Research Article

Rolf Egert, Nina Gerber, Jasmin Haunschild*, Philipp Kuehn, and Verena Zimmermann

Towards Resilient Critical Infrastructures – Motivating Users to Contribute to Smart Grid Resilience

https://doi.org/10.1515/icom-2021-0021

Abstract: Smart cities aim at improving efficiency while providing safety and security by merging conventional infrastructures with information and communication technology. One strategy for mitigating hazardous situations and improving the overall resilience of the system is to involve citizens. For instance, smart grids involve *prosumers*—capable of producing and consuming electricity—who can adjust their electricity profile dynamically (i. e., decrease or increase electricity consumption), or use their local production to supply electricity to the grid. This mitigates the impact of peak consumption periods on the grid and makes it easier for operators to control the grid. This involvement of prosumers is accompanied by numerous socio-technical challenges, including motivating citizens to contribute by adjusting their electricity consumption to the requirements of the energy grid. Towards this end, this work investigates motivational strategies and tools, including nudging, persuasive technologies, and incentives, that can be leveraged to increase the motivation of citizens. We discuss long-term and side effects and ethical and privacy considerations, before portraying bug bounty programs, gamification and apps as technologies and strategies to communicate the motivational strategies to citizens.

Keywords: Smart Grid, Motivation, Nudging, Prosumers, Critical Infrastructures, Citizens, Resilience

***Corresponding author: Jasmin Haunschild,** Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC), Darmstadt, Germany, e-mail: haunschild@peasec.tu-darmstadt.de, ORCID: https://orcid.org/0000-0002-6215-7973
Rolf Egert, Technical University of Darmstadt, Telekooperation Lab, Darmstadt, Germany, e-mail: egert@tk.tu-darmstadt.de
Nina Gerber, Verena Zimmermann, Technical University of Darmstadt, Work and Engineering Psychology (FAI), Darmstadt, Germany, e-mails: n.gerber@psychologie.tu-darmstadt.de, zimmermann@psychologie.tu-darmstadt.de
Philipp Kuehn, Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC), Darmstadt, Germany, e-mail: kuehn@peasec.tu-darmstadt.de

1 Introduction: The Smart Grid, Prosumers and Resilience

Smart cities are envisioned to encompass highly digitized and strongly interconnected infrastructures, like the energy grid, water supply, and telecommunication. Some of these systems or organizations, called Critical Infrastructures (CIs), provide vital services for nations' society and economy. Failures or attacks on these CIs can impair crucial services and severely threaten public safety and security [81].

This is particularly true for the energy grid, which provides a continuous supply of electricity for millions of consumers, despite the ever-increasing energy-technical demand of modern societies [50]. However, since failures and attacks cannot be fully prevented, a high degree of resilience is crucial for minimizing hazardous consequences for all involved. Resilience can be defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" [52, p. XXXVI].

In the context of energy grids, conglomerates have always been responsible for maintaining a stable operation by adjusting production to the needs of the consumers. In recent years, energy grids have transitioned from the conventional fossil-fuelled and top-down controlled systems towards increasingly distributed Smart Grids that strongly rely on renewable energy sources. Whilst these developments have obvious benefits, they introduce their own share of challenges, such as high volatility as the production of renewable energy depends on ever-changing environmental factors, like wind and solar radiation. On top of that, the role of consumers changes. Traditionally, their role within conventional energy grids was a passive one, where they freely consumed electricity provided by large producers, whilst being largely unaware of the impact of their actions and the feats that need to be accomplished by operators to provide a continuous supply with electricity. These consumers have evolved into increasingly active *prosumers*, supported by information and communication technology (ICT) and capable of producing and consuming electricity [28]. This means that the balancing of demand and supply in SGs becomes more complex as the set of interdependent participants in a SG strongly increases.

Consequently, notions of safety and security in these complex and interconnected systems cannot solely be based on technical aspects but increasingly depend on the behavior of citizens. It is thus important to consider citizens as active contributors to safety and security, in terms of stabilizing the SG to prevent hazardous incidents as well as in terms of coping with and recovering from emergency situations such as blackouts, e. g., through emergency preparation and coping strategies [103].

Numerous options for citizens to contribute to the safety and security of SGs are already available in current energy grids, e. g., adapting consumption behavior to avoid high consumption during peak hours, and studies have investigated the conditions under which citizens are prepared to cease control over energy consumption [31] or motivations for reducing consumption [75]. Yet, some of these aspects cannot be regulated or mandated without compromising the autonomy and freedom of choice of individuals, while others require the provision of certain technologies and technological knowledge. Thus, one challenge lies in enabling and motivating users to voluntarily contribute to the safety and security of smart grids, especially if their "resilient" behavior might result in compromises or restrictions for themselves for the benefit of others. An additional challenge lies in sustaining motivation and the targeted behaviors in the long term.

Across different disciplines, strategies such as nudges or incentives have been explored to shift citizens' decisions or behaviors [91, 77]. Yet, motivating citizens to "resilient" behaviors within complex and interconnected CIs remains a new and unsolved challenge.

Applying insights from various disciplines, we will shed light on the following research question: *How can citizens be motivated to actively contribute to the safety and security of connected CIs, such as smart grids?* This paper presents and discusses different strategies for motivating citizens to contribute to safety and security of CIs from an interdisciplinary point of view. As a prominent representative of CIs, smart grids are used as an example to illustrate each strategy with practical examples.

The remainder of the paper is structured as follows: Section 2 on motivational approaches presents strategies to motivate citizens to contribute to SG safety and security along with practical examples from an interdisciplinary viewpoint. We then discuss the presented strategies with regard to their long-term effects, ethical challenges, as well as practical implications in Section 3 and present visions of citizen participation through bug bounty programs, gamification, and the use of apps in Section 4. Section 5 summarizes the findings.

2 Motivating Users and Citizens to Contribute to Safety and Security in Smart Cities

In general, motivation can be defined as the overall desire or willingness of someone to do something [73]. This section presents theoretical frameworks and approaches for motivating users to choose certain options for action or to show specific behaviors. The approaches represent an interdisciplinary perspective with insights from various disciplines, such as pedagogy (e. g., information provision), behavioral economics (e. g., nudging), psychology (e. g., persuasive technologies), and politics (e. g., incentives). While the approaches differ in their theoretical background, their perspective on the human being, and their intentions, they rely on similar mechanisms to transfer these intentions. Each approach is presented with some examples for motivating citizens to contribute to smart grid safety and security. Furthermore, the differences, overlaps, and possibilities for combining approaches will be discussed in Section 2.5.

2.1 Information and Education

Information provision serves to bridge a potential knowledge gap between citizens (or laypersons) and a knowledgeable third party, such as an organization, the state, or experts of various kinds to improve the decision-making process [18]. Education and information provision can be regarded as essential for achieving transparency and for empowering citizens with different levels of background knowledge and skills to make informed privacy and security decisions where incomplete or asymmetric information is the norm [2]. However, too much information can be overwhelming for the user.

For example, research found that information provision through notices is seldom working in practice [18]. Obar and Oeldorf-Hirsch [71] showed that privacy policies and terms of service are rarely read and Florêncio et al. [35] found that password creation suggestions are seldom followed, despite year-long advice. Previous work from the security and privacy area thus suggests that information should be provided in a concise format considering the user's mental models (e. g., using known metaphors) [76], and that standardization of information (e. g., standardized labels) [57] may support understanding. Examples for standardized labels related to smart grids are energy labels on electric devices and suggestions for standardized privacy labels indicating how organizations make use of the citizens' personal data [56].

Information and Education Examples

Examples for practical information provision to motivate citizens in contributing to smart grid safety and security are already discussed in the literature [40, 45]. This research confirms that the simple provision of information (e. g., using in-house displays that provide information about the electricity consumption) is insufficient to motivate citizens. In comparison, if information provision is combined with other techniques, such as incentive-based approaches, the probability of citizens contributing to the safety and security of the grid can be increased [49, 14, 5]. For example, it was shown that the decision-making of citizens can be improved by providing information on smart meters and facilitating the choice of time-of-use tariffs in combination with personalized estimated costs as an incentive [14].

2.2 Nudging

Nudges [97] are small tweaks of physical or digital decision interfaces aiming to encourage "wiser" decisions, e. g., secure behavior, without limiting or significantly influencing peoples' choice set. Nudges generally work by activating automatic cognitive processes such as biases or heuristics [18, 43].

Nudges have been successfully applied in a large range of physical contexts such as encouraging healthy nutrition [60], organ donation [104], or physical activity [102]. In addition, nudging has found its way into the digital and cyber space, including password creation [78, 46], WiFi selection [101], and privacy-friendly app choices [12]. An example is that of using a position effect to make people choose a secure WiFi option in a public place such as an airport. When the secure WiFi option appeared first in the selection list, more people tended to choose that option [107]. As such, nudging might be a promising strategy to encourage certain decisions within the smart city context in which physical and digital spaces become increasingly intertwined.

Nudge Examples

Nudges towards pro-environmental decisions have often been summarized under the term "Green Nudges" [87]. Previous research on green nudges showed that users can be nudged towards saving electricity by providing them feedback on their consumption behavior or comparisons with other users [11, 6]. However, these nudges may also create unintended effects. For example, those households that usually consumed less than average, unexpectedly increased their energy consumption [88], perhaps because of a tendency to go with the norm. These side effects could be mitigated by including an indication of desirable behavior [88]. On the level of providers, exemplary nudges include enrolling clients in green energy sources in their contracts per default [93] and research confirmed that more people select green energy choices when those are presented as the default [74].

Schubert [87] suggests the use of an *Ambient Orb*, as a green nudge, which changes its color to indicate the current smart grid load. Even though imagined in the context of climate change, a similar intervention could serve to increase users' awareness of the grid's load factor and may encourage users to contribute to the grid's stability.

Zhao and John [105] examined the use of framing nudges to encourage users to build community resilience through preparation for natural disasters, e. g., by storing food or household retrofitting. They used the examples of a hurricane, earthquake, or flood and applied the choices to invest in physical mitigations, an insurance, or to do nothing with the chance that no adverse consequences arise. In general, the percentage of people choosing to invest was higher when the decision was framed as a gain. Even though the contexts of the study slightly differed from the smart grid one, the results might be transferable.

2.3 Persuasive Technologies

Persuasive technologies are interactive technologies that aim to change the attitude or behavior of the respective user [37]. Whereas nudges can exert influence on a subconscious level, influence from persuasive technologies always comes from a conscious interaction with the technology. Hence, users make an active decision to change their behavior in a certain way (e. g., to reduce CO_2 emissions) and use technologies that support them in this desired behavioral change. Consequently, persuasive technologies are designed for more far-reaching behavioral changes than nudges, which are not intended to restrict the user's scope for decision-making.

The concept of persuasive technologies was first described by Fogg [37]. He postulates that three factors must be present at the same time for a change in behavior to occur: motivation, ability, and a prompt [36]. Possible motivators include gaining pleasure (or preventing pain), hope (or overcoming fear), and winning social acceptance (or preventing social rejection). The aspect of ability focuses on one's resources, e. g., in terms of time, money, or physical strength. However, according to the Fogg Behavior Model (FBM), even if people score high on motivation and ability, they still need to be prompted to exercise a certain behavior.

Persuasive Technology Examples

Multiple studies examine the potential of persuasive technologies to encourage energy saving. Beheshtian et al. [13] explore the possibilities of a persuasive social robot aiming to facilitate sustainable behavior—such as saving energy—in shared living spaces. Most of their 20 participants agreed that social components such as comparing their energy consumption with other flats and competing against others could motivate them to save energy. They also liked the idea of getting points and rewards as well as information about how to save energy. Takayama et al. [94] describe the successful gamification approach, which implements several social feedback mechanisms, e. g., by allowing families to compare their CO_2 emissions against those of their neighbors.

Bourgeois et al. [15] developed and tested four different interventions aiming to motivate households who produce their own "green" energy to shift their laundry activities to maximize the use of their self-generated energy. The results of an 8-month field study with 18 households suggest that while feedback mechanisms fail to motivate a behavior change, proactive suggestions as well as contextual control (e. g., replacement of the control panel with a tablet that offers the opportunity to either start the washing process immediately or automatically at the best time) seem promising for facilitating behavior change.

2.4 Incentives

The participation of laypersons in processes for maintaining the continuous operation of CIs is often—if not always—accompanied by some kind of *burden*, such as a partial blackout for prosumers who offer reserve capacity. Therefore, rational choice strategies suggests that such burdens should be adequately compensated. In this context, *incentives* aim to alleviate the participation of laypersons by directly or indirectly providing a compensation. In comparison to persuasive technologies (see Section 2.3), which aim to motivate people in making active decisions, incentives use direct or indirect mechanism for reimbursing certain user behaviors.

Psychological theories differentiate between intrinsic or extrinsic motivation, i. e., whether the motivator lies within the execution of a certain action or in the consequences of the completed action [82]. Exemplary findings analyzing the intrinsic motivators behind graffiti spraying identified, e. g., sensation seeking, a flow experience, creativity, and camaraderie [83]. Extrinsic motivators include monetary, social, or other rewards, such as job-related benefits [62, 86]. The differentiation can be relevant when designing interventions or choosing incentives to motivate a certain behavior. Research showed that intrinsically motivated behavior can be crowded out when offering extrinsic incentives, e. g., when offering children a reward for an action they formerly enjoyed doing [21].

Incentive Examples

Incentivization is a strategy that has been used within the energy grid for decades. Various pricing strategies exist, which aim to encourage the consumers in the grid to adjust their behavior, like time-of-use prices, real-time pricing, and inclining block-rate pricing [1, 49, 14, 5]. The majority of these strategies is based on indirect reimbursement strategies, where consumers can manage to *pay less* if they adhere to the behavior, which is suggested by the strategies (e. g., avoid strong electricity consumption during peak-consumption hours, where prices are high). Such strategies have been successfully used within Home Energy Management Systems (HEMSs) as an incentive for automatically scheduling the use of appliances to maximize the monetary benefits of the consumers [67].

2.5 Combination of Approaches

The presented interventions differ with regard to their theoretical background, their disciplinary viewpoints, and their intentions even though they may sometimes make use of similar measures to achieve their aim (see Table 1). However, the approaches also show a certain degree of overlap in the mechanisms they use. For example, incentivization encourages users to pick a certain option and to overcome burdens e. g., increased efforts or downsides. Persuasive technologies instead make use of incentives to support users in their self-chosen behavior changes and

Table 1: Overview over the criteria for differentiating the presented interventions.

	Information Provision	Nudges	Persuasive Technologies	Incentives
Cognitive process	reflective	automatic	reflective	reflective
Primary target	decision & behavior	decision	behavior	decision
Degree of coercion	low	medium	low	high
Degree of interaction	low/medium	low	high	low
Resources provider	low	low	high	high
Resources user	high	low	high	low

aims. Incentivization also partially overlaps with nudging. Even though Thaler and Sunstein [97] exclude "significant" economic incentives from the nudge definition, the criterion is rather vague so that other incentives such as social rewards may still fulfill the nudge definition.

Research showed that the combination of interventions, such as several persuasive technology mechanisms [65] or information provision and nudging [60, 107, 92] can even be beneficial.

Yet, researchers and practitioners should be aware of these overlaps to clearly position, design, and purposefully combine their interventions. Additionally, they should bear in mind the different theoretical concepts behind and the implications of different approaches in order to anticipate and avoid potential negative side effects or unintended outcomes.

3 Evaluation and Discussion

The analysis of motivational aspects and technologies to implement them shows that there are many avenues to enhance the integration of prosumers to contribute to the resilience of CIs. While the given examples mainly portray the energy sector, similar challenges exist with regard to other CIs. The water sector is also grappling with involving citizens in reducing and steering water consumption and with communicating with consumers [48, 69, 61]. In choosing and adapting motivational strategies, ethics, privacy aspects, as well as potential side effects should be considered.

3.1 Ethical Considerations

Guidelines for ethical psychological research [9, 29, 98] suggest to respect persons and their autonomy, to maximize beneficence, to practice justice, to work according to scientific integrity standards, and to take on social responsibility. These meta guidelines can also well inform the depletion of measures to motivate citizens to or to make citizens behave in a certain way.

For example, citizens could be respected by being informed transparently about the measures and their purpose, and by looking for solutions that do not unnecessarily compromise citizens' autonomy. Exemplary strategies following that approach are educational approaches aiming to increase knowledge and awareness, persuasive technologies that foster the active interaction with the user, or nudges that aim to encourage certain choices without limiting the choice set. In terms of nudges, research suggests that transparent "hybrid nudges", i. e., the combination of nudges with information provision, may be especially favorable due to the enhanced transparency of the intervention [78].

The beneficence of deployed measures for the safety, security, and welfare of citizens could be weighed against potential costs and risks for individuals, e. g., the need to give up on privacy or certain privileges in emergency situations. Citizens could be motivated to accept potential constraints by highlighting desirable social norms and the contribution to the common good or by compensating downsides with suitable incentives.

Deployed measures could be rated in terms of justice such as whether certain societal groups are discriminated or excluded. This could be the case if certain benefits or functionalities are only available to people with certain devices or levels of expertise. For example, persuasive technologies should be designed to be usable and accessible for different age groups such as children and seniors.

It is reasonable to evaluate all deployed measures in terms of their scientific integrity and quality to ensure effectiveness and to identify possibly unanticipated or unintended consequences. An example is the intervention aiming to reduce energy consumption through social comparison and which found that people who were below the average surprisingly increased consumption. This outcome could only be identified and mitigated through suitable evaluation [88].

Finally, decision-makers bear considerable social responsibility. They should be aware of the potential short-term and long-term consequences of their actions considering the before-mentioned guidelines. For example, the use of high financial incentives might lead people to engage in activities against their will out of financial despair. This might not only negatively affect the citizens themselves, but may also compromise the long-term effectiveness of the measure, especially when the incentive is taken away at some point.

Yet, the decision to deploy certain measures is definitely not an easy one. Challenges remain, such as when to compromise autonomy and limit freedom of choice. Which situations justify constraining strategies such as laws or restrictions? In case of limited resources, who should benefit in which way? How can accessibility and non-discrimination be ensured given different age groups, technical equipment, and varying levels of expertise? Which measure should be deployed when scientific evidence is scarce or contradictory? An approach for targeting these important questions, that is already practiced in some cases [25], is the depletion of an interdisciplinary ethical committee that evaluates processes and deployed measures from various perspectives.

3.2 Privacy Aspects

With the ongoing digitalization of cities and public spaces, the privacy of citizens is gaining in importance. Here, the General Data Protection Regulation (GDPR) is of relevance, which since 2016 is part of EU law on data protection. By addressing data transfer in particular, the aim of the GDPR is to give individuals control over their data and to provide uniform regulations for privacy in IT in the EU. The GDPR holds users accountable for the protection of their data by requesting informed consent for the use of their data [99]. However, with increasing data collection in public spaces, e. g., by cameras and sensors, it quickly becomes impossible for citizens to keep track of the collection of their data. It is furthermore hardly possible to decline the collection of one's data in public spaces without restricting one's behavior, e. g., by avoiding to visit certain public places.

Yet, cities sometimes might need to collect data of their citizens for safety or security purposes. This has been subject of heated discussions before, e. g., when the interior ministry in Germany tested facial recognition cameras at the Berlin-Südkreuz station in 2018 [23], or recently in the course of the introduction of the German Corona-Warn-App [17]. German citizens tend to express concerns about governmental surveillance, but in an Orwellian manner they usually lack concern in the context of data collection by private organizations like Google or Facebook [8]. While this is often explained by the historical experiences of being spied on and prosecuted by the Gestapo and Stasi [38], it remains unclear how governmental agencies should deal with this fear of their citizens of being under surveillance. Research is needed to address this issue and explore possibilities for communicating decisions about technical implementations regarding data collection and privacy protection to the general population. This is especially important in case the population is expected to collaborate in the data collection, e. g., by installing and using the Corona-Warn-App, by reporting information about safety or security related incidents, or by participating as prosumers in SGs [27].

However, research on crisis apps suggests that users are willing to make privacy concessions to increase security [96]. A possible solution for supporting citizens in keeping track of and managing the collection of their data could be the provision of a digital privacy assistant [20]. This assistant could be implemented, e. g., as a mobile solution in the form of an app. Combining machine learning and manual input, the assistant would be able to semi-automatically identify the privacy preferences of its user and communicate and enforce them to data collecting devices in the public space.

3.3 Long-Term and Side Effects

Long-term and side effects of relying on technology to communicate with and motivate prosumers can be the exclusion of segments of the population. Therefore, different preferences of various socio-demographic groups should be considered. While age differences should not be overstated, certain aspects such as internet self-efficacy are often different for older or younger people [19]. Research on warning apps indicates that while many preferences are universal, women are partly interested in different warning topics than men [55]. Similarly, women and men are likely to have deviating considerations for their energy use, leading to differences in peak energy consumption and thus requiring different motivations for desired behaviors. The implementation of motivational strategies and choice of technologies should consider such differences and ensure that no groups are excluded. Such differences may also be relevant for motivating various demographic groups, who may respond differently to motivation strategies.

Introducing technologies that connect prosumers and CIs creates further vulnerabilities in the system. At the same time, citizens typically behave insecurely online [108], potentially leading to another weak link when it comes to securing CIs. Any technology used to integrate prosumers should thus consider the cybersecurity risk and CI resilience [51]. Moreover, nudging may compromise users' autonomy if they are not aware of the subtle or covert influence [64, 44], or cause reactance on the users' side due to the perceived manipulation. This issue could be addressed by making nudges more transparent [97, 70], e. g. by combining them with other approaches such as information provision. Initial research indicates that increasing the transparency of the nudge does not necessarily comprise its efficacy but may even be useful [60, 107]. In addition, involving users should ensure that psychological needs are considered. For example, research indicates that even without additional extrinsic motivation such as praise, the mere recognition of the contribution goes a long way in keeping participants motivated [10].

4 Visions for Citizen Participation

This section discusses the contribution of citizens to infrastructure resilience as an aspect of citizen participation. As such, it introduces bug bounty programs, gamification, and apps as strategies to foster citizen involvement and highlights the use of apps to engage citizens in different contexts.

4.1 Bug Bounty Programs

BBPs can be understood as a form of crowdsourced penetration testing, where the identification of IT system weaknesses are financially rewarded [26]. While using bug bounty rewards is cheaper than employing many cybersecurity experts for penetration testing, individuals who participate are mainly motivated by their contribution to public safety and the recognition of their community [59].

However, the (cyber-)security of any CI should be preserved when involving individuals, since they are crucial for a functioning society [51]. Hence, it is prohibited to let civilians interact directly with critical parts in such systems or to test them for crisis scenarios [4]. However, when looking at the field of Critical Information Infrastructures (CIIs), which are considered a subset of CIs [22], we see a shift towards the participation of individuals to secure these systems. For example, BBPs are used by large IT companies like Microsoft, Facebook, and Google. Such programs allow white-hat hackers to hack promoted systems and report vulnerabilities found in exchange for a (usually monetary) reward. This has been shown with great success, since large IT infrastructures are becoming too complex for teams to find vulnerabilities and defend systems against cyber attacks. Not only companies, but also agencies in the U.S. like the Department of Defense (DoD) [68] use this kind of civil participation to strengthen the security of their IT infrastructure. Since then, it has become a trend in the U.S. to use BBPs as a method of discovering vulnerabilities, even in CI [30]. With the emergence of more ICT systems in CIs, these systems are getting inherently insecure, due to insecure hard- and software components [32, 72]. A bug bounty approach could potentially increase the security of such, thus, increase the reliability and resilience, due to the lack of aforementioned vulnerabilities. IT security experts (or even less skilled participants) would be able to directly interact with the CIs, to report vulnerabilities, and eventually to confirm strong defensive measures in terms of IT security. Another benefit of this approach is the potentially increasing trust of civilians in these infrastructures, because of a direct participation possibility.

However, this approach requires a controlled involvement of individuals. Precautions must be taken to exclude criminal actors from interacting with security-relevant information and systems. In addition, when vulnerabilities are triggered, users interact with systems in unexpected ways, i. e., by crashing the system or escalating privileges. Hence, it is imperative to provide enough backup systems to seamlessly swap out compromised systems or even to separate active and inactive (e. g., backup) facilities and replicate a realistic workflow in the systems under investigation (e. g., by replicating old protocols), before enabling BBPs. Moreover, due to the possible installation of backdoor software, a thorough observation of system logs and user behavior is necessary to mitigate both problems. IT forensics might be necessary to ensure a proper functioning of the system state after investigation before reinstalling the systems into the real world. Otherwise, *testing systems* might never be allowed to enter as live-system, but may solely be used for security testing in this simulated environment.

Overall, BBPs have a high potential to increase the security of CIs. Currently existing bug bounty formats need to be adapted to the high security needs of CIs and additional security measures must be installed to be of use in this domain.

4.2 Gamification

Gamification refers to a concept that transfers designs, mechanics, and heuristics of games into a non-gaming context to enrich the user experience by invoking feelings like excitement and joy [24]. The goal is to leverage the users' intrinsic motivation for playing games in a pragmatic context that aims to fulfill specific goals [47]. To achieve these goals, game mechanics aim to increase the motivation of users to adjust their behavior [89]. Literature shows that gamification has been successfully applied in various domains, like mobile education [90], redesigning of business processes [58], and cybersecurity [33]. Furthermore, gamification has been successfully applied in the context of urban infrastructures. For instance, prominent examples aim at influencing the water consumption of citizens and aid water utilities in improving their strategies for system operation [84, 63]. In the domain of energy grids, gamification is used to achieve reductions in peak demand and costs for infrastructure operators [39, 7, 53, 54].

In practice, commonly applied game mechanics are, among others, scoring systems, levels, and achievements [106]. For instance, Gnauk et al. [39] proposed a prototypical demand dispatch system for energy grids, which allows citizens to communicate available flexibilities (i. e., variable consumption periods for local appliances) to control authorities. Authorities can leverage these variable consumption times to optimize the operation of the grid by scheduling the consumption accordingly or negotiate changes. For decisions citizens make that improve the overall demand dispatch operations, they are rewarded with *Earth Saver Points* which can be used to earn titles in the context of the application (e. g., Eco Hero) or gain small extrinsic rewards.

Despite the success of gamification in various fields, the effective application of the concept is challenging [42]. Several concepts and methods that have been discussed within this work need to be combined carefully. For instance, the representation of information for citizens must be carefully designed, to prevent overwhelming effects and discouragement (see Section 2.1). Furthermore, interaction interfaces need to be designed thoroughly to support citizens in conducting beneficial actions intuitively (see Section 2.2). Furthermore, aspects like the voluntariness of tasks, the nature of the system (e. g., pragmatic or hedonic), and the general citizen involvement and attitude can strongly influence the applicability of gamification [42, 41].

Overall, gamification represents a promising technique to increase the involvement of citizens with actions to improve safety and security of smart city infrastructures. The possibilities for potential applications are numerous, but each concept needs to be carefully designed in order to be effective.

4.3 Crisis Communication and Apps

Due to the importance of time in communicating the state of the energy system and potential crises, typical tools for a day-to-day interface would be apps. For example, warning apps typically deal with the communication between emergency services and citizens, but ICTs are also used for coordination among citizens or among agencies [79]. Due to the dynamic nature of crises, mobile crisis applications are commonly used for (1) gathering data from the crowd, (2) organizing collaboration during disasters, (3) spreading official information, (4) collecting and processing data for situational awareness, (5) allowing users to notify others during disasters [95]. Apps are also already commonplace for owners of solar panels, to adapt their energy use to their own production. Technologies such as home energy management systems are being developed that help prosumers manage their energy reserves and consumption [85]. Such tools that enable prosumers to make situation and device specific choices are particularly relevant as prosumers are more resistant to remotely versus personally controlled changes to device operations for balancing the grid [66]. Typically, such information would be offered on demand, as *pull* rather than *push* information, requiring prosumers to proactively search for the relevant information, e. g., by opening their app. In case of emergencies, *push* messages increase the likelihood that crisis information is noticed immediately. These systems are already used in warning apps. Typical warnings include information about the incident as well as instructions on how to behave [34]. However, CIs do not typically have channels particularly for emergency communication. Instead, their communication with citizens relates mainly to public relations and corporate crisis management.

Borrowing from crisis informatics, modes of communication should be established that (1) communicate the state of the system so that prosumers can make informed decisions and (2) communicate urgently needed action or emergency concessions to increase prosumers' timely cooperation. One aspect to consider is whether to use general-purpose or built-for-purpose tools. General-purpose tools are familiar and relevant in daily life [95], because they primarily fulfill a function not related to warnings, such as weather apps that also warn about extreme weather or the German Ministry of Health's use of the messenger apps WhatsApp and Telegram for COVID-19 related information and behavioral recommendations [16]. Built-for-purpose tools, in contrast, are only used in emergencies, which are rare, but they are more adaptable to their specific functions. In warning apps, such as FEMA or KATWARN, this includes the option to determine a geographic area of interest or content areas, such as traffic, weather, or cyber crime [55, 80]. Regarding the use of specific apps for communication with prosumers to increase resilience, we suggest that four main challenges exists. Firstly, despite the fact that a large proportion of citizens regard warning apps as important, they are seldom used. In 2019, only 16,5 % of German citizens were using any warning app, although over 60 % agreed that they were relevant and 65 % demanded that all warnings should be centralized in one app [55]. Therefore, secondly, the relevance of a tool is dependent on the number and relevance of the organizations providing it. Hence, a warning tool that involves prosumers should be relevant to users' daily life and include several infrastructures. This could mean combining a general energy consumption and production app with a warning or motivational feature or building on channels that are already wide-spread, such as commonly used messaging apps. The third challenge relates to indications that citizens prefer tools that enable them to be active contributors, e. g., to help as witnesses and in the search for missing people, and that have elements of two-way communication [55]. Finally, apps for specific purposes have specific usability requirements. While many insights from crisis informatics can be applied to resilience communication, warning apps' usability requirements [96] may not be identical with the requirements for motivating the co-production of resilience with prosumers. In order to be appealing, prosumers should be involved in studying the particular usability requirements for such tools, e. g. the personalization and notification options.

Likewise, many nations are currently focusing on the use of tracing apps to combat the COVID-19 pandemic, thereby relying on citizens to collaborate in data collection and notification, i. e., tracing social contacts and notifying potential contacts of a positively tested person [3]. Which features are relevant for the mass acceptance of such an app seems to depend on how citizens feel about the general concept of such an app. While critics seem to place particular emphasis on privacy and societal benefit, the undecided may be mainly convinced by the app's convenience, and advocates are likely to use the app regardless of its features [100]. All motivating approaches introduced in Section 2 are suited for implementation in form of a mobile app. Further, these approaches could (1) increase citizen engagement to participate in apps they have already installed, such as contact tracing apps in the context of COVID-19, (2) motivate more citizens to install such apps in the first place, e. g., by educating citizens about the app's functionality and privacy aspects or by rewarding them for the app installation, and (3) serve as a framework for the development of new apps which aim to maximize users' motivation for collaboration. To increase the relevance of such an app, it may combine several aspects of citizens' contributions to the common good, which may require the coordination between several infrastructure providers or the coordination by administrative agencies. In this context, smart city initiatives may be a good place to start, as they are already implementing public digitization, of which CIs could be one of several areas for involving citizens.

5 Conclusion

The energy sector represents a leading example for increasingly involving citizens to actively participate and contribute to resilience of the system as a whole. With the changing role of consumers towards prosumers—capable of consuming and producing electricity—the potential for participation is further increased. While this introduces numerous technical challenges, social aspects like awareness and motivation become increasingly important. For instance, studies have already investigated prosumers' conditions for ceding different levels of autonomy over their electricity consumption, combined with different compensation schemes. Furthermore, social and intrinsic motivations have been explored in the context of consumption reduction and sustainability. In this work, we showed that a variety of options are available for motivating prosumers in the energy sector. These motivational strategies can be enhanced by ICTs that offer new ways of communicating with prosumers, of informing about the state of the system, about crises, or prosumers contributions. Infrastructure providers should thus explore recreating their communication strategies in manners that involve their users and prosumers. While the examples presented in this work mostly refer to the energy sector, we emphasize that presented concepts and strategies can be applied to other sectors as well.

Funding: This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the LOEWE initiative (Hesse, Germany) within the emergenCITY centre.

References

[1] J. Abushnaf, A. Rassau, and W. Górnisiewicz. Impact of dynamic energy pricing schemes on a novel multi-user home energy management system. *Electric Power Systems Research*, 125: 124–132, 2015. 10.1016/j.epsr.2015.04.003.

[2] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50 (3): 1–41, 2017. 10.1145/3054926.

[3] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha. A survey of COVID-19 contact tracing apps. *IEEE Access*, 8: 134577–134601, 2020. 10.1109/ACCESS.2020.3010226.

[4] C. Alcaraz and S. Zeadally. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection (IJCIP)*, 8: 53–66, 2015. 10.1016/j.ijcip.2014.12.002.

[5] H. Allcott. Real time pricing and electricity markets. *Harvard University*, 7, 2009.

[6] H. Allcott. Social norms and energy conservation. *Journal of Public Economics*, 95 (9-10): 1082–1095, 2011. 10.1016/j.jpubeco.2011.03.003.

[7] T. AlSkaif, I. Lampropoulos, M. van den Broek, and W. van Sark. Gamification-based framework for engagement of residential customers in energy applications. *Energy Research & Social Science*, 44: 187–195, 2018. ISSN 2214-6296. 10.1016/j.erss.2018.04.043. URL https://www.sciencedirect.com/science/article/pii/S2214629618304420.

[8] S. Altmann, L. Milsom, H. Zillessen, R. Blasone, F. Gerdon, R. Bach, F. Kreuter, D. Nosenzo, S. Toussaert, and J. Abeler. Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR Mhealth Uhealth*, 8 (8): e19857, 8 2020. ISSN 2291-5222. 10.2196/19857.

[9] American Psychological Association. Ethical Principles of Psychologists and Code of Conduct, 2016. http://www.apa.org/ethics/code/index.aspx (Accessed 18 May 2018).

[10] D. Ariely, E. Kamenica, and D. Prelec. Man's search for meaning: The case of legos. *Journal of Economic Behavior & Organization*, 67 (3): 671–677, 2008. ISSN 0167-2681. 10.1016/j.jebo.2008.01.004. URL https://www.sciencedirect.com/science/article/pii/S0167268108000127.

[11] I. Ayres, S. Raseman, and A. Shih. Evidence from two large field experiments that peer comparison feedback can reduce residential energy usage. *The Journal of Law, Economics, and Organization*, 29 (5): 992–1022, 2013. 10.1093/jleo/ews020.

[12] R. Balebako, P. G. Leon, H. Almuhimedi, P. G. Kelley, J. Mugan, A. Acquisti, L. F. Cranor, and N. Sadeh. Nudging users towards privacy on mobile devices. In *Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*, pages 193–201. Citeseer, 2011.

[13] N. Beheshtian, S. Moradi, A. Ahtinen, K. Väänanen, K. Kähkonen, and M. Laine. Greenlife: A persuasive social robot to enhance the sustainable behavior in shared living spaces. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society, NordiCHI '20*. Association for Computing Machinery, New York, NY, USA, 2020. ISBN 9781450375795. 10.1145/3419249.3420143.

[14] C. A. Belton and P. D. Lunn. Smart choices? An experimental study of smart meters and time-of-use tariffs in Ireland. *Energy Policy*, 140: 111243, 2020. 10.1016/j.enpol.2020.111243.

[15] J. Bourgeois, J. van der Linden, G. Kortuem, B. A. Price, and C. Rimmer. Conversations with my washing machine: An in-the-wild study of demand shifting with self-generated energy. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp '14*, pages 459–470. Association for Computing Machinery, New York, NY, USA, 2014. ISBN 9781450329682. 10.1145/2632048.2632106.

[16] Bundesministerium für Gesundheit. Informationen zum Coronavirus, 2021. https://www.bundesgesundheitsministerium.de/coronavirus.html (Accessed 23 June 2021).

[17] M. Burgess. Coronavirus contact tracing apps were meant to save us. They won't, 2020. https://www.wired.co.uk/article/contact-tracing-apps-coronavirus (Accessed 23 June 2021).

[18] R. Calo. Code, nudge, or notice? *IOWA LAW REVIEW*, 99 (773): 773–802, 2014.

[19] J. E. Chung, N. Park, H. Wang, J. Fulk, and M. McLaughlin. Age differences in perceptions of online community participation among non-users: An extension of the technology acceptance model. *Computers in Human Behavior*, 26 (6): 1674–1684, 2010. ISSN 0747-5632. 10.1016/j.chb.2010.06.016. URL https://www.sciencedirect.com/science/article/pii/S0747563210001883.

[20] J. Colnago, Y. Feng, T. Palanivel, S. Pearman, M. Ung, A. Acquisti, L. F. Cranor, and N. Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI '20*, pages 1–13. Association for Computing Machinery, New York, NY, USA, 2020. ISBN 9781450367080. 10.1145/3313831.3376389.

[21] E. L. Deci. *Intrinsic Motivation*. Plenum, New York, NY, USA, 1975.

[22] T. Dehling, S. Lins, and A. Sunyaev. Security of critical information infrastructures. In *Information Technology for Peace and Security*, pages 319–339. Springer Fachmedien Wiesbaden, Wiesbaden, 2019. 10.1007/978-3-658-25652-4_15.

[23] J. Delcker. Big Brother in Berlin, 2018. https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/ (Accessed 23 June 2021).

[24] S. Deterding, D. Dixon, R. Khaled, and L. Nacke. From game design elements to gamefulness: Defining "gamification". In

Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, MindTrek '11, pages 9–15. Association for Computing Machinery, New York, NY, USA, 2011. ISBN 9781450308168. 10.1145/2181037.2181040.

[25] Digitalstadt Darmstadt. Ethik- & Technologiebeirat - Unterstützung für die Digitalstadt Darmstadt, 2018. https://www.digitalstadt-darmstadt.de/news/ethik-technologiebeirat/ (Accessed 17 December 2020).

[26] A. Y. Ding, G. L. De Jesus, and M. Janssen. Ethical hacking for boosting IoT vulnerability management: A first look into bug bounty programs and responsible disclosure. In *Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing, ICTRS '19*, pages 49–55. Association for Computing Machinery, New York, NY, USA, 2019. ISBN 9781450376693. 10.1145/3357767.3357774.

[27] S. Döbelt, M. Jung, M. Busch, and M. Tscheligi. Consumers' privacy concerns and implications for a privacy preserving smart grid architecture – results of an Austrian study. *Energy Research & Social Science*, 9: 137–145, 2015. ISSN 2214-6296. 10.1016/j.erss.2015.08.022. URL https://www.sciencedirect.com/science/article/pii/S2214629615300451. Special Issue on Smart Grids and the Social Sciences.

[28] R. Egert, J. Daubert, S. Marsh, and M. Mühlhäuser. Exploring energy grid resilience: The impact of data, prosumer awareness, and action. *Patterns*, 2 (6): 100258, 2021.

[29] European Federation of Psychologists' Association. Meta-code of ethics, 2005. https://www.bdp-verband.de/binaries/content/assets/beruf/efpa_metacode_en.pdf (Accessed 23 June 2021).

[30] A. Eversden. The latest Pentagon bug bounty revealed a critical vulnerability, 2019. https://www.fifthdomain.com/dod/2019/10/14/the-latest-pentagon-bug-bounty-revealed-a-critical-vulnerability/ (Accessed 23 June 2021).

[31] M. J. Fell, D. Shipworth, G. M. Huebner, and C. A. Elwell. Public acceptability of domestic demand-side response in Great Britain: The role of automation and direct load control. *Energy Research & Social Science*, 9: 72–84, 2015. ISSN 2214-6296. 10.1016/j.erss.2015.08.023. URL https://www.sciencedirect.com/science/article/pii/S2214629615300463. Special Issue on Smart Grids and the Social Sciences.

[32] N. Ferris and S. van Renssen. Cybersecurity threats escalate in the energy sector, 2021. https://energymonitor.ai/technology/digitalisation/cybersecurity-threats-escalate-in-the-energy-sector (Accessed 23 June 2021).

[33] G. Fink, D. Best, D. Manz, V. Popovsky, and B. Endicott-Popovsky. Gamification for measuring cyber security situational awareness. In D. Schmorrow and C. Fidopiastis, editors, *Foundations of Augmented Cognition. AC 2013*. Lecture Notes in Computer Science, volume 8027, pages 656–665. Springer, 2013. 10.1007/978-3-642-39454-6_70.

[34] D. Fischer, D. Bonaretti, and K. Fischbach. Effective use of mobile-enabled emergency warning systems. In *Proceedings of the 28th European Conference on Information Systems (ECIS)*, June 2020. URL https://aisel.aisnet.org/ecis2020_rp/130.

[35] D. Florêncio, C. Herley, and P. C. Van Oorschot. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pages 575–590, 2014.

[36] B. Fogg. A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology, Persuasive '09*. Association for Computing Machinery, New York, NY, USA, 2009. ISBN 9781605583761. 10.1145/1541948.1541999.

[37] B. J. Fogg. Persuasive technology: Using computers to change what we think and do. *Ubiquity*, 2002 (December), Dec. 2002. 10.1145/764008.763957.

[38] N. Gerber, V. Zimmermann, B. Henhapl, S. Emeröz, and M. Volkamer. Finally Johnny can encrypt: But does this make him feel more secure? In *Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018*. Association for Computing Machinery, New York, NY, USA, 2018. ISBN 9781450364485. 10.1145/3230833.3230859.

[39] B. Gnauk, L. Dannecker, and M. Hahmann. Leveraging gamification in demand dispatch systems. In *Proceedings of the 2012 Joint EDBT/ICDT workshops*, pages 103–110, 2012.

[40] M. Goulden, B. Bedwell, S. Rennick-Egglestone, T. Rodden, and A. Spence. Smart grids, smart users? The role of the user in demand side management. *Energy Research & Social Science*, 2: 21–29, 2014. 10.1016/j.erss.2014.04.008.

[41] J. Hamari and J. Koivisto. Social motivations to use gamification: an empirical study of gamifying exercise. In *Proceedings of the European Conference on Information Systems (ECIS 2013)*. AIS, 2013. URL https://aisel.aisnet.org/ecis2013_cr/105//.

[42] J. Hamari, J. Koivisto, and H. Sarsa. Does gamification work? – A literature review of empirical studies on gamification. In *2014 47th Hawaii International Conference on System Sciences*, pages 3025–3034. IEEE, 2014.

[43] P. G. Hansen. The definition of nudge and libertarian paternalism: Does the hand fit the glove? *European Journal of Risk Regulation*, 7 (1): 155–174, 2016. 10.1017/S1867299X00005468.

[44] P. G. Hansen and A. M. Jespersen. Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy. *European Journal of Risk Regulation*, 4 (1): 3–28, 2013. 10.1017/S1867299X00002762.

[45] T. Hargreaves, M. Nye, and J. Burgess. Keeping energy visible? exploring how householders interact with feedback from smart energy monitors in the longer term. *Energy Policy*, 52: 126–134, 2013. 10.1016/j.enpol.2012.03.027. URL https://www.sciencedirect.com/science/article/pii/S0301421512002327.

[46] K. Hartwig and C. Reuter. Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behaviour & Information Technology*, 1–24, 2021. ISSN 0144-929X. 10.1080/0144929X.2021.1876167.

[47] M. Hassenzahl. The Thing and I: Understanding the relationship between the user and the product. In M.A. Blythe, K. Overbeeke, A.F. Monk, P.C. Wright, editors, *Funology: From Usability to Enjoyment*, 2003.

[48] O. Heino and A.-V. Anttiroiko. Utility-customer communication: The case of water utilities. *Public Works Management & Policy*, 21 (3): 220–230, 2016. 10.1177/1087724X15606738.

[49] K. Herter. Residential implementation of critical-peak

pricing of electricity. *Energy Policy*, 35 (4): 2121–2130, 2007. 10.1016/j.enpol.2006.06.019. URL https://www.sciencedirect.com/science/article/pii/S0301421506002783.

[50] P. Hines, K. Balasubramaniam, and E. C. Sanchez. Cascading failures in power grids. *IEEE Potentials*, 28 (5): 24–30, 2009. 10.1109/MPOT.2009.933498.

[51] M. Hollick and S. Katzenbeisser. Resilient critical infrastructures. In C. Reuter, editor, *Information Technology for Peace and Security*, pages 305–318. Springer Vieweg, Wiesbaden, 2019. 10.1007/978-3-658-25652-4_14.

[52] E. Hollnagel. *Resilience Engineering in Practice: A Guidebook*. Ashgate Publishing, Ltd., 2010.

[53] D. Johnson, E. Horton, R. Mulcahy, and M. Foth. Gamification and serious games within the domain of domestic energy consumption: A systematic review. *Renewable and Sustainable Energy Reviews*, 73: 249–264, 2017. ISSN 1364-0321. 10.1016/j.rser.2017.01.134. URL https://www.sciencedirect.com/science/article/pii/S1364032117301478.

[54] A. Kashani and Y. Ozturk. Residential energy consumer behavior modification via gamification. In *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)*, pages 1221–1225, 2017. 10.1109/ICRERA.2017.8191247.

[55] M.-A. Kaufhold, J. Haunschild, and C. Reuter. Warning the public: A survey on attitudes, expectations and use of mobile crisis apps in Germany. In *Proceedings of the 28th European Conference on Information Systems (ECIS 2020)*. AIS, 2020. ISBN 978-1-7336325-1-5. URL https://aisel.aisnet.org/ecis2020_rp/84/.

[56] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A “nutrition label” for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS ’09*, pages 1–12. Association for Computing Machinery, New York, NY, USA, 2009. ISBN 9781605587363. 10.1145/1572532.1572538.

[57] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI ’10*, pages 1573–1582. Association for Computing Machinery, New York, NY, USA, 2010. ISBN 9781605589299. 10.1145/1753326.1753561.

[58] O. Korn and A. Schmidt. Gamification of business processes: Re-designing work in production and service industry. *Procedia Manufacturing*, 3: 3424–3431, 2015. 10.1016/j.promfg.2015.07.616.

[59] M. W. Kranenbarg, T. J. Holt, and J. van der Ham. Don’t shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science*, 7 (16): 1–9, 2018. 10.1186/s40163-018-0090-8.

[60] F. M. Kroese, D. R. Marchiori, and D. T. de Ridder. Nudging healthy food choices: A field experiment at the train station. *Journal of Public Health*, 38 (2): e133–e137, 2015. 10.1093/pubmed/fdv096.

[61] C. Laspidou. ICT and stakeholder participation for improved urban water management in the cities of the future. *Water Utility Journal*, 8: 79–85, 2014.

[62] M. R. Lepper and D. Greene. *The Hidden Costs of Reward: New Perspectives on the Psychology of Human Motivation*. Psychology Press, 2015.

[63] G. Luca, P. Fraternali, P. Chiara, B. Giorgia, A. D. D. Santos, A. Roberto, and R. Valentina. A gamification framework for customer engagement and sustainable water usage promotion. In *E-proceedings of the 36th IAHR World Congress*, 2015.

[64] D. MacKay and A. Robinson. The ethics of organ donor registration policies: nudges and respect for autonomy. *The American Journal of Bioethics*, 16 (11): 3–12, 2016. 10.1080/15265161.2016.1222007.

[65] J. Matthews, K. Win, H. Oinas-Kukkonen, and M. Freeman. Persuasive technology in mobile applications promoting physical activity: a systematic review. *Journal of Medical Systems*, 40 (72): 1–13, 2015. 10.1007/s10916-015-0425-x.

[66] L. Michaels and Y. Parag. Motivations and barriers to integrating ‘prosuming’services into the future decentralized electricity grid: Findings from Israel. *Energy Research & Social Science*, 21: 70–83, 2016. 10.1016/j.erss.2016.06.023. URL https://www.sciencedirect.com/science/article/pii/S2214629616301529.

[67] A.-H. Mohsenian-Rad, V. W. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia. Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. *IEEE Transactions on Smart Grid*, 1 (3): 320–331, 2010. 10.1109/TSG.2010.2089069.

[68] L. H. Newman. Department of Defense’s ’Hack the Pentagon’ Bug Bounty Program Helps Fix Thousands of Bugs, 2017. https://www.wired.com/story/hack-the-pentagon-bug-bounty-results/ (Accessed 23 June 2021).

[69] J. Novak, M. Melenhorst, I. Micheel, C. Pasini, P. Fraternali, and A. Rizzoli. Integrating behavioural change and gamified incentive modelling for stimulating water saving. *Environmental Modelling & Software*, 102: 120–137, 2018. ISSN 1364-8152. 10.1016/j.envsoft.2017.11.038. URL https://www.sciencedirect.com/science/article/pii/S1364815216311288.

[70] T. R. Nys and B. Engelen. Judging nudging: Answering the manipulation objection. *Political Studies*, 65 (1): 199–214, 2017. 10.1177/0032321716629487.

[71] J. A. Obar and A. Oeldorf-Hirsch. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23 (1): 128–147, 2020. 10.1080/1369118X.2018.1486870.

[72] I. Onyeji, M. Bazilian, and C. Bronk. Cyber security and critical energy infrastructure. *The Electricity Journal*, 27 (2): 52–60, 2014. ISSN 1040-6190. 10.1016/j.tej.2014.01.011. URL https://www.sciencedirect.com/science/article/pii/S1040619014000268.

[73] Oxford English Dictionary. Oxford English Dictionary – motivation, 2020. https://www.oed.com/view/Entry/122708?redirectedFrom=motivation#eid (Accessed 16 December 2020).

[74] D. Pichert and K. V. Katsikopoulos. Green defaults: Information presentation and pro-environmental behaviour. *Journal of Environmental Psychology*, 28 (1): 63–73, 2008. 10.1016/j.jenvp.2007.09.004. URL https://www.sciencedirect.com/science/article/pii/S0272494407000758.

[75] B. W. Pratt and J. D. Erickson. Defeat the peak: Behavioral insights for electricity demand response program design. *Energy Research & Social Science*, 61: 101352, 2020. ISSN 2214-6296. 10.1016/j.erss.2019.101352. URL https://www.

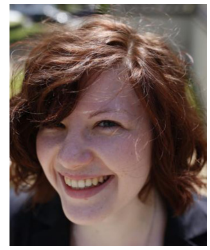
sciencedirect.com/science/article/pii/S2214629619304384.
[76] F. Raja, K. Hawkey, S. Hsu, K.-L. C. Wang, and K. Beznosov. A brick wall, a locked door, and a bandit: A physical security metaphor for firewall warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS '11*, pages 1–20. Association for Computing Machinery, New York, NY, USA, 2011. ISBN 9781450309110. 10.1145/2078827.2078829.
[77] S. Ranchordás. Nudging citizens through technology in smart cities. *International Review of Law, Computers & Technology*, 34 (3): 254–276, 2020. 10.1080/13600869.2019.1590928.
[78] K. Renaud and V. Zimmermann. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy*, 3 (2): 228–258, 2019. 10.1017/bpp.2018.3.
[79] C. Reuter and M. A. Kaufhold. Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics. *Journal of Contingencies and Crisis Management*, 26 (1): 41–57, 2018. ISSN 1468-5973. 10.1111/1468-5973.12196.
[80] C. Reuter, M. Kaufhold, I. Leopold, and H. Knipp. KATWARN, NINA, or FEMA? Multi-method study on distribution, use, and public views on crisis apps. In *Proceedings of the 25th European Conference on Information Systems (ECIS)*, pages 2187–2201, 2017. URL https://aisel.aisnet.org/ecis2017_rp/139.
[81] C. Reuter, J. Haunschild, M. Hollick, M. Mühlhäuser, J. Vogt, and M. Kreutzer. Towards secure urban infrastructures: Cyber security challenges for information and communication technology in smart cities. In *Mensch und Computer 2020 – Workshopband*. Gesellschaft für Informatik e. V., 2020. 10.18420/muc2020-ws117-408.
[82] F. Rheinberg. Intrinsische Motivation. In V. Brandstätter and J. H. Otto, editors, *Handbuch der Allgemeinen Psychologie–Motivation und Emotion*, volume 11, pages 258–265. Hogrefe, Göttingen, 2009.
[83] F. Rheinberg and Y. Manig. Was macht Spaß am Graffiti-Sprayen?: Eine induktive Anreizanalyse. *Report Psychologie*, 28, 2003.
[84] A. E. Rizzoli, A. Castelletti, P. Fraternali, and J. Novak. Demo Abstract: SmartH2O, demonstrating the impact of gamification technologies for saving water. *Computer Science – Research and Development*, 33 (1): 275–276, 2018. 10.1007/s00450-017-0380-5.
[85] N. Romero Herrera, J. Rutten, and D. V. Keyson. Designing ampul: Empowerment to home energy prosumers. In D. V. Keyson, O. Guerra-Santin, and D. Lockton, editors, *Living Labs: Design and Assessment of Sustainable Living*, pages 309–323. Springer International Publishing, Cham, 2017. ISBN 978-3-319-33527-8. 10.1007/978-3-319-33527-8_24.
[86] R. M. Ryan and E. L. Deci. Chapter 2 – when rewards compete with nature: The undermining of intrinsic motivation and self-regulation. In C. Sansone and J. M. Harackiewicz, editors, *Intrinsic and Extrinsic Motivation*, Educational Psychology, pages 13–54. Elsevier, 2000. 10.1016/B978-012619070-0/50024-6. URL https://www.sciencedirect.com/science/article/pii/B9780126190700500246.
[87] C. Schubert. Green nudges: Do they work? Are they ethical? *Ecological Economics*, 132: 329–342, 2017. 10.1016/j.ecolecon.2016.11.009.
[88] P. W. Schultz, J. M. Nolan, R. B. Cialdini, N. J. Goldstein, and V. Griskevicius. The constructive, destructive, and reconstructive power of social norms. *Psychological Science*, 18 (5): 429–434, 2007. 10.1111/j.1467-9280.2007.01917.x.
[89] S. Stieglitz, C. Lattemann, S. Robra-Bissantz, R. Zarnekow, and T. Brockmann. *Gamification*. Springer, 2017.
[90] C.-H. Su and C.-H. Cheng. A mobile gamification learning system for improving the learning motivation and achievements. *Journal of Computer Assisted Learning*, 31 (3): 268–286, 2015. 10.1111/jcal.12088.
[91] C. R. Sunstein. Behavioural economics, consumption and environmental protection. In *Handbook of Research on Sustainable Consumption*. Edward Elgar Publishing, 2015a. 10.2139/ssrn.2296015.
[92] C. R. Sunstein. Nudges do not undermine human agency. *Journal of Consumer Policy*, 38 (3): 207–210, 2015b. 10.1007/s10603-015-9289-1.
[93] C. R. Sunstein and L. A. Reisch. Climate-friendly default rules. *Discussion Paper No. 87809/2016 Harvard Law School Cambridge, MA 02138*, 2016.
[94] C. Takayama, V. Lehdonvirta, M. Shiraishi, Y. Washio, H. Kimura, and T. Nakajima. Ecoisland: A system for persuading users to reduce CO_2 emissions. In *Proceedings of the 2009 Software Technologies for Future Dependable Distributed Systems, STFSSD '09*, pages 59–63. IEEE Computer Society, USA, 2009. ISBN 9780769535722. 10.1109/STFSSD.2009.8.
[95] M. L. Tan, R. Prasanna, K. Stock, E. Hudson-Doyle, G. Leonard, and D. Johnston. Mobile applications in crisis informatics literature: A systematic review. *International Journal of Disaster Risk Reduction*, 24: 297–311, 2017. 10.1016/j.ijdrr.2017.06.009. URL https://www.sciencedirect.com/science/article/pii/S2212420916307130.
[96] M. L. Tan, R. Prasanna, K. Stock, E. E. Doyle, G. Leonard, and D. Johnston. Understanding end-users' perspectives: Towards developing usability guidelines for disaster apps. *Progress in Disaster Science*, 7: 100–118, 2020. ISSN 2590-0617. 10.1016/j.pdisas.2020.100118. URL https://www.sciencedirect.com/science/article/pii/S2590061720300557.
[97] R. H. Thaler and C. R. Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, New Haven, CT, US, 2008.
[98] The British Psychological Society. Code of human research ethics, 2014. https://www.bps.org.uk/news-and-policy/bps-code-human-research-ethics-2nd-edition-2014 (Accessed 18 May 2018).
[99] The European Data Protection Board. Guidelines 05/2020 on consent under regulation 2016/679, 2020.
[100] S. Trang, M. Trenz, W. H. Weiger, M. Tarafdar, and C. M. Cheung. One app to trace them all? examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, 29 (4): 415–428, 2020. 10.1080/0960085X.2020.1784046.
[101] J. Turland, L. Coventry, D. Jeske, P. Briggs, and A. van Moorsel. Nudging towards security: Developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI Conference, British HCI '15*, pages 193–201. Association for Computing Machinery, New York, NY, USA, 2015. 10.1145/2783446.2783588.
[102] I. Van der Meiden, H. Kok, and G. Van der Velde. Nudging physical activity in offices. *Journal of Facilities Management*,

2019. 10.1108/JFM-10-2018-0063.
[103] U. Wethal. Practices, provision and protest: Power outages in rural Norwegian households. *Energy Research & Social Science*, 62: 101388, 2020. ISSN 2214-6296. 10.1016/j.erss.2019.101388. URL https://www.sciencedirect.com/science/article/pii/S2214629619301938.
[104] K. P. Whyte, E. Selinger, A. L. Caplan, and J. Sadowski. Nudge, nudge or shove, shove — the right way for nudges to increase the supply of donated cadaver organs. *The American Journal of Bioethics*, 12 (2): 32–39, 2012. 10.1080/15265161.2011.634484.
[105] M. Zhao and R. John. Building community resilience using gain-loss framing to nudge homeowner mitigation and insurance decision-making. In *Proceedings of the 54th Hawaii International Conference on System Sciences*, page 2206, 2021. 10.24251/HICSS.2021.271.
[106] G. Zichermann and C. Cunningham. *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps*. O'Reilly Media, 2011.
[107] V. Zimmermann and K. Renaud. The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 28 (1): 1–45, 2021. 10.1145/3429888.
[108] M. Zwilling, G. Klien, D. Lesjak, Łukasz Wiechetek, F. Cetin, and H. N. Basim. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1–16, 2020. 10.1080/08874417.2020.1712269.

Bionotes

Rolf Egert
Technical University of Darmstadt, Telekooperation Lab, Darmstadt, Germany
egert@tk.tu-darmstadt.de

Rolf Egert is a Ph.D. student in the area of "Smart Protection in Infrastructures and Networks" (SPIN) at the Telekooperation Lab, Technische Universität Darmstadt under the direction of Prof. Max Mühlhäuser. Since 2020, he coordinates the security research of the Telecooperation Lab as the Area Head of SPIN. His current research interests include IT-security aspects in the domain of smart energy grids, bio-inspired optimization approaches, and resilient complex system infrastructures.



Nina Gerber
Technical University of Darmstadt, Work and Engineering Psychology (FAI), Darmstadt, Germany
n.gerber@psychologie.tu-darmstadt.de

Dr. Nina Gerber is a post-doctoral researcher in the research group "Work and Engineering Psychology" (FAI) at the Department of Psychology at the Technical University of Darmstadt. Her research interests are primarily in the areas of usable privacy & security, human-machine interaction, and human-centred product design. Previously, she was a doctoral researcher at the department of computer science at the Technical University of Darmstadt and at the Institute of Applied Informatics and Formal Description Methods at KIT.

Jasmin Haunschild
Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC), Darmstadt, Germany
haunschild@peasec.tu-darmstadt.de

Jasmin Haunschild has been a researcher and doctoral student at PEASEC since 2019. For her Ph.D. in Computer Science, she investigates the design of technologies in safety and security related settings and their influence on agency-citizen relationships. In the mission SecUrban of the National Research Center for Applied Cybersecurity ATHENE, she applies this to the context of smart city digitalization. Previously, she worked at the Chair of International Relations at TU Braunschweig and Royal Holloway College, University of London.

Philipp Kuehn
Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC), Darmstadt, Germany
kuehn@peasec.tu-darmstadt.de

Philipp Kühn is a researcher and doctoral student at Science and Technology for Peace and Security (PEASEC) in the department of Computer Science of the Technical University of Darmstadt since 2020. He is currently working in the ATHENE Mission Secure Urban Infrastructures and the project CYWARN. His research evolves around the topics of gathering information for the field of information security out of open-source information sources, its preparation, and analysis.

Verena Zimmermann
Technical University of Darmstadt, Work and Engineering Psychology (FAI), Darmstadt, Germany
zimmermann@psychologie.tu-darmstadt.de

Dr. Verena Zimmermann is a post-doctoral researcher in the working group "Work and Engineering Psychology" at the Department of Psychology. Working in different research projects within the National Research Center of Applied Cybersecucity (CRISP) Verena Zimmermann is concerned with Human Factors in Security and Safety. Her research interests include usable authentication and communication, nudging in security and privacy, and user-centered design of smart devices and environments.