Article

Science, Technology, & Human Values
2021, Vol. 46(6) 1316-1339
© The Author(s) 2021
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0162243921992844
journals.sagepub.com/home/sth
SAGE

Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses

Nina Klimburg-Witjes[1] **and Alexander Wentland**[2]

Abstract

Today, social engineering techniques are the most common way of committing cybercrimes through the intrusion and infection of computer systems. Cybersecurity experts use the term "social engineering" to highlight the "human factor" in digitized systems, as social engineering attacks aim at manipulating people to reveal sensitive information. In this paper, we explore how discursive framings of individual versus collective security by cybersecurity experts redefine roles and responsibilities at the digitalized workplace. We will first show how the rhetorical figure of the deficient user is constructed vis-à-vis notions of (in)security in social engineering discourses. Second, we will investigate the normative tensions that these

[1] University of Vienna, Austria
[2] Technical University of Munich, Germany

Corresponding Author:
Nina Klimburg-Witjes, University of Vienna, Universitätsstrasse 7, 1010 Vienna, Wien 1010, Austria.
Email: nina.witjes@univie.ac.at

practices create. To do so, we link work in science and technology studies on the politics of deficit construction to recent work in critical security studies on securitization and resilience. Empirically, our analysis builds on a multi-sited conference ethnography during three cybersecurity conferences as well as an extensive document analysis. Our findings suggest a redistribution of institutional responsibility to the individual user through three distinct social engineering story lines—"the oblivious employee," "speaking code and social," and "fixing human flaws." Finally, we propose to open up the discourse on social engineering and its inscribed politics of deficit construction and securitization and advocate for companies and policy makers to establish and foster a culture of collective cyber in/security and corporate responsibility.

Keywords
cybersecurity, hacking, social engineering, politics of deficit construction, securitization, resilience, critical security studies

Introduction

Today, social engineering techniques are the most common way of committing cybercrimes through the intrusion and infection of computer systems and information technology (IT) infrastructures (Abraham and Chengalur-Smith 2010, 183). Cybersecurity experts use the term "social engineering" to highlight the "human factor" in digitized systems. As a set of attack strategies, social engineering refers to manipulating people to reveal sensitive information. Most known perhaps are phishing attacks, which is when unsuspecting users are asked to click on a faulty link and, by doing so, enable hackers to install malware and enter the system. In all cases, social engineering attacks involve a combination of social interactions and technological exploits, leaving cybersecurity professionals in companies and government organizations alike struggling to develop effective countermeasures.

Several high-profile cases of social engineering attacks have recently caught the attention of both IT security experts and political commentators. For instance, in 2020, hackers targeted the social media platform Twitter, including the accounts of celebrities such as Bill Gates, Elon Musk, and Kanye West as well as the public profiles of former US President Barack Obama and then Democratic nominee Joe Biden. The hackers used their temporary access to solicit cryptocurrency payments from the hacked accounts' followers. Despite the relatively small financial damage and a inconsequential dent in Twitter's reputation, this incident revealed the widespread potential for social engineering attacks, as the hackers used the company's customer support to gain access to those accounts—not a technical backdoor in the web service's software (Polak 2020). In reports about the incident from an internal investigation, Twitter explains that it was not the network that the hackers targeted but that they "misled certain employees" and "exploited human vulnerabilities" (Twitter 2020). The report concludes: "This was a striking reminder of how important each person on our team is in protecting our service." As many companies that suffer from social engineering attacks do, Twitter framed this incident as the product of social manipulation, not as the failure of a security system.

This is only one example of the increasing insecurities of digital infrastructures due to social engineering practices. As a consequence, the cybersecurity industry is at an all-time high (Grand View Research 2020). In particular, the convergence of technical skills and insights into social behavior required for the identification and defense of social engineering attacks has given rise a growing expert community—what some call a cybersecurity hype (Shires 2018, 33). In particular, in discussions among the social engineering expert community, the user of IT systems (e.g., employees) is often framed as the main source of risk. Compared to other forms of cybercrime, practices of and discourses on social engineering alike put the human front and center. Hackers consider these predictable patterns in human behavior as a gateway into the technical, material layer of computer networks (Hadnagy 2010; Krombholz et al. 2015). With "people" being often seen as the "weakest link in information security" (Lineberry 2007), cybersecurity has become increasingly individualized and asymmetrically treated: current discourses on social engineering are much more concerned with the supposedly unwitty, deceivable, and unpredictable user than the technical side of cybersecurity.

In this paper, we explore how social engineering experts—for example, hackers, cybersecurity professionals, and institutional stakeholders—imagine possible solutions to the supposed "people problem" in cybersecurity. With cyberattack strategies being increasingly framed as a social rather than a technical problem, we trace the discursive strategies of cybersecurity experts, and the consequences of such human-centered deficit framings in which users are seen as the main risk factor. We understand users as those working with digital technologies, e.g. employees at companies, government agencies, and research institutions, as opposed to experts whose task it is to design secure systems and to maintain the security and operation of IT systems. Employees are the most common target of social engineering attacks, as they have access to critical organizational systems (Aldawood, Alashoor, and Skinner 2020). We specifically focus on those discourses on social engineering attacks against employees that take place during their work time and while using a company's or institution's IT infrastructure. At the same time, we see that boundaries between in-office work time and working from other places have become blurry as employees increasingly use private devices to log into the company's network remotely or bring their own laptops to work. The COVID-19 pandemic has accelerated this trend, as lockdown measures have forced many companies and employees into remote work. This blurring of boundaries benefits social engineering attacks that exploit the interface between company security and individual behavior, as hackers target primarily individual employees through social expectations.

The paper unfolds as follows: first, we will outline our conceptual approach that links work in science and technology studies (STS) on the politics of deficit construction to recent work in critical security studies (CSS) on securitization and resilience. Second, we introduce the empirical material collected during a multi-sited conference ethnography of three leading cybersecurity conferences in Las Vegas and Vienna. In the concluding section, we argue that attributing fault to the supposedly uneducated or unwitty user is a strategy to cope with the complexity and uncertainty that come with digitalization. Contributing to the emerging conversations between STS and CSS on cyber in/security, we propose to extend the discourse on social engineering and the inscribed politics of deficit construction and securitization. Instead, we advocate for companies and policy makers to establish and foster a culture of cybersecurity and corporate responsibility. Moreover, we argue that social engineering is not a problem to be left in the domain of security and technical expertise but needs to be discussed as a severe challenge for digitized societies, as it alters everyday life settings such as the workplace and questions predominant notions of security and resilience.

Theoretical Approach

In the following, we first explore the sociopolitical processes and ontological practices through which the deficient user is constructed vis-à-vis notions of (in)security in social engineering discourses and identify the relevant differences between these positions. Second, we investigate the moral and normative problems that these practices create and emphasize why the differences are important. To do so, the theoretical part of this paper links the concept of deficit construction to work from CSS on resilience as a response to the growing securitization and related uncertainties in the field of cybersecurity.

The Politics of Deficit Construction in Social Engineering Expert Discourses

Many cybersecurity experts frame social engineering attacks as a question of technological literacy and knowledge. According to this perspective, security incidents occur because an employee did not observe common security practices nor detect manipulative techniques used by hackers. This alleged knowledge deficit is understood to be the main attack vector through which intruders can then bypass security measures and access digital infrastructures. Such framing turns the implied "deficient user" into a security risk. Employees without the proper expertise to detect suspicious activities and react accordingly are said to need additional training as to avoid becoming security risks to their employer. This narrative of users as lacking, deficient, or ignorant closely resembles what STS scholars have observed in the discourse around the public understanding of science and technology (PUS). Conventional approaches in PUS have promoted the idea that controversies around the risks and benefits of scientific advances can be mitigated through improved science communication and education (Bodmer and Wilkins 1992). This view does not imagine the public to be a reasonable group of actors who collectively guide scientific questions or set boundaries based on moral concerns. Rather, it is expected that uninformed parts of the public would indeed trust the scientific community's judgment if they shared the same (or a sufficient) degree of expertise and insight.

Work in STS offers productive inroads into the normative social practice of deficit construction around science, technology, and innovation (Jasanoff 2016; Pfotenhauer, Juhl, and Aarden 2019; Wynne 1992) and illuminates how lay understandings obtain legitimacy as expertise in its own right. This viewpoint draws attention to several theoretical problems relevant to our analysis: (1) arrogance/institutional language of expert bodies, (2) overlooking valuable contributions from lay people, (3) misplacing the problem (and solution). Studies in risk communication, for instance, have shown that a common but misguided response to controversies around contentious topics is to call for a more comprehensive education for those seemingly opposed to scientific facts and technological progress (Abell and Lederman

2007). While this perspective has received broad institutional support, critics have highlighted the framing of citizens as essentially “deficient.” This implicit process of deficit construction does not refer to a simple lag in the dissemination of knowledge. Since science and technology are central to the modern world, “scientific illiteracy is viewed as a moral problem, leaving people incapable of understanding the world around them and incapable of acting rationally in that world” (Sismondo 2010, 174). In other words, obtaining an understanding and appreciation of science—or professionalized expertise—becomes a civic duty for any individual who wants to participate in contemporary social and political life.

Moreover, work in STS has examined how scientists and other professional experts have established themselves as the only legitimate gatekeepers for credible knowledge, thus excluding other potentially affected actors as contributors of potential solutions (Felt and Fochler 2010). In their critique of persistent narratives around the public understanding of science in society, scholars have argued that elevating narrowly defined expertise as the only legitimate source of authority not only excludes other kinds of knowledge and experience but also sidelines those who frame an issue in terms of values rather than facts (Wynne 1992, 2006; Irwin 2014).

The politics of deficit construction have become particularly pronounced around solution- and innovation-oriented imaginaries. Pfotenhauer, Juhl, and Aarden (2019) have observed how policy makers and economic advisors view entire regions and countries in terms of their capacity to bring forward technological innovation. The authors propose an analytic framework that attends to five distinct layers of deficit construction: (1) who diagnoses what kind of deficit, while (2) proposing remedies to address this deficit? Equally important are the (3) forms of expertise considered legitimate in addressing these deficits as well as the (4) social orders implied by the proposed technoscientific solution. Finally, they ask, (5) what are considered the “standards of success,” particularly “the corollary normative implications of the intervention” (Pfotenhauer, Juhl, and Aarden 2019, 896)? We take these five layers of deficit construction—combined with the concepts of securitization and resilience—as a point of departure for our inquiry. In the empirical section, we mobilize the framework to trace how social engineering experts construct the deficient user in cybersecurity discourses. Three distinct social engineering story lines have emerged in an iterative exchange between our theoretical perspective and interpretative analysis of the empirical material, namely “the oblivious employee,” “speaking code and social,” “fixing human flaws.”

Constituting something as deficient—be it computer user or an entire economy—starts with diagnosing a problem that needs to be solved. However, what counts as a viable solution is often already inscribed into the problem's definition. Morozov (2013) eloquently demonstrates this in his account of Silicon Valley's "solutionist" answers to all problems of the modern world, including irrational human behavior. However, such seemingly elegant fixes to complex societal conditions shift responsibility away from collective deliberation and political decision making onto the individual, who is expected to contribute to envisioned social orders by self-optimization (Morozov 2013, 6). Mozorov's notion of solutionism resonates with the Sismondo's (2010) claim that scientific illiteracy is being turned into a moral problem. The institutional embedding of expertise creates a hierarchy in which the individual needs to change in order to address a societal problem, not the institutions. Both Morozov (2013) and Pfotenhauer, Juhl, and Aarden (2019) note that deficit and solutionist approaches tend to obscure the reasons why something is seen as a problem worth fixing in the first place and distract from alternative framings. In the second part of our theory section, we connect the analytical framework of deficit construction with insights from CSS on processes of securitization and resilience. Combining both literatures allows us to illuminate social engineering discourse and similar settings in which both IT security expertise and deficit framings are coproduced.

Securitization and Resilience: Risky Users and the Redistribution of Responsibility

As an analytical lens, the concept of securitization allows us to trace how security problems are established and how actors consider and collectively respond to other actors, events, and objects as a threat (Balzacq 2005; Bigo 2014; Booth 2005). In short, such a perspective shifts the attention from looking at security as a stable entity or intangible ideal notion, on the one hand, to the study of those practices and actors that make security, on the other. Practices and discourses by security professionals of various kinds lend particular constructions and framings of (in)security legitimacy (Balzacq, Léonard, and Ruzicka 2016; Collier 2018). Recent work at the intersections of CSS and STS specifically attends to the oftentimes routinized practices and mundane physical actions through which security is constructed, and how cybersecurity experts shape the stabilization processes of security issues; that is, moving phenomena from an invisible and intangible realm toward one in which they can be communicated, acted upon, and managed (Liebetrau and Christensen 2020; Dunn Cavelty 2018; Balzacq and Cavelty 2016; Barnard-Wills and Ashenden 2012). Focusing on "the creation of networks of professionals of (in)security, the systems of meaning they generate and the productive power of their practices" (C. A. S. E. Collective 2006, 458; see also Bigo 2014; McDonald 2008) helps us to understand how social engineering practices and discourses co-constitute the deficient user as the main challenge to cybersecurity.

Within such a "techno-securitizing processes" (Ellis 2019), the daily work routine of employees, when connected to the internet, emerges as a realm where security professionals practice protection and thus become folded into the security practice itself. In other words, risk management and precautionary methods are enacted within our work environments, as much as upon them (Hansen and Nissenbaum 2009). Through daily activities such as training, meetings, social media, and what Huysman (2011) called "little security nothings" (p. 327)—paper bins, screens, hand written notes, even family photos—become active parts of securitizing processes spurred by social engineering. This, in turn, adds to the inherent insecurity of computer systems (Edwards 1997, 290), by meshing policing with insurance practice, business with national security, and individual with collective vulnerabilities (Amoore and Goede 2008). Within these cybersecuritizations of everyday (work) life, the individual is then simultaneously called upon as being responsible for processes of collective security as well as a potential liability and even a threat to it.

With risk and uncertainty increasing, so are the calls for more resilient subjects and to "responsibilize the population and individual subjects with concrete tasks to create conditions that re-establish normality" (Kaufmann 2013, 59). Enjoying the status of a "superhero," concepts and practices of resilience have proliferated into a wide range of security issues and policy domains over the last decade (Dunn Cavelty, Kaufmann, and Søby Kristensen 2015, 4). Moreover, recent work in CSS and other fields has examined the emerging concept of (cyber) "resilience" toward disruption, crisis, and catastrophe, acknowledging that total security is an illusion (Lentzos and Rose 2009). The key assumption of resilience thinking includes an understanding of security as dependent on the subject itself and "its resilience to detrimental events," such as maintaining stability, survival, and safety (Dunn Cavelty, Kaufmann, and Søby Kristensen 2015, 5). Within the resilience paradigm, it is assumed that a collective state of total security can never be reached but rather a dynamic "self-making of this particular state of security" that is then referred to the individual subject (Kaufmann 2013, 59; see also Chandler 2014; Reid 2012). In a sense, resilience governance then entails the redistribution of "responsibility to societal members, who become their own 'apparatus of security'" (Kaufmann 2013, 61).

Linking both approaches allows us to see the broader societal issue at stake here—from changing work routines and novel forms of expertise and epistemic authority in legitimizing security issues, to the politics of deficit construction and calls for more resilience as key elements in any securitization process. Both concepts, the deficit model and resilience, entail a normative assumption of shifting from collective to individual responsibility: They depart from an understanding of the individual subject as "lacking"—either of sufficient education and knowledge to arrive at informed decisions in the case of the deficit model or the capacity to respond to crisis and disruption with adequate self-protection in the case of the resilience paradigm. What is more, both conceptualizations are future-oriented in the sense that they argue for the empowering potential of transformation as the "productive engagement of failure" (Kaufmann 2016, 2012). Finally, deficit constructions and the resilience paradigm intend to activate the subject to act out security as well as innovation, with responsibility for both secure and innovative societies being firmly placed in neoliberal logic of governance in which problems and solutions alike center around the individual (Walker and Cooper 2011; Methmann and Oels 2015). In the next section, we outline our empirical material and the methodological approach we used to trace how deficit constructions and resilience are mobilized in social engineering discourses.

Methodological Approach and Fieldwork

Our analysis draws on ethnographic fieldwork, namely, participant observation and eleven semi-structured key informant interviews, conducted during three international conferences on cybersecurity and hacking. One conference was the Vienna Cyber Security Week in January 2018, targeted mainly at government agencies. The other two conferences were Black Hat and Defcon, which took place in Las Vegas in July 2017. Especially the latter two are leading events in this field, attracting an audience of roughly 20,000 each year. Black Hat is the more corporate conference, as it mainly addresses IT companies, different industries, and start-ups, as well government agencies, for example, law enforcement, finance, and the defense sector. Defcon is a more informal and creative conference, with a mixed audience spanning from hackers and IT professionals to journalists, nongovernmental organizations in the field of privacy, activists, researchers, and, to a lesser extent, government employees. In recent years, both conferences have featured an increased number of talks on "human factors" in cybersecurity, and even a social engineering Village (comparable to a section at academic conferences) at the 25th Defcon in 2017.

In addition to the growing community of hackers and self-taught practitioners, an industry of consulting firms has identified the insecurity related to social engineering as a highly profitable market gap.

Conferences like these are seismographs of the debates, key issues, and social interactions of their respective fields and thus thick sites for anthropological investigations (Falzon 2009; Høyer Leivestad and Nyqvist 2017) What is more, we understand these large events, from keynote talks, lunch conversations, panel discussions, and working groups, to Maker Spaces, B2B meetings, and after-parties as active sociopolitical spaces in which we can explore the processes through which knowledge and expertise are performed, generated, (con)tested, or stabilized (Hajer 2009). Following Campbell et al. (2014, 5), attending to the conference allows us to understand how "contextualized interactions produce social realities like understandings of particular problems and the power relations brought into being in addressing those problems." In addition, and due to the oftentimes sensitive character of cybersecurity issues, we carried out informal interviews and discussions with participants, for instance, during coffee breaks or while queuing for a talk.

We analyzed the empirical material by drawing on Hajer's (2009) approach of argumentative discourse analysis that, in a Foucauldian tradition, understands discourse as "an ensemble of notions, ideas, concepts, and categorizations through which meaning is allocated to social and physical phenomena, and which is produced and reproduced in an identifiable set of practices" (p. 64). Such an approach explores and renders visible how and under which conditions a specific discourse becomes dominant. Particularly relevant for our paper is the notion of story lines—condensed key elements of an otherwise very broad and transnational discourse on social engineering—around which discourse coalitions organize themselves and impose their view of reality on others (Müller and Witjes 2014).

Our material includes both ethnographic material and primary documents such as publications, pamphlets, company statements, and websites. Using Qualitative Data Analysis software, we applied in vivo coding techniques to an initial set of documents in order to generate early working hypotheses and questions for our fieldwork-based interviews. After we conducted the fieldwork, we consolidated the coding tree and refined our initial assumptions. This inductive analysis was followed by axial coding, specifically focusing on notions of "users," "security," "risk," "expertise," and “responsibility” that appeared in a variety of materials and across sites. From here, we identified three main story lines, namely, “the oblivious employee,” “speaking code and social,” “fixing human flaws.” Finally, we applied the concepts of “deficit construction” and “securitization” to understand and explain emerging patterns in our results and relate our findings to broader concerns within STS and critical security studies.

Empirical Analysis

Problem Diagnosis: The Oblivious Employee

While technology and humans are both depicted as risk vectors in cyber-physical systems, it is the human susceptibility to errors that is seen as the main problem in current cybersecurity discourses. It became visible throughout our interviews and during the conference talks that humans are seen to be the “weakest link” (IP 1; 3, 4, 5), as is condensed in the statement, for example, that “users are the problem, not the system” (IP 2). Here, the figure of “stupid people” was invoked frequently to point to the perceived inability of users to adapt to the increasingly complex sociotechnical challenges brought by ICT, regardless of “how much education and training is thrown upon them” (IP 4). This particular quote already indicates how users are considered as too naïve to take care of any sufficient protection measures or incapable of adapting precautionary measures such as complex passwords or double-checking a telephone call from an alleged colleague who is asking for confidential information. Most IT security experts have been fully aware of the fact that employees are dealing with a situation they have not actively brought about and that was unimaginable a few decades ago. Interestingly, one of our interviewees stated that the burden of keeping one’s company secure has multiplied by the number of employees they have: “A while ago, you had a fence, a guard with a flashlight and a German shepherd at the gate, and your premises were basically secured” (IP 1).

This statement nicely illustrates the abovementioned individualization of the risk discourse: risk is mainly seen as individual risk that increases with the number of employees. As this interviewee stated, it is now up to them to keep the network secure, as every employee must be as cautious and well trained in spotting suspicious activity as the guard at the gate (IP 1). At the same time, an interviewee acknowledged that working conditions and responsibilities for non-security-related activities might constrain everyday social engineering awareness, stating that “Of course this is not the people’s primary job. They are office workers, accountants, technicians. How are they supposed to handle targeted phishing attacks deliberately designed for them, while going about their regular business?" (IP 7). This statement is one of the rare moments in which interviewees pointed to the challenges that arise for employees when tasked with activities that are usually not within their scope of responsibility, such as identifying malicious software. However, in most accounts, hackers were portrayed as criminals who are threatening organizations, though often with a certain admiration of their smartness, dauntlessness, and innovative methods. The employees who could not prevent being attacked, in turn, were framed as naive and even as the bigger risk. According to our interview partners, and in line with the academic literature in the field (Tetri and Vuorinen 2013; Nyamsuren and Choi 2007), the key explanation offered for the success of social engineering was that it triggers emotional biases.

Hackers often persuade potential victims with appeals to strong emotions, such as excitement or fear, establish interpersonal relationships, or create a feeling of trust and commitment (Workman 2008, 662). This tendency to trust, as the following quote indicates, opens the door for attackers in the same way a friendly receptionist would, as Hulme (2015) has argued in a blogpost on social engineering: "Humans are fairly dumb; we are easily led; trust readily and we have this natural tendency (for the most part) to think other folk have our best interests in mind." This and similar accounts show how experts link what they see as a lack of knowledge and education about social engineering with useŕs affections such as excitement or trust in others. The discursive framing of users thus mobilizes two alleged deficits, nonknowledge or ignorance as well as affect and kindness as risk factors in work environments.

The Role of Expertise: Speaking Code and Social

In this section, we show how social engineering expertise is constituted, performed, and enacted in practice. We begin with a field note taken at Defcon about an encounter between a social engineering expert and a group of conference participants that took place near a popular bar in the early evening, after most talks and panels were finished.

A participant approached a group of people waiting in line for a panel on social engineering. He offered them a small silver can containing pepper, in his words "very hot pepper that will make you cry like a baby." One member of the group eventually took the can, poured some of the red powder on the back of his hand, and licked it off. The crowd cheered while he started to cough and retch. The one who offered the can was smiling and solemnly handed it over to him: now it was his turn to pick someone from outside his group for this challenge. This rite of passage continued several times, and almost everyone who took the pepper stayed with the group.

During a later interview with the initiator of this challenge, it turned out that he was not doing this just for fun. Rather, he was the owner of a very successful "penetration testing" business. He used this as a way to train his skills to trick people into uncomfortable situations they actually enjoyed through the sense of community he created as well as to make new business contacts for his company. His clients—mostly business corporations but also government agencies—hire him to test the risk awareness of their employees and thereby, knowingly or not, put them under extreme stress. Afterward, his company reports these "human security breaches" to the executives and offers training on how to prevent these "mistakes." According to this interview partner, everyone could fall for these attacks and the harder it is to "socially engineer" someone, the more he and others would appreciate the challenge (IP 8).

This field note already entails some of the key elements in the constitution of social engineering expertise and the processes through which a deficient user is constructed. First, it shows us that in most cases, social engineering experts combine the social skills needed for social engineering attacks with their technical background and experience. However, unlike in other fields of IT security, their epistemic authority does not mainly derive from superior technical skills. Rather, their role as experts stems from the fact that they can speak both languages—"code" and "social," a juxtaposition that was often used by interview partners and presenters alike. This way, experts claim to provide knowledge and insights into both human behavior and technical aspects. This self-representation then establishes the ground on which social engineering experts can act as powerful securitizing actors, as we often observed. To keep up their business model, they maintain and reinforce a narrative of inherent insecurity and constant threat that speaks to both human insecurities and diffuse fears of being the one responsible for putting the entire company at risk and making the technology susceptible to errors. In the case described above, however, a social engineering expert was engineering his peers, those who might have given talks about how to avoid social engineering attacks only hours ago. Although this was not performed on the conferencés main stage but in a relatively informal setting, it pointed our attention to a key aspect of this story line that came up in many talks, namely, that "nobody is safe, everybody could become a victim, even experts" (IP 6). It serves as a fundamental precondition to successfully offer expertise to educate people in order to make them less vulnerable.

As Wolff (2016) points out, the “desire to profit from providing [cybersecurity] training may lead to too much competition” with the result that cybersecurity qualifications are of uncertain value. In this view, cybersecurity experience can be understood as an apprenticeship in which professionals first mimic and then successfully inhabit the role of experts, pronouncing authoritatively on cybersecurity risks. This leads to our third observation, namely, a recursive expert/lay people relationship in the constitution of social engineering expertise.

Proposed Remedies and Measures of Success: Fixing Human Flaws

With social engineering as the number one attack vector for cybercrime, unsolvable human biases, and complex sociotechnical uncertainties, how then does the community envision and perform possible remedies for the social engineering problem? And which actions count as a success?

The most obvious solution proposed in the talks, interviews, and on websites was more training and education. However, in his talk at Black Hat, “Why most cybersecurity trainings fail,” Arun Vishwanath, Chief Technology Officer at Avant Research Group, a cybersecurity research and advisory firm, contended that the majority of user-focused “cybersecurity awareness trainings” are not effective since the expenses for benefits from training outweigh the loss from attacks. Even after several trainings, people still click on faulty links or can be talked into giving away sensitive information. On the other hand, companies and governments continue to spend large amounts of money for security companies to teach their employees how to protect against social engineering attacks.

According to Viswanath, successful social engineering is not a result of the proverbial people problem but a problem of “our understanding of people.” For him, the main challenge rather comes from the companieś “inability to diagnose what ails the patient.” In order to sort out those employees most likely to fall for a social engineering attack, Vishwanath developed the Cyber Risk Index (CRI), a quantitative metric to identify the employees that potentially become victims of spear phishing by turning to their individual behavior at work and beyond.

Conceptualized as a self-report survey, the CRI comprises forty questions about habits and work routines (e.g., driving while texting), heuristics (not noticing a missing “s” on a fake Starbucks domain name), individual cyber risks beliefs (e.g., word is safer than PDF), and (the not further specified category of) "personality." After filling out the form, employees are then scored depending on their individual answers, with their score providing the basis to decide who gets access to a company's or institutioń's more sensitive networks. The basic idea of the CRI is to protect a company from allegedly "risky employees," for instance, by removing them from any responsible tasks in advance and by using embarrassment as a motivation for employees (by making the bad CRI scores publicly visible).

This was in line with prevalent notions during talks and panel discussion at the Black Hat conference about the need "to identify the weak links in the organization," "to track and improve individual readiness and cyberattack resilience," or "to embarrass and eventually fire stupid people."

Comparing social engineering to a spreading disease, Vishwanath constructed the user as a patient who simply needs to be better diagnosed to protect their environment from possible threats and to act more responsibly and risk-aware in the future. Experts often relied on metaphors from the realms of medicine and psychology to diagnose the ills of the" "stupid user," and the limited effectiveness of cybersecurity awareness trainings, equating employees with patients and themselves or the broader social engineering expert community as the doctors: the "ones who take care of the stupid people because they need us" (IP 2). The patient comparison used here is part of a broader discourse and a related training and software industry on cyber hygiene. Here, cybersecurity experts attend to the risks and harms that come from malicious hackers as virus or infection, pushing companies to strengthen their defense, in particular with regard to social engineering. These medical metaphors support the securitization of individuals in the dangerous realm of the digital, where it is understood that "cyber insecurities are generated by individuals who behave irresponsibly thus compromising the health of the whole" (Hansen and Nissenbaum 2009, 1166).

It is the human risk that trumps the technical risk and leads to a securitization of both employees and companies. The latter are often not willing to share information about how they have been attacked due to fear of competitive advantage, liability, or regulation. Vulnerability is thus seen as arising primarily from human "flaws," not technical ones: thus, it is not a technological fix that is seen as the solution to the security problem but rather a "cure" of the human weaknesses, among which are traits like being curious and supportive that are generally seen as relevant soft skills. Resilience, achieved through additional education and training, then becomes the proposed solution to and standard of success for the deficient user problem.

Discussion: Toward a Productive Engagement with Failure

Drawing on interviews and participant observation at three cybersecurity conferences, we have explored how cybersecurity experts frame social engineering as a rapidly increasing and potentially catastrophic risk to companies and other organizations.

First, a deficit is constructed (the user) with calls for more experts and training as its remedy. As in many other fields, the "technification" (Hansen and Nissenbaum 2009, 12) of cybersecurity constructs the technical as a realm where the public is lacking a sufficient understanding and must turn to the experts. This deficit diagnosis has paved the way for a growing body of knowledge on social engineering attacks and countermeasures as well as an emerging industry of consulting firms, which offer remedies to what we have called "the oblivious employee." Such remedies often take the shape of increased "cyber hygiene" and "cyber self-defense" trainings. While such programs can improve an organization's cybersecurity, they might have severe implications for the way the employee, instead of the attacker, becomes securitized, resulting in their removal from certain security-relevant tasks with potentially severe consequences for their motivation and income as well as future job prospects.

Second, social engineering experts have drawn on what they deem "human weaknesses" when it comes to both diagnosing the solution and prescribing a remedy. Consequently, company executives and IT departments prematurely judge and look out for the "oblivious employee," a person lacking enough security knowledge and practical skill to deal with potential social engineering attacks, thus falling below organization's security standards. Experts in different professions and policy domains define and assess what makes up the body of proper IT security knowledge and practice. Consequently, the aim is to identify, "diagnose," and "solve" problematic cases within a given company or organization, as the CRI shows. What is more, the user/employee is not only framed as a problem but is also kept from having any influence on the security practice and, as a result, their own work life. It seems that there is a trend where large organizations simultaneously centralize decision-making processes while exporting the consequences onto the workers.

Third, the underlying and constantly reinforced narrative of social engineering is that of an unavoidable threat. Not all employees can be trained effectively, and attackers will always develop novel ways to trick even the most trained user into novel social engineering traps. In turn, "more expertise" is required to respond to the securitized "oblivious" user who is simultaneously framed as a risk to security and called upon as a responsible guardian of the company's security.

Vulnerabilities, inherent to any technological system, were conceived as risk and mainly assigned to the user who, in turn, was framed as the weakest link and, paradoxically, a larger threat to cybersecurity than the attackers—a story line that was powerfully employed and maintained by cybersecurity experts. We understand this particular construction of deficits as a key element of the resilience paradigm, in which the individual is simultaneously called upon to be responsible for processes of collective security while also being viewed as a potential liability and even a threat to it.

What has been missing from the social engineering discourse is a perspective on social engineering that does not immediately problematize the user but considers the generative potential of being at risk as tightly interwoven with social norms as well as technical rationalities (Bijker 2006; Hommels, Mesman, and Bijker 2014). However, the securitization of the workplace in the context of IT security has also revealed the need to open up the issue of cybersecurity for democratic participation within organizations and, as a societal challenge, reconsider the "technological commitments" that entail deficit politics in terms of their "discursive, institutional, economic, and infrastructural attachments to particular technological pathways" (Stirling 2008, 265) while neglecting others. Already there are doubts about how helpful the prevalent diagnosis of human gullibility is and how desirable or even viable the prescribed remedies are among cybersecurity practitioners. The current discourse around social engineering offers a way to critically engage with possible futures tied to our treatment of risk and vulnerability, including potential adaptive capacities and opportunities (Keulartz and Schermer 2014).

Conclusion

In our analysis, we have shown how responsibility for cybersecurity is individualized through three distinct story lines, namely, "the oblivious employee," "speaking code and social," and "fixing human flaws." The frequently invoked figure of the "stupid user" who is susceptible to social engineering correlates with a shift in responsibility from a collective concern to the individual employee. It also resonates with a more general trend to create "flexible" working environments, for example, working from home or "bring your own device" policies, which has blurred the boundaries between the to-be-protected organization and the oftentimes less maintained and securitized personal sociotechnical environment of its employees. While social engineering trainings conceive the user as inherently oblivious and uninformed, the deliberate blurring of boundaries between work and personal life exposes users to cyberattacks even further. The security paradigm sidelines questions about why new vulnerabilities have emerged in the first place and how to deal with them collectively in more responsible ways rather than through technical fixes or a patchwork of company-mandated user guidelines. What is more, social engineering experts have rarely considered the broader consequences for a labor force when enacting measures to protect a company's data and communication. To the contrary, anything that increases security seems like a legitimate move forward and does not warrant additional participation from a company's workforce. However, unlike the proponents of scientific literacy, who assume the "enlightened citizen" to be an achievable goal, social engineering experts admit that security is a very fragile, at best temporary state, anticipating the known unknowns of ever new forms of attacks. The concept of resilience is then mobilized as a way to cope with the dynamically changing sociotechnical uncertainties that arise from digitalization while staying flexible enough to point to the users ́s need for "becoming better" without necessarily re-organizing IT security infrastructures and strategies in a more sustainable way.

We suggest that the solution lies not in ever novel forms of user-centered risk governance that pathologizes the individual user, tech savvy or not. Instead, company executives, regulators, and IT engineers should address the issue of social engineering on a collective level, paying more attention to the increasing uncertainties and unintended consequences that the current work regime has produced. We have proposed an analysis that highlights how changing configurations of security and neoliberal work regimes shape the construction of novel sociotechnical deficits and, in turn, how the politics of deficit construction play out in processes of securitization and related calls for resilience. Acknowledging the inherent and inevitable vulnerability of cyber-physical networks and interactions may then open up avenues for building trust between management, IT departments, and employees rather, than securitizing the user as deficient in highly complex processes of maintaining cybersecurity. This would contribute much to the normative discussion that is currently emerging among IT security communities, with calls for companies and policy makers alike to strengthen regulatory frameworks for addressing cybersecurity breaches that were enabled by users. Cybersecurity is a heterogeneous, constantly renegotiated process, rather than an objective condition or status quo to be eventually reached (Simon and de Goede 2015, 3). In other words, it is a matter of concern rather than a matter of fact with its ontological status being both political and open to contestation (Liebetrau and Christensen 2020).

Engaging with how different realities of cyber in/security are enacted and negotiated is important to understand the politics of deficit construction at play in digitized (work) environments and, eventually, to arrive at a culture of cybersecurity that acknowledges the inevitable vulnerability of sociotechnical systems and makes risk a collective rather than individual matter of concern.

Acknowledgments

The authors would like to thank Sebastian Pfotenhauer, Joakim Juhl, and Erik Aarden for starting a conversation on the politics of deficit construction and for their insightful comments on earlier versions of the paper. We also thank the two anonymous reviewers and the editors of *Science, Technology, & Human Values*, Katie Vann and Ed Hackett, for their careful suggestions and helpful feedback. Finally, we are grateful to our informants who provided us with valuable insights into the field.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Nina Klimburg-Witjes https://orcid.org/0000-0003-0583-8788
Alexander Wentland https://orcid.org/0000-0003-3080-8599

References

Abell, Sandra K., and Norman G. Lederman, eds. 2007. *Handbook of Research on Science Education*. Mahwah, NJ: Lawrence Erlbaum Associates.

Abraham, Sherly, and InduShobha Chengalur-Smith. 2010. "An Overview of Social Engineering Malware: Trends, Tactics, and Implications." *Technology in Society* 32 (3): 183-96. doi: 10.1016/j.techsoc.2010.07.001.

Aldawood, Hussain, Tawfiq Alashoor, and Geoffrey Skinner. 2020. "Does Awareness of Social Engineering Make Employees More Secure?" *International Journal of Computer Applications* 177 (38): 45-49. doi: 10.5120/ijca2020919891.

Amoore, Louise, and Marieke de Goede, Eds. 2008. *Risk and the War on Terror*. New York: Routledge.

Balzacq, Thierry. 2005. "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11 (2): 171-201. doi: 10.1177/1354066105052960.

Balzacq, Thierry, and Myriam Dunn Cavelty. 2016. "A Theory of Actor-network for Cyber-security." *European Journal of International Security* 1 (02): 176-98. doi: 10.1017/eis.2016.8.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. 2016. "'Securitization' Revisited: Theory and Cases." *International Relations* 30 (4): 494-531. doi: 10.1177/0047117815596590.

Barnard-Wills, David, and Debi Ashenden. 2012. "Securing Virtual Space." *Space and Culture* 15 (2): 110-23. doi: 10.1177/1206331211430016.

Bigo, Didier. 2014. "The (in)Securitization Practices of the Three Universes of EU Border Control: Military/Navy—Border Guards/Police—Database Analysts. Edited by Karine Côté-Boucher, Federica Infantino, and Mark B. Salter." *Security Dialogue* 45 (3): 209-25. doi: 10.1177/0967010614530459.

Bijker, Wiebe E. 2006. "The Vulnerability of Technological Culture." In *Cultures of Technology and the Quest for Innovation*, edited by Helga Nowotny, 52-69. New York: Berghahn Books.

Bodmer, Walter, and Janice Wilkins. 1992. "Research to Improve Public Understanding Programmes." *Public Understanding of Science* 1 (1): 7-10. doi: 10.1088/0963-6625/1/1/001.

Booth, Ken, ed. 2005. *Critical Security Studies and World Politics. Critical Security Studies*. Boulder, CO: Lynne Rienner.

Campbell, Lisa M., Catherine Corson, Noella J. Gray, Kenneth I. MacDonald, and J. Peter Brosius. 2014. "Studying Global Environmental Meetings to Understand Global Environmental Governance: Collaborative Event Ethnography at the Tenth Conference of the Parties to the Convention on Biological Diversity." *Global Environmental Politics* 14 (3): 1-20. doi: 10.1162/GLEP_e_00236.

C. A. S. E Collective. 2006. "Critical Approaches to Security in Europe: A Networked Manifesto." *Security Dialogue* 37 (4): 443-87. doi: 10.1177/0967010606073085.

Chandler, David. 2014. *Resilience: The Governance of Complexity. Critical Issues in Global Politics*. New York: Routledge.

Collier, Jamie. 2018. "Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision." *Politics and Governance* 6 (2): 13. doi: 10.17645/pag.v6i2.1324.

Dunn Cavelty, Myriam. 2018. "Cybersecurity Research Meets Science and Technology Studies." *Politics and Governance* 6 (2): 22. doi: 10.17645/pag.v6i2.1385.

Dunn Cavelty, Myriam, Mareile Kaufmann, and Kristian Søby Kristensen. 2015. "Resilience and (in)Security: Practices, Subjects, Temporalities." *Security Dialogue* 46 (1): 3-14. doi: 10.1177/0967010614559637.

Edwards, Paul N. 1997. *The Closed World: Computers and the Politics of Discourse in Cold War America*, First MIT Pr. Paperb ed. Inside Technology. Cambridge, MA: MIT.

Ellis, Darren. 2019. "Techno-securitisation of Everyday Life and Cultures of Surveillance-apatheia." *Science as Culture* 29 (1): 1-19.

Falzon, Mark-Anthony, ed. 2009. *Multi-sited Ethnography: Theory, Praxis and Locality in Contemporary Research*. Burlington, VT: Ashgate.

Felt, Ulrike, and Maximilian Fochler. 2010. "Machineries for Making Publics: Inscribing and De-scribing Publics in Public Engagement." *Minerva* 48 (3): 219-38.

Grand View Research. 2020. "Cyber Security Market Size." Accessed January 30, 2021. https://www.grandviewresearch.com/industry-analysis/cyber-security-market.

Hadnagy, Christopher. 2010. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley.

Hajer, Maarten A. 2009. *Authoritative Governance: Policy-making in the Age of Mediatization*. New York: Oxford University Press.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (4): 1155-75. doi: 10.1111/j.1468-2478.2009.00572.x.

Hommels, Anique, Jessica Mesman, and Wiebe E. Bijker, eds. 2014. *Vulnerability in Technological Cultures: New Directions in Research and Governance. Inside Technology*. Cambridge, MA: The MIT Press.

Hege, Leivestad Høyer, and Anette Nyqvist. 2017. *Ethnographies of Conferences and Trade Fairs: Shaping Industries, Creating Professionals*. Cham, Switzerland: Springer International Publishing Imprint, Palgrave Macmillan.

Hulme, George. 2015. "The 2015 Social Engineering Survival Guide What You Need to Know to Keep Your Enterprise Secure from Social Engineering Exploits." *CSO Online (blog)*. 2015. Accessed January 30, 2021. https://www.csoonline.com/article/2864598/the-2015-social-engineering-survival-guide.html.

Huysmans, Jef. 2011. "What's in an Act? On Security Speech Acts and Little Security Nothings." *Security Dialogue* 42 (4–5): 371-83. doi: 10.1177/0967010611418713.

Irwin, Alan. 2014. “From Deficit to Democracy (Re-visited).” *Public Understanding of Science* 23 (1): 71-76.

Jasanoff, Sheila. 2016. “A Century of Reason: Experts and Citizens in the Administrative State.” In *The Progressives’ Century*, edited by Stephen Skowronek, Stephen M. Engel, and Bruce Ackerman, 382-404. The Yale ISPS Series. New Haven CT: Yale University Press.

Kaufmann, Mareile. 2013. “Emergent Self-organisation in Emergencies: Resilience Rationales in Interconnected Societies.” *Resilience* 1 (1): 53-68. doi: 10.1080/21693293.2013.765742.

Kaufmann, Mareile. 2016. “Exercising Emergencies: Resilience, Affect and Acting out Security.” *Security Dialogue* 47 (2): 99-116. doi: 10.1177/0967010615613209.

Keulartz, Jozef, and Maartje Schermer. 2014. “A Pragmatist Approach to the Governance of Vulnerability.” In *Vulnerability in Technological Cultures. New Directions in Research and Governance*, edited by Anique Hommels, Jessica Mesmann, and Wiebe E. Bijker, 285-304. Inside Technology. Cambridge, MA: MIT Press.

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. “Advanced Social Engineering Attacks.” *Journal of Information Security and Applications* 22 (2015): 113-22. doi: 10.1016/j.jisa.2014.09.005.

Lentzos, Filippa, and Nikolas Rose. 2009. “Governing Insecurity: Contingency Planning, Protection, Resilience.” *Economy and Society* 38 (2): 230-54. doi: 10.1080/03085140902786611.

Liebetrau, Tobias, and Kristoffer Kjærgaard Christensen. 2020. “The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites, and Spaces.” *European Journal of International Security* 6 (1): 1-19.

Lineberry, Steven. 2007. “The Human Element: The Weakest Link in Information Security.” *Journal of Accountancy*. Accessed January 30, 2021. https://www.journalofaccountancy.com/issues/2007/nov/thehumanelementtheweakestlinkininformationsecurity.html.

McDonald, Matt. 2008. “Securitization and the Construction of Security.” *European Journal of International Relations* 14 (4): 563-87. doi: 10.1177/1354066108097553.

Methmann, Chris, and Angela Oels. 2015. “From ‘Fearing’ to ‘Empowering’ Climate Refugees: Governing Climate-induced Migration in the Name of Resilience.” *Security Dialogue* 46 (1): 51-68. doi: 10.1177/0967010614552548.

Morozov, Evgeny. 2013. *To Save Everything, Click Here*, 1st ed. New York: PublicAffairs.

Müller, Ruth, and Nina Witjes. 2014. “Of Red Threads and Green Dragons: Austrian Sociotechnical Imaginaries about STI cooperation with China.” In *The Global*

Politics of Science and Technology: Perspectives, Cases and Methods (Volume 2), edited by Maximilian Mayer, Mariana Carpes, and Ruth Knoblich, 47-65. Berlin, Germany: Springer.

Nyamsuren, Enkhbold, and Ho-Jin Choi. 2007. “Preventing Social Engineering in Ubiquitous Environment.” *Future Generation Communication and Networking* 2:573-77.

Pfotenhauer, Sebastian M., Joakim Juhl, and Erik Aarden. 2019. “Challenging the ‘Deficit Model’ of Innovation: Framing Policy Issues under the Innovation Imperative.” *Research Policy* 48 (4): 895-904. doi: 10.1016/j.respol.2018.10.015.

Polak, Niloo Razi Howe Matt. 2020. “The Twitter Hack Shows a Major Cybersecurity Vulnerability: Employees.” *Slate Magazine*, July 21. Accessed January 30, 2021. https://slate.com/technology/2020/07/twitter-hack-human-weakness.html.

Reid, Julian. 2012. “The Disastrous and Politically Debased Subject of Resilience.” *Development Dialogue* 58 (1): 67-79.

Shires, James. 2018. “Enacting Expertise: Ritual and Risk in Cybersecurity.” *Politics and Governance* 6 (2): 31. doi: 10.17645/pag.v6i2.1329.

Simon, Stephanie, and Marieke de Goede. 2015. “Cybersecurity, Bureaucratic Vitalism and European Emergency.” *Theory, Culture & Society* 32 (2): 79-106. doi: 10.1177/0263276414560415.

Sismondo, Sergio. 2010. *An Introduction to Science and Technology Studies*, 2nd ed. Malden, MA: Wiley-Blackwell.

Stirling, Andy. 2008. “‘Opening Up’ and ‘Closing Down’: Power, Participation, and Pluralism in the Social Appraisal of Technology.” *Science, Technology, & Human Values* 33 (2): 262-94. doi: 10.1177/0162243907311265.

Tetri, Pekka, and Jukka Vuorinen. 2013. “Dissecting Social Engineering.” *Behaviour & Information Technology* 32 (10): 1014-23. doi: 10.1080/0144929X.2013.763860.

Twitter. 2020. “An Update on Our Security Incident and What We Know so Far.” July 30. Accessed January 30, 2021. https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.

Walker, Jeremy, and Melinda Cooper. 2011. “Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation.” *Security Dialogue* 42 (2): 143-60. doi: 10.1177/0967010611399616.

Wolff, Josephine. 2016. “Why Computer Science Programs Don’t Require Cybersecurity Classes.” *Slate Magazine*, April 14. Accessed January 30, 2021. https://slate.com/technology/2016/04/why-computer-science-programs-dont-require-cybersecurity-classes.html.

Workman, Michael. 2008. "Wisecrackers: A Theory-grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security." *Journal of the American Society for Information Science and Technology* 59 (4): 662-74. doi: 10.1002/asi.20779.

Wynne, Brian. 1992. "Misunderstood Misunderstanding: Social Identities and Public Uptake of Science." *Public Understanding of Science* 1 (3): 281-304. doi: 10.1088/0963-6625/1/3/004.

Wynne, Brian. 2006. "Public Engagement as a Means of Restoring Public Trust in Science—Hitting the Notes, but Missing the Music?" *Public Health Genomics* 9 (3): 211-20. doi: 10.1159/000092659.

Author Biographies

Nina Klimburg-Witjes is a postdoctoral researcher at the Department of Science and Technology Studies at the University of Vienna. In her work at the intersection of science and technology studies and critical security studies, she explores the role of technological innovation and knowledge practices in securitization processes. Tracing the entanglements between industries, political institutions, and users, she is interested in how (visions of) sociotechnical vulnerabilities are co-produced with security devices and policy, with a particular focus on space technologies and sensor infrastructures.

Alexander Wentland is a postdoctoral researcher and project group leader at the Munich Center for Technology and Society (MCTS) at the Technical University of Munich. His work focuses on the politics of innovation, sustainability transitions, and regional legacies in the imagination of social order vis-à-vis technology.