Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P204-cd

Hybrid and Information Warfare: Challenging Topics for Risk Communication

Christine Große

Risk and Crisis Research Centre, Department of Communication, Quality Management and Information Systems, Mid Sweden University, Sundsvall, Sweden. Email: christine.grosse[at]miun.se

This study seeks to enhance current understandings of the risk communication challenges associated with the information-related means employed in cyber space to exert inappropriate influence, which frequently focus on paralyzing people and undermining stability. These means can be part of a hybrid warfare strategy located in the gray zone between the poles of peace and war, which indicates the long-term and subtle character of such a strategy. Maneuvers to conceal invasive interventions that mask activities, confuse responses, and disguise actual intentions constitute particular challenges. This paper presents the results of a literature review that applied a snowball sampling approach and concentrated on uncovering the threat landscape and recognition of the gray zone. The results highlight the emergence of information and cyber conflicts, including state operations and discreditation, along with specific techniques, such as trolling and bots, in the Swedish context and beyond. The findings illustrate some challenges for risk communication in information and cyber warfare and their implications for research and practice.

Keywords: Hybrid conflict, gray zone, information warfare, cyber policy, information systems, security, socio-technical systems, governance, risk communication.

1. Introduction

While not essentially new, since the 2000s, the concept of hybrid conflicts, also referred to as *gray zone*, has attracted attention over and above traditional forms of military confrontation or war. Following the Cold War, the attacks on the World Trade Center and Pentagon in 1993 and 2001, and the current war in Ukraine, perceptions of ways to exercise power over others have developed. In addition, innovation, rapid technological development, the increasing use of the Internet, and globalized supply chains are transforming the landscape of vulnerabilities and surfaces available on which influence can be exerted.

The combinations of methods within hybrid approaches greatly exceed those of military forms of war, such as conventional, nuclear, biochemical, and electronic/information warfare. Hybrid approaches also include non-military forms, such as financial, trade, and propaganda warfare, and above-military forms, such as cultural, intelligence, and fictious/fabrication warfare (Callard and Faber 2002). In particular, the term *hybrid* represents the utilization of a range of political, military, and non-military means for the achievement of a desired goal, while minimizing the risks that accompany direct military confrontation (Dayspring 2015). Consequently, influencing or manipulating public opinion towards desired outcomes has become a prominent aspect of attempts to wield power over others. In the age of globalized markets, mass communication technologies, and Internet-based services, the opportunities for entities to exert power, beyond the reach of land-based military forces, are rapidly increasing. These include cyber-attacks, propaganda, disinformation, or critical infrastructure disruptions. Of particular interest are maneuvers that mask invasive interventions, for example by unmanned vehicles (Konert and Balcerak, 2021), to confuse responses and conceal intentions. These issues are especially challenging for risk communication, since such maneuvers seek to obfuscate concrete events and not only maintain a high level of uncertainty about the threat but also promote confusion.

The aim of this paper is to enhance current understandings of risk communication challenges regarding information-related means that exert inappropriate influence and which often focus on paralyzing people and undermining stability (Liang and Xiangsui 1999). The present inquiry analyzes factors that affect understandings of information warfare, its orchestration, and the acceptance of related risk communication in Sweden and beyond. The results show that hybrid and information warfare are complex subjects for public risk communication and produce a number of implications for research and practice.

2. Background and Previous Research

2.1. The Gray Zone of Power Projection

The notation of *hybrid warfare* recognizes an aggressor willing to violate a target, whereas the term *gray zone* is dissociated from the potential aggressor, who more often appears in an obfuscated manner in this zone. The gray zone encompasses a spectrum of means and states of conflict between the poles of peace and war, which indicates its relatively long-term and subtle nature (e.g. Dayspring 2015, Oskarsson 2017). Previous conflicts have shown that actors not only exercise forms of power to establish strategic objectives but specifically employ means to violate another state's sovereignty during times of peace. Consequently, the weaponization of soft power means, such as the economic, diplomatic, and informational aspects of the method spectrum, have recently received increased attention. In particular, the plethora and diversity of available means have enlarged the concept of warfare and, in turn, enabled "the enlargement of the war-related activities" (Liang and Xiangsui 1999).

Nye defines national power as the ability of a nation to attract or coerce another entity to attain a preferred goal (Nye 2011). The core elements used to describe the strategic power of a state include diplomatic, informational, economic, financial, intelligence, military, and legal/law enforcement means (e.g. Oskarsson 2017). Three aspects are particularly relevant in affecting an international relationship: commanding change, controlling agendas, and establishing preferences (Nye 2011). While the two former aspects are more likely to be central to traditional forms of warfare, the latter is rather difficult to induce in a military form. Thus, influencing or manipulating public opinion towards a desired outcome has become a prominent aspect of attempts to project power onto others. Power projection describes the ability of an entity to exercise power over a distance (Dayspring 2015). In the age of globalization and digitalization, the opportunities to exert power are rapidly increasing and include the use of disinformation or cyber-attacks that disrupt critical infrastructure services. Of specific interest are maneuvers that conceal invasive interventions, such as deception and denial, to mask activities, confuse responses, and disguise actual intentions. Such maneuvers constitute a particular challenge for risk communication due to a lack of clarity regarding a situation and the variety of interpretations that may be available.

2.2. Information and Communication

The essential property of information is that it "represents some part of the world as being a certain way" (Fallis 2015). In particular, information is an artifact that has semantic or representational content, for example, objects that contain certain descriptions or summaries (Buckland 1991). While misinformation covers content that consists of honest mistakes or overly subtle satire, disinformation is regarded as misleading information whose intention and purpose is to mislead (Fallis 2015). A previous study reviewed the phenomenon of disinformation and existing typologies of false information, particularly the underlying motives, facticity, and verifiability of disinformation (Kapantai et al. 2021). Motives for employing disinformation include financial, ideological, and psychological purposes, culminating in the information-related means employed in computerized warfare in general and information warfare in particular. The former refers to any kind of influence primarily exercised with the aid of information technologies; the latter addresses the actual information that is obtained and suppressed or manipulated and disseminated for misleading purposes. Since these forms of power projection are increasingly employed in the cyber space, which connects computers, phones, Internet-of-Things devices, orbital communication satellites, cyber-physical systems in critical infrastructures, and, ultimately, people, the term "information and cyber warfare" aggregates these means of critical violation.

To differentiate between information, misinformation, and disinformation, various information quality attributes can be employed, hence, the following criteria are suggested (e.g. Große 2021, Tudjman and Mikelic 2003):

- *Authority* – the author(s), sponsor(s), and copyrights are disclosed
- *Accuracy* – information is correct, flawless, and certified free of error
- *Objectivity* – information is unbiased, unprejudiced, and impartial
- *Timeliness/Currency* – information, source, and context are up to date and updateable
- *Completeness* – information is of sufficient breadth, depth, and scope
- *Representation* – information is well-organized, concise, and consistent as well as interpretable, readable, and considerate of the human ability to analyze information

For example, along with the COVID-19 pandemic, an "infodemic" has emerged in which a variety of information has been published, composed of both accurate and inaccurate information (Song et al. 2021). This infodemic has influenced the public to mistrust official information and to employ treatments that have endangered people's health (Song et al. 2021).

Accordingly, risk communication regarding disinformation and information warfare needs to be clear and transparent but also provide meta information, that is, additional information about the piece of communication that enables receivers to distinguish information from mis- and disinformation. In addition to including the original author(s) and source(s), the piece of communication should (a) be verifiable through evidence or facts; (b) reflect several, possibly conflicting, points of view; (c) be up to date; (d) be comprehensive; and (e) be consistent and understandable (cf. Tudjman and Mikelic 2003).

3. Methodology

The research for this paper reviewed literature addressing gray zone threats and corresponding cyber and information-related means and risks.

The data collection applied a snowball sampling approach because the complex subject rendered protocol-driven search strategies insufficient for accessing samples of literature with the targeted characteristics (Webster and Watson 2002). The method involved using existing publications to identify related articles among their references and citations. The sampling regarding risk communication challenges in the realm of hybrid, cyber, and information warfare continued until sufficient data saturation.

The analysis of the collected literature concentrated on unfolding the threat landscape and the recognition of the gray zone as presented in the literature. The analysis investigated the emergence of information and cyber conflicts, including state operations and discreditation, and specific techniques, such as trolling and bots, related to both the Swedish context and beyond.

4. Analysis of an Entangled Arena

4.1. The Evolving Threat Landscape

In addition to combinations of means that involve traditional military combat, campaigns that weaponize information and the related technology to achieve desired outcomes are increasing (Waltzman 2017). Several reasons for this increase can be distinguished that stem from rapid developments in recent decades. These include the growing availability of technological means; the increased application of information technology in the private and public sectors, which is particularly sensitive in critical infrastructure sectors; the widespread use of Internet-based applications and social media; and the anonymity that allows influence to be established and power to be exercised (Waltzman 2017). Despite the fact that disinformation is a reasonably traditional method in conflicts (see e.g., Fallis 2015), it has significantly developed in recent years owing to the plethora of new techniques available for the production and dissemination of intentionally misleading information. Recent examples include the rise of "deepfakes" – synthetic, visual disinformation (Mirsky and Lee 2022, Vaccari and Chadwick 2020, Westerlund 2019), "trolling" – online personas influencing popular sentiment by instigating arguments (Dayspring 2015, Linvill and Warren 2020, Martin et al. 2019) for the purpose of "cognitive hacking" – exploiting an audience's predisposition towards an acceptable explanation of a particular event or situation (Waltzman 2017), and various forms of cyber-attacks that disturb critical infrastructure and supply chains (CISA, 2021, ICS-CERT, 2021, Singer 2015, Stevens 2020).

Although the concept of hybrid warfare is not new, the entanglement of various information systems, the Internet, and critical infrastructures within society widens the arena for a considerable spectrum of opportunities to exert power, induce instability, or gain improper influence. One of the first Internet battles described in the academic literature is the sudden disappearance of the Internet in Tallinn, Estonia in 2007 (e.g. Evron 2008). During the three weeks that followed, the Estonian Internet infrastructure was subjugated to a number of attacks, such as distributed denial-of-service attacks, DNS-server attacks, and mass email and comment spam. At the same time, Estonia was destabilized by a domestic conflict and long-standing political tensions with Russia (Herzog 2011, Schmidt 2013), which amplified the distraction and confusion. This example of orchestrated information and cyber warfare has provided insights into both the technical and psychosocial means that can be deployed by, for example, bot nets, online mobs (Evron 2008), and untraceable hacktivists (Herzog 2011). It also demonstrates the consequences of such attacks on important infrastructures and services, which constitute the backbone of society through interaction among several critical infrastructure sectors. In addition, this event indicates not only that such a hybrid risk was perceived as highly improbable, but also that the global nature of information dissemination through the Internet, supply chains, and service provisions necessitates a change in public and political attitudes to cybercrime and information warfare (Evron 2008).

4.2. The Gray Zone and the Swedish Context

The gray zone has gained increasing global attention in recent years, as has been the case in Sweden. A report of the Swedish Armed Forces (2018) on future defense directions mentions terms related to "gray zone" 59 times and "cyber" 69 times. The Swedish government has also recognized that the threat stemming from hybrid warfare constitutes a threat scenario that must be prioritized (Prop. 2020/21:30).

The Swedish Armed Forces conclude the following with regard to hybrid warfare and the emerging need for enhanced collaboration between military and civil defense: "The gray zone threat crosses government boundaries and the aggressor strives to circumvent the foundations of the state's tools for institutional violence. The handling of the gray zone problem is therefore characterized by a mixture of military means and means that fall outside the Armed Forces' area of responsibility and must therefore be coordinated based on a holistic view of the challenges" (Swedish Armed Forces 2018).

This perspective emphasizes that defense against hybrid warfare requires a broader spectrum of means, including both those applied in the political sphere and those available within the business and individual spheres. In addition, it acknowledges the increasing potential impact of information and cyber warfare, particularly when integrated into hybrid warfare (ibid). One obvious difficulty is the question of who is responsible for handling events located within the gray zone. The Armed Forces are traditionally responsible for handling military confrontation, such as armed battles, mostly in a state of war. However, the situation within the gray zone is much less clear. Hence, an opponent who is expected to act anonymously and with a negligent sense of responsibility benefits from official difficulties in distinguishing intentional and coordinated actions from random events and accidents (Gunneriusson 2019).

Recently, the Swedish government has recognized that hybrid threats are being directed against Sweden, primarily targeting civil targets such as media and critical infrastructures (Prop. 2020/21:30). In particular, the report acknowledges the uncertainty that is inherent in the gray zone between states of peace and war. Therefore, the government proposes to improve civil defense, even in times of peace, to enhance civil preparedness and resistance against disturbances in critical infrastructures and the exertion of malevolent influence (ibid). The report outlines that the ability to handle hybrid threats, especially those related to cyber warfare such as disinformation, manipulation of public opinion, and disruption of critical supplies, is becoming increasingly important, thus, necessitating, among other strategies, efforts to establish public-private partnerships and a proper risk communication to the public (ibid).

The fact that information and cyber security has become an increasingly important foreign and national security policy issue in Sweden is evident in the 2020 decision to establish the National Cyber Security Centre. The government has commissioned the Swedish Armed Forces, the Swedish Armed Forces Radio Institute, the Security Police, and the Swedish Civil Contingencies Agency to deepen their collaboration in the context of cyber security and, ultimately, to establish and develop the National Cyber Security Centre (Ministry of Defense 2020). This collaboration will also include the Swedish Defense Materiel Administration, the Police Authority, and the National Post and Telecom Agency as well as additional, unspecified, public and private actors (ibid). However, the policy document clearly states that "Sweden's security, competitiveness, and prosperity rest to a large extent on digital foundations. It is important that the possibilities of digitalization be utilized while managing risks. Cyber threats to Sweden and Swedish interests are extensive" (ibid). This statement underlines the relevance of research and practice regarding information and cyber warfare and security, including risk communication, in the Swedish context and beyond.

4.3. Information and Cyber-Related Conflicts

4.3.1. Research on State-Related Operations

One branch of research has focused on the capacity, objectives, and maneuvers of Russian hybrid warfare, specifically concentrating on the potential of cyber operations and (dis-) information campaigns. For example, studies have emphasized the risks induced by affecting national command and control abilities (Bachmann and Gunneriusson 2015) and the Russian digital media ecosystems established in Western democracies (Ünver 2019). Russia's move beyond propaganda into the digitally entangled global information space to maintain and further extend its influence has been another research subject (Abrams 2016). In addition, the conflicts between Russia and Ukraine and Russia and the US have been analyzed. In both cases, the weaponization of information through digital channels, such as social media, was the focus. Research on the conflict involving Ukraine highlights the dynamics of digital disinformation and the role of citizens in attempts to influence local and global public opinion (Golovchenko et al. 2018). The study highlights that citizens play a significant role in escalating or de-escalating such conflicts in the digital sphere: "they are the most active drivers of both disinformation and attempts to counter such information" (ibid.). In particular, the paper indicates that tweets by citizens are four times more likely to be retweeted than tweets by other users (ibid.); a fact that could attract "active measures" (see Abrams 2016) to recruit local hacktivists into a so-called troll army (see e.g., Dayspring 2015). Research on the conflict between Russia and the US analyzed influence exerted in the form of disinformation to polarize U.S. voters (Howard et al. 2018). This analysis shows not only the technical but also strategical advancements of the employed means, for example, the sophisticated exploitation and broad deployment of methods using both a number of social media platforms, such as Facebook, Twitter, Instagram, and YouTube, and microtargeting to approach citizens and individuals, respectively (ibid). The U.S. election is also subject to another study that has investigated the rise of "Russian Trolls" and the role of "fake news" in available Twitter data. It demonstrates that the communication strategy primarily appealed to an identity logic rather than an informational logic of false information (Jensen 2018), which would be consistent with the above considerations regarding the role of citizens in information campaigns. Another study compared an American analysis of the U.S. election with a Russian equivalent, the so-called Gerasimov doctrine (Klein 2018). The study highlights their common logics – any foreign support for the promotion of democracy can be identified as a means for destabilization (ibid) – which makes effectively employed messages on social media a subject of concern.

China and Iran have also attracted research on the gaps in military and non-military innovation and the role of applying emerging technologies from the commercial sector for power projection or defense in the US and Europe (Fiott 2017). China has invested considerable effort in expanding its political and economic influence in the world; for example, by supporting the development of a world news agency that broadcasts its own television programs globally via satellite (Hong 2011). In addition, the virtual space has become important. Research has revealed that the Chinese regime utilizes a substantial number of online activists to post cheerleading, factual reporting, and non-argumentative praise of current government activities or officials to strategically distract the public from collective action and create positive sentiment in the media (King et al. 2017). Recent examples from the literature show that China maintains a full spectrum of competencies in technologically enabled narrative propaganda, even though China does not appear to be as successful in connecting with or engaging audiences as other state actors such as Russia, Iran, and others (DiResta et al. 2022). However, fostering non-engagement should not be underestimated as part of a political strategy to appear as a confident, inspirational, trustworthy, and leading partner to the world. Another example of a seemingly unsuccessful attempt to shape public discourse can be seen in China's criticism of Swedish media and public discourse since 2018, which prompted massive rejection of China's apparently politically motivated propaganda campaign in Sweden (Jerdén and Bohman 2019). However, the COVID-19 outbreak quickly changed the global media focus. In the realm of the pandemic, visual and textual representations of emergency responses and crisis management aimed at concerned audiences have elicited attention. Research on Facebook messages has described how Chinese and U.S. media utilized tone and imagery to frame the positive or negative connotations of messages, for example, with regard to hurriedly constructed medical facilities (Molter and DiResta 2020). Such comparisons further illustrate the difficulties in separating lobbying, propaganda, and mis- and disinformation from information, as well as cyber and information warfare. Considerations on the framing of such subjects for a target audience should therefore be of certain interest to research and the practice of risk communication, especially regarding cyber and information-related risks.

4.3.2. Discreditation and Fake News

While state-related disinformation is a matter of concern in research and practice, the discreditation of international, non-governmental organizations can also be a means to infect public opinion and to embed disinformation campaigns in an overarching narrative. For example, a case study has analyzed the effect of master narratives on the creditability of dis-/information in the context of the humanitarian work of the White Helmets (a volunteer rescue group) in Syria (Levinger 2018). Most of the related literature emphasizes the importance of addressing disinformation campaigns. Suggestions for courses of action include refuting falsehoods with facts and opposing the misleading information with coherent and compelling counter-stories (ibid). However, detecting and mitigating comprehensive disinformation campaigns, which may extend over long periods and a wide range of distribution channels and tools, appear to be complex tasks. In particular, when considering the individual's role in spreading misinformation, the need for rethinking an adequate defense in such contexts may be advisable.

Critical moments of public life combined with the global diffusion of social media seem to provide the perfect scenery for foreign disinformation campaigns, irrespective of whether or not they are initiated by national actors. Hence, another branch of research focuses on the (re-)incarnation of fake news in the Internet age, for example, by analyzing its utilization and effectivity in disinformation campaigns in order to exercise political power and the mechanisms applied to reach a widespread audience. Although the term "fake news" comprises a spectrum of false information, such as news satire, news parody, fabrication, manipulation, advertising, and propaganda (Tandoc et al. 2017), it is now more often used to refer to disinformation or to discredit facts and reporting.

However, to understand the – often highly politicized – phenomenon of fake news, the particular social, cultural, and political context must be understood, as a study of fake news from a journalism perspective in South Africa has demonstrated (Wasserman 2020). In general, the literature highlights that misinformation has reached a new level and signifies a knowledge gap regarding the vulnerability of societies to manipulation efforts conducted by malicious actors (Lazer et al. 2018). For example, one study of the 2006 Israeli election analyzed the interaction between several types of media and its effect on political attitudes. It demonstrated that a higher exposure to "fake news" combined with lower mediation through correct information resulted in a stronger belief in the realism of fake news (Balmas 2014). This might be an additional reason for the emergence of politically motivated trolling. Another study has indicated that age, education, and familiarization with digital information play greater roles in the belief in and dissemination of fake news than the political inclination of individuals, even when right-wing supporters exhibit a greater tendency to accept fake news, irrespective of whether they are pro-left or pro-right (Baptista et al. 2021). In addition, the growing number of state actors spreading propaganda and misinformation through social media has contributed to this global phenomenon (Bradshaw and Howard 2018), which renders analyses of the causes, means, and consequences of information and cyber warfare more complex for society.

4.4. Trolling and Bots

A study in the Turkish context has indicated that individual activities in the form of trolling are relatively spontaneous and unorganized (Saka 2018). An analysis of the behavior of Twitter users identified as state-sponsored and the content they disseminated has shown that these users were active over a long period and reached a significant number of other users; however, their overall influence seemed relatively modest (Zannettou et al. 2019). Moreover, another study in the Chinese context indicated that a somewhat controlled pro-regime troll army might even contribute to the formation of public opinions that are contrary to the initiator's intention (Rongbin 2015).

Alongside technological developments, methods and tools to disseminate information and disinformation are also developing and becoming both more sophisticated and varied. For example, bots (short for "software robots") have advanced considerably. Today, they populate many socio-technical systems, such as social media or other chats, generally to post content automatically, but also to search the Web for information, engage in interactions, steal information, appear as human users, and gain greater influence (Ferrara et al. 2016). Thus, social bots have become an effective tool, in addition to human trolls, for spreading disinformation and amplifying its influence across the Web. Although research has focused on mechanisms to detect bots in the social media ecosystem, their number and agendas remain unknown (ibid.). For example, an analysis of Twitter bots in the context of a dispute between Saudi Arabia and Qatar in 2017 identified a range of different bots, from domestic and foreign commercial sources, that together significantly distorted the discussions on social media (Nimmo, 2018). In addition, another study of Twitter messages in the context of the 2018 mass protests in Iran identified a number of social bots and detected their negative impact on the sentiment in the political debate (Thieltges et al. 2018).

This automation of content production and impact creation renders the previously mentioned proposal of opposing the misleading information with coherent and compelling counter-stories (Levinger 2018) nearly impossible. Whereas some researchers already imagine social media as a machine-to-machine ecosystem with human navigation (Ferrara et al. 2016), others emphasize the opportunity such technology presents to unite rather than to divide, for example, in the context of violation prevention in Kenya (Brown & Livingston 2018). Other suggestions include the clearer disclosure of state-sponsored communication on commercial platforms (Molter and DiResta 2020) and the consideration of the critical role of infrastructure accessibility for digital communication and social media use (Rohde et al. 2016).

5. Concluding Remarks

The analysis and examples provided illustrate that the gray zone and hybrid, information, and cyber warfare are complex subjects for risk communication, which carry a number of intertwined challenges. First, the concrete object of a communication piece is difficult to define. Second, the audience of this information piece is heterogenic and thus user-based specification of the content is required. Third, the visual, textual, or physical forms of information frame the content and are likely to affect public sentiment. Fourth, distribution channels provide different opportunities to reach people, while any specific selection simultaneously excludes people who do not have access to this selection. Fifth, the information piece must clearly state its objective(s) and sources. Finally, the information should be consistent with other policies and communication regarding the overall topic.

Further research could address the lack of in-depth understanding concerning information and cyber security policy-making and the conditions that enable successful and inclusive risk communication on information and cyber warfare.

References

Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal* 15(1): 5–31.

Bachmann, S. D. and Gunneriusson, H. (2015). Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere. *Georgetown Journal of International Affairs* 16: 198-211.

Balmas, M. (2014). When Fake News Becomes Real. *Communication Research* 41(3): 430–454.

Baptista, J. P., Correia, E., Gradim, A. and Piñeiro-Naval, V. (2021). The Influence of Political Ideology on Fake News Belief: The Portuguese Case. *Publications* 9(2): 23.

Bradshaw, S. and Howard, P. N. (2018). The Global Organization of Social Media Disinformation Campaigns.*Journal of International Affairs* 71(1.5):23–32.

Brown, R. and Livingston, L. (2018). A New Approach to Assessing the Role of Technology in Spurring and Mitigating Conflict: Evidence from Research and Practice. *Journal of International Affairs* 71(1.5): 77–86.

Buckland, M. K. (1991). Information as thing. *Journal of the Am Society for Information Science* 42(5): 351–360.

Callard, J. and Faber, p. (2002). An Emerging Synthesis for a New Way of War: Combination Warfare and Future Innovation. *Geo J of International Affairs* 3(1): 61–68.

CISA [Cybersecurity and Infrastructure Security Agency] (2021). *Eviction Guidance for Networks Affected by the SolarWinds and Active Directory M365 Compromise: Analysis Report 21-134A*.

Dayspring, S. M. (2015). *Toward a Theory of Hybrid Warfare: The Russian Conduct of War During Peace*. Master Thesis. Naval Postgraduate School, California.

DiResta, R., Miller, C., Molter, V., Pomfret, J. and Tiffert, G. (2022). *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives*. Cyber Policy Center. Stanford University, Stanford.

Evron, G. (2008). Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War. *Georgetown Journal of International Affairs*: 121-126.

Fallis, D. (2015). What Is Disinformation? *Library Trends* 63(3): 401–426.

Ferrara, E., Varol, O., Davis, C., Menczer, F. and Flammini, A. (2016). The rise of social bots. *Communications of the ACM* 59(7): 96–104.

Fiott, D. (2017). A Revolution Too Far?: US Defence Innovation, Europe and NATO's Military-Technological Gap. *Journal of Strategic Studies* 40(3): 417–437.

Golovchenko, Y., Hartmann, M. and Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation. *International Affairs* 94(5): 975–994.

Große, C. (2021). Enhanced Information Management in Inter-organisational Planning for Critical Infrastructure Protection: Case and Framework. In: *Proc 7th Int Conf on Information Systems Security and Privacy*. SCITEPRESS Publications: 319–330.

Gunneriusson, H. (2019). Hybrid Warfare and Deniability as Understood by the Military. *Polish Political Science Yearbook* 48(2).

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security* 4(2): 49–60.

Hong, J. (2011). From the World's Largest Propaganda Machine to a Multipurposed Global News Agency: Factors in and Implications of Xinhua's Transformation Since 1978. *Political Communication* 28(3): 377–393.

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J. and Francois, C. (2018). *The IRA and Political Polarization in the United States, 2012-2018: Computational Propaganda Research Project*, Oxford, UK.

ICS-CERT (2021). Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT. Available online: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Jensen, M. (2018). Russian Trolls and Fake News: Information or Identity Logics? *Journal of International Affairs* 71(1.5): 115–124.

Jerdén, B. and Bohman, V. (2019). *China's propaganda campaign in Sweden, 2018-2019. UI Brief 4/2019*, Stockholm.

Kapantai, E., Christopoulou, A., Berberidis, C. and Peristeras, V. (2021). A systematic literature review on disinformation: Toward a unified taxonomical framework. *New Media & Society* 23(5): 1301–1326.

King, G., Pan, J. and Roberts, M. E. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review* 111(3): 484–501.

Klein, H. (2018). Information Warfare and Information Operations: Russian and U.S. Perspectives. *Journal of International Affairs* 71(1.5): 135–142.

Konert, A. and Balcerzak, T. (2021). Military autonomous drones (UAVs) - from fantasy to reality. Legal and Ethical implications. Transp. Research Procedia, 59, 292-299.

Lazer, D. M. J., Baum, M. A. and Benkler, Y. et al. (2018). The science of fake news. *Science (New York, N.Y.)* 359(6380): 1094–1096.

Levinger, M. (2018). Master Narratives of Disinformation Campaigns. *Journal of International Affairs* 71(1.5): 125–134.

Liang, Q. and Xiangsui, W. (1999). *Unrestricted Warfare: Two Air Force Senior Colonels on Scenarios for War and the Operational Art in an Era of Globalization*. PLA Literature and Arts Publishing House, Beijing.

Linvill, D. L. and Warren, P. L. (2020). Troll Factories: Manufacturing Specialized Disinformation on Twitter. *Political Communication* 37(4): 447–467.

Martin, D. A., Shapiro, J. N. and Nedashkovskaya, M. (2019). Recent Trends in Online Foreign Influence Efforts. *Journal of Information Warfare* 18(3): 15–48.

Ministry of Defense (2020). *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter. Fö2019/01330.*, Stockholm.

Mirsky, Y. and Lee, W. (2022). The Creation and Detection of Deepfakes. *ACM Computing Surveys* 54(1): 1–41.

Molter, V. and DiResta, R. (2020). Pandemics & Propaganda: How Chinese State Media Creates and Propagates CCP Coronavirus Narratives. *Harvard Kennedy School Misinformation Review*.

Nye, J. S. (2011). *Future of power: Its changing nature and use in the twenty-first century*. Public Affairs, New York, NY.

Oskarsson, K. (2017). The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone. *NATO Allied Command Transformation Open Publications* 1(2).

Prop. 2020/21:30 (2020). *Regeringens proposition: Totalförsvaret 2021–2025.*, Stockholm.

Rohde, M., Aal, K., Misaki, K., Randall, D., Weibert, A. and Wulf, V. (2016). Out of Syria: Mobile Media in Use at the Time of Civil War. *International Journal of Human-Computer Interaction* 32(7): 515–531.

Rongbin, H. (2015). Manufacturing Consent in Cyberspace: China's "Fifty-Cent Army". *Journal of Current Chinese Affairs* 44(2): 105–134.

Saka, E. (2018). Social Media in Turkey as a Space for Political Battles: AKTrolls and other Politically motivated trolling. *Middle East Critique* 27(2): 161–177.

Schmidt, A. (2013). The Estonian Cyberattacks. In: Healey, J. (ed.) *The Fierce Domain – Conflicts in Cyberspace 1986-2012*. Atlantic Council, Washington, D.C.

Singer, P. W. (2015). Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons. *Case Western Reserve Journal of Iternational Law* 47(1).

Song, X., Petrak, J., Jiang, Y., Singh, I., Maynard, D. and Bontcheva, K. (2021). Classification aware neural topic model for COVID-19 disinformation categorisation. *PloS one* 16(2): e0247086.

Stevens, C. (2020). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy* 41(1): 129–152.

Swedish Armed Forces (2018). *Tillväxt för ett starkare försvar.*, Stockholm.

Tandoc, E. C., Lim, Z. W. L. and Ling, R. (2017). Defining "Fake News". *Digital Journalism* 6(2): 137–153.

Thieltges, A., Papakyriakopoulos, O., Serrano, J. C. M. and Hegelich, S. (2018). Effects of Social Bots in the Iran-Debate on Twitter ArXiv:1805.10105.

Tudjman, M. and Mikelic, N. (2003). Information Science: Science about Information Misinformation and Disinformation. In: Informing Science Institute.

Vaccari, C. and Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media + Society* 6(1): 205630512090340.

Waltzman, R. (2017). *The Weaponization of Information: The Need for Cognitive Security: CT-473*, Santa Monica, California.

Wasserman, H. (2020). Fake news from Africa: Panics, politics and paradigms. *Journalism* 21(1): 3–16.

Webster, J. and Watson, R. T. (2002). Analysing the past to prepare for the future: Writing a literature review. *MIS Quarterly* 26(2): xiii–xxiii.

Westerlund, M. (2019). The Emergence of Deepfake Technology A Review. *Technology Innovation Management Review* 9(11): 39–52.

Ünver, A. H. (2019). *Russian Digital Media and Information Ecosystem in Turkey*. Centre for Economics and Foreign Policy Studies.

Zannettou, S., Caulfield, T., Cristofaro, E. D., Sirivianos, M., Stringhini, G. and Blackburn, J. (2019). Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web arXiv:1801.09288v2.