Strategies for Combating Adversarial Information Operations: Theory and Practical Applications

Alberto Federico Olivieri and Rosanna E. Guadagno
University of Oulu, Finland

Alberto.Olivieri@oulu.fi
Rosanna.Guadagno@oulu.fi
https://orcid.org/0000-0001-7223-3522
https://orcid.org/0000-0001-8247-5154

Abstract: In the contemporary information landscape, the proliferation of disinformation and propaganda poses a significant challenge to societal discourse and democratic processes. This paper proposes a multi-disciplinary approach to combatting adversarial information operations, drawing upon theoretical frameworks and practical applications. Theoretical foundations are established through an examination of the Persuasive System Design (PSD) model (Oinas-Kukkonen, 2013) and its parallels with propaganda tactics. By analyzing the shared flaws and vulnerabilities, insights emerge into the manipulation techniques employed by threat actors in online information spaces. Building upon this theoretical framework, the paper presents a proactive strategy for countering disinformation: the development of Early Warning and Control Systems (EWACS). These systems leverage AI-assisted narrative discovery to monitor the digital information landscape continuously. By identifying emerging threats and inauthentic activity, strategic communicators gain valuable insights for crafting counter-narratives and pre-emptive communication strategies. Key components of the proposed approach include deterrence by denial and resilience-building measures. By shifting the cost-gain calculation of adversaries and enhancing societal resilience, the aim is to create an environment where propagandists face increased challenges in achieving their objectives. This paper emphasizes the importance of collaboration between diverse stakeholders, including governmental organizations, academia, NGOs, and journalists. By harnessing the collective expertise from multiple fields, more effective strategies can be developed to safeguard information integrity and restore public trust. In conclusion, this paper advocates for a convergence of theory and practice in addressing the complex challenges posed by adversarial information operations. By integrating theoretical insights with practical applications, the proposed approach offers a holistic framework for countering disinformation and propaganda in contemporary information environments.

Keywords: Disinformation, Propaganda, Persuasive System Design (PSD), Early Warning and Control Systems (EWACS), Information Operations (IO), Resilience Building

1. Introduction

This work will explore how threat actors utilize online disinformation tactics that inadvertently adhere to principles found in the PSD (Persuasive System Design) model (Oinas-Kukkonen, 2013), and then it will focus on actionable intervention that can be implemented to improve resilience in the targeted population. The principles of the PSD model can be used to constructively influence behavior, but the focus here will be on the misapplication of the model and its key issues. The Information Operations (IO) conducted on social networks by threat actors share the same advantages, but also weaknesses, of the model, even though the model itself is not deliberately applied.

Building on this foundational analysis, this paper aims to glean insights from the study of the PSD model that will strengthen our understanding of how we can effectively curb online propaganda. This path will shed light on the importance of an Early Warning and Control System (EWACS) for the Information Space. Viewing the model from this novel perspective reveals that the correct direction in conducting anti-propaganda measures should be based on both social and technological strategies. We need to improve in multiple areas: firstly, by improving our monitoring capabilities in the information landscape to intercept viral trends and narratives at early stages before their full potential can be unleashed, thus allowing the deployment of more effective seeding strategies. Secondly, by developing better crisis communication strategies, and communication risk assessments, to create a stronger and more robust information environment. Lastly, by enhancing interactions and information sharing between governmental organizations, universities, NGOs, and journalists to restore their damaged reputation (from relentless propaganda attacks, and own errors) in the eyes of the wider public, as to build resilience through stronger media literacy and utilizing the social proof effect.

These suggestions are not new (Pamment and Palmertz, 2023), but we argue that the emergence of a natural convergence in multiple academic fields suggesting the same approaches should be seen as a strong indicator of their potential to achieve positive effects in building resilience if these strategies are implemented in our societies.

This paper is divided into four sections; in the first one we will define what Propaganda, Disinformation, and Misinformation are. Multiple disciplines have slightly different definitions and to avoid confusion it is fundamental to create an initial concordance in terminology. The second section will focus more on the key components of the PSD model, and how we can see those principles mirrored into IOs, with a focus on the weaknesses that the parallel drawn by the PSD will uncover. The last section will discuss the need for a robust EWACS for the Information Space is needed, and the presence of a natural convergence from multiple fields will be highlighted.

2. Definitions: Propaganda, Disinformation, Misinformation, Information Operation, and Information Warfare

Propaganda Operations, or alternatively known as Information Operations (IO), are not necessarily done with malign intent. The definition of "propaganda" as a neutral action has been proposed by Jowett and O'Donnell (Jowett and O'donnell, 2018). In their work propaganda is defined as "The deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist (p. 6)". This definition creates a picture of something not necessarily negative, as it can describe social awareness campaigns, made with the intent of public benefit such as reducing the abuse of alcohol. Of course, Propaganda is not only used for benign purposes, but it can be leveraged with nefarious intents, covertly, and using falsehoods and deception. Thus, propaganda is divided into three main categories, using as a labelling principle the openness of the original source, and the trustworthiness of the information. The three types of Propaganda are White, Grey, and Black (Ivan, Chiru and Arcos, 2023). White Propaganda occurs when both the source of the information is known, and the information strives to achieve accuracy (Jowett and O'donnell, 2018). An example is the aforementioned campaign against the abuse of alcohol. Black propaganda happens when the source is unknown, or when a façade obscures the real source. In this case, the information is untrue, fabricated or presented as to spread disinformation (Jowett and O'donnell, 2018). A well-known example is Operation Denver (Kramer and Savage, 2020), the disinformation campaign regarding AIDS in Africa. This disinformation campaign was conducted by the Soviet Union during the Cold War, falsely attributing the origin of the AIDS virus to US military experiments. Lastly, Grey propaganda is a mix between the two, where the source could be correctly identifiable, and the information quality is uncertain (Jowett and O'donnell, 2018). Current narratives coming from both the Russian and the Ukrainian sides regarding the situation on the Ukrainian war frontlines can fall under this category.

The utilization of propaganda is not new but has evolved through the ages along human communication. The Epic of Gilgamesh, one of the earliest pieces of literature, illustrates early uses of propaganda to influence societal views on governance and spirituality. After the First World War, the term came to be perceived as more and more negative, and it quickly reached the connotation that nowadays is common (Jowett and O'donnell, 2018). Propaganda theory and propaganda tactics were refined during the cold war era, where the current Russian model find its roots (Hosaka, 2023). This approach, known as "active measures" (активные мероприятия), was born before internet and social media where available, but its principles and methodologies where enhanced, not diminished, by these new technologies (Randolph, Labriny and DiOrio, 2023).

With the advent of social media, the dynamics of propaganda have transformed dramatically. These platforms have facilitated not only the maintenance and creation of relationships but also the spread of propaganda through new forms of communication. As propaganda and communication are inextricably linked, the social media platforms gave threat actors new vectors to spread fake news and disinformation through targeted advertisement (Guadagno and Guttieri, 2021). This technology has multiple advantages for threat actors, such as deniability, ease of deployment, reduced costs, and is not restricted by national borders. These are some of the advantages of using the internet, and social media in particular, as a new vector of IO.

This growing environment is ripe for bad actors to implement inexpensive but widespread IOs. In the Russian's approach, single IOs are often parts of a bigger Information War (IW) effort, targeted at both the leadership and at the population of adversarial countries (Lilly, 2022). This IOs are conducted in what is called by the Russian leadership the Information Space, and it is similar but not equal to the western Cyber Space. In this paper we will continue to use the term Information, instead of Cyber, as it more aptly describes the adversarial vision of their operations, where technical and psychological dimensions coexist and enhance each other as the two main components of IW (Lilly, 2022). It is also worth noting how Russian doctrine have a more nuanced and varied definition of what is considered warfare. While a black and white approach is more common in the western circles, where the concept of warfare is often relegated to only describing kinetic military action, the USSR, and

now Russia, have enhanced their warfare toolkit with non-military and non-kinetic tools (Lilly, 2022). This different vision of what constitute warfare creates the current situation where Russian is, from their doctrinal point of view, conducting a form of warfare against its adversaries, mainly western countries, while these countries still struggle to answer to this threat properly and adequately, or even acknowledging it as such.

In attacks directed to the leadership and to the population of an adversarial country, the psychological approach of IOs relies often on the use of disinformation. Disinformation is, at its core, a type of information, but it also possesses two more attributes, it is misleading, and it was purposefully created to be so. It is misleading and not necessarily false, as it does not need to be, as the intent is to disrupt the information space. The IOs are often based on a central "rational core", that is then misrepresented (Pasquetto et al., 2022), to push the audience to reach the propagandist conclusions, or at least to make them doubt other sources of information, leading to inaction. The intentionality of disinformation combined with its misleading nature sets disinformation apart from other kinds of information. For example, misinformation retains the misleading nature of disinformation, but lacks the intentionality to create it. Disinformation can manifest in various forms, such as deceptive advertising, government propaganda, doctored photographs, forged documents, fake maps, internet frauds, fake websites, manipulated Wikipedia entries, fake online engagement, and more (Fallis, 2015).

Considering the change that happened over time in the popular perception of propaganda, now equated in the minds of many to IW, and the widespread use of disinformation in the IO as we just described, there is no surprise that new definitions that blur the line between the two have appeared. The NATO STRATCOM CoE had recently published its definition of propaganda: "The essence of propaganda is therefore not to tell one lie, but an embellished web of truths and lies towards constructing a new 'alternative truth'". The author also emphasizes the co-production dimension of propaganda, she argues how individual needs of self-identity and self-validation are exploited by the propagandist to create with the recipient a narrative of mixed lies and truths supporting a shared fantasy (Fry, 2022). This definition is coherent and consistent with what is now perceived by the public, and it has a function of its own in differentiating Black and Grey Propaganda activities from the White Propaganda that many nations rightfully and openly deploy. The definition accurately describes what the Russian leadership calls Information Warfare, but it could lead to confusion and misunderstanding with what is considered Propaganda in other academic fields. This is a cautionary example of how much the terminology could be somewhat difficult to navigate through and it can change between authors, fields, or time. While writing about this subject, brief descriptions of what definitions are being used by the authors throughout the paper would greatly improve readability.

3. The PSD Model Key Issues and Its Misapplication in Information Operations

In the papers describing the PSD model a strong emphasis is placed on how information technology inherently influences user attitudes and behaviors (Oinas-Kukkonen, 2013). The PSD model was developed to embed effective strategies into interactive technologies that have the potential to change the users' attitudes or behaviors through persuasive features and psychological tactics. The influence can be particularly evident in platforms that implement some level of constraint on the form or the length of the user expression, thus forcing them to adapt the kind and scope of their messaging. A simple example is X (the platform formerly known as Twitter), where the limited number of characters, and the branching in separate sub threads of a discussion, influence the form of expression and communication patterns. The peculiar arrangement of X somehow limits long and complex interactions, and they cannot be easily followed by other users. The limitations of certain platforms and how they can be optimally utilized, and what kind of platform is more suited for a specific use, are characteristics that are also taken into consideration by threat actors. They maximize reach and potential network growth and retention through this deep understanding of the social network tools at hand. An example of this is the social media platform Telegram. The platform is well known to function as a backup messaging board for various agents of influence. They take advantage of the lack of any sort of moderation, in order to keep their ability to communicate and organize when facing bans, thus retaining their user base. This was documented during the Facebook ban wave of the 2020 presidential election, which heavily hit Italian QAnon groups. Those groups were able to mitigate the hit of the bans with minimal loss of followers, as the influence actors managing those groups had already laid down their own cross-platform network. Through their telegram channel the actors where able to push the majority of their userbase back into their newly made Facebook groups (Pasquetto et al., 2022).

Another key issue emerging from the PSD model is directly derived from the principles of commitment and cognitive consistency (Cialdini, Petty and Cacioppo, 1981). These principles can be summarized with the understanding that people, in general, tend to change their attitude and behaviors, to avoid cognitive

dissonance. This human tendency can be easily exploited by threat actors, as it was by Chinese guards during the Korean war. In stark contrast with WWII, where Prisoners of War (POWs) collaboration with the enemy was effectively absent, nearly all the US servicemen captured during the Korean war helped their captors. This was done by making the POWs initially commit to small, and seemingly innocuous statements against the US or favorable to the communist governments in exchange for small improvements to their lives as POWs. Then the requests for collaboration ramped up in scope and commitment, with the POWs finding more and more difficult to break out of the cycle. The more they collaborated, the more collaboration the Chinese obtained from them. To be consistent with themselves and their actions, they were, little by little, drawn into committing more and more on the idea of collaboration, and eventually, becoming too committed to refuse actual acts of collaboration (Cialdini, 2009).

The third key issue of the PSD model postulate concerns what persuasive strategies are used by the persuader: direct or indirect routes for persuasion are both viable. Nevertheless, in the article it is stressed how "in the era of information overflow, people are often forced to use indirect cues more often than before, because of the abundance of information to be handled. When an individual sees relevant cues, heuristics are triggered. These may also be called cognitive shorthands, shortcuts, or rules of thumb." (Oinas-Kukkonen and Harjumaa, 2018). This consideration is deeply ingrained in Russian's IW tactics as we previously discussed (Pasquetto et al., 2022). The threat actors often build upon a central kernel of truth that everybody knows or agrees on, at an instinctual level, to then twist this "rational core" with the aim to push the target audience towards their desired outcome.

The Fourth postulate defines how the persuasion is not immediate. The process is often slow and incremental (Oinas-Kukkonen and Harjumaa, 2018). A good example of how an incremental process of persuasion can be implemented over time was already described. The process of "becoming" a collaborator that Chinese guards subjected the US POWs described previously (Cialdini, 2009), perfectly fit this postulate.

The last three postulates of the PSD model: Openness, Unobtrusiveness, and Usefulness & Ease of Use (Oinas-Kukkonen and Harjumaa, 2018), are absent in the most common forms of IOs on social media platforms. It can be argued that some of these postulates can still be valid in other contexts. As an example of employment of the Usefulness & Ease of Use is a website developed with the intent of providing a news aggregator, with integrated translations from English to Italian, of English QAnon material to Italian QAnon members (Pasquetto et al., 2022). This was extremely useful as Italy English literacy is one of the lowest in Europe, especially in older generations, the most likely to be the core audience of the QAnon groups.

This short examination of the key issues of the PSD model suggests that threat actors are aware of the key actions and procedures they can perform to influence behaviors and attitudes. Their actions and processes now are again charted on a better known and studied terrain. This reliance on already known tactics helps in deconstructing their action, and thus letting us gain actionable intelligence in the proper counteraction to deploy for curbing their IOs.

4. Proactive Strategies Against Disinformation: Shifting Toward Anticipatory Measures

As previously discussed, information is a crucial resource for all individuals. We rely on it while planning our lives, evaluating situations, and taking both minor and major decisions. People's understanding of the world is shaped by their information environment, and they also continuously influence it. However, as explored earlier, the current information landscape is often cluttered with an abundance of conflicting information, and this state complicates, delays, or otherwise impairs the direct decision-making processes. The situation is further disrupted by threat actors who are willing to exploit these chaotic conditions, consciously injecting false and damaging narratives into the system. These actions ultimately undermine the public discourse and everyone's democratic process, as they deliberately target the vulnerabilities proper of the current high-information environment (Guadagno, Okdie and Muscanell, 2013; Quattrociocchi, Scala and Sunstein, 2016; Guadagno, 2021; Arcos and Arribas, 2023).

To confront and reduce the damage to our societies, the prevailing approach now employed by most actors revolves around debunking. However, this approach suffers from inherent flaws: it is often too slow to effectively counteract the spread of false narratives, and it's inherently reactive. By the time any corrections or retractions are issued, the public has already been significantly exposed to, and potentially influenced by, these narratives. Furthermore, there is a high likelihood that many individuals will not encounter these corrective statements. This current state of affairs is not a long-term solution to the ever-evolving attack on our information landscape, thus, there is a dire need for a transition towards more proactive strategies. Scholarly work on the subject increasingly recognizes the limitation of the current reactive approaches to disinformation. While not explicitly

tied to deterrence studies, the solutions proposed align naturally with deterrence principles, and are fundamental for a more proactive approach to the issue (Kennedy et al., 2017; Pamment and Palmertz, 2023).

Deterrence can be subdivided into Deterrence by Denial and by Punishment. While both methods can and should be available in the toolkit of a country, the main principle for deterring IOs is Deterrence by Denial. This form of deterrence can be achieved by shifting the cost-gain calculation of the adversary, making it more challenging for attackers to achieve their goals without increased effort. Deterrence thus is not only relegated to direct punishment, but the power to hurt can be seen as increasing the adversary's costs associated with a specific action (Schelling, 2020). This approach to attain deterrence aligns with the concept of resilience. Increasing resilience creates an environment where the attacker must invest more resources, and achieving previous results is all but guaranteed (Kennedy et al., 2017). Population resilience can be enhanced through improving media literacy, digital monitoring, risk assessment from a communication perspective, and open-source capabilities (Pamment and Palmertz, 2023).

The necessity for digital monitoring is thoroughly examined in “Anticipatory Approaches to Disinformation, Warning and Supporting Technologies”. In this article the authors are keen to suggest adapting tools and practices developed from issue and crisis management to the forecasting of disinformation attacks (Arcos and Arribas, 2023). This stress on the ability to forecast should be cojoined by an in-depth analysis of previously observed adversarial behavior (Lilly, 2022), and with a strict and honest self-assessment of our own vulnerabilities as a society (Arcos and Arribas, 2023). Taking all these suggestions into account, it should be possible to develop Early Warning and Control System (EWACS) tools for the Information Space. Such EWACS systems would provide strategic communicators with a crucial margin of maneuver to develop in a timely fashion counter-narratives, initiate prebunking campaigns, or deploy other communication strategies tailored to mitigate the impact of disinformation. These tools are vital for safeguarding the integrity of our information ecosystem by allowing us to respond proactively to emerging threats.

There is a strong consensus between scholars and practitioners alike about the need for a paradigm shift from traditional reactive methods to a more proactive, strategic approach in combating disinformation. By prioritizing the development and implementation of early warning systems, it should be possible to significantly mitigate the spread of disinformation, and restore the integrity of our information space, while also strengthening internal societal discourse. However, as we refine these tools and the theory behind them, it is imperative to ensure that these interventions in the information space are conducted with a deep respect for individual freedoms and free speech. It is crucial that the people in charge of combating disinformation do not become “arbiters of truth”. This balance is essential for maintaining the public’s trust and the effectiveness of our efforts against disinformation.

5. Conclusion: Synthesizing PSD Model Insights with Proactive Disinformation Strategies

This paper focuses on how Persuasive System Design (PSD) Key Issues are involuntarily reflected in the modus-operandi of threat actors conducting IOs. This unintended reliance on well-known principles opens the possibility of exploiting the inherent weaknesses of the model, thus enabling the creation of more robust and coherent defense tools and practices. The misapplication of the first four PSD postulates can be curbed using ideas and suggestions coming from other disciplines. This natural convergence of various independent disciplines suggests a high chance of success if these actions and tools are to be implemented and developed.

Applying Constraints and Expression: The PSD model focuses on the influence of the Information Systems, and it has already been discussed how threat actors can exploit their strongpoints and vulnerabilities to obtain the desired outcomes from their use. One of the most important abilities of any social media, and of the internet in general, is the ability of storing information, and this should be leveraged in our favor. The PSD model, following Deterrence by Denial principles, suggests that any EWACS tool should be developed with old material, already known threat actors and their affiliation, discovered botnets, and other historical data. This will enable faster labeling and discovery of new narratives that are pushed on the scene, and labeling by proximity new actors, botnets, websites, and other sources of disinformation. In short, we should exploit the ability of information retention to create an expanding database thus reducing the timeframe for action attribution and better recognizing organized narrative spread.

Proactive Commitment Strategies: The PSD's observation that individuals seek to maintain consistent commitments is currently exploited against our open and free information environment. On the other side, it also proves how preemptive strategies like prebunking can be highly effective. This point is inherently linked to the early attribution and warning that where the focus of the previous point. With the knowledge that an IO is

taking place, authorities should strive to introduce as soon as possible into the system accurate information. This will help shield the majority of the public from the harm of disinformation.

Utilizing Indirect Persuasion: Another link in our actionable suggestions chain is the use of indirect persuasion during prebunking campaigns. Among others, a technique that can be used to enhance the effectiveness of prebunking messaging is the evocation of strong emotions into the audience. Negative emotions are often used by threat actors to deliver their message, as they can shut down our more conscious decision-making process. It is also possible to enhance with strong emotions the counter-narratives of the prebunking campaign, keeping strict factuality. The public should be reminded of the presence of people with ill-intent that are actively trying to deceive them. If done properly, with corroborating evidence, this course of action will enhance the audience diffidence towards outside manipulatory tactics. These tactics will cut short the vital initial momentum of adversarial IOs.

Sustained Persuasive Efforts: While EWACS tools, deployed with state-of-the-art persuasive tactics, and corroborated with factual evidence, are fundamental for curbing, the acute phases of an IO, long term proactive and continuous solution, are to be employed. The fundamental need for proofing future generation against these campaigns is highlighted both by the PSD model and by many practitioners in the field of debunking. Now more than ever decision makers should commit to the creation of persistent initiatives to bolster media literacy and critical thinking. This will prove fundamental to creating a public that is resilient to the current and future intensification of misleading campaigns.

The push for both new tools, and long-term media literacy campaigns should be simultaneous. Tools like EWACS are focused on the crisis management of strategic communication but cannot be deemed a long-term solution that builds consistent behavior and attitude change in how people consume information. On the other hand, media literacy and critical thinking campaigns are tools well suited for those goals, but lack penetration into older strata of the public, suffer from the technology age gap, and are not suited at all for crisis management. These systems are essential for both preempting threats and strengthening the overall resilience of communities against the complex tactics employed in contemporary information warfare.

Nevertheless, it is crucial that ethical and legal standards are kept front and center during all the development phases of these tools. It's vital that our approach to win the Information war that is being waged against us respects individual rights and freedom of speech. Thus, our defenses will enhance, and not compromise, the dynamism and openness of the public discourse. Our security needs should strike a balance with our commitment to democratic and liberal values.

References

Arcos, R. and Arribas, C.M. (2023) 'Anticipatory Approaches to Disinformation, Warning and Supporting Technologies', in Routledge Handbook of Disinformation and National Security. Routledge, pp. 401–416.

Cialdini, R.B. (2009) Influence: Science and practice. Pearson education Boston, MA.

Cialdini, R.B., Petty, R.E. and Cacioppo, J.T. (1981) 'Attitude and attitude change', Annual review of psychology, 32(1), pp. 357–404.

Fallis, D. (2015) 'What is disinformation?', Library trends, 63(3), pp. 401–426.

Fry, E. (2022) 'Persuasion Not Propaganda: Overcoming Controversies of Domestic Influence in NATO Military Strategic Communications', Defence Strategic Communications, 11(11), pp. 177–213.

Guadagno, R.E. (2021) 'From Russia with Love: A Social Psychological Analysis of Information Warfare in the Social Media Age', in Democracy in the Disinformation Age. Routledge, pp. 182–200.

Guadagno, R.E. and Guttieri, K. (2021) 'Fake news and information warfare: An examination of the political and psychological processes from the digital sphere to the real world', in Research anthology on fake news, political warfare, and combatting the spread of misinformation. IGI Global, pp. 218–242.

Guadagno, R.E., Okdie, B.M. and Muscanell, N.L. (2013) 'Have we all Just Become "Robo-Sapiens"? Reflections on social influence processes in the Internet age', Psychological inquiry, 24(4), pp. 301–309.

Hosaka, S. (2023) 'Cold War Active Measures', in Routledge Handbook of Disinformation and National Security. Routledge, pp. 45–58.

Ivan, C., Chiru, I. and Arcos, R. (2023) 'Hybrid Security Threats and the Information Domain: Concepts and Definitions', in Routledge Handbook of Disinformation and National Security. Routledge, pp. 9–19.

Jowett, G.S. and O'donnell, V. (2018) Propaganda & persuasion. Sage publications.

Kennedy, J.F. et al. (2017) 'Deterrence and Dissuasion in Cyberspace', International Security, 41(3), pp. 44–71. Available at: https://doi.org/10.1162/ISEC_A_00266.

Kramer, M. and Savage, D. (2020) 'Lessons from Operation "Denver,"the KGB's Massive AIDS Disinformation Campaign', Journal of Cold War Studies, 22(1).

Lilly, B. (2022) Russian information warfare : assault on democracies in the cyber wild west. Naval Institute Press. Available at: https://books.google.com/books/about/Russian_Information_Warfare.html?id=ek7TzgEACAAJ (Accessed: 29 February 2024).

Oinas-Kukkonen, H. (2013) 'A foundation for the study of behavior change support systems', Personal and ubiquitous computing, 17, pp. 1223–1235.

Oinas-Kukkonen, H. and Harjumaa, M. (2018) 'Key Issues, Process Model and System Features', Routledge handbook of policy design [Preprint].

Pamment, J. and Palmertz, B. (2023) 'Deterrence by Denial and Resilience Building', in Routledge Handbook of Disinformation and National Security. Routledge, pp. 20–30.

Pasquetto, I. V et al. (2022) 'Disinformation as Infrastructure: Making and maintaining the QAnon conspiracy on Italian digital media', Proceedings of the ACM on Human-Computer Interaction, 6(CSCW1), pp. 1–31.

Quattrociocchi, W., Scala, A. and Sunstein, C.R. (2016) 'Echo Chambers on Facebook', SSRN Electronic Journal [Preprint]. Available at: https://doi.org/10.2139/SSRN.2795110.

Randolph, H.P., Labriny, D. and DiOrio, A. (2023) 'Historical Disinformation Practices: Learning From The Russians', in Routledge Handbook of Disinformation and National Security. Routledge, pp. 59–83.

Schelling, T.C. (2020) Arms and influence. Yale University Press.