccessible to a large part of the population due to high usage costs" (Stolwijk, 1990, translation by the author).

Many hackers also recognized the risks of storing personal information on computers. They criticized how carelessly users handled confidential information and how easily government and corporate systems could be breached (Gonggrijp et al., 1989; Reijnders, 2023). The fact that these systems were so easily accessible, and that "boys as young as 13 could freely roam a million-dollar network" (Stolwijk, 1990, translation by the author) was seen as unacceptable by these hackers.

Hackers saw breaking into systems as a way to highlight this poor security. Often, gaining access did not involve much; sometimes, guessing common passwords was enough (Jacobs, 1985). A prominent hacker summarized their work: "What we do is in the public interest, even if our motivation is usually different" (Stolwijk, 1990, translation by the author). They understood that exposing vulnerabilities was beneficial to the public, even if it wasn't always their primary motivation.

In the Netherlands in 1985, about 20 computer hackers were active, behaving as "gentleman burglars" ("Kraken van computers kinderspel," 1985, translation by the author) who did not misuse the information they illegally obtained but reported the vulnerabilities to the affected parties. Some of their hacks, like the one at the Dutch Postal Service, made big news. In this case, the hackers did not misuse the data, which could have caused significant financial damage. The postal service praised the "neat way the gentlemen handled it" (Schmidt, 1985, translation by the author) and decided to improve their security.

However, most hacked parties, often companies, did not take vulnerability reports seriously and did not improve their security (Reijnders, 2023). For this reason, hackers often sought publicity to draw attention to vulnerabilities and pressure companies to take security more seriously. This approach, later known as "full disclosure" (Goerzen & Coleman, 2020), was not well received by the hacked parties, as it caused reputational damage and made the company more vulnerable because others could exploit the vulnerabilities as well. During this period, Dutch companies also suffered from computer fraudsters: hackers who exploited systems for personal gain (Jacobs, 1985). Despite this, many companies did not report hacks, as it would not generate good publicity and because hacking was not illegal at the time.

In 1985, hackers hacked the National Institute for Public Health and the Environment. This was the first time it became publicly known that a Dutch government institution had been hacked. The hackers had accessed sensitive patient information. The hacker who publicized the hack said he wanted to prove that citizens' privacy was not sufficiently protected ("Computers Philips en RIVM gekraakt," 1985). This hack caused political upheaval, and the minister of justice took a tough measure: He promised that hacking would be criminalized (Reijnders, 2023; Schmidt, 1985).

Reactions to this proposal varied. Some argued that as society becomes increasingly dependent on computer systems, it is important to regulate their use and misuse properly (Stolwijk, 1990). However, there was also criticism: Wasn't the real problem that companies took too few security measures? These measures were available but often expensive and not prioritized. Wouldn't it be better to solve this issue rather than criminalize hacking?

Hackers received support from the academic world. Computer science professor Israël Samuel Herschberg from Delft University regularly sought publicity to argue that these hackers were not criminals; in fact, they did good work by identifying insecure systems ("Computers vaak zo lek als een mandje," 1987). According to Herschberg, these hackers worked according to an ethic: They reported the vulnerability to the owner, gave them time to fix it, and only sought publicity if that failed. Herschberg also argued that hacking was the only way to get companies to improve their security. Academics tried to bring this to the fore through scientific publications but without success. From an academic perspective, hacking was seen as a legitimate way to disclose vulnerabilities.

In the United States at that time, the media increasingly reported on spectacular computer crackers, who became the public face of the hacker community (Jordan, 2008; Nissenbaum, 2004). As a result, the term "hacker" acquired a negative connotation and became increasingly associated with computer users who broke into computer systems by exploiting vulnerabilities (Oliver & Randolph, 2022). Following the example of the United States, which began taking tougher action against hackers from 1990 onwards—such as the arrest of hacker Kevin Mitnick, who was portrayed in the media as a "life-threatening genius" (Reijnders, 2023) and held in pre-trial detention for five years; and Operation Sundevil, which cracked down on illegal computer hacking (Goerzen & Coleman, 2022)—the climate in the Netherlands also became stricter. After an extensive eight-year-long legal process and heated parliamentary debates, in 1993 the Computer Crime Act was introduced (Koops, 2005). The maximum penalty for hacking or "computer trespassing" was four years' imprisonment or a fine of €11,250 (Koops, 2005). Nowadays, the maximum penalty for computer trespassing in the Netherlands is a fine of €22,500 and four years' imprisonment.

3.2. Period 2 (1993–2018): Hackers as Tolerated Participants

Shortly after the introduction of the Computer Crime Act, the first hacker in the Netherlands was prosecuted. Although the hacker did not cause any direct damage, he did cause inconvenience because the system had to be reconfigured ("Computerkraker voor de rechter," 1995). He was held in pre-trial detention for 38 days and sentenced to a six-month suspended prison sentence and a fine of 5,000 guilders (€2,200; "Nederlandse rechtbank vonnist," 1993; Reijnders, 2023).

The new law marked the end of an era for many hackers who had been freely exploring computer networks. Some took concrete measures, such as setting up an internet service provider so they no longer had to hack

to access the internet. One of the founders later described the establishment of this provider as "an initiative to avoid ending up in prison" (Groenteman, 2006, translation by the author). This internet provider, named XS4ALL, continued to operate as a reputable provider until 2019 and played a significant role in making internet access available to the general public (Reijnders, 2023).

However, the hacker subculture began to fade. The magazine Hack-Tic was discontinued in 1995. Some hackers quit hacking because they then faced prison sentences. Others continued to hack but did so in secret ("Lastig Hack-Tic houdt op op papier te bestaan," 1995). For example, hackers would anonymously disclose a vulnerability in collaboration with a journalist, sometimes after first warning the hacked party. This practice would later become known as "responsible disclosure" (RD).

This period thus begins with the criminalization of hacking. However, due to a multitude of developments in various institutional arenas, the value of disclosing vulnerabilities for cybersecurity is reconsidered during this period, making it possible for hackers, to some extent, to continue disclosing vulnerabilities. In the following subsections, I will discuss these developments and the impact they have had.

3.2.1. Lawsuit Casts a Positive Light on Vulnerability Disclosure

Within computer science, vulnerability testing remained a legitimate research method. In 2008, researchers from the Dutch Radboud University found a vulnerability in a chip created by the Dutch company NXP that was used worldwide in access systems to buildings and public transport, such as the London metro and Dutch trains. The researchers wanted to publish this vulnerability at a scientific conference to warn about the insecurity of the chip. Moreover, they wanted to demonstrate that the security principle that NXP used in this chip was flawed. Seven months before the planned publication, the researchers contacted NXP to report the leak so that NXP could fix it. NXP appreciated the vulnerability report, but wanted to prevent publication and, therefore, filed a lawsuit against the researchers (Rechtbank Arnhem, 2008; van 't Hof, 2015).

NXP argued that the publication of the article should be prevented because it would harm NXP and cause serious societal and security problems, as it would enable others to crack the chip as well. The researchers argued that the article's publication falls under the freedom of expression protected by the European Convention on Human Rights and should therefore not be stopped. The judge concluded that the security risks were caused by NXP's unsafe chip, not by the fact that researchers would publish the vulnerability. Moreover, the judge stated that publicizing vulnerabilities is in the public interest. The publication could, therefore, continue.

The judge's ruling was a legal milestone (van 't Hof, 2015) that changed the perspective on vulnerability disclosure: The judge allowed the publication of a vulnerability discovered by hacking based on the right to freedom of expression and the promotion of the public good (Rechtbank Arnhem, 2008). This court ruling placed the hackers/researchers in a new role, equivalent to that of a whistleblower or journalist. With this ruling, the societal value of disclosing vulnerabilities—at the expense of financial and reputational harm for the ICT vendor—was established in the Dutch jurisprudence.

3.2.2. Companies and Hackers Start to Collaborate

Also in the rest of the world, hackers continued to detect vulnerabilities. In the United States, the computer industry increasingly started to understand the value of hacking techniques, like full disclosure, and hackers themselves (Goerzen & Coleman, 2022). Yet, hackers continued to face the risk of legal repercussions. Therefore, in 2009, American hackers started the "No More Free Bugs" campaign to initiate consultations for better compensation and recognition for hackers who voluntarily disclose vulnerabilities (Ellis & Stevens, 2022). As a result, American companies set up "bug bounty" programs, allowing hackers to receive a financial reward after disclosing a vulnerability. In addition, companies introduced RD policies. RD refers to the practice of reporting a vulnerability directly to the affected party so that it can be fixed before publication. Companies with an RD policy invite hackers to find vulnerabilities in their systems, and if hackers follow their guidelines, the company pledges not to press charges. In 2012, Dutch telecom companies were the first to adopt an RD guideline.

While in the United States, the commercialization of vulnerability disclosure flourished, in the Netherlands, reporting vulnerabilities retained its voluntary nature for a time. Hackers usually did not receive a financial reward, but a public "thank you" and a t-shirt instead. If hackers disclosed a vulnerability in a government ICT system, for instance, they would receive a t-shirt saying "I hacked the Dutch government and all I got was this lousy t-shirt" (van 't Hof, 2015). However, recently also in the Netherlands, the commercial bug bounty practice is gaining ground, with bug bounty platforms like Intigriti.

3.2.3. Cyber Crisis Launches Cybersecurity on the Political Agenda

Meanwhile, the role of hackers in Dutch cybersecurity governance received political attention. In 2011, the Diginotar hack took place in the Netherlands, which was considered a "wake-up call" (Dutch Safety Board, 2012) that launched cybersecurity on the political agenda. In this hack, the Dutch company Diginotar, which issues certificates for websites, was hacked, and the reliability of a wide range of websites in the Netherlands was no longer guaranteed. The hack was claimed by an Iranian hacker (Wollaars & Kaboly, 2011). This caused a major political stir in the Netherlands because a hack with such a concrete effect had never occurred before (van der Meulen, 2013).

This crisis led, among others, to the establishment of the National Cyber Security Centre, which had as its aim coordinating national cyber threats. This crisis also encouraged politicians to reconsider the role of volunteer hackers in promoting cybersecurity. A member of parliament asked: "Is the minister prepared to investigate how the government can improve the security of its computer systems with the expertise of hackers, without the hackers suffering legal consequences?" (Tweede Kamer, 2011, translation by the author). The minister of security and justice promised that this would be investigated (Tweede Kamer, 2012).

3.2.4. The Government Introduces a Tolerance Policy for Hacking

In 2013, the Dutch government took the first step in the drawing up of new policy regarding vulnerability disclosure: the RD guideline (National Cyber Security Centre, 2013). The guideline explained how companies can draw up an RD policy to promote cooperation with hackers. It was based on existing RD policies of companies in the Netherlands and was essentially an encouragement of self-regulation between hackers and companies.

By publishing this guideline, the Dutch government took a position: "Ethical hacking" positively contributes to society and this should be encouraged instead of punished. The Netherlands was the first country in the European Union to draw up a national RD policy (European Union Agency for Cybersecurity, 2022). Yet, the guideline was negatively received by the hacker community because the law for computer trespassing remained intact (de Winter, 2013; Hoepman, 2013). As such, the responsibilities of hackers and companies were out of balance: Hackers were only allowed to report vulnerabilities to companies with their own RD policy, while companies were only encouraged and not obliged to have such a policy set up—thus, hackers often still faced a risk of being prosecuted. As a result, the initial problem of unattended vulnerabilities remained effectively unresolved.

3.2.5. Lawsuit as a Breeding Ground for RD Principles

In a criminal case in 2013, the jurisprudence regarding vulnerability disclosure was further developed. In this case, a patient of a health institution noticed the (weak) password of a doctor (van 't Hof, 2015). The password gave access to the computer system which contained sensitive patient data. The patient reported the security breach to the institution, but he did not receive a—in his opinion—quick response, after which he reported the leak to the media. He invited a local television broadcaster and he downloaded (anonymized) patient data as evidence. After publicizing the leak, the healthcare institution pressed charges against this "hacker" and the case appeared in court (Rechtbank Oost-Brabant, 2013).

The central question in the lawsuit was: Was this patient a whistleblower and did he serve the public interest by reporting this leak to the media, or did he go too far? The judge stated that three principles are important to assess whether the hacker disclosed the security breach responsibly: Did he act in the public interest? Did his action comply with the proportionality principle, i.e., did the suspect not go further than was necessary to achieve his goal? And did his action comply with the subsidiarity principle, i.e., were there no other, less far-reaching ways to achieve the goal? According to the judge, the hacker met the first principle: He served the public interest with his disclosure. However, he did not comply with the last two principles: The hacker could have given the organization more time to respond to the vulnerability report before disclosing the breach publicly, and he did not have to download patient data to report the vulnerability successfully. Therefore, the hacker received a fine of €750.

After this ruling, the principles of public interest, proportionality, and subsidiarity were adopted by the Public Prosecution Service in their policy on how to deal with "ethical hackers" (College van Procureurs-Generaal, 2013). Within a criminal investigation, these three principles formed the assessment framework for a "responsible disclosure." The minister of justice announced two years later that no hackers had been prosecuted whose hack complied with these principles since 2013 (Tweede Kamer, 2015a), and available court cases verify this until 2022.

3.2.6. New Governmental Policy Balances the Responsibilities Between Companies and Hackers

In 2015, the House of Representatives criticized government policy, defending that hackers should be able to report vulnerabilities to companies without their own RD policy (Tweede Kamer, 2015b). After the evaluation of the national RD policy in 2015, which concluded that RD contributes to strengthening the digital resilience of the Netherlands (Tweede Kamer, 2015a), and discussions with the hacker community

(Tweede Kamer, 2018), an updated version of the policy was published in 2018. The original name "responsible disclosure," indicating the responsibility that hackers must take to report vulnerabilities, was adapted to "coordinated vulnerability disclosure" (CVD), emphasizing the fact that both parties, the hacker and the recipient, must handle communication about the vulnerability responsibly. The principles of public interest, proportionality, and subsidiarity were included in the policy. If a hacker reports a vulnerability to an organization and works according to these principles, the hacker is not punishable, even if a company does not have its own CVD policy.

At this time, the combination of governmental policy and jurisprudence made vulnerability disclosure without facing punishment possible again—to a certain extent. The law against computer trespassing continued to exist, but because sufficient jurisprudence had been developed, hackers who hack according to the CVD principles did not have much to fear in court. The Dutch policy is, therefore, a tolerance policy, a form of "positive eliciting" (Harms, 2017, p. 1): Hacking is allowed, and hackers are encouraged to do so, provided they act according to the CVD principles.

3.3. Period 3 (2018–2022): Hackers Recognized as Crucial Participants

The new national policy and jurisprudence provided new possibilities: Hacking was allowed if hackers adhered to the CVD principles. As a result, hackers started to act in accordance with these principles. By doing so, they claimed a legitimate role in cybersecurity governance.

In 2019, the Dutch Institute for Vulnerability Disclosure (DIVD) was founded. DIVD is an organization of volunteers who scour the internet for vulnerabilities. DIVD hackers structurally violate the Computer Crime Act when they search for vulnerabilities. But because they work according to a code of conduct that includes the CVD principles, they avoid prosecution. Furthermore, being part of an established community increases the chance that a receiver of a vulnerability report takes the breach seriously (van 't Hof, 2021, p. 217).

In recent years, DIVD and other volunteer hackers have played a central role in Dutch cybersecurity governance. Notably, there are gaps within formal Dutch cybersecurity governance: There is no central desk for receiving and sharing information about security threats with all affected parties. The National Cyber Security Centre coordinates and shares security threats, but its mandate is limited to "vital" companies and organizations, such as electricity and water suppliers. Consequently, non-vital companies and smaller organizations do not receive crucial cybersecurity information, putting them at a disadvantage. Additionally, the distinction between vital and non-vital companies is becoming increasingly blurred due to chain dependency.

Volunteer hackers fill this gap by scanning organizations for vulnerabilities and personally notifying them when their systems are vulnerable. In 2019, DIVD security researchers played a crucial role in a major cybersecurity crisis by directly notifying the organizations that were at risk of being attacked (van 't Hof, 2021). Also, DIVD is setting up an academy in which novice hackers can learn the skills of hacking according to the CVD guidelines.

Volunteer hackers now have a unique role in the cybersecurity network and they are tolerated when they hack to find vulnerabilities if they adhere to the CVD principles. The role of volunteer hackers in maintaining cybersecurity is increasingly recognized by the Dutch government. The Dutch Safety Board concluded in their investigation of a major cybersecurity incident caused by the Citrix vulnerability in 2020 that "volunteer

security researchers played a crucial role in incident response" (Dutch Safety Board, 2021, translation by the author). The role of volunteer hackers was also repeatedly referred to as crucial and indispensable during debates in the Dutch parliament (Tweede Kamer, 2022a). Since 2022, DIVD has received a temporary subsidy to strengthen cyber resilience in non-vital sectors.

However, the government also recognizes that the contribution of these hackers is voluntary and, therefore, not structurally guaranteed (Dutch Safety Board, 2021). Members of parliament have called for a more formally embedded role of volunteer hackers in cybersecurity governance (Tweede Kamer, 2022a). However, formalizing volunteer hacker communities would not be beneficial, as it would prevent them from continuing their activities. A government organization cannot actively scan for weaknesses without a legal basis (Tweede Kamer, 2022a). Consequently, members of parliament requested the government to set up a multi-year subsidy scheme to structurally finance "ethical hacker collectives" (Tweede Kamer, 2022b).

As of 2022, volunteer hackers who search for vulnerabilities have secured a central role in the Dutch cybersecurity landscape. They are supported by government policies and legal precedents. This new role of hackers as allies is now firmly established within the cybersecurity community. However, the government is currently figuring out how to ensure their voluntary contributions, as Dutch cybersecurity has become partially dependent on their efforts.

4. Discussion

This case study has shown the role of Dutch volunteer hackers in the development of the Dutch vulnerability disclosure policy. Since the 1980s, hackers have aimed to make the internet safer by exposing vulnerabilities. Initially, the Dutch government viewed hacking as inherently illegal, which hindered these efforts. Hackers' contributions were not accepted as a form of participation, and the government criminalized hacking, positioning hackers as part of the problem. However, over time, the government's and other stakeholders' perspectives shifted. Today, the contributions of volunteer hackers to cybersecurity governance are recognized and encouraged, albeit to a limited extent.

The hackers described in this case study can be seen as part of a public emerging to address collective concerns. Hackers' activities represent a form of material participation (Marres, 2012). Through their interactions with digital technologies in private, social, and public spheres, these hackers have played a central role in addressing cybersecurity vulnerabilities, showcasing technological citizenship. Hackers highlighted the importance of cybersecurity across political, corporate, scientific, and public agendas, prompting solutions from the government and private sector. While some hackers may have had political motivations, many hackers disclosed vulnerabilities for personal development, a sense of justice, satisfaction in finding flaws, collaboration or competition with others, or peer recognition (Jordan, 2008; Weulen Kranenbarg et al., 2018). Despite their varied motivations, these hackers' actions over the past 40 years have had political impacts. Each hack to disclose vulnerabilities has contributed to raising awareness about the importance of cybersecurity. By disclosing vulnerabilities, the hackers have initiated discussions on responsibility and accountability for securing digital systems, making their private acts have public consequences.

By moving between private, social, and public spheres, the volunteer hackers navigated hostile institutions. Depending on their goals and context, they could disclose vulnerabilities either directly or publicly. Public

disclosure aimed to raise awareness and exert pressure on the affected party to take action, particularly if no measures had been implemented. In contrast, direct disclosure was most effective when there was strong collaboration with the recipient, such as companies with established RD or CVD policies, or when national policies and legal frameworks permitted it.

Further, the hackers united around shared goals to strengthen their position against hostile stakeholders, forming a social community. Although campaigns such as the "No More Free Bugs"—which raised awareness about the unfair treatment volunteer hackers faced from the private sector—took place in the United States, they impacted developments in the Netherlands. By establishing DIVD, hackers leveraged national policies and legal frameworks under CVD principles. DIVD hackers addressed security gaps left by the Dutch government and private sector, exemplifying technological citizenship in the social sphere where citizens tackle issues neglected by the government and market (Gardenier et al., 2024). These hackers organized to address societal cybersecurity gaps overlooked by companies and government agencies. Cybersecurity companies often miss threats to civil society (Maschmeyer et al., 2020), and the National Cyber Security Centre focuses only on vital infrastructure, leaving many organizations unprotected. These volunteer hackers filled this gap. Through community building and active engagement, these hackers have gained credibility among other cybersecurity stakeholders, enabling them to continue disclosing vulnerabilities on a national scale. With the bug bounty industry gaining ground in the Netherlands, these hackers can also increasingly take on this role with financial incentives.

In summary, this case illustrates that participation in the digital age spans private, public, and social spheres, with citizens navigating these realms based on their goals and hostile or supportive institutional elements.

4.1. Vulnerability Disclosure Enabled or Constrained by Institutional Arrangements

The case study further illustrates how institutions can enable or constrain citizen participation (cf. Giddens, 1984). As shown here, participation can be uninvited (Wynne, 2007) and may face obstacles if not recognized or endorsed by institutions. Institutions govern the behavior of individuals within a specific domain in society, enabling certain behaviors while restricting others (Greif, 2006). The institutions of legislation, the judiciary, science, and government have all played a role in regulating the behavior of hackers in this case. Some institutions constrained hacking in certain periods, while other rules enabled hacking under certain conditions in later periods. Table 1 provides an overview of how particular institutions regulated the behavior of hackers over different periods.

During the first period, hacking was new and emerging, not confined by any policies or laws, allowing hackers to operate freely. In the second period, hacking was criminalized, and hackers faced severe restrictions on their ability to disclose vulnerabilities, making it nearly impossible for them to continue their work without risking prison sentences or fines. The prospect of a legal sanction deterred hackers from continuing to hack after it was criminalized in 1993. This impeded the practice of vulnerability disclosure, even though hackers and computer scientists recognized its value for maintaining cybersecurity as early as the 1980s. In the third period, hacking became legitimized under certain conditions, enabling hackers to continue addressing collective issues by disclosing vulnerabilities. This demonstrates that institutions can both constrain and enable citizens to deal with the opportunities and risks of digitization.

Table 1. Overview of how institutions regulated the behavior of hackers.

Period	Hostility or support by institutions	Behavior by hackers
1	Hacking is first unseen, and later criminalized by the Dutch government. Within the computer science community, disclosing vulnerabilities is seen as a legitimate practice.	Hackers find and disclose vulnerabilities.
2	Hacking is criminalized, but the public value of vulnerability disclosure is recognized through court cases, the collaboration between hackers and the private sector, and a cybercrisis that generated awareness for cybersecurity. This leads to new government policy that tolerates hacking under certain conditions.	Some hackers quit hacking, others continue to disclose vulnerabilities, but in secret.
3	The Dutch government recognizes hackers as crucial participants in cybersecurity governance and searches for structural support.	Hackers find and disclose vulnerabilities according to CVD principles.

4.2. Hackers Playing a Central Role in Legitimizing Their Participation

Importantly, hackers played a central role in legitimizing their participation by influencing the change of rules and norms within institutions. They engaged across private, social, and public spheres, interacting with various institutional organizations—including legislators and the private sector—to shape vulnerability disclosure as a legitimate form of citizen participation.

In the second period, the Dutch government's hostility towards hackers diminished as the societal impact of vulnerabilities and the crucial role of hackers in addressing them became clear. Over time, institutional arrangements that initially rejected vulnerability disclosure evolved. Notably, the Dutch government was not the primary driver of these changes. This shift resulted from developments and interactions among various institutions, including the judiciary, the private sector, science, and the parliament. Hostility towards hackers faded as stakeholders increasingly recognized the societal value of vulnerability disclosure: Private sector companies began collaborating with hackers, and vulnerability disclosure remained a legitimate research area in computer science. The judiciary's recognition of vulnerability disclosure as a public good marked a pivotal shift in legitimizing hackers' contributions. Additionally, a disruptive cyber crisis further shifted the government's perspective on vulnerability disclosure.

This evolution aligns with the systemic approach to deliberative democracy, which assumes that deliberation, democratic engagement, and legitimacy are distributed across various societal fora, including legislatures, companies, universities, voluntary organizations, and the judiciary (Mansbridge et al., 2012). It highlights that the state is not the sole agent in certifying or rejecting participation; other institutions also play a role in the legitimization process. The case demonstrates how multiple stakeholders jointly shaped the practice of vulnerability disclosure into a new and responsible form of citizen participation. Eventually, the Dutch government, the private sector, and the hacker community shaped norms around vulnerability disclosure to benefit the public good and foster technological citizenship. They explored how hacking could strengthen cybersecurity while acknowledging the dangers posed by malicious hackers, who are, after all, the security risk. Even well-meaning hackers sometimes caused harm by publicly disclosing vulnerabilities, possibly further damaging the vulnerable party. Therefore, it was essential to establish norms to guide vulnerability disclosure and make it a responsible practice.

Hackers' participation over 40 years has had various effects. Politics, policymaking, technology development, cybersecurity crises, corporate perceptions of hackers, and the judiciary have all influenced what counts as "participation" in Dutch cybersecurity governance. This does not mean that before government policy on vulnerability disclosure, hackers were not "participating," or that their hacking before RD principles was not "responsible." Importantly, by examining the various ways hackers participate and the role of institutions in either supporting or limiting their actions, it becomes evident that their involvement is shaped by how institutions—such as politics, the judiciary, and science—either include, validate, or exclude citizens, all within the context of ongoing technological advancements. As this case demonstrated, citizens play a crucial and mutually shaping role in these developments, particularly concerning issues like vulnerability disclosure. They drive new forms of participation to address collective issues, actively influencing how these issues are understood and acted upon. Through their interactions with technology in private, social, and public spheres, citizens influence the role of digital technology in society. It is essential that these diverse forms of citizen participation are recognized and supported by institutions, enabling citizens to address their concerns and, in doing so, promote democracy in an increasingly digital world.

How, in this case, could volunteer hackers be further supported? The Dutch government is currently searching for a way to structurally back hackers' participation to ensure the cyber-security of the Netherlands, given the country's partial reliance on their efforts. However, this case demonstrates that institutionalizing hackers—by making them a state entity—would undermine the initiative itself. The effectiveness of hackers in their current role relies on their independence and volunteer nature. Rather, institutional support that can take various shapes or forms is necessary to ensure the endurance of this form of voluntary citizen participation.

The role of hackers could be strengthened by finding ways to support their independent and voluntary work. Legal frameworks regarding hacking could be adjusted to ensure that disclosing vulnerabilities is not treated as a criminal offense, thus alleviating the legal risks hackers still face. For example, research into security vulnerabilities could be framed as a right, accompanied by a responsibility to disclose findings in a manner that enhances information security (van Daalen, 2022). Additionally, promoting the practice of CVD within the hacking community could encourage novice hackers to follow CVD guidelines, inspired by positive peer examples (Weulen Kranenbarg et al., 2018). Policymakers could also support bug bounty programs based on commercial or community-driven CVD initiatives (Zrahia, 2024). With the contributions of volunteer hackers now recognized, it becomes possible to identify effective ways to support their constructive efforts to address the public interest.

5. Conclusion

This article has demonstrated the role of voluntary hackers in addressing ICT vulnerabilities in the Netherlands. Although hacking has been illegal since 1993, hackers who find and disclose vulnerabilities directly to ICT vendors are now tolerated and play a crucial role in Dutch cybersecurity governance. The Dutch government, the private sector, and the hacker community have collaboratively shaped the practices and norms surrounding vulnerability disclosure, making it a practice of technological citizenship that benefits the public good.

The hackers described in this case emerged as a public to address and shape the issues caused by the digitization of society through hacking. This case demonstrates that while citizens can play a vital role in tackling issues related to digitization, their contributions can remain unrecognized or constrained by

institutions. It also shows how institutions can support citizen participation when citizens' contributions to the governance of digitization are recognized. Furthermore, it emphasizes the crucial role that citizens play in shaping these institutions to legitimize new forms of participation. The case of Dutch volunteer hackers demonstrates that it is essential to acknowledge and empower citizens' contributions to the governance of digitization and enable technological citizenship in various domains to foster a resilient democratic digital society.

Funding

This research was supported by the Dutch Research Council (NWO) [410.19.004]. Publication of this article in open access was made possible through the institutional membership agreement between the Eindhoven University of Technology and Cogitatio Press.

Conflict of Interests

The author declares no conflict of interests.

References

Arendt, H. (1958). *The human condition*. University of Chicago Press.

Benjakob, O. (2022, April 5). The NSO file: A complete (updating) list of individuals targeted with Pegasus spyware. *Haaretz*. https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000

Benjamin, R. (2022). *Viral justice: How we grow the world we want*. Princeton University Press.

Boulianne, S. (2015). Social media use and participation: A meta-analysis of current research. *Information, Communication & Society*, *18*(5), 524–538. https://doi.org/10.1080/1369118X.2015.1008542

Chilvers, J., & Kearnes, M. (Eds.). (2015). *Remaking participation: Science, environment and emergent publics*. Routledge. https://doi.org/10.4324/9780203797693

Chilvers, J., & Kearnes, M. (2020). Remaking participation in science and democracy. *Science, Technology, & Human Values*, *45*(3), 347–380. https://doi.org/10.1177/0162243919850885

College van Procureurs-Generaal. (2013). *Responsible disclosure (hoe te handelen bij ethische hackers?)*. Openbaar Ministerie.

Computerkraker voor de rechter. (1995, February 17). *Het Parool*, 6.

Computers Philips en RIVM gekraakt. (1985, December 3). *Het Vrije Volk*, 1.

Computers vaak zo lek als een mandje. (1987, October 16). *Het Parool*, 11.

Davies, S. R. (2015). Participation as pleasure: Citizenship and science communication. In J. Chilvers & M. Kearnes (Eds.), *Remaking participation: Science, environment and emergent publics* (pp. 162–177). Routledge.

Dewey, J. (2016). *The public and its problems: An essay in political inquiry*. Swallow Press.

de Winter, B. (2013, January 3). Responsible disclosure richtlijn is onverantwoord risico. *HP/De Tijd*. https://www.hpdetijd.nl/2013-01-03/responsible-disclosure-richtlijn-is-onverantwoord-risico

Dutch Safety Board. (2012). *The Diginotar incident. Why safety fails to attract enough attention from public administrators*.

Dutch Safety Board. (2021). *Vulnerable through software—Lessons resulting from security breaches relating to Citrix software*.

Ellis, R., & Stevens, Y. (2022). *Bounty everything: Hackers and the making of the global bug marketplace*. Data & Society.

European Union Agency for Cybersecurity. (2022). *Coordinated vulnerability disclosure policies in the EU*.

Fischli, R., & Muldoon, J. (2024). Empowering digital democracy. *Perspectives on Politics*, *22*(3), 819–835. https://doi.org/10.1017/S1537592724000409

Gardenier, A. M. (2024). Strengthening the role of citizens in governing disruptive technologies: The case of Dutch volunteer hackers. In D. H. de la Iglesia, J. F. de Paz Santana, & A. J. López Rivero (Eds.), *New trends in disruptive technologies, tech ethics, and artificial intelligence* (pp. 399–409). Springer Nature. https://doi.org/10.1007/978-3-031-66635-3_35

Gardenier, A. M., van Est, R., & Royakkers, L. (2024). Technological citizenship in times of digitization: An integrative framework. *Digital Society*, *3*(2), Article 21. https://doi.org/10.1007/s44206-024-00106-1

Giddens, A. (1984). *The constitution of society: Outline of a theory of structuration*. Polity Press.

Goerzen, M., & Coleman, G. (2020). Hacking security. *Logic(s)*, *10*. https://logicmag.io/security/hacking-security

Goerzen, M., & Coleman, G. (2022). *Wearing many hats: The rise of the professional security hacker*. Data & Society.

Gonggrijp, R., Poelman, P., Acker, H., Tx, D., J., & The Key. (1989). *Hack-Tic: Tijdschrift voor techno-anarchisten*, *1*(1). https://www.hacktic.nl/magazine/0101.htm

Greif, A. (2006). *Institutions and the path to the modern economy: Lessons from medieval trade*. Cambridge University Press. https://doi.org/10.1017/CBO9780511791307

Harms, K. (2017). Positieve uitlokking van ethisch hacken. *Netherlands Journal of Legal Philosophy*, *46*(2), 196–207.

Hoepman, J.-H. (2013, January 4). Leidraad responsible disclosure behoeft aanscherping (door te leren van ervaringen in de luchtvaart). *On Privacy, Security, & ….* https://blog.xot.nl/2013/01/04/leidraad-responsible-disclosure-behoeft-aanscherping-door-te-leren-van-ervaringen-in-de-luchtvaart/index.html

Hovik, S., & Giannoumis, G. A. (2022). Linkages between citizen participation, digital technology, and urban development. In S. Hovik, G. A. Giannoumis, K. Reichborn-Kjennerud, J. M. Ruano, I. McShane, & S. Legard (Eds.), *Citizen participation in the information society: Comparing participatory channels in urban development* (pp. 1–23). Springer. https://doi.org/10.1007/978-3-030-99940-7_1

Jacobs, J. (1985). *Kraken en computers: Telecommunicatie en veiligheid*. Veen.

Groenteman, G. (2006). *Human profiel over Rop Gonggrijp* [Television broadcast]. Humanistische Omroep.

Jordan, T. (2008). *Hacking: Digital media and technological determinism*. Polity Press.

Kävrestad, J., Furnell, S., & Nohlberg, M. (2024). User perception of context-based micro-training—A method for cybersecurity training. *Information Security Journal: A Global Perspective*, *33*(2), 121–137. https://doi.org/10.1080/19393555.2023.2222713

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "deficient user" in cybersecurity discourses. *Science, Technology, & Human Values*, *46*(6), 1316–1339.

Koops, B.-J. (2005). Cybercrime legislation in the Netherlands. *Cybercrime and Security*, *2005*(4), 1–20.

Kraken van computers kinderspel—'oen' breekt codes van rijksdienst. (1985, December 3). *Het Parool*, 3.

Lastig Hack-Tic houdt op op papier te bestaan. (1995, January 16). *Het Parool*, 9.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Dell Publishing.

Mansbridge, J., Bohman, J., Chambers, S., Christiano, T., Fung, A., Parkinson, J., & Warren, M. E. (2012). A systemic approach to deliberative democracy. In J. Parkinson & J. Mansbridge (Eds.), *Deliberative systems: Deliberative democracy at the large scale* (pp. 1–26). Cambridge University Press.

Marres, N. (2007). The issues deserve more credit. *Social Studies of Science*, *37*, 759–780.

Marres, N. (2012). *Material participation: Technology, the environment and everyday publics*. Palgrave Macmillan.

Marres, N. (2023). How to turn politics around: Things, the earth, ecology. *Science, Technology, & Human Values*, *48*(5), 973–998. https://doi.org/10.1177/01622439231190884

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2020). A tale of two cybers—How threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, *18*(1), 1–20. https://doi.org/10.1080/19331681.2020.1776658

National Cyber Security Centre. (2013). *Leidraad om te komen tot een praktijk van responsible disclosure*. Ministerie van Veiligheid en Justitie.

Nederlandse rechtbank vonnist voor het eerst een computerkraker. (1993, March 3). *Trouw*, 3.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society*, *6*(2), 195–217. https://doi.org/10.1177/1461444804041445

Oliver, D., & Randolph, A. B. (2022). Hacker definitions in information systems research. *Journal of Computer Information Systems*, *62*(2), 397–409. https://doi.org/10.1080/08874417.2020.1833379

Rechtbank Arnhem. (2008, July 18). ECLI:NL:RBARN:2008:BD7578

Rechtbank Oost-Brabant. (2013, February 15). ECLI:NL:RBOBR:2013:BZ1157

Reijnders, M. (2023). *De hackers die Nederland veranderden: De spannende geschiedenis van XS4ALL*. Podium.

Rustema, R. (2001). *The rise and fall of DDS: Evaluating the ambitions of Amsterdam's digital city* [Unpublished doctoral dissertation]. University of Amsterdam.

Schmidt, M. (1985, December 3). Journalist breekt via telefoon in bij computer rijksinstituut. *De Volkskrant*, 1.

Stikker, M. (2019). *Het internet is stuk, maar we kunnen het repareren*. De Geus.

Stolwijk, E. (1990, May 17). Wet schrikt computerkrakers niet af. *Algemeen Dagblad*, 3.

Tweede Kamer. (2011). *Debat over diginotar en ict-problemen bij de overheid* (Handeling H-tk-20112012-12-26).

Tweede Kamer. (2012). *Verslag van een algemeen overleg informatie- en communicatietechnologie (ICT)* (Kamerstukken 26643-240).

Tweede Kamer. (2015a). *Brief van de minister van Veiligheid en Justitie* (Kamerstukken 26643-342).

Tweede Kamer. (2015b). *Verslag van een algemeen overleg informatie- en communicatietechnologie (ICT)* (Kamerstukken 26643-354).

Tweede Kamer. (2018). *Verslag van een algemeen overleg informatie- en communicatietechnologie (ICT)* (Kamerstukken 26 643–551).

Tweede Kamer. (2022a). *Verslag van een wetsgevingsoverleg* (Kamerstukken 36084-11).

Tweede Kamer. (2022b). *Verslag van een wetsgevingsoverleg* (Kamerstukken 36200-VII-116).

van 't Hof, C. (2015). *Helpende hackers. Verantwoorde onthullingen in het digitale polderlandschap*. Tek Tok.

van 't Hof, C. (2021). *Cyberellende was nog nooit zo leuk. Onthullende verhalen uit de wereld van informatiebeveiligers en hackers*. Tek Tok.

van Daalen, O. (2022). In defense of offense: Information security research under the right to science. *Computer Law & Security Review*, 46, Article 105706. https://doi.org/10.1016/j.clsr.2022.105706

van der Meulen, N. (2013). Diginotar: Dissecting the first Dutch digital disaster. *Journal of Strategic Security*, *6*(2), 46–58.

Weulen Kranenbarg, M., Holt, T. J., & van der Ham, J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science*, *7*(1), Article 16. https://doi.org/10.1186/s40163-018-0090-8

Wollaars, J., & Kaboly, R. (2011, September 9). Iraanse hacker: Ik deed het in m'n eentje. *NOS*. https://nos.nl/artikel/271232-iraanse-hacker-ik-deed-het-in-m-n-eentje

Wynne, B. (2007). Public participation in science and technology: Performing and obscuring a political–

conceptual category mistake. *East Asian Science, Technology and Society: An International Journal*, *1*(1), 99–110. https://doi.org/10.1215/s12280-007-9004-7

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

Zrahia, A. (2024). Navigating vulnerability markets and bug bounty programs: A public policy perspective. *Internet Policy Review*, *13*(1). https://doi.org/10.14763/2024.1.1740

About the Author

Anne Marte Gardenier is a PhD candidate at Eindhoven University of Technology, focusing on "technological citizenship." Her research examines how citizens contribute to strengthening the resilience of democratic societies in the face of digitization. By exploring the intersection of technology and civic engagement, her work aims to better understand the role of citizens in shaping the digital society.