(Dis)information warfare: Risks for businesses

Luke Tredinnick

This issue of Out-of-the-Box addresses the threat of information warfare for commercial organisations, and examines the role of information professionals in mitigating those risks. It first explores the nature of information warfare, before examining the threats to business posed by aggressive actions in the information domain. Finally it looks at the role of information professionals in assessing, understanding and managing risk.

This paper addresses the threats of information warfare for commercial organisations, and explores the role of information professionals in mitigating those risks. In particular it addresses the problem of orchestrated disinformation campaigns and their potential knock-on effects for business. In recent years the involvement of state actors in interstate disinformation campaigns has become a familiar part of the information landscape. As information technology and in particular social media have become increasingly integral parts of the economic, social and political context, the vulnerability of civil discourse to political interference has increased. But while the white noise of targeted disinformation and misinformation campaigns has become a perpetual accompaniment to contemporary life, the return of interstate war in Europe has raised concerns about the vulnerabilities of contemporary information and communications infrastructure to more concerted efforts to disrupt civil discourse. We may not be on the brink of an information war, but the potential for interstate aggression in the information domain has become more real.

A lot has been written about the nature and threat of information warfare over the past 30 years, most of that research and analysis has explored the strategic, security, and infrastructure risks (e.g., Libicki, 1995; Denning, 1999; Ventre, 2016). Comparatively little has addressed the threats to commercial business: the kinds of disruption an information war might bring. Still less has addressed the role of information professionals in mitigating these risks. This paper unboxes those risks for commercial organisations and explores the role that information professionals can play in their mitigation. It argues that the threat of information warfare should be taken seriously, and that organisations should be planning to mitigate those risks before they become apparent. The paper is divided into a number of sections. The first part will explore the nature of information warfare, the different forms that it might take, and the role of state and non-state actors. The second part will examine how and why information warfare might impact on commercial operations. Finally the paper addresses the role of information professionals in planning for and mitigating these risks.

The nature of information warfare

Information warfare describes the pursuit of strategic advantage by nation states through domination of the infosphere, including the manipulation of information to instil false beliefs, and attacks on information infrastructure to degrade the ability of an enemy to counter or mitigate these actions. NATO (2022) have described information warfare as:

> an operation conducted in order to gain an information advantage over the opponent. It consists in controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. Information warfare is not a new phenomenon, yet it contains innovative elements as the, effect of technological development, which results in information being disseminated faster and on a larger scale. (NATO, 2022)

While the infosphere within which information warfare operates includes the whole information ecology of online and offline environments (Floridi, 1999), in practical terms contemporary information wars predominantly exploit the possibilities of the digital space.

Control of information in the pursuit of strategic advantage has of course always been a part of warfare, particularly in respect of propaganda, intelligence and the deployment of strategic misinformation. Nevertheless information warfare differs from these prior uses of information in warfare in the prioritising action within the information domain, and the strategic significance of that action. Dominating the information space not only becomes a strategic priority but also a means of pursuing strategic aims in its own right. Stein (1995) has argued that "information warfare is about the way humans think and, more important, the way humans make decisions". This emphasises the degree to which influencing public opinions, as much as controlling the means of information dissemination, is central to the nature of information warfare. It follows that disinformation is becoming more strategically important to achieving strategic ends. Di Pietro et al. argue that

> The ever increasing convergence between the cyber and physical worlds, is making more and more difficult to disentangle the critical systems that make up our societies. As a consequence, a single carefully-crafted and perfectly-timed piece of (dis)information can now potentially make or break elections, governments, economies and infrastructures, thus granting a tremendous leverage in the hands of those who know how to weaponize and manipulate these critical systems (2021: 6)

Information warfare is therefore a concept that that addressed the implications of messages as much as it does the implications of the media via which they are transmitted. But while this emphasises the disinformation aspects of information warfare, the concept also encompasses a range of other actions.

An information war should be differentiated from a cyber war. Cyber warfare describes the use of cyber-attacks against enemy state to cause disruption, or material harm to vital computer and infrastructure systems such as defence systems, transportation and energy infrastructure, and communications. The typical tools of cyberwarfare are malware, denial of service attacks, and hacking. While these strategies may be elements of an information war, information warfare also describes the intention to control the information space within which global international relations takes place. This includes disruptive cyber-attacks but also misinformation and disinformation attacks that seek to get inside the decision-making loop. Nevertheless cyber warfare and information warfare share a basic asymmetry in which the advantage is often not with the more developed nations; the greater the dependency of a society on information and communications networks the more vulnerable it becomes to cyber activism and cyber attacks. Therefore technologically advanced societies will tend to be more vulnerable to actions arising from information warfare.

The targets of an information war are potentially diverse, including general populations, government infrastructure, economic stability, and military forces, therefore the consequences of an information war are difficult to predict. An information war may be visible, or it may be covert; it may be conducted by state actors, by non-state actors, or by a combination of the two. An information war may not therefore be associated with conventional warfare, and it may be difficult to determine when one takes place, who the actors are, and what strategic aim is being pursued. Information warfare might masquerade as or be mistaken for cybercrime. However the motivations driving information warfare are different from those driving cybercrime and the outcomes manifest in different ways. This fundamental difference in motivation and outcome drive the differences in risks and mitigations that businesses face.

The nebulous nature of the risks associated with information warfare drive some of the difficulties in effectively mitigating those risks. Nevertheless we can identify typical elements that might for a part of interstate aggression in the information domain. These include:

- **Cyber-attacks on critical infrastructure:** perhaps the most well-known example of a cyber attack on critical infrastructure was Stuxnet worm which targeted Iran's uranium enrichment facility at Nalanz in 2010. Stuxnet targeted four previously unknown vulnerabilities in the Windows operating system. This unusual profile suggested the involvement of state actors, and although no state has admitted responsibility, the Stuxnet attack is widely believed to have originated in a collaboration between Israeli and US security service (Lindsay, 2013). The Stuxnet worm was the first example of malware design to cause physical damage to specific infrastructure, and resulted in the destruction of almost 1000 centrifuges used in the enrichment of uranium by causing them to spin out of control after it was brought into the facility on an infected USB device (Baezner and Robin, 2017). However the attack also had global consequences when the malware escaped into the wild infecting over 60,000 computers worldwide (Farwell and Rohozinski, 2011) . The Stuxnet worm highlights how cyber-attacks can have material consequences leading to the destruction of and damage to key critical infrastructure. Typical targets might include transportation, health or finance infrastructure, with the aim of degrading the state, undermining morale, or creating distraction and confusion. Because contemporary societies are highly dependent of computerised automation, the potential for similar attacks to cause significant and unpredictable damage and disruption are quite significant, presenting a series of risks to the commercial environment within which businesses operate.

- **Influence operations**: a more familiar aspect of information warfare is the influence operation, a form of propaganda that seeks to influence the outlook and views of a population so as to affect their behaviour. In fact influence operations have become a normal part of international relations in the social media age, although their effectiveness in driving behavioural change is unclear. Contemporary influence operations tend to combine fabricated content, the use of botnets, troll factories or paid content producers to reproduce particular messages, and sometimes the use of AI driven deep fakes and social media agents. Influence operations can also been aimed at provoking social unrest or social conflict by exacerbating existing tensions, such as for example in relation to culture war issues. Influence operations have the potential therefore to affect the social context within which commercial operations take place, but also to directly or indirectly damage brands, customer and client relationships, and commercial communications.

- **Misinformation and disinformation**: closely related to the influence operation is the disinformation and misinformation attack. These rely on similar strategies to the influence operation, but tend to be associated with sowing confusions rather than influencing attitudes on a population level. Thus a disinformation and misinformation campaign might involve deliberately contradictory messages, or flooding social media with intentionally fake content in order to undermine trust in authoritative sources or authorised narratives by overwhelming the ability of individuals to make sense of the information that they are receiving. Misinformation and disinformation campaigns have the potential to influence the business contexts, stoking fears about non-existent threats that may alter the behaviour of clients, customers or employees, and creating small-scale social disturbances. More importantly, once established, untruths can prove persistent. A good example of this is misinformation and disinformation associated with the Covid-19 pandemic; while much was organic some part of the misinformation and disinformation around Covid-19 was connected to state-sponsored action. These have had long-lasting consequences for attitudes towards public health measures and messages.

- **Data manipulation**: data manipulation describes the use of data to undermine a particular strategic action. Data has become fundamental to the ways in which contemporary societies operate; we produce and use vast amounts of data in economic and social activity every day. However as we have previously addressed in *Business Information Review,* the provenance of data at the point of use is not always as transparent as it could be (Tredinnick, 2023). Decisions that are taken on the basis of data are therefore vulnerable to the manipulation of those data sources in order to achieve a particular outcome. We have all become familiar with the concept of data theft, but data manipulation attacks involve not stealing data from an organisation, but making subtle changes to that data which are likely to go unrecognised with the intention of achieving a particular outcome.

- **Economic disruption:** another potential target of information warfare is economic disruption, covering a wide range of potential targets, from stock markets, to banking and electronic funds transfer systems. The reliance of contemporary economies on digital networks makes them particularly vulnerable to attack, and the potential destabilising effects of this are significant. Economic disruption is also one area where business is likely to be most effective, with the potential to damage payments, payroll, and investments, or undermine the context within which commercial operations take place.

- **Communications interception and hijacking:** finally an information war may include elements of communications interception and hijacking. There have been several cases, for example, where cyber activism groups have taken over television broadcast systems in order to broadcast propaganda for a particular cause. Television and radio

> networks are attractive targets because of their wide influence. But communications hijacking may also include infiltrating mobile networks, disrupting internet communications, or disrupting the communications of regulators, commercial businesses, or significant individuals. The aim may be to disrupt the ability for individuals and organizations to effectively communicate, or to hijack communications channels as part of influence operations. Nevertheless because of the significance of communications and in particular the internet to contemporary commercial organizations, attacks on communications networks may have significant consequences for businesses.

The current Russo-Ukranian war gives an indication of how information warfare might develop. Both sides in the conflict have used social media to define the global and local narratives, drawing on platforms such as Twitter, TikTok, Telelgram, YouTube and Facebook. The volume of content created has been immense and has drawn billions of global monthly views. The aim of these influence operations is often not to convince populations of the veracity of the content itself, but to undermine trust in all sources of information so as to disrupt the discourse around the conduct of the war, and create confusion about which accounts are reliable. In an influential report Lucas and Pomeranzev have written about Russia's misinformation and disinformation strategy that:

> Unlike Soviet propaganda, Russia's contemporary methods of information warfare do not crudely promote the Kremlin's agenda. Instead, they are calibrated to confuse, befuddle and distract (Lucas and Pomeranzev, 2016).

Thus much of this content has been of relatively low quality – easily identifiable footage from other conflicts or training exercises, easily discredited claims, or obvious deep fake content. Russia has also sought to control internal perceptions about the conflict by restricting access to external sources including social media and traditional media outlets, effectively banning a range of social media and traditional media services. In addition Ukrainian internet services have come under attack on several occasions. The conflict has also provided examples of communications systems hijacking; the widely discussed vulnerability in Russian Communications has reportedly been exploited by Ukranian forces who have allowed Russian forces to connect to Ukranian mobile networks allowing the messages to be intercepted and movements tracked. In addition online activist group *Anonymous* claimed to hack Russian state television services in order to broadcast pro-Ukranian messages (Milmo, 2022). While the elements of information warfare have been relatively limited in scope, they do indicate the potential broad spectrum of threats that aggressive use of the information domain might involve, and in particular highlight how control of public perceptions through social media has become an increasingly important part of conflict.

Of most current concern are influence operations and misinformation. This is because to a significant degree the use of influence operations, misinformation and disinformation is already a part of the global context of international relations. Zannettou et al. (2019) have provided a useful typology of misinformation, differentiating between fabricated information, propaganda, conspiracy theories, hoaxes, biased information, rumours, clickbait and satirical content mistaken for factual information. They also highlight the different actors involved in spreading false information, including bots, trolls, criminal organizations, activist or political organisations, governments, state-sponsored individuals, journalists, "useful idiots", and individuals who stand to benefit from the spread of misinformation. This complexity in forms of content, in kinds of actor and in underlying motivation highlights both the vulnerability of contemporary communications networks to subversion, but also the difficulty in identifying, managing and mitigating the effects of false information. State-sponsored influence operations are an attractive means of leveraging national interests precisely because they are covert, low-level, and difficult to pin against the actions of an individual state.

In addition concern has shifted to the role of generative AI in information warfare and in influence operations in particular. Large language models have the characteristic of *truthiness,* a term coined by US television host Stephen Colbert to describe how information can feel correct (Mouton, 2023). Mouton has argued that:

> despite lacking factual accuracy, content with a highly coherent logical structure can influence how smart, sophisticated people decide whether something is true or not. Our cognitive biases mean well-written content or compelling visuals have the power to make claims seem more true than they are (Mouton, 2023).

Large language models also allow the production of influence operations at scale, and an element of automation in the distribution of content. However AI also has a role in combatting misinformation and disinformation. Cassauwers (2019) details a number of projects using AI technologies to combat misinformation and disinformation, and Santos (2023) discusses the application of both language analysis and sentiment analysis in combatting misinformation.

Information warfare and business

Information warfare may not appear to be a significant risk to business at this time, and indeed it is easy to assume that the risks that it presents are largely the same as those that arise from cybercrime in general, and that therefore no specific mitigation is required. However while the risks are small, they are not negligible, and the potential for rapid escalation of those risks highlights the needs for prior planning. We may not be on the brink of an information war, but interstate aggression in the information domain is a real and present phenomenon, and the asymmetrical nature of that threat makes it not only a serious concern, but something we need to plan for. Zannettou et al. emphasize the currency of that risk, writing that:

> A new era of Information Warfare has arrived. Various actors, including state-sponsored ones, are weaponizing information on Online Social Networks to run false-information campaigns with targeted manipulation of public opinion (ZANNETTOU et al., 2019)

The issues associated with aggressive state actions in the information domain are not a hypothetical future threat, but are in a limited but clear way already part of international relations.

There are a number of clear reasons to take seriously the threat of information warfare for business now. In the first place we have already seen the potential for strategically targeted disinformation campaigns associated with significant political events to disrupt business planning and operations, and in some cases to transform the context within which commercial businesses operate. The involvement of state actors in influence campaigns around Brexit, the US elections, and the Covid-19 pandemic underlines that influence. Indeed the Russian/Ukraine conflict has not only drawn attention to the wider vulnerabilities posed by our reliance on information systems of different kinds, but also provided multiple examples of the kinds of strategies that might feature in an information war, and provide a good opportunity for assessing and analysing risk. These kinds of experiences highlight the potential for a sustained information war to cause significant and long-term problems for commercial organisations. Secondly, we know that a number of politically unstable states have invested heavily in cyber capabilities over recent years, particularly North Korea which has increasingly relied on cybercrime for political influence and revenue generation. Raska (2023) for example has written that:

> North Korea’s cyber and information operations have provided Pyongyang with a range of relatively low-cost asymmetric options to demonstrate power without any visible military commitments… raising hundreds of millions of dollars to support the regime (Raska, 2023: 172)

In addition a number of nations with well-developed cyber capabilities have experienced periods of significant political instability, including Russia, the United States, Britain and China. Therefore the potential for aggressive actions in the information domain is already present, and to some degree already a part of our contemporary communications context. Thirdly, businesses have become more reliant on distributed information services, and in particular cloud services, which may be particularly vulnerable to a determined cyber attack. This is particular the case in the post-pandemic period, where a greater reliance on distributed services has been a common response to addressing the post-pandemic business environment. Therefore the knock-on effects of aggressive actions in the information sphere have a greater potential to disrupt business operations that previously. Finally we have seen in the last 5 years rapid advancements in artificial intelligence AI), and the increasing use of AI in cybercrime of different kinds, suggesting future potential for AI in targeted information attacks.

If information warfare is a risk that it is worth exploring, it might be assumed that the targets and tactics of an information war are likely to be in broad terms similar to those deployed in cybercrime or in general misinformation campaigns. Therefore it might be assumed that no specific mitigation is necessary in planning for information warfare than that already accounted for by planning in mitigation of the more common and real threats. However this is a mistaken assumption on a number of grounds. In the first place unlike traditional cybercrime, information warfare is likely to be broad spectrum – that is to say consist of multiple simultaneous forms of attack. Secondly cyber crime generally targets the low hanging fruit of poor information security practice, where as the motivation to cause widespread disruption means that information warfare attacks are likely to be more determined and aimed at strategically important targets. Finally it might be assumed that businesses are unlikely to be direct targets of aggressive actions by state actors. However commercial organisations are vulnerable to actions arising from information warfare for a number of reasons: they provide softer targets than government or military targets, are unlikely to directly retaliate, often have valuable information assets, and their disruption can have a wider destabilising effect.

Most importantly an information war may not be immediately apparent as such, and may be subject to rapid escalation once it becomes apparent. Information warfare is therefore not a threat that bears only on governments, but also has a bearing on commercial operations and professional practice. By the time that we are thinking about retrospective mitigation, it may already be too late. The risks to business from information warfare are of two kinds: (1) direct attacks on the business aimed at strategical advantage from disrupting a particular company, sector, or form of commercial operation, and (2) indirect consequences of actions not directly targeting the individual business of the immediate commercial environment within which it operates.

Direct attacks can be of any of the forms given above. It may include for example using cyber-attacks on the business infrastructure to generate strategic advantage, such as for example disrupting economic activity through attacks on critical infrastructure such as banks, financial institutions, or even regulatory bodies. Alternatively it may include disinformation or misinformation campaigns designed to disrupt the operation of key businesses or key sectors by undermining trust, such as for example disinformation campaigns aimed to undermine the position of key individuals or key organisations particular those with senior level and infrastructure roles. It may include disinformation that exploits the reputation of an existing company, individual or organisation in order as part of an influence operation, for example spoofing content from a regulatory body. It may include direct manipulation of data to undermine the operation of the business or to achieve some other financial or strategic outcome. These kinds of direct attacks generally fall within the organisation's cyber security policy and practice, and for most large organisations should already be well addressed.

Indirect attacks confront business with contingency planning for a range of potential scenarios following-on from serious disruption of the national infrastructure, including transportation networks, power networks, political stability, regulatory environment, international relations, and so on. For most organisations these kinds of indirect risks are unlikely to fall within the scope of the cyber-security policy and practice, although may be addressed in disaster and recovery planning. While recent instability in the business context resulting from global events such as the Covid-19 pandemic and local events such as Brexit mean that many businesses should be better prepared for dealing with these kinds of indirect effect, the broad-spectrum of disruption that might accompany aggressive action in the information sphere is something that needs addressing. This sections addresses the very real collateral disruption that might arise from acts of information warfare that is principally aimed at disrupting the operation of the state, but that has knock-on effects for business and society.

We can identify some of the key risks to business operations arising from knock-on effects of hostile actions in the information domain:

- **Risks to reputation:** one significant risk that businesses should consider are reputations risks arising from direct or indirect attacks, or from the manipulation of individuals and their actions within the social media sphere. There are a broad spectrum of risks here to consider including from the ways in which an organisation may inadvertently become parts of information, misinformation or disinformation campaigns, the knock-on reputational damage from direct attacks, and the risks of employees sharing or circulating misinformation. Reputational risks can also include risks by association with individuals or organisations perceived to be involved in or targets of information war.

- **Business disruption:** or more direct concern is the potential for information warfare to significant disrupt the context of business operations, including creating market or economic instability, undermining consumer or client trust, and creating practical difficulties in providing or using information services, and in communications. This includes the knock-on effects on international trade, and on supply chains. It may also include disruption to transportation networks or communications networks that make it difficult for employees to effectively work, and disrupt the day-to-day operation of the business.

- **Communications threats:** different kinds of communications networks from the internet to mobile communications have become vital to the ways in which contemporary business operates. This is particularly the case as services have shifted to the cloud, meaning that reliable communications is a business critical issue for many businesses. Unfortunately disrupting communications systems is likely to be one of the most attractive targets for an information warfare campaign, because communications networks are by definition particularly vulnerable to forms of cyber attack.

- **Ransomware attacks:** while we might associate ransomware with criminal rather than state action, ransomware has become an increasing focus on information warfare discussion. This is in part because of the potential to conduct covert attacks masquerading as criminal action, partly because ransomware attacks have the potential to cause significant disruption in their own right, preventing key organisations from exploiting critical information assets, and partly because the information and data obtained during a ransom attack may itself be of value. What differentiates criminal and strategic ransomware attacks is the degree to which organisations are specifically targeted for strategic reasons. The 2027 ransomware attack on the UK National Health Service, which affected over 60 health trusts, indicated just how vulnerable some key state organisations are to this threat.

Information warfare and the information professional

While many of the security issues associated with information warfare might sit more fully within the domain of cybersecurity expertise, the blended nature of information warfare means that information professionals also have a role to play in mitigating the risks. This is particularly in respect of aspects of information warfare that might not feature in a typica cyber-security strategy: misinformation and disinformation campaigns, influence campaigns, attacks on critical infrastructure, and economic disruption. More to the point because an information warfare may feature a coherent blend of traditional cybersecurity attacks and such “softer” tactics, an integrated approach to risk mitigation is necessary. Commercial information professionals are often in a position to understand these wider issues, and act as intermediaries between technical expertise and business management.

There are a number of key areas in which the skills and expertise of business information and knowledge professionals are of direct relevance to planning for and mitigating the threats posed by information warfare:

- **Risk registers:** We tend to think of critical infrastructure in material terms: as the buildings, networks, applications and databases that sustain commercial operation. Nevertheless as information itself have become a more important part of the commercial environment, information sets and information sources can increasingly be considered business-critical assets. Since information warfare may lead to significant and widespread disruption to communications networks, and to access to information resources, a first step in thinking about mitigation is understanding the critical information resources without which business operations cannot operate, and how to protect them from the knock-on effects of an information attack. Because business information professionals often deal with planning and delivering key information resources they are well placed to understand business critical information assets and services.

- **Human risks:** information professionals tend to have good professional insight into information behaviours and the ways in which individuals respond to, use and manage their information environment. As we have seen (Laybats and Tredinnick, 2016; Tredinnick, 2023) information behaviours and information seeking strategies often drive the spread of misinformation and disinformation, and drive indirect threats to business in the information sphere. As a consequence business information and knowledge professionals are well placed to understand and mitigate those risks within specific organisational contexts.

- **User education:** there is a role for information professionals in user education in relation to information literacy, the dangers of misinformation, and employee actions in the workplace, as well as leading on the development of strategies to mitigate and address the consequences of interstate aggression in the information sphere.

- **Monitoring and threat intelligence:** the skills of business librarians and commercial information and knowledge professionals in business research and analytics give them an important role in monitoring the wider context and identifying risks to the business at an early stage.

- **Incident response planning:** business information professionals can play a central role incident response planning, leveraging their expertise in collaboration with IT, cybersecurity, and senior management to develop comprehensive plans that address the specific needs of the organisation in response to threats posed by aggressive actions in the information domain.

More importantly perhaps information professionals tend to have a more human-centred understanding of information and its use within organisational contexts that understands risk less as a matter of cyber-security and more in terms of human behaviours, needs, desires and habits, and the integration of systems and people. Unlike cyberwar, information warfare is not principally a matter of attacks on physical system and networks; the actions associated with information warfare tend to blend cyber-attacks with operations designed to hack human behaviours and sentiments. It is therefore important to go beyond the risks associated with network architecture and distributed computing systems to incorporate the role of humans as a part of risk assessment, planning and mitigation.

Conclusion

This paper has explored the nature of information warfare and the potential for interstate aggression in the information domain to disrupt business processes. While the threat of information warfare remains largely hypothetical, the last decade has demonstrated an increasing tendency for states to act in the information arena, particularly through influence campaigns, but also in terms of cyber-espionage and cybercrime. There is a very real potential for actions of this kind to create significant disruption, and this is something for which commercial organisations should be planning. This paper has argued that because of their expertise in understanding information behaviour, information professionals in the commercial sector have an important role to play in mitigating those risks.

References

- Baezner M, Robin P (2017) *Stuxnet (No. 4)*. ETH Zurich.
- CASSAUWERS Tom (2019) Can artificial intelligence help end fake news? *Horizon: The EU Research and Innovation Magazine* (April). Available at: https://ec.europa.eu/research-and-innovation/en/horizon-magazine/can-artificial-intelligence-help-end-fake-news.
- Denning DER (1999) *Information Warfare and Security*. New York: Addison-Wesley, vol. 4.
- Di Pietro R, Raponi S, Caprolu M, et al. (2021) *New Dimensions of Information Warfare*. Springer International Publishing, 1–4.
- Farwell JP, Rohozinski R (2011) Stuxnet and the Future of Cyber War, *Survival*, 53:1, 23-40.
- Floridi L (1999) *Philosophy and Computing: An Introduction*. New York: Routledge.
- Laybats C, Tredinnick L (2016) Post-Truth, information and emotion. *Business Information Review* 33(4): 204–206.
- Libicki MC (1995) *What Is Information Warfare?* Washington DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 97.
- Lindsay JR (2013) Stuxnet and the limits of cyber warfare. *Security Studies* 22(3): 365–404.

- Lucas E, Pomeranzev P (2016) *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. Washington: The Center for European Policy Analysis, 1–66.
- Milmo D (2022) *Anonymous: The Hacker Collective that Has Declared Cyberwar on Russia*. The Guardian. 27th February 2022, Available at: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia (accessed: 01st August 2023).
- Mouton C (2023) *ChatGPT Is Creating New Risks for National Security*. Available at: https://www.defensenews.com/opinion/2023/07/20/chatgpt-is-creating-new-risks-for-national-security/(accessed: 01 August 2023).
- NATO (2022), Media - (Dis)Information - Security: Information Warfare, North Atlantic Treaty Organisation (NATO), available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf [accessed: 15th August 2023]
- Raska M (2023), North Korea’s evolving cyber strategies and operations: towards weapons of mass effectiveness, in: Snyder SA, Park KA (2023), *North Korea’s Foreign Policy*, London: Rowman and Littlefield.
- Santos FCC (2023) Artificial intelligence in automated detection of disinformation: a thematic analysis. *Journalism and Media* 4(2): 679–687.
- Stein GJ (1995) Information Warfare. *Airpower* 9(1): 30–54.
- Tredinnick L (2023) Dangerous data: analytics and information behaviour in the commercial world. *Business Information Review* 40(1): 10–20.
- Ventre D (2016) *Information Warfare*. John Wiley & Sons.
- Zannettou S, Sirivianos M, Blackburn J, et al. (2019) The web of false information: rumors, fake news, hoaxes, clickbait, and various other shenanigans. *Journal of Data and Information Quality (JDIQ)* 11(3): 1–37.