Short Abstract

People are cyber-responsibilized by neo-liberal governments; this leaves them vulnerable to attack. De-responsibilization requires a trusting relationship. Uncertainty plays a role, and we explore this.

Long Abstract

Neoliberal governments cyber responsibilize their citizens: giving them a great deal of advice and expecting them to take care of their personal cyber security. While this strategy works well in other domains, it does not seem to be effective in the cyber security domain. Citizens are often unable to embrace their cyber responsibilities for a variety of reasons. As a consequence, many fall victim to cyber-attacks. It might be necessary to de-responsibilize citizens, provide citizens with more support. This requires citizens to be willing to accept their government's de-responsibilization intervention and to be willing to be supported in this way. Here, we consider the factors that would make citizens more or less likely to be willing to be cyber de-responsibilized.

Envisaging the role of Uncertainty in Acceptance of Cyber De-responsibilization

Karen Renaud, University of Strathclyde, UK; Rhodes University, South Africa
Stephen Flowerday, Rhodes University, South Africa
Karl van der Schyff, Rhodes University, South Africa

Introduction

Norbert Elias argues that the ability to take responsibility is part of a “civilizing process”[13]. Neoliberal governments appear to agree with this, because they have "responsibilized" their citizens in many domains[36]. Pellandini-Simányi and Conte explain that the concept of responsibilization refers to: (1) assigning of responsibility to citizens, and (2) the social-cultural factors that persuade citizens to embrace assigned responsibilities[27]. The aim of responsibilization is to "*transform individuals into self-reflexive, self-produced do-it-yourself projects*" (p.60)[12]: independent and self-steering. Trnka and Trundle argue that the aim is to produce "*self-reliant citizens who do not make too many demands on government services*" (p.2)[39]. Citizens, in essence, are required to take responsibility for many aspects of their lives without expecting government support or intervention beyond the provision of advice.

While responsibilization has indeed been effective in some areas, its application has not been universally successful. In some areas, citizens have not been able to embrace the assigned responsibilities. Researchers report on the negative side effects of responsibilization in several domains: prostitution, travel, safety and children's education, with others raising questions about the wisdom of responsibilizing citizens, citing the fact that it does not lead to resilience, but instead leads to anxiety, guilt, and hyper-vigilance, and is onerous and counterproductive[10]. Byrne points out that responsibilization is structurally blind and ignores risk differences, which is why it is not necessarily an effective population-level strategy[11].

Renaud et al. argue that a responsibilization strategy is likely to fail when the domain within which it is applied is characterized by two dimensions: (1) citizens needing skills that are not possessed by the general population, and (2) when a citizen's inability to shoulder their responsibilities will impact on other citizens[31]. Cyber security is a prime example of this. Cyber security skills are relatively rare in the general population, and computer viruses can proliferate across networks, meaning that one person's failure to secure their device is likely to cause harm to other

people's devices and compromise their information. The surge in cyber attacks globally suggests that cyber criminals are exploit the consequences of a failed responsibilization approach in the cyber domain.

Harford points out that Adam Smith attributed economic growth to the division of labour[17]. Today's responsibilized citizen is their own financial manager, their own educational advisor and attempts to secure their own Internet-connected devices. Harford argues that we are all "slow-motion" multitasking and that this interferes with our ability to be productive. Besides responsibilization leading to a situation where we are not as productive as a division of labour would engender, we might not even be very good at all the roles we are expected to embrace. This seems especially true in the cyber security domain, where neo-liberal responsibilizing governments expect everyone to be a cyber expert of sorts.

Renaud et al. argue that governments need to do more to support their citizens in the cyber domain[32]. In essence, they are arguing for a measure of *de-responsibilization* of citizens. Such de-responsibilization has occurred in other domains, such as governments protecting their citizens from slave traders[34], fire-fighting, and prostitution[32]. These areas all demonstrate Renaud et al.'s two dimensions: they require specialist skills, and a failure to deal with the responsibility can lead to calamitous or contagious consequences[31].

However, de-responsibilization requires citizens to accept more support, i.e., they have to trust the government to manage a measure of their cyber security for them. Many government trust models exist in the research literature, but the factors that lead to acceptance of cyber de-responsibilization have not received attention as yet.

What would such cyber de-responsibilization look like? It might mean that governments underwrite one specific antivirus and malware software package or recommend using a particular VPN – removing uncertainty caused by the multiplicity of available products. They might explicitly support citizens who have fallen victim to cyber-attacks rather than their having to rely on the marketplace for this kind of assistance. Finally, they might make "Smartphone clinics" available so that people can take their devices to have them checked out for hidden infections and suboptimal configurations.

All of this can only work if there is a basic level of trust in the government and a willingness to accept de-responsibilization in this space. This is not a given in our modern times, especially post-pandemic. For example, Rayner writes about the use of fear by the UK government during the pandemic[30]. The public's comments on this article make interesting reading, e.g., "*Don't be afraid of the pandemic, but be very afraid of the government response to the pandemic.*" and "*a pusillanimous government prepared to terrify people and pay them to stay at home*". On the 3rd April 2021, someone posted on Twitter as shown in Figure 1. These attitudes are likely to carry over into other domains, such as cyber security. Certainly, they are not conducive to a trusting relationship.

Figure 1: Twitter post 3rd April 2021 (Anonymised)

The research question we sought to answer in this paper was thus: "*What is the role of uncertainty in influencing citizens' willingness to be cyber de-responsibilized, and what factors feed into such uncertainty?*"

Related Research: Responsibilization

Responsibilization has its roots in the neoliberal tradition, seeming to instantiate a commitment to individual freedom[8]. A great deal of research has been published to capture the nature and dimensions of responsibilization[41]. Researchers contemplate the practice of responsibilization, its processes, its dynamic nature and examine how responsibilization works in practice[9].

Some researchers have carried out studies to determine how well citizens can accept the responsibilities assigned to them in different domains. For example, Hildebrandt et al. assess public support for less responsibilization and more support for those who engage in risky sexual behaviours[19]. Hart argues that the responsibilization of criminals who have served their time is inappropriate because a this approach does not provide the level of support they need[18].

The cyber responsibilization of citizens is the domain of interest in this paper. There has not been much attention paid to the consequences of this commonplace responsibilization. Bannelier and Christakis deal with responsibilization at the State level and proposes that States, policymakers and businesses ought to work together to counteract cyber security threats[3]. Renaud et al. analysed the cyber security policies of the Five Eyes countries and reveal evidence that their citizens are indeed cyber responsibilized[32]. They argue that this is an unwise strategy. Renaud et al. point out that due to the nature of cyber security and the skills required to apply the needed precautions, citizens need more government support[31]. Strawser and Joy also ask whether it is reasonable to assume that the average citizen will have the skills to embrace their cyber responsibilities[37].

Gray also makes the point that responsibilization affects people differently, especially when power issues are not acknowledged[14]. Ekendahl et al. explain that responsibilization often myopically focuses on a person's behaviours instead of considering *why* people behave in a particular way[12]. As such, it is a particularly naïve strategy. This seems to apply to the cyber domain too, given that people's insecure cyber-related behaviours, or lack of precautionary behaviours, are likely to be symptoms of other issues which will not be solved by bombarding people with information and leaving them to get on with it.

Trnka and Trundle argue that the assumption that people will respond to responsibilization moves by meekly embracing and accepting such responsibilities is naïve[38]. People can respond by deliberately carrying out irresponsible acts, and many find the imposition of responsibility to be burdensome. They argue that the responsibilization discourse often focuses on self-sufficiency, but does not consider the individual's obligations to those in their social circles and accountabilities to others. That being so, much of the responsibilization discourse is naïve. It builds on an assumption of an autonomous capable citizen is unrealistic because it does not account for "*the nuances of multiple responsibilities*" (p. 3). In particular, by focusing so myopically on individual responsibility for self-care, it neglects citizens' social care responsibilities. There is much evidence that responsibilization often fails[31]. Rose and Lentzos argue that "*projects for inculcating responsibility divide subjects into actual citizens, potential citizens, failed citizens, or anticitizens on the basis of their presumed or demonstrated capacity—or lack of capacity—to exercise responsibility; or their willful refusal of the demands to be- come responsible*" (p.28)[35]. Given that some citizens live in a responsibilized world, where the imposition of such responsibility is unrealistic, we have to find a way to de-responsibilize them because responsibilization is clearly not working.

When those who have been assigned a particular responsibility are not capable of handling it, other institutions will step in to fill the gap. Given that the average citizen, who is currently responsibilized when it comes to cyber security[32], probably does not have sufficient capability, this might well happen. Those stepping in naturally charge for their services, and it is likely that many of those who need support and assistance the most will not receive it unless it is provided by volunteers[20]. In general, leaving citizens at the mercy of profit-seeking organizations tends not to work well in high-risk areas. Population levels of capability is a critical aspect in triggering de-responsibilization initiatives[27]. Even experts disagree about the most important precautions that the average computer user ought to implement[21], which points to the elusiveness of cyber skills. Widespread cyber responsibilization of the average citizen needs to be re-considered[32].

De-Responsibilization

Pellandini-Simányi and Conte (2020) explain that "*de-responsibilization operates through a top-down, sovereign form of governance. It does not replace, yet constrains the fields of neoliberal governmentality and responsibilization, constituting a hybrid governance system of 'controlled freedom'*" (p.1)[27]. Hence, it requires collaboration between government and citizen[27]. In some cases, it is latterly acknowledged that disasters have occurred because responsibilities have been assigned to those who should not have to handle them. Pellandini-Simányi and Conte explain that after the widespread slump of 2008, the over borrowing was blamed on Hungarian banks' unethical behaviours rather than on people not embracing their responsibilities like good citizens[27].

Some researchers consider how de-responsibilization could be achieved[27], but the cyber domain is not directly addressed. As a starting point, we need first to consider the relationship between the government and the responsibilized citizen.

Prior finds that responsibilization sometimes implies monitoring of responsibilized citizens to ensure that they are embracing their responsibilities[29]. This is not done in order to intervene and assist, but rather to make judgements about how well they are doing what they are supposed to do. Phoenix and Kelly, studying responsibilization in the same domain, say that responsibilization is an effort to transform 'young offenders' into self-governing 'young citizens' (p. 421)[28]. Ekendahl et al. argue that responsibilization might well create a situation where the person's rights are conditioned based on how well they behave[12]. Prior concludes that responsibilized citizens may lose trust in those who are responsibilizing them[29]. There is evidence of prevailing low trust in government[25]. Any mistrust, whatever the source, is likely to influence attitudes towards accepting de-responsibilization-related offers of support, given that **reputation** is so crucial in encouraging trust. In particular, reputation and experience in interacting with an entity increase the **predictability** of their behaviours[1].

Gudykunst emphasized that an ability to verify another party's behaviour alleviates anxiety and vulnerability brought about by high uncertainty[16]. This line of reasoning is based on the argument that if the parties lack confidence in their ability to predict the other's behaviour, feelings of vulnerability will exist. This suggests that uncertainty can only be **reduced by information shared**, also that knowledge as to the condition of this information will affect the (un)certainty level. To tie this in with predictability, Kellermann and Reynolds conducted a series of experiments on uncertainty provoking situations and found that when the target's behaviour became more deviant (i.e. increasing unpredictability), the level of uncertainty increased[22].

Grimmelikhuijsen and Knies explain that if two conditions are present in a particular situation, **trust** becomes particularly relevant to a relationship, and both apply to the cyber domain[15]:

(1) *Risk*: in cyber, this comes from two sources: the first is that governments exert power over citizens, and this can be abused; the second source of risk comes from the activities of cyber criminals targeting citizens.
(2) *Interdependence*: Grimmelikhuijsen and Knies point out that in the allocation of responsibilities to either citizens and government, they are particularly interdependent[15]. Governments rely on citizens to implement cyber precautions and report cyber attacks. Governments, on the other hand, need to pursue, apprehend and prosecute cyber criminals, and ensure that the services they offer online are secured so that citizen data is not leaked[32].

The notion of trust, according to Mayer et al., is that it is the willingness of a trustee (the recipient of trust or the party to be trusted) to perform a particular function important to the trustor (the party that trusts the target party)[24]. Establishing trust is thus likely to be central to the de-responsibilization discourse because it will introduce a measure of interdependence into the relationship between the citizen and the government in a risk-laden context. In particular, de-responsibilization in the cyber domain would require citizens to be willing to trust the government to manage their cyber security *for them* to a certain extent. Torkzadeh and Dhillon argue for the importance of reducing uncertainty in establishing trust[38].

Grimmelikhuijsen and Knies explain that trust can be measured on three dimensions: **benevolence**, **integrity** and **competence**, and this provides us with the three factors that will also influence trust in government in terms of de-responsibilization[15]. When the relationship is a new one, as suggested by a new de-responsibilization endeavour, attention should be paid to building trust.

Trust requires the reduction of **uncertainty** over time[26]. It is important for citizens to know where responsibilities lie. León discovered that citizens find it difficult to attribute responsibility correctly when these have been distributed and devolved to different levels of government[23]. If people don't know who has the responsibility for something, or do not know how to fulfil their own responsibilities, they are likely to experience uncertainty, and probably reduced trust in government.

It is thus helpful to understand the factors that reduce uncertainty and, by implication, build trust. Berger and Calabrese propose a theory that focuses on the potential influence of uncertainty during the beginning of a trusting relationship[7]. According to Berger and Clabrese's definition (p.41) uncertainty about the other party is an "*(in)ability to predict and explain actions*". Even though their study dealt with individuals and their behaviours, the principles are relevant to the cyber de-responsibilization of citizens. In particular, existing trust in government, based on their previous performance in other domains, is likely to carry over when new trust needs to be established[6].

There is some evidence that the modern 21st century citizen generally suffers from uncertainty, even without the cyber dimension being considered. This is perhaps due to being responsibilized: they are left to take care of themselves, which essentially means that being responsibilized denies them the information to allow them to construct expectations and certainty about how de-responsibilization in this domain might work for them. Uncertainty might also be caused by changes in society that have occurred over the last few decades[2]. Eminent authors characterize the changes in society in different ways. Sociologist Bauman argues that modern society is essentially a shift from a previously solid state to a new liquid state[4]. This state-imposed individualism has created existential fear. Bauman and Haugard argue that in this new society people are dominated by uncertainty and insecurity[5]. Bauman explains that the neoliberal state (i.e., the state that creates the responsibilized citizen) has shifted responsibilities onto individual shoulders[4]. In doing so, he argues that they cultivate insecurities and uncertainties. Another writer who has written about how society has changed is criminologist Young, who writes about the "Exclusive Society"[40]. In particular, he explains that the "new" society is infused with risk and uncertainty. Young explains that while difference can be tolerated, because differences can be ironed out as people learn to comply with societal norms, *difficulties* are not accepted. He argues that those who experience difficulties are generally targeted by education and if that fails, rejected and excluded. Hence responsibilized citizens are likely to experience varying levels of uncertainty, depending on the difficulties they experience in coping with different facets of their lives.

Cyber security skills are rare, and those with these skills are highly sought after. The uncertainties that Bauman and Young refer to are likely to be experienced by many who have difficulties in coping with cyber security. This is especially so when the responsibility for cyber security is placed on an individual's shoulders with little accompanying support, especially if they don't have the requisite skills to manage their devices and information securely[31]. The responsibilized citizen who is unable to embrace that responsibility, for whatever reason, risks being blamed if things go wrong[14]. This is particularly true in cyber security[33].

Some people do not trust **technology**, and are uncomfortable with it. This might prevent meaningful collaboration between citizen and government in technology-related domains, such as cyber security.

At the core of responsibilization is the idea that people are **capable** of taking the responsibility and carrying out the required actions or that they can be made capable by providing sufficient information. The previous discussion highlights the difficulties some people experience: i.e., many people are unlikely to have the required abilities to secure their own information and devices and to repel cyber-attacks. If these citizens are given responsibility without having the required capabilities, they are likely to experience uncertainty. This might well influence their response to any de-responsibilization initiatives.

Model and Discussion

Figure 2 extends Berger and Calabrese's *Uncertainty Reduction Theory* based on the factors identified in the previous section i.e., those that are likely to influence citizens' willingness to be cyber de-responsibilized[7].

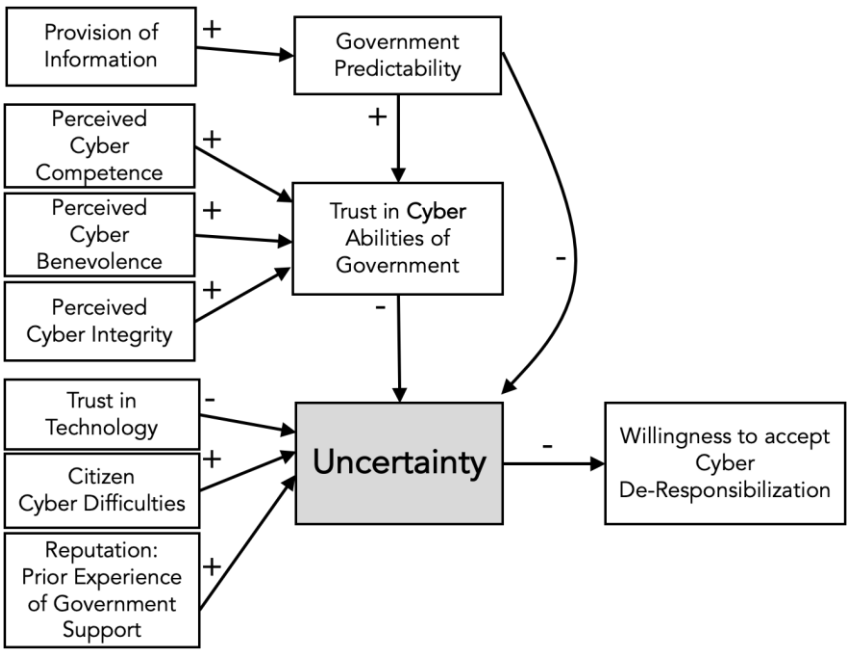

Figure 2: Applying Berger and Calabrese to the cyber domain[7]

Future Research

We plan to carry out an investigation to validate the model proposed in Figure 2, so that we can answer the question stated in the Introduction: "*What is the role of uncertainty in influencing citizens' willingness to be cyber de-responsibilized, and what factors feed into such uncertainty?*"

Conclusion

With neoliberalism firmly on the global agenda, it is not surprising that citizens struggle to keep up with the increasing responsibilities that the 21st century brings. This includes cyber security complexities, which require specialist skills that are clearly beyond the average persons' capabilities. As governments grapple with the changes they face, they have intentionally or unintentionally responsibilized their citizens regarding cyber security. Simultaneously, many citizens do not trust their governments, with uncertainty characterising and colouring the relationship. Our thesis on this ever-growing cyber security problem is for governments to build trust with their citizens and de-responsibilize them concerning the cyber security domain. Due to the sensitivity of the domain, we cannot see cyber security de-responsibilization taking place without increased trust between citizens and their governments, which can only flow if uncertainty is reduced.

About the Authors

Karen Renaud is a Scottish computing Scientist at the University of Strathclyde in Glasgow, working on all aspects of Human-Centred Security and Privacy. Her research been funded by the Association of Commonwealth Universities, the Royal Society, the Royal Academy of Engineers and the Fulbright Commission. She is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. Her research approach is multi-disciplinary, essentially learning from other, more established, fields and harnessing methods and techniques from other disciplines to understand and influence cyber security behaviours.

Stephen Flowerday is a Professor in the Department of Information Systems at Rhodes University. He is also the Head of Department. He holds a BSc and an MBA, as well as a doctoral degree (IT). His research interests lie in the field of cybersecurity, behavioural information security, and information security management. Over the last sixteen years, he has authored and co-authored in excess of 120 refereed publications.

Karl van der Schyff holds a BSc, MSc and PhD degree. His field of interest lies in behavioral information security, information privacy, Cyberpsychology, and PLS path modeling. He has authored and co-authored several refereed publications in addition to reviewing publications within the senior scholars' basket of IS journals, such as the Journal of the Association for Information Systems (JAIS).

References

1. H. Afzal, M. A. Khan, K. ur Rehman, I. Ali & S. Wajahat. Consumer's trust in the brand: Can it be built through brand reputation, brand competence and brand predictability. *International Business Research*, 3(1):43-51, 2010
2. A. Angriawan & R. A. Thakur. parsimonious model of the antecedents and consequence of online trust: An uncertainty perspective. *Journal of Internet Commerce*, 7(1), 74-94, 2008.
3. K. Bannelier and T. Christakis. *Cyber-attacks – prevention-reactions: The role of states and private actors*, 2017. Les Cahiers de la Revue Défense Nationale, Paris https://ssrn.com/abstract=2941988.
4. Z. Bauman. *Liquid Times*: *Living in an Age of Uncertainty*, Cambridge, UK: Polity, 2007.
5. Z. Bauman & M. Haugaard (2008) Liquid modernity and power: A dialogue with Zygmunt Bauman, *Journal of Power*, 1(2):111-130, DOI: 10.1080/17540290802227536
6. A. Beldad, T. van der Geest, M. de Jong & M. Steehouder. A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government Information Quarterly*, 29(1): 41-49. 2012.

7. R. Berger & R. J. Calabrese. Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research*, 1(2): 99-112. 1974.
8. T. Biebricher. & E. V. Johnson. What's wrong with neoliberalism? *New Political Science*, 34(2): 202-211, 2012.
9. R. Birk. Making responsible residents: On 'responsibilization' within local community work in marginalized residential areas in Denmark. *Sociological Review*, 66(3):608–622, 2018.
10. B. Brown. Responsibilization and recovery: shifting responsibilities on the journey through mental health care to social engagement. *Social Theory and Health*, 19: 92–109, 2021.
11. K. Byrne. *A partnership's capacity for community impact understood through neoliberal technologies of risk and responsibilization: A look at Worcester Massachusetts' Senator Charles E. Shannon Jr. community safety initiative partnership*. Master's thesis, International Development, Community and Environment, Clark University, 2016.
12. M. Ekendahl, J. Månsson, and P. Karlsson. Risk and responsibilization: resistance and compliance in Swedish treatment for youth cannabis use. *Drugs: Education, Prevention and Policy*, 27(1):60–68, 2019.
13. N. Elias. *The History of Manners: The Civilizing Process*, vol. 1. New York: Pantheon. 1978
14. G. C. Gray. The responsibilization strategy of health and safety: Neo-liberalism and the reconfiguration of individual responsibility for risk. *The British Journal of Criminology*, 49(3): 326-342, 2009.
15. S. Grimmelikhuijsen and E. Knies. "Validating a scale for citizen trust in government organizations." *International Review of Administrative Sciences,* 83(3): 583-601, 2017.
16. W.B. Gudykunst. A model of uncertainty reduction in intercultural encounters. *Journal of Language and Social Psychology*, 4(2):79-98, 1985.
17. T. Harford. *Technology has turned back the clock on productivity*. Retrieved 10 April 2021 from: https://timharford.com/2021/04/technology-has-turned-back-the-clock-on-productivity/. 2021.
18. E. L. Hart. Women prisoners and the drive for desistance: capital and responsibilization as a barrier to change. *Women & Criminal Justice*. May 27;27(3):151-69, 2017.
19. T. Hildebrandt, L. Bode, and J. Ng. Responsibilization and sexual stigma under austerity: surveying public support for government-funded PrEP in England. *Sexuality Research and Social Policy*, 17: **64**3–653, 2020.
20. S. Ilcan & T. Basok. Community government: Voluntary agencies, social justice, and the responsibilization of citizens. *Citizenship Studies*, 8(2): 129-144, 2004.
21. I. Ion, R. Reeder, and S. Consolvo. "… No one can hack my mind": Comparing Expert and Non-Expert Security Practices." In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, pp. 327-346. 2015.
22. K. Kellermann and R. Reynolds. When ignorance is bliss: The role of motivation to reduce uncertainty in uncertainty reduction theory. *Human Communication Research*, 17(1): 5-75, 1990
23. S. León. How do citizens attribute responsibility in multilevel states? Learning, biases and asymmetric federalism. Evidence from Spain. *Electoral Studies*, 31(1): 120–130, 2012. https://doi.org/10.1016/j. electstud.2011.09.003.
24. R. C. Mayer, J. H. Davis & F. D. Schoorman. An integrative model of organizational trust. *Academy of Management Review*, 20(3): 709-734, 19**95**.
25. OECD. *Trust in Government*. Retrieved 28 March 2021 from: https://www.oecd.org/gov/trust-in-government.htm. 2019
26. W. B. Pearce. Trust in interpersonal communication. *Speech Monographs*. 41(3): 236-244, 1974.
27. L. Pellandini-Simányi & L. Conte. Consumer de-responsibilization: changing notions of consumer subjects and market moralities after the 2008–9 financial crisis. *Consumption Markets & Culture,* pp. 1-26. 2020.
28. J. Phoenix and L. Kelly. 'You have to do it for yourself': Responsibilization in youth justice and young people's situated knowledge of youth justice practice. *British Journal of Criminology*, 53(3): 419–437, 2013.
29. F. Prior. Security Culture: Surveillance and Responsibilization in a Prisoner Reentry Organization. *Journal of Contemporary Ethnography*, 49(3): 390–413, 2020.
30. G. Rayner. State of fear: how ministers 'used covert tactics' to keep scared public at home. Retrieved 3 April 2021 from: https://www.telegraph.co.uk/news/2021/04/02/state-fear-ministers-used-covert-tactics-keep-scared-public/. 2021.
31. K. Renaud, S. Flowerday, M. Warkentin, P. Cockshott, and C. Orgeron. Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious? *Computers & Security*, 78: 198–211, 2018.
32. K. Renaud, C. Orgeron, M. Warkentin, and P. E. French. Cyber security responsibilization: An evaluation of the intervention approaches adopted by the five eyes countries and China. *Public Administration Review*, 80(4): 577–589, 2020.
33. K. Renaud, A. Musarurwa & V. Zimmermann. Contemplating blame in cybersecurity. Proceedings of the 16th International Conference on Cyber Warfare and Security (ICCWS) (pp. 309-317), 2021.
34. N. A Rodger. The safeguard of the sea: a naval history of Britain. 660-1649. Penguin: UK. 2004.
35. N. Rose and F. Lentzos. Making Us Resilient: Responsible Citizens for Uncertain Times. In: S. Trnka and C. Trundle. eds. *Competing responsibilities: the ethics and politics of contemporary life.* (pp. 27-*48*), Duke University Press. 2017.
36. M. Siltaoja, V. Malin and M. Pyykkönen. 'We are all responsible now': Governmentality and responsibilized subjects in corporate social responsibility. *Management Learning*, 46(4), pp.444-460. 2015.
37. J. Strawser and D. J. Joy. Cyber security and user responsibility: Surprising normative differences. *Procedia Manufacturing*, 3:1101–1108, 2015. https://doi.org/10.1016/j.promfg.2015.07.183.
38. G. Torkzadeh & G. Dhillon. Measuring factors that influence the success of Internet commerce. *Information Systems Research*, 13(2): 187-204, 2002.
39. S. Trnka and C. Trundle. Reckoning Personal Responsibility, Care for the Other, and the Social Contract in Contemporary Life. In: S. Trnka and C. Trundle. eds. *Competing responsibilities: the ethics and politics of contemporary life.* (pp. 1-26), Duke University Press. 2017.

40. J. Young. *The Exclusive Society*. SAGE: London. 1999.
41. M. Zajko, Mike. "Telecom Responsibilization: Internet Governance, Surveillance, and New Roles for Intermediaries." *Canadian Journal of Communication* 41(1):75-93. 2016.