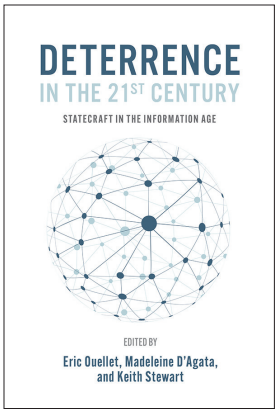
UNIVERSITY OF CALGARY
Press



DETERRENCE IN THE 21ST CENTURY: STATECRAFT IN THE INFORMATION AGE

Edited by Eric Ouellet, Madeleine D'Agata, and Keith Stewart

ISBN 978-1-77385-404-5

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

Conclusion

Keith Stewart and Madeleine D'Agata

Eric Ouellet's introduction to this volume set out a series of essential questions. The chapters that followed provided expert insights that offer a starting point for addressing the critical issues faced. However, we are far from having clear solutions at this point. In soliciting contributions, the net was cast wide, as befits a problem set as challenging as this. The aim was to examine the implications of the changing information environment (IE) for security at all levels, including national security and the security of individuals and organizations. The major theme of the book has been the harnessing of information to achieve strategic influence internationally by a range of actors, both state and non-state, most recently in the context of renewed and overt great power competition, but equally during the period since the fall of the Berlin Wall and particularly in the wake of September 2001. In modern times, the perennial problem of disinformation has resurfaced, promulgated widely using novel media, especially since the development of social media and Web 2.0, and this has been highlighted in the material presented by many of the authors. However, this is not the only challenge posed by the constantly changing nature of the IE, and other critical concerns have been discussed here—for example, the opportunities afforded malign actors to harness cyber means to threaten critical infrastructure and military capability.

Perhaps the most basic question we face is how to achieve security in the face of the challenges posed by adversary action that exploits the IE. This can be considered at a number of levels of analysis; for example, the personal security of individuals and their assets, operations security for military, police, and other security services that must guard essential information, and, ultimately, national security. The diversity of material in this book reflects this. At

the national strategic level, our security has rested, since the end of the Second World War, on the achievement of mutual deterrence based on the threat of massive retaliation with nuclear weapons. Thus, paraphrasing the challenge laid down by Dr. Ouellet in the introductory chapter, it is important to ask to what extent a deterrence-based posture has the potential to maintain security given information-based challenges and threats, and if so, how do deterrence theory and practice need to adapt to this new reality? This line of inquiry led Ouellet to a number of supplementary questions, including the following: Given the salience of the threat posed by adversarial disinformation, to what extent can it be deterred? If so, is it possible to deter disinformation or other information-based threats through the threat of punishment, or is a different approach required? If deterrence is found to be a viable approach, then what do we need to understand about our adversaries in terms of their perception of costs and benefits that might enable us to achieve a deterrence stance? How should Canada and its allies face up to these challenges, and are there any ways in which the West might begin to fight back? Importantly, how can we achieve all of the foregoing and still conform to our own legal and ethical standards without being brought to the level of our adversaries? This volume has provided a diverse set of insights from leading international experts that have a bearing on all of these problems and more. This final chapter presents reflections on some of the above questions based on a selective distillation of some information from the preceding chapters combined with material from other sources with the aim of offering a series of concluding thoughts.

Perspectives on the Challenge of Deterrence in the IE

We have seen that the spread of misinformation and disinformation in the IE has increased dramatically in the past few years around the world, often severely impacting individuals and organizations and causing confusion, panic, and, on occasion, distrust in government (Bennett & Livingston, 2018; Liu & Huang, 2020). Geography offers little protection against this scourge, and Canada and Canadians, among other polities, have been increasingly targeted in recent years. Certain nations have been, and continue to be, at the forefront of the spread of disinformation, impacting elections in the United States as well as more recently propagating falsehoods surrounding COVID-19 (US Department of State, 2020). Not only does such disinformation lead to financial losses—for example, at the time of writing, $7.75 million has been lost to COVID-19 fraud in Canada according to the Canadian Anti-Fraud

Centre (2021)—it also discourages susceptible individuals from following public health guidelines and promotes vaccine hesitancy, potentially, in the end, contributing to the further spread of COVID-19. Moreover, whether we are discussing cyberspace, or the IE more broadly, it is recognized that it is extremely difficult to defend against adversarial activity. In their chapter Leuprecht and Szeman identified several attributes of the IE that present significant challenges. These include its interconnectedness, which enables adversaries to generate effect without concern for geography or political borders, the relatively low costs of entry, and the possibility of engagement in continuous offensive operations. Adaptation of deterrence for the challenges of the IE must take account of these characteristics.

As noted in the chapter by Jackson, despite the importance being placed on deterring the spread of disinformation in Canada from a security and safety standpoint, there is actually little consensus from academia or policy-makers on how exactly Canada should defend itself. As that author points out, part of the problem is a lack of consensus on defining disinformation, which Jackson and others approach as a societal and cultural issue as much as one of security. Disinformation is typically understood to imply the intentional spreading of deliberately false information. This contrasts with misinformation, which implies the unintentional dissemination of similarly false or inaccurate information. Thus, by many definitions, disinformation is meant to intentionally and maliciously mislead others. And yet, it is not always possible to ascertain intention. Jackson stresses that government efforts aimed at attenuating the spread of disinformation need to proceed with caution to ensure they are not perceived as interfering with freedom of speech.

A consistent theme in this book has been the observation that the IE, and specifically the Internet and social media, have substantially increased the potential for adversaries to engage in information operations (IO) against competitor nations, effectively overcoming geographical and territorial boundaries to a variety of ends, including the spreading of false narratives and propaganda, enabling clandestine access to information and networks, and interference with control systems for civilian and military infrastructure. Chapters in this volume have examined the activities of specific competitor nations. For example, the chapters by Heide and by Seaboyer and Jolicoeur focus on Russia and China, respectively, while Bar-Gil examines information activities directed against Israel by Iran and its proxies, as well as examples of Russian IE tactics. This work demonstrates that, in addition to seeking to

catch up with the West in terms of IE capability, the adversary powers considered here have taken the opportunity to adapt technologies to their own preferred methods. For example, Seaboyer and Jolicoeur describe China's policy of "informationalization," which has, in part, enabled the Chinese Communist Party (CCP) to exploit tools, originally conceived of as enabling the free exchange of information, to bound and manipulate the narratives to which Chinese citizens have access.

In a similar vein to Seaboyer and Jolicoeur's comments on China, Heide reminds us that Russia also engages extensively in the IE internally, as well as externally. Heide points out that this contrasts with democratic nations that only conduct IO on operations (in almost all cases abroad). Domestically, both have a specific focus on maintaining the mood and morale of their populations and armed forces by controlling the information and ideas that they can access with a view to avoiding any threat to the authority of the ruling regimes through dissent or uprisings. After a degree of thawing in the late 1980s and '90s, Chinese and Russian authorities are again exerting a high degree of control over the IE of their citizens. While the technologies have changed, the intention is reminiscent of earlier attempts to block access to information from the outside world—for example, Soviet radio jamming operations against Radio Free Europe and Radio Liberty, which broadcast from Munich during the Cold War to provide domestic news to audiences behind the Iron Curtain.[1] Today's equivalent is manifest in the complex system of technological control and enforced censorship that has been dubbed the "Great Firewall of China."[2] Stittmatter (2018) describes the techniques of "intimidation, censorship, and propaganda" that enabled the CCP to take back control of the Internet after a period of relative freedom before 2012. Deletion of social media accounts, blocking of websites, restrictions on the numbers of persons with whom a social media user can share information, and the introduction of fake information, among others, are all cited as techniques through which the CCP was able to fulfil the leader's command to "win back the commanding heights of the internet" (Stittmatter, 2018, p. 70). Similar to the point made by Leuprecht and Szeman regarding the possibilities provided by the IE for engagement in persistent operations, these authors observe that, in their external affairs, both Russia and China appear to adopt a posture of constant conflict, notably in the IE, where they are able, in Lindsay and Gartzke's (2019) terms, to inflict some harm "through cyber exploitation,

covert infiltration, and other 'gray zone' provocations that fall below clear thresholds of . . . retaliation" (p. 15).

Russian operations in the IE are constant and are aimed widely at all sections of the targeted nations, including the military, civil society, and policy-makers. Bar-Gil's chapter describes a struggle for "the global mindset." That author also observes that, compared to some of its adversaries, Israel is at a relative disadvantage owing to the breadth and sophistication of its information infrastructure and, by extension, its dependence on such technology-enabled systems, which leaves it exposed to information and cyber-attacks. This echoes Lindsay and Gartzke's (2019) observation that "It is possible and much feared in some circles, that weaker states and nonstate actors might exploit the technologies of globalization to undermine the conventional military advantages of great powers" (p. 3). In this regard, it is interesting that Bar-Gil notes that access to the IE means that malicious activity that "what was formerly a gradual, professional psychological impact is now a high-speed action that even the least competent, remote, and disassembled forces may conduct due to technological improvements." As Leuprecht and Szeman observed, in the modern IE, the costs of entry are low.

Several authors in this volume point to the use of proxies as part of operations in the IE. Bar-Gil describes how Iran provides capability to its allies Hezbollah and Hamas to enable operations against Israel, and in some cases directs specific cyber operations, thus achieving the benefits of deniability while overcoming the disadvantages of physical dislocation from its target. Heide provides a very comprehensive description of the multitude of proxy channels adopted by Russia in its IO, noting the overt use of third-party organizations such as state media as well as a range of "grey" and "black" means that again confer plausible deniability. Seaboyer and Jolicoeur describe how the CCP exploits various levels of the Chinese and foreign media domestically and externally with a view to controlling its message. In addition, they outline how China is able to expand its technical capability for IO via manipulation of academic and industrial relationships, blurring the lines between civil and military research and development and industrial capacity.

As mentioned previously, the challenges addressed by this volume require consideration at several different levels of analysis. While the foregoing comments relate exclusively to the national strategic level, it would be wrong to ignore the fact that engagement with the IE occurs at the individual level, and thus effort must be expended in understanding the risks associated

with individual actions and the contexts in which individual actors operate. Although the IE can serve as an environment that facilitates positive human interaction, as observed by Ducol et al. (2016), deviant behaviours, attitudes, and beliefs are of great concern and can lead to serious consequences for individuals such as cyber-bullying, cyber-stalking (Hango, 2016), and fraud (Canadian Anti-Fraud Centre, 2021; Johnson, 2019), among others. Research suggests that certain types of individuals are particularly susceptible to being influenced in the IE. For instance, D'Agata and colleague found links between lowered Honesty-Humility (one of the six factors of personality) and greater online disinhibition, engagement in risky online behaviours (D'Agata & Kwantes, 2020), and engagement with strangers online (D'Agata, Kwantes, & Holden, 2021). These are examples of behaviours that can increase not only one's exposure to adversaries and criminals, but also one's susceptibility to oversharing or behaving in unsafe ways online. Peter et al. (2021) found certain individuals, such as younger adults, to be more susceptible to belief in disinformation or conspiracy theories. Furthermore, psychological tendencies or needs seem to be influential in the IE; for instance, as noted in the chapters by Meharg and by Speckhard and Ellenberg, the need to belong or connect with others or establish one's identity can promote engagement with strangers online. Moreover, for some, these needs may be met in the IE more so than in real-world settings. For instance, research has found a link between heightened real-life social isolation as well as social anxiety and increased comfort with or reliance on online communication (e.g., Whaite et al., 2018; Prizant-Passal et al., 2016). Speckhard and Ellenberg found that in extreme cases, such a need can result in individuals being radicalized, leading to even more serious outcomes such as engaging in illegal activity. More concerning, these authors also note that the sophistication extremists and extremist organizations display in the IE is particularly challenging to effectively counter or dispel.

How Should Deterrence Theory Change to Match the Challenges of the IE?

A number of the contributors to this volume have observed that classical models of deterrence require revision to address the realities of the early twenty-first century. As Jackson and Leuprecht and Szeman have all pointed out, to effectively deter in the IE, Canada and its allies must update their deterrence theory and practice. The changes necessitating such a rethink are in large part bound up, as Cimbala and Lowther and Ankersen, for example, have

pointed out, with changes within the IE itself. Ankersen chapter includes the observation that "what has changed are the "operant media through which and with which opponents" communicate, while Cimbala and Lowther note in theirs that "the nuclear-cyber relationship . . . makes deterrence a much more complex task." Nevertheless, material presented in this volume provides some grounds for optimism that the fundamental aspects of deterrence, such as communication, credibility, and risk calculation, are broadly similar today when compared with the immediate post-1945 period, and are likely to remain so with the consequence that deterrence continues as a possibility in the modern era. Stressing the importance of the non-physical elements of deterrence such as credibility and communication, Ankersen states that a "material bias" focused on, for example, weapons systems, has directed attention from the fact that "deterrence actually operates—has always operated—in the information environment." Thus, Ankersen sees contextual change in terms of the means, that is to say the information technology that enables communication between the deterring parties.

Self-knowledge of vulnerability to threat is essential to building preparedness and resilience in anticipation of likely future attacks, as was stressed by Robinson in a paper that emphasized the requirement for "synchronised and systemic" (2019, p. 8) responses to adversary hybrid tactics. Similar to Ankersen, Robinson notes that while many of the threats facing NATO nations are not new, the means that an adversary might employ, such as cyber, are. Thus, Robinson emphasizes the need for deterrence theory and strategies to address such change, and notes that new approaches, including non-kinetic options, have developed with a view to deterring hybrid threats.

Lastly, Ankersen's comments align well with many of the other authors in this volume with regard to the likely benefits of dissuasion through defence in a "deterrence by denial" approach. The framework of cyber threats presented by Ankersen provides a useful means for structuring an integrated defensive posture across all domains and environments, based on an understanding of the various threat categories. Many authors in this volume have stressed the importance of promoting resilience in order to be positioned to engage in deterrence by denial. Jackson's chapter includes the observation that doing so "not only mitigates harmful effects of hostile influence, but also changes adversaries' cost-benefit analyses by denying them (technical or strategic/political) benefits." Jackson adds that such efforts may need to be carried out in coordination with governments, private actors, and civilians.

Deterrence is a form of influence operation in that it seeks to achieve psychological effects in a decision maker with a view to guiding that individual to behave in a certain way. Smith (2005) summed up the basis for all deterrence in noting that, "In short, the real target of someone wishing to deter is the mind of the opposing decision maker" (p. 190). Deterrence theory has seen regular revision in the light of real-world contextual changes, for example, the end of the Cold War. It has also adapted to take account of research that used observational studies to examine the fundamental assumptions of the theory. For example, Jervis (1985) lamented the fact that an examination of case studies demonstrated that "participants almost never have a good understanding of each other's perspective, goals or specific actions. Signals that seem clear to the sender are missed or misinterpreted by the receiver, actions meant to convey one impression often leave quite a different one" (p. 1). Jervis further stated that classical deterrence theory was flawed to the extent that it relied on deductive logic rather than an examination of real-world experience, and that it was "based on the premise that people are highly rational" (p. 1). The aim of Jervis and colleagues (1985) was to strengthen the theory and its application with an improved understanding of, among other things, how, in the real-world, officials and institutions of state process information, how humans make decisions, and the cognitive and other biases that may undermine those processes. Thus, it is to be hoped that adaptation to the realities of the modern IE should represent a continuation of a process of evolution rather than a major transformation.

A very good example of an adaptation of deterrence theory that appears well-suited to the challenges of IE-mediated deterrence was described in Wilner's chapter in the context of counterterrorism. Wilner describes the development of a novel theoretical approach based upon deterrence by de-legitimization that "weighs on an adversary's normative or ideological perspective" with a view to undermining the logic upon which their use of terror tactics is based by "targeting and degrading the ideological motivation that guides support for and participation in terrorism." This raises an important issue—namely, the development of a sound understanding of an adversary (as well as that adversary's supporters and potential supporters) to see how justification for their actions is achieved, and consequently how it might be undermined. Wilner's chapter extends the application of the notion of deterrence by de-legitimization by applying it to the issue of deterrence in the IE, advocating specifically for the establishment of international norms

for actors' behaviour within the IE, for more publicity for breaches of acceptable behaviour, and, lastly, for proactive efforts within society to strengthen shared basic principles with a view to achieving collective resilience. Citing Doorn and Brinkel, Wilner stresses the importance of building and enabling trust and credibility within our societies in order to establish "societal counterweights to malicious propaganda and disinformation campaigns." As noted in Jackson's chapter, Canada's responses to disinformation are broad, and future research is needed to better understand how these responses could be better refined as well as tailored to different situations.

Understanding Adversaries in Order to Deter Them

In their chapter, Cimbala and Lowther note that part of the process of adapting deterrence to the modern strategic environment is a recognition that there is a requirement for "tailored" approaches, based on an in-depth understanding of the specific adversary to be deterred. Ankersen likewise stresses the importance of the development of an improved appreciation of the adversary and, citing Jervis, notes the importance of understanding how potential adversaries view the world in order to understand their behaviour and, ultimately, their intentions. Moreover, Ankersen emphasizes the fundamental psychological nature of deterrence, quoting Filipidou (2020) and Jervis et al. (1985), who refer to it, respectively, as "a state of mind" and "a psychological relationship." Perhaps the essential point in Ankersen's chapter is that, by focusing on the intended effects of adversary action, it should be possible to discern these actors' goals and therefore how they would perceive the likely costs and benefits of their actions. The contention is that the apparent "uniqueness" of cyber, which Ankersen argues is "overstated" and is based on a focus on means and capability, can be bypassed, thereby allowing a more integrated perspective of the threat and enabling a comprehensive view of deterrence that includes cyber. This, according to Ankersen, is essential to deterrence via threat of reprisal, since "without an appreciation for what the intended effects or benefits of an attack are, it is difficult to calibrate the costs necessary to dissuade an opponent from carrying it out."

Cimbala and Lowther point out that nuclear crisis management is "both a competitive and a co-operative endeavour" and emphasize that communication is essential to enable each party to demonstrate its appreciation of a situation to the other. Seen in this way, deterrence is reliant on the development and maintenance of an effective relationship between the parties based

on clear communication. In addition, they underline the importance of each side developing a clear and accurate understanding of their adversary's intentions and capabilities upon which to base risk assessment and course-of-action decision making. These observations align with early iterations of deterrence theory. For example, Schelling (1966) pointed out that "a hot line can help to improvise arms control in a crisis: but there is a more pervasive dialogue about arms control all the time between the US and the Soviet Union. . . . I have in mind . . . the continuous process by which the USSR and the US interpret each other's intentions and convey their own" (p. 264). Cimbala and Lowther's focus is on nuclear crisis management, but these elements are central to all deterrence relationships, whether in a crisis or in a steady state.

In their chapter, Schleifer and Ansbacher provide their perspective on the deterrent relationship between Israel and Hamas. They judge that Hamas has achieved an appropriate appreciation of Israeli decision makers' perception of risk and is therefore managing to deter them by shaping public opinion with respect to the acceptability or otherwise of the probable costs of specific military action. Their chapter provides a series of examples of how, in their opinion, a combination of terror tactics, disinformation, and influencing international opinion has enabled Hamas to achieve this deterrence despite Israel's military advantages.

Importantly, the chapters in section 1 of this volume emphasize the critical element of credibility in deterrence communication. This comprises, at least, the extent to which the party receiving the deterrent message believes that their adversary has both the capability claimed and the intention and will to use that capability in the circumstances specified. This is, in turn, dependent on issues such as the credibility of the source of the deterrent message and the effectiveness of the transmission of that message, neither of which can be assumed. Even heads of state can fall foul of this basic requirement. For example, as Keegan (2005) reminds us, by 2002 Saddam Hussein was "a victim of his own fictions and evasions. Because of his systematic mendacity, he had lost the capacity to persuade anyone that he was telling the truth" (p. 113).

Understanding Situations

More than one author in this volume touched on the critical issue of protagonists' ability to achieve and maintain what Endsley (e.g., 1995) and others have called "situation awareness" and, particularly in the case of Cimbala and Lowther's chapter, the dangers of protagonists not being able to maintain

such an appreciation. The implication is that the increasing speed and complexity of situations mediated in the IE renders the achievement and maintenance of situation awareness extremely difficult and thus increases risk of misdiagnosis, miscalculation, and human error. In particular, they provide several examples of how cyber operations have the potential, deliberately or inadvertently, to skew or undermine an opponent's understanding, as may be the case, for example, through the manipulation of information within an adversary's C4ISR systems, or through disruption of their internal communications, or perhaps through direct interference with the systems controlling the weapons themselves. A critical element of Cimbala and Lowther's argument is that having lost situational awareness, participants could feel increased pressure to take pre-emptive action.

Many of the situational characteristics described by the authors in this volume, and in particular the crisis-management situations discussed by Cimbala and Lowther, such as limited time, situational ambiguity, and changing conditions, are in line with applied settings studied by psychologists interested in "naturalistic decision making" (NDM), notably Klein (e.g., 2008). Their studies of fire commanders, process control operators, surgical teams, and military commanders, to name a few, demonstrated, much as Jervis observed, that, placed in such situations, people tend not to conform to best practices predicted by rational decision theory. Rather, in time-compressed emergency environments, the experts reported using prior experience and knowledge rapidly to categorize the situation and generate as adequate a response as possible in terms of a course of action. Cimbala and Lowther make a similar observation citing the work of March and Simon. Indeed, Simon (e.g., 1978) had, as part of the development of a theory of bounded rationality in the 1950s, dubbed such decision making "satisficing," that is, finding a solution that is satisfactory and sufficient relative to the decision maker's level of aspiration. Cimbala and Lowther quite rightly make the chilling observation that in the context of nuclear crisis management, there is simply no margin for error. In view of the foregoing, there is no suggestion that what has been described is the "best" way to make decisions; rather the implication is that under extreme time pressure, with a need to respond to stay ahead of a dynamic situation, it may be the only possible way to respond within the capacity of human decision makers. One useful conclusion of the NDM work is that in order to promote good decision making, we should focus on optimizing, as much as possible, the conditions under

which decision makers make decisions. Their work strongly suggests that a focus on achievement and maintenance of situational awareness, a high-functioning command team and organization to support the decision maker, and efficient communications and coordination are key. Cimbala and Lowther's work shows us a variety of ways in which cyber means might be used by an adversary to undermine these critical structures and processes. The implication of the NDM research is that, as well as hardening against cyber intrusion, organizations should seek to optimize the decision-making context, for example, through training, improved organizational design, and, if available, decision-support systems.

Cimbala and Lowther point out that currently we can only "speculate about the impact of cyber-attacks and efforts to inject technical disinformation into systems responsible for nuclear crisis management." Nevertheless, their chapter provides a range of scenarios that could be used in modelling, experimentation, and simulation with a view to achieving an improved appreciation of the demands of such situations. Such work could provide the basis for improved preparation and potentially training and education for decision makers and their teams. In addition, such an approach offers some hope that we might achieve some degree of deterrence by denial, hardening our critical systems and augmenting the resilience of our people and organizations with a view to avoiding crisis escalation.

How Can Canada and Its Allies Achieve Increased Resilience?

A number of the chapters in this volume have implications for how states might achieve increased resilience. The IE has been leveraged by criminals and adversaries now for many years in an effort to influence, intimidate, manipulate, and radicalize individuals. Multiple streams of research exist in this domain to better understand what makes individuals vulnerable to others' manipulations in the IE, as well as strategies or techniques that can be employed to reduce the effects of such efforts. Furthermore, understanding the motivations and techniques employed by our adversaries can help in the development of methods to deter such actions in the IE. In addition, as discussed in the chapter by Porter, an examination of the online influence campaigns employed by our adversaries is needed in order to better understand how to build resilience in our own personnel and citizens and to engage in deterrence by denial.

The authors in this volume provide several recommendations for specific interventions to promote resilience, including technological developments to aid identification of adversary IO and hardening of critical civilian and military systems. Bar-Gil and Heide both favour augmenting such tools with a range of non-technical interventions, for example, training and education. Heide proposes that both the general public and the media would benefit from the ability to identify malicious IO more effectively, and Bar-Gil advocates for training military and civilian audiences alike in critical thinking about information, especially that which is presented in social media. In fact, there is a great deal of research, particularly in the field of psychology, that highlights the benefits of critical thinking, such that analytical thinking is associated with lowered belief in disinformation (e.g., Bronstein et al., 2019; D'Agata, Kwantes, Peter, & Vallikanthan, 2021). Heide points out that adversaries benefit from ordinary persons unintentionally spreading their falsehoods as misinformation, and consequently invest time and energy in its creation and dissemination through a broad range of media, both state-sponsored and commercial, for example, TV, radio, and fake accounts on social media platforms. Bar-Gil stresses the potential for limiting the success of such tactics through promotion of "digital literacy," efforts that have been shown to be successful in limiting the spread of false messages. In addition, both authors address the controversial topic of governments restricting access to specific media within their own nations, with Bar-Gil discussing the potential use of specific instruments under Israeli law, and Heide advocating the blocking of access to Western audiences for news outlets spreading propaganda and disinformation and the cutting of funding sources for organizations involved in malicious IO.

With respect to the challenge of developing strong counter-narratives to challenge adversary influence operations and disinformation, we need to address the question of when our strategic communications might be considered equivalent to an adversary's propaganda. Some authors even seem to have attempted to rehabilitate the term "propaganda." Cull (2015) argues that most propaganda is, at base, an attempt to hinder the advance of an opposing idea, and as such could conceivably be considered defensive "counter propaganda." Employing the same term, Taylor (2002) expressed the view that "propaganda"[3] is required "on behalf of . . . peace" (p. 439).

At the tactical level, Cull describes actions to counter a specific message and cites the work of the US Information Agency in identifying and

debunking Soviet disinformation rumours in the 1980s. At the strategic level Cull sees "a communications policy" (2015, p. 3) aimed at adversary propaganda, for example, the US information campaign during the Cold War and British foreign-language broadcasts aimed to counter totalitarian propaganda in the 1930s. Interestingly, Cull also notes that, "In our own time China's large scale spending on cultural outreach and international broadcasting is seen by Beijing as a corrective to the western bias of global media outlets" (p. 3), and as such is, in their eyes, essentially a counter-propaganda exercise. To this we could doubtless add their construction of a "golden shield" containing and protecting "an internet with Chinese characteristics" (Strittmatter, 2018, p. 79) and enabling their near total control of the information that Chinese citizens can access.

How Might Canada and Its Allies Respond?

The chapters by Bar-Gil and Heide present proposals for solutions to achieve deterrence in the face of the threats they describe. As a general point, it is possible to conclude that both authors advocate an approach that can be characterised as "deterrence by denial" based on the achievement of high levels of resilience in the states, institutions, and systems discussed. Moreover, we should also note that in advocating an approach based on proactive strategic communications, Heide is, in parallel, proposing a form of pre-emption in the IE. This, it is suggested, is important to ensure that audiences are presented with "truthful accounts" before being exposed to the adversary's disinformation, which Heide notes may be harder for individuals to discount once internalized.

In order to begin to achieve the necessary resilience, Heide stresses that Canada needs to develop strong narratives tailored to specific audiences that explain "what defines Canada, its beliefs, and its actions." In order to achieve this, Heide proposes that Canada needs a strategic communications capability that is always active in order to deter adversary IO in a pre-emptive fashion. In addition, Heide suggests monitoring and analysis of adversary messaging combined with the development and dissemination of Canadian narratives.

The proposed developments outlined above, as well as others described in detail in the individual chapters, may have the potential to both bolster resilience and harden Western societies against the malign information activities of adversary powers. Nevertheless, in formulating policy and doctrine for such a capability there would be many questions that would need to be addressed,

not least those in the moral and ethical spheres. Indeed, it will be essential to be prepared to address any suggestion that in responding within the IE Western nations could risk constructing a mirror image of the structures and tactics they are seeking to counter. Certainly, the development of information-related capability by government and military in the West is sometimes treated with suspicion by domestic audiences. For example, Galeotti (2017) suggests that strategic communications "could perhaps be glibly described as 'propaganda we like'" (p. 1). Taylor (2002) similarly points out that there is "an entire range of euphemisms" (p. 437) within which we can assume "strategic communications" would figure. Taylor expressed the view that democracies "tend to delude themselves that they are not in the business of propaganda" (p. 437), arguing that it is assessed to consist of untruths and to be conducted only by undemocratic parties. The crux of Taylor's paper was that at that time, as now, "when certain value systems are under attack . . . they . . . need to be defended . . . by a reaffirmation of the values that were being challenged" (p. 440–1). Moreover, Taylor stated the opinion that this should be a job for governments owing to a concern that "the free, democratic media of any country have become an unreliable mirror of the true nature of that society by virtue of the increasingly commercialised environment in which they now operate" (p. 439).

Both Heide and Bar-Gil recommend the development of analytic capability aimed at understanding adversary IO aims and approaches with a view to identifying domestic capability gaps and developing countermeasures. For example, Bar-Gil notes that Internet and social media present opportunities for the collection of relevant open-source intelligence (OSINT), and that such information has the potential to be used to underpin proactive responses. Bar-Gil provides the example of the Bellingcat investigations into the shooting down of Malaysian Airlines Flight 17 over Ukraine. Moreover, Bar-Gil describes how OSINT, based on an adversary's social media presence, has provided the foundations for responses both within the IE and, in a cross-domain response, in physical action.

One area that perhaps received less attention is the notion of cross-domain operations or cross-domain deterrence as a means to respond to, or get ahead of, hostile information activities. Cull, for example, emphasizes that "not all propaganda is best countered in the communications sphere . . . [and that] addressing the source of the propaganda can prove an effective strategy for counter propaganda" (2015, p. 14). Illustrating that, when conducted

by unscrupulous state actors, this can involve drastic and illegal measures, Cull provides the example of the assassination of a Bulgarian journalist by Romanian operatives. Bar-Gil provides examples of the use of physical attack in response to cyber activities noting that these were intended to degrade the adversary's IE capability and simultaneously deliver a deterrent message. Such examples highlight the need for governments to engage in an examination of ethics and proportionality in adopting cross-domain tactics.

With this in mind, democratic nations might do well to ask about the extent to which the proposals put forward by Bar-Gil and Heide require the establishment of completely new capability, or whether what is needed is, in part, the re-establishment of capability that has seen under-investment in recent times. Taylor noted that reductions in US public diplomacy in the 1990s, such as cuts to Voice of America broadcasts to the Middle East, had led to "an information vacuum which was then vacated by the morass of lies, rumours and disinformation generated by its adversaries" (p. 439). In a similar vein, in a 2005 article published on the BBC website announcing cuts to World Service broadcasts in eight languages, including Polish and Hungarian, the head of its Polish-language service was quoted as saying that, while they found the BBC's position on Europe "somewhat optimistic," they acknowledged that central Europe "is not the greatest geopolitical need at the moment" ("BBC East Europe voices silenced," 2005). Clearly, we have the benefit of hindsight in having seen the increasing tensions in central and eastern Europe in recent years and the rise of quasi-authoritarianism in some quarters. The conclusion must be that over time the specific focus of counter-adversary IO will shift, and the capability that we build to support such operations must possess the flexibility needed to address new requirements from time to time. It would seem reasonable to suggest that the chapters in this book have demonstrated enough basic similarities in the techniques employed by a range of potential adversaries that such a capability could be created, although this does not necessarily address the problem that area expertise cannot be created in short order.

The chapters in this book have provided a range of useful recommendations for the enhancement of democratic nations' capacity to operate in the IE that might broadly be characterized as falling into developments in the areas of analytic capability and proactive information capabilities. It should be advantageous to such efforts that similar capability has existed in the past and that lessons learned from the experience of the twentieth century are

available. The exception might well be, as Ankersen notes, the substantial changes in the media, systems, and organizations that constitute the modern IE. The arms race in communications and information technology is unlikely to slow soon, and it is clearly the case that it will be those nations that can adapt to the new environment and harness the opportunities presented to achieve their strategic goals that will come out on top in the information battle.

Leuprecht and Szeman propose that Canada may not have sufficient resources to carry out "persistent engagement" and should instead look to partner with the United States. Jackson notes that Canada's "attempts to deter strategic disinformation have included accelerated efforts to strengthen cyber defence and resilience and to develop legislation and norms to hamper disinformation efforts, especially during elections. More generally, there have been efforts to increase co-operation and to share more information (about disinformation) to 'deny' actors (further) access at the domestic and international levels."

Final Thoughts

This volume has covered a very wide range of topics in an attempt to conduct a preliminary examination of the risk presented by adversary activities in the IE and methods through which democratic nations might respond. We have seen a general consensus that the IE has rendered geographic boundaries less relevant to malign actors who are able to exploit connectivity to conduct operations against the West. Our networked environment also affords these adversaries the opportunity to achieve their strategic intentions incrementally and without crossing the threshold that would trigger a more robust response. The implication is that there is also asymmetry in acceptability of methods. The West is rightly much less ready to use methods that would be considered illegal and unethical to achieve its aims. Thus, we are assailed by a constant barrage of disinformation that has the potential to decay the credibility and trust citizens have in the essential institutions of state and society. Meanwhile the same capabilities are targeted internally at the populations of nations like China and North Korea by governments who simultaneously exert near total control over the information their people can access.

A challenge facing defence departments in the IE is ensuring that operations are targeted toward our adversaries as well ensuring no harm comes to domestic populations in the process. The IE allows for individuals and

groups to disguise their true identities when operating online, making it more difficult to identify who they are, and to prevent them from continuing to engage in nefarious activities against our armed forces and citizens. In addition, it is extremely difficult to fully measure the scope and depth of targeted online campaigns. As discussed by Porter and colleagues, techniques aimed at assessing attitudes indirectly offer one approach to help quantify the scope and depth, however, more sophisticated techniques, perhaps based on cutting-edge technologies such as machine learning, may be needed. A challenge facing defence analysts and researchers in particular is an inability to directly study and understand our adversaries. As discussed in the chapter by Speckhard and Ellenberg, work on defectors can be enlightening, but it is not sufficient in its own right. Continued work in this area focused on creative ways to assess and understand adversaries and their campaigns is needed.

Research aimed at identifying vulnerabilities in individuals to being influenced and/or radicalized online can be key to the development of strategies and techniques to help reduce such vulnerabilities. Moreover, such work can help promote resilience in our own personnel and citizens by identifying approaches to help individuals more thoroughly consider and examine information online before behaving hastily. In addition, research in this domain has the potential to inform areas such as public affairs as to the types of messaging that could be effective at promoting resilience against influence and disinformation in the IE. Finally, as mentioned, evaluating the effectiveness of adversary online campaigns might help identify means to deter similar campaigns in the future. More research in the area of deterrence in the IE is needed. Moreover, a move toward a more integrated approach with other areas of government may be needed in order to better capture the effects, scope, and depth of our adversaries' actions in the IE, in an effort to deter attacks in the future.

A repeated theme in this volume has been a recognition that if potential adversaries are able to sidestep our attempts to deter their activities through threat of reprisal, then we need to expand our repertoire of deterrence methods to achieve deterrence by denial. A variety of proposals have been made throughout the book that, when taken in aggregate, amount to the beginnings of a recipe for how Canada and its allies can begin to reinforce the essential resilience of our societies and state institutions built up over hundreds of years, and in so doing, face up to the new authoritarian regimes that seek to undermine us. For example, training of military personnel and education

for the general population is required to enable them to navigate the IE safely and securely; training and simulation will help our civil and military crisis responders and decision makers respond in the face of adversary escalation; increased understanding of adversaries will offer the capacity to anticipate their stratagems, achieve early warning, and counter their propaganda; and an improved understanding of the structure of their ideology will enable de-legitimization in the eyes of their own populations and the wider world. Perhaps most importantly, there is the undercurrent of a confidence that the West has prevailed in the past in the face of opposing narratives and that it can do so again by building an information infrastructure to counter adversary narrative and present a strong alternative.

NOTES

1 These stations were particularly threatening to the Soviet authorities since they attempted to provide news about events in the targeted nations based on local sources (e.g., Kind-Kovács, 2013).

2 For example, Strittmatter (2018) observes that "China's attempt to censor the web, as the former US president Bill Clinton joked, was like 'trying to nail Jell-O to the wall.' That was in the year 2000. The Chinese listened to the prophecy, and swiftly built a new great wall: the Great Firewall" (p. 61).

3 It might be argued that, in part, Taylor's paper is an attempt to rehabilitate the term "propaganda," which, it is argued, is essential in defence of democratic values—in Taylor's terms, "democratic propaganda."

REFERENCES

BBC East Europe voices silenced. (2005, 21 December). *BBC News*. http://news.bbc.co.uk/2/hi/europe/4550102.stm

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication, 33*(2), 122–39. https://doi.org/10.1177/0267323118760317

Bronstein, M. V., Pennycook, G., Bear, A., Rand, D. G., & Cannon, T. D. (2019). Belief in fake news is associated with delusionality, dogmatism, religious fundamentalism, and reduced analytic thinking. *Journal of Applied Research in Memory and Cognition, 8*(1), 108–17.

Canadian Anti-Fraud Centre. (2021). Homepage. https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Cull, N. J. (2015). *Counter propaganda: Cases from US Public diplomacy and beyond*. Legatum Institute.

D'Agata, M. T., & Kwantes, P. J. (2020). Personality factors predicting disinhibited and risky online behaviors. *Journal of Individual Differences, 41*(4), 199–206. https://doi.org/10.1027/1614-0001/a000321

D'Agata, M. T., Kwantes, P. J., & Holden, R. R. (2021). Psychological factors related to self-disclosure and relationship formation in the online environment. *Personal Relationships, 28*(2), 230–50. https://doi.org/10.1111/pere.12361

D'Agata, M., Kwantes, P., Peter, E., & Vallikanthan, J. (2021). Testing tactics to reduce belief in fake news in a North American sample. Defence Research and Development Canada, Scientific Letter, DRDC-RDDC-2021-L338.

Ducol, B., Bouchard, M., Davies, G., Ouellet, M., & Neudecker, C. (2016). *Assessment of the state of knowledge: Connections between research on the social psychology of the Internet and violent extremism*. TSAS: The Canadian Network for Research on Terrorism, Security, and Society.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors,* 37(1), 32–64. https://doi.org/10.1518/001872095779049543

Hango, D. W. (2016). Cyberbullying and cyberstalking among Internet users aged 15 to 29 in Canada. *Insights on Canadian Society.* Statistics Canada. https://www150.statcan.gc.ca/n1/pub/75-006-x/2016001/article/14693-eng.htm

Galeotti, M. (2017, 22 February). "Propaganda needs to be clever, smart and efficient," but Russian army's "information troops" are not just propagandists. *In Moscow's Shadows*. https://inmoscowsshadows.wordpress.com/2017/02/22/propaganda-needs-to-be-clever-smart-and-efficient-but-russian-armys-information-troops-are-not-just-propagandists/

Jervis, R. (1985). Introduction: Approach and assumptions. In Jervis, R., Lebow, R., & Stein, J. (Eds.), *Psychology and deterrence* (pp. 1–12). Johns Hopkins University Press.

Jervis, R., Lebow, R., & Stein, J. (1985). *Psychology and deterrence.* Johns Hopkins University Press.

Johnson, E. (2019, 20 January). TD Bank should have seen "red flags" as senior lost $732 K in romance scam, son says. *CBC News*. https://www.cbc.ca/news/canada/toronto/senior-wires-life-savings-through-td-bank-in-romance-scam-1.4980649

Keegan, J. (2005). *The Iraq War.* Vintage.

Kind-Kovács, F. (2013). Voices, letters, and literature through the Iron Curtain: exiles and the (trans)mission of radio in the Cold War. *Cold War History*, 13(2), 193–219. https://doi.org/10.1080/14682745.2012.746666

Klein, G. (2008). Naturalistic decision making. *Human Factors, 50*(3), 456–60. https://journals.sagepub.com/doi/pdf/10.1518/001872008X288385?casa_token=RHLPXO5oURYAAAAA:f5s9qqlfAsbEmNT9_VD33eWJIXiQGvQjqm2wHeQyTDBorN_yqFCtKRvAFwOf_ywzzs00pB5mm8q4iw

Lindsay, J. R. & Gartske, E. (2019). Introduction: Cross-domain deterrence, from practice to theory. In E. Gartzke & J. R. Lindsay (Eds.), *Cross-domain deterrence: Strategy in an era of complexity* (pp. 1–25). Oxford University Press.

Liu, P. L., & Huang, L. V. (2020). Digital disinformation about COVID-19 and the third-person effect: Examining the channel differences and negative emotional outcomes. *Cyberpsychology, Behavior, and Social Networking, 23*(11), 789–93. https://doi.org/10.1089/cyber.2020.0363

March, J. G., & Simon, H. A. (1958). *Organizations*. John Wiley and Sons.

Peter, E., D'Agata, M., Kwantes, P., & Vallikanthan, J. (2021). *Individual differences in susceptibility to disinformation*. Scientific Report, DRDC-RDDC-2021-R114. Defence Research and Development Canada.

Prizant-Passal, S., Shechner, T., & Aderka, I. M. (2016). Social anxiety and Internet use—a meta-analysis: What do we know? What are we missing? *Computers in Human Behavior, 62*, 221–9. https://doi.org/10.1016/j.chb.2016.04.003

Robinson, E. (2019). *Hybrid warfare and modern deterrence theory.* Scientific Letter, DRDC-RDDC-2019-L184. Defence Research and Development Canada.

Schelling, T. C. (1966). *Arms and influence.* Yale University Press.

Simon, H. A. (1978, 8 December). *Rational decision-making in business organizations*. Nobel Memorial Lecture. http://www.nobelprize.org/uploads/2018/06/simon-lecture

Smith, R. (2005). *The utility of force: The art of war in the modern world.* Allen Lane.

Strittmatter, K (2018). *We have been harmonized: Life in China's surveillance state.* Custom House.

Taylor, P.M. (2002). Strategic communications or democratic propaganda? *Journalism Studies, 3*(3), 437–41. https://doi.org/10.1080/14616700220145641

US Department of State. (2020). *GEC special report: Pillars of Russia's disinformation and propaganda ecosystem*. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

Whaite, E. O., Shensa, A., Sidani, J. E., Colditz, J. B., & Primack, B. A. (2018). Social media use, personality characteristics, and social isolation among young adults in the United States. *Personality and Individual Differences, 124*, 45–50. https://doi.org/10.1016/j.paid.2017.10.030

Afterword

What does the future hold for us as it relates to deterrence and disinformation? Surely not clarity and certainty. The world shall continue to be VUCA (volatile, uncertain, chaotic, and ambiguous) as it has always been since humans have started to organize themselves in social groups. One could argue that the world is VUCA because it describes the human condition, i.e., our capacity and need to "gossip" as the most social animal on earth, as well as our predispositions to perceive threats coming from others we don't necessarily know or understand. I'm sure that in the year 166, Marcus Aurelius would have found the world very VUCA while battling a pandemic, insurgencies, constant wars, and instability on the borders of the Roman Empire. The world is VUCA because we can't predict the future nor control or predict human behaviour.

One could think that highly sophisticated modern communication systems could dissipate these frictions and ambiguities. As many experts rightly pointed out, the advances in communication technologies and social media have added additional layers of complexity to human interactions where anyone can reach wide audiences instantaneously without having the correct information at the source. In other words, *anything goes*, and it goes fast. In the international security environment and international relations disciplines we should therefore expect a real challenge in terms of deterring threats and disinformation. And this will not go away anytime soon.

I could offer that framing disinformation in the context of others (adversaries, competitors, and allies) may be useful in the sense that disinformation to us may represent the reality or the truth for others. In my view, this scenario is even more dangerous, as fighting deeply engrained beliefs is more complex than merely associating disinformation with spreading lies. As such, we could argue that the invasion of Ukraine has been in the works for many years as the West consistently ignored Putin's sense of threat coming from a NATO on its continued expansion course to the East since 1999. And the same could be said for China. To qualify Russia's action as barbaric and

unnecessary in the twenty-first century is not helpful. In a VUCA world, we should expect the unexpected. Although we know we have no ill intent or plans to threaten Russia and China, these state leaders *feel* threatened and their rhetoric, behaviours, and information campaigns reflect just that.

Although deterrence consists in a wide range and combination of different scalable means, maybe it starts with establishing trust, one conversation at a time in the back rooms of diplomacy walking in with our eyes wide open. Establishing trust could mean taking seriously others' sense of feeling threatened. Simply put, maybe deterrence starts by proactively treating our adversaries, competitors, and allies with respect. Especially when we disagree. We should not underestimate the disarming long-term effects of honesty, transparency, and coherent comprehensive approaches.

Lieutenant-General Jennie Carignan,
Chief of Professional Conduct and Culture
7 June 2022

Postface

In the early hours of 7 October 2023, the terrorist organization Hamas launched a massive and surprise multi-pronged attack against Israel, resulting in the murder of more than 1,200 Israeli citizens, most of them civilians. This attack was also marked by numerous acts of extreme brutality by the Hamas attackers, including the murder of children and babies, rape, torture, body desecration, and burning captives alive. The Hamas terrorists' exactions were very similar in scope and cruelty to those of the Islamic State. As of this writing, Israel has launched a massive air and land operation to defeat Hamas into Gaza and has mobilized an unprecedented number of reservists. Hamas-related agencies are claiming that there have been over 11,000 casualties among the Palestinians. It is not yet known if the conflict between Israel and Hamas will escalate to involve other actors, nor how long the military operations in Gaza will last.

The chapter by Ron Schleifer and Yair Ansbacher was written before these horrible and tragic events, but it was to some degree predictive. There is no doubt that Israel was deceived by its adversary and indeed self-deterred in taking decisive actions against Hamas prior to 7 October 2023. This weaker self-imposed deterrence posture may have also, at a more unconscious level, contributed to the Israeli intelligence failures and Israel's political authorities' lack of attention to warning signs received. Furthermore, as Schleifer and Ansbacher noted, Hamas had developed a quasi-air force and navy, and it made the most of them in its murderous rampage.

On the more specific topic of disinformation, although Hamas did try to muddy the waters about the cruelty of its actions, it does not seem to have worked. Many supporters of Hamas and critics of Israel in the Western world have either changed their views or remained silent. Most Arab states have taken a moderate tone, and only a handful have celebrated Hamas' exactions, mostly Iran and its proxies such as Syria and Hezbollah. Israel has been quite effective in showing the world the actual cruelty of Hamas and in preventing Hamas disinformation to flourish. As it has been the case in all

conflicts involving Israel since military operations in Lebanon in the 1980s, international public pressures and contested press coverage are now influencing the potential scope of Israeli operations. However, in a most cynical way, Hamas, by copying the example of the Islamic State, has changed the disinformation and deterrence context against itself. As the authors noted, "So far, Hamas has been successful in maintaining the psychological and informational notion that invading and permanently occupying the Gaza Strip is an unthinkable option." This is no more the case.

—Eric Ouellet

LIST OF ABBREVIATIONS

AAA	Actor and audience analysis
AIDS	Acquired immunodeficiency syndrome
AMP	Affect-misattribution procedure
APA	American Psychological Association
ASEAN	Association of Southeast Asian Nations
AUM	Anxiety/uncertainty management theory
BBC	British Broadcasting Corporation
BMD	Ballistic missile defense
CAF	Canadian Armed Forces
CCP	Chinese Communist Party
CDC	Centers for Disease Control and Prevention
C4ISR	Command, control, communications, computers, intelligence, surveillance, and reconnaissance
CIA	Central Intelligence Agency
CIDB	Canadian Incidents Database
CNO	Computer network operations
COGAT	Coordinator of Government Activities in the Territories (Israel)
COTS	Commercial off-the-shelf
CPD	Central Propaganda Department (People's Republic of China)
CPI	Cyber Power Index
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DCCC	Democratic Congressional Campaign Committee
DDOS	Distributed denial of service
D5	Degrade, deny, disrupt, destroy, deceive
DND	Department of National Defence
DOD	Department of Defense
DRDC	Defence Research and Development Canada

EC	Error choice
EFP	Enhanced Forward Presence (NATO)
EP	Evaluative priming
EU	European Union
EW	Electronic warfare
FBI	Federal Bureau of Investigation
5G	Fifth-generation telecommunications network
FSB	Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii (Federal Security Service; Russian internal security agency)
FTF	Foreign terrorist fighters
G7	Group of Seven
G20	Group of Twenty
GAC	Global Affairs Canada
GGE	Group of Governmental Experts
GRM	Gaza Reconstruction Mechanism
GRU	Glavnoye Razvedyvatelnoye Upravlenie (Main Intelligence Directorate; Soviet and Russian military intelligence)
HIV	Human immunodeficiency virus
IAF	Israeli Air Force
IAT	Implicit association task
ICC	International Criminal Court
ICS/SCADA	Industrial control systems/supervisory control and data acquisition
IDF	Israel Defense Forces
IE	Information environment
IHL	International humanitarian law
Incel	Involuntary celibate
IO	Information operation
IR	International relations
IRA	Internet Research Agency
IRB	Institutional Review Board
ISIS	Islamic State of Iraq and Syria
IT	Information technology
ITW/AA	Integrated tactical warning and attack assessment
IW	Information warfare

KGB	Komitet Gosudarstvennoy Bezopasnosti (Committee for State Security; Soviet internal security and foreign intelligence agency)
LET	Lost email technique
LLT	Lost letter technique
LW	Legal warfare
MAD	Mutually assured destruction
MIIT	Ministry of Industry and Information Technology (People's Republic of China)
NATO	North Atlantic Treaty Organization
NCSA	National Cyber Security Authority (Israel)
NC3	Nuclear command, control, and communication
NDM	Naturalistic decision making
NIS	New Israeli shekel
NIST	National Institute of Standards
OAS	Organization of American States
ODNI	Office of the Director of National Intelligence
OSCE	Organization for Security and Cooperation in Europe
OSINT	Open-source intelligence
OST	Ontological security theory
PGS	Prompt global strike
PLA	People's Liberation Army (People's Republic of China)
PRC	People's Republic of China
PRC	Popular Resistance Committees (Gaza)
PSYOPS	Psychological operations
QR	Quick response
R&D	Research and development
RCMP	Royal Canadian Mounted Police
RPG	Rocket-propelled grenade
RRM	Rapid response mechanism
RT	Russian state-controlled media organization (formerly known as Russia Today)
SCO	Shanghai Cooperation Organisation
SDF	Syrian Democratic Forces
SIOP	Single integrated operational plan

SITE	Security and Intelligence Threats to Elections
SSF	Strategic Support Force
SSHRC	Social Science and Humanities Research Council
START	Strategic Arms Reduction Treaty
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
USCYBERCOM	United States Cyber Command
VPN	Virtual private network
VTS	Voice of the Strait
VTSM	Violent transnational social movements
VUCA	Volatile, uncertain, chaotic, and ambiguous
WHO	World Health Organization
WMD	Weapons of mass destruction

About the Authors

Christopher Ankersen is a clinical professor of global affairs at New York University's Center for Global Affairs, where he leads the global risk specialization. Prior to joining NYU in 2017, Dr. Ankersen worked at the United Nations; was a consultant to businesses, governments, and militaries; and served as an officer in the Canadian Armed Forces with Princess Patricia's Canadian Light Infantry, deploying on missions with the UN and NATO. Christopher Ankersen holds a BA (hons) in international politics and history from Royal Roads Military College (Canada) and an MSc and PhD in international relations from the London School of Economics and Political Science.

Yair Ansbacher has been serving in the IDF's Special Operations Forces for two decades. He is a senior research associate for defence at the Kohelet Policy Forum in Israel. A postgraduate student at Bar-Ilan University, Mr. Ansbacher's doctoral thesis is on the impact of SOF on the modern battlefield.

Stephen J. Cimbala is distinguished professor of political science, Penn State Brandywine, an American Studies Faculty member, and is the author of numerous books and articles in the fields of international security studies, defence policy, nuclear weapons and arms control, and intelligence. He received bis BA in journalism from Penn State University in 1965. Steve received an MA and PhD (1969) in political science from the University of Wisconsin, Madison. He serves on the editorial boards of various professional journals, has consulted for a number of government agencies and defence contractors, and is frequently quoted in the media on national security topics.

Maddie D'Agata received her PhD in social-personality psychology from Queen's University in 2017 and has been employed by the Department of National Defence since 2016. From 2017 to 2022, she was a defence scientist in the Intelligence, Influence, and Collaboration Section at Defence Research and Development Canada's Toronto Research Centre. She conducted research

in two main areas: mental health and influence activities. Her work on influence activities was focused on identifying what makes individuals susceptible to being influenced within the cyber context. She is now responsible for leading a team that enables the broadened awareness and communication of DND/CAF's evidence-based research findings on conduct and culture such that they are actionable by decision makers and senior leadership.

Molly Ellenberg is a research fellow at the International Center for the Study of Violent Extremism. Molly is a doctoral student in social psychology at the University of Maryland. She holds an MA in forensic psychology from the George Washington University and a BS in psychology with a specialization in clinical psychology from UC San Diego. Her research focuses on radicalization to and de-radicalization from militant jihadist and white supremacist violent extremism, the quest for significance, and intolerance of uncertainty. Molly has presented original research at NATO Advanced Research Workshops and Advanced Training Courses, the International Summit on Violence, Abuse, and Trauma, the GCTC International Counter Terrorism Conference, UC San Diego Research Conferences, and for security professionals in the European Union.

Leandre R. Fabrigar is a professor of psychology at Queen's University in Kingston, Ontario. He has co-authored more than 110 publications. Most of his publications fall within the domain of the psychology of attitudes and persuasion or within the domain of research methodology. Dr. Fabrigar's research has appeared in a number of journals, including the *Journal of Personality and Social Psychology*, the *Personality and Social Psychology Bulletin*, the *Journal of Experimental Social Psychology*, the *Personality and Social Psychology Review*, *Psychological Science*, the *Psychological Bulletin*, and *Psychological Methods*. He has been elected to membership in the Society of Multivariate Experimental Psychology and is a fellow of the Society for Experimental Social Psychology, the Society for Personality and Social Psychology, the Association for Psychological Science, and the Midwestern Psychological Association. Dr. Fabrigar has served as an associate editor for the *Journal of Experimental Social Psychology* and as co-editor for the *Personality and Social Psychology Bulletin*.

Rachel Lea Heide works for Canada's Department of National Defence as a defence scientist/strategic analyst in Defence Research and Development Canada's Centre for Operational Research and Analysis. Foci include space, pilot shortages, peace support operations, capacity building, information operations, humanitarian assistance and disaster relief, future security trends, concept development, war gaming, terrorism and counter-insurgency, and war diary research. Dr. Heide is also an air force historian, specializing in the period from 1916 to 1946. She has researched air force organization, training, leadership, morale, professionalization, mutinies, accident investigation, and government policy. She has also instructed distance learning courses in Canadian history and Canadian military history for Algonquin College, the Canadian Forces College, and the Royal Military College.

Nicole J. Jackson is associate professor at the School for International Studies, Simon Fraser University, Vancouver. She teaches and researches in the areas of security studies and foreign policy analysis, concentrating in particular on Russia and Central Asia. Her first book, *Russian Foreign Policy and the CIS: Theories, Debates and Actions*, examined Russian ideas and debates over military involvement in Georgia, Moldova, and Tajikistan. Most of her research focuses on Russia's involvement in the post-Soviet space, including the securitization of trafficking in Central Asia, Russia's policies toward Central Asia, and Russia's involvement in regional organizations. More recently she has written on Russia's approach to outer space and NATO and Canadian approaches to hybrid threats and disinformation. She is currently writing on countering disinformation in the context of the Russia-Ukraine war, as well as a comparative analysis of Russia's military involvement in the former Soviet space.

Pierre Jolicoeur is full professor in the Department of Political Science at Royal Military College of Canada. Specialist of the former Soviet Union and southeastern Europe, his research focuses on secessionist movements, foreign policy, federalism, and cyber security. At RMCC, he teaches international relations and comparative politics. Through NATO programs, he also taught in Moldova and in the former Yugoslav Republic of Macedonia. Author or co-author of 2 books, 10 articles in peer-reviewed journals, 23 book chapters, his publications, in both French and English, have appeared in *Études internationales*, the *Journal of Borderland Studies*, the *Canadian Journal of*

Foreign Policy, and *Connections*. He has also contributed to the public debate, notably by publishing 29 articles in the *Point de mire* series, which he edited between 2000 and 2006, contributing 20 op-eds (*Le Devoir*, *La Presse*, *Whig Standard*), and giving numerous interviews. He has been the RMCC representative to the Canadian Federation for the Humanities and Social Sciences since 2011.

Christian Leuprecht is a Class of 1965 Distinguished Professor in Leadership, Department of Political Science and Economics, Royal Military College, editor-in-chief of the *Canadian Military Journal*, director of the Institute of Intergovernmental Relations in the School of Policy Studies at Queen's University, senior fellow at the Macdonald Laurier Institute, and adjunct research professor in the Australian Graduate School of Policing and Security, Charles Sturt University.

Adam Lowther is director of Strategic Deterrence Programs at the National Strategic Research Institute at the University of Nebraska, US Strategic Command's university-affiliated research centre. He holds a PhD in political science from the University of Alabama. Adam previously taught at the US Army's School of Advanced Military Studies. He also served as the founding director of the School of Advanced Nuclear Deterrence Studies, Kirtland AFB. Dr. Lowther was also the director of the Center for Academic and Professional Journals at the Air Force Research Institute (AFRI), Maxwell AFB. Prior to assuming this position, Adam was a research professor at AFRI, where he led and participated in a number of studies directed by the chief of staff of the air force. Early in his career, Dr. Lowther served in the US Navy aboard the USS *Ramage* (DDG-61). He also served at CINCUSNAVEUR-London and with NMCB 17.

Sara Meharg is a global authority on the economic, cultural, and security reconstruction of post-disaster and post-conflict environments. Dr. Meharg is assistant professor at the Canadian Forces College and is the recent recipient of the prestigious Top Women in Defence and Security 2020 award. She is a recognized expert in managing the competing interests of defence, diplomacy, and development stakeholders in post-disaster and post-conflict planning. Dr. Meharg has extensive teaching experience at the undergraduate and graduate levels, and of note, with more than 1,100 senior military officers and civil servants, in institutional, operational, and cross-cultural contexts

across national and international settings. She holds a bachelor of landscape architecture from the University of Guelph, a master of arts in war studies from the Royal Military College of Canada, and a PhD in cultural geography from Queen's University, where she studied the intentional destruction of cultural heritage sites during contemporary armed warfare. Dr. Meharg has served as a research fellow with organizations such as the Centre for Security and Defence Studies, the Canadian Global Affairs Institute, and the Security and Defence Forum.

Eric Ouellet is full professor of leadership, command, and management with the Department of Defence Studies at the Royal Military College of Canada as well as the Canadian Forces College (CFC). He is currently the academic lead for the Centre for National Security Studies, located at CFC. He holds bachelor's and master's degrees from Université Laval, Quebec City, and a PhD from York University, Toronto. His academic research and publications cover issues such as disinformation, institutional analysis and theory, organizational theory, counter-insurgency, military adaptation to irregular warfare, post-heroic warfare, special operation forces, defence planning, terrorist organizations, military sociology, and anomalous aerial phenomena. He is member of the international board of the Inter-University Seminar on Armed Forces and Society.

Ronald D. Porter (Major, Ret.) has developed expertise in attitude measurement and personnel selection in both academic and applied collaborations. He has published in the areas of attitude measurement, exploratory factor analysis, and personnel selection. Presently, Dr. Porter is an adjunct professor at Queen's University. Previously, he served in the Canadian Forces, where he developed an officer-selection process and validated several selection instruments as a member of the CF Human Resources research unit before being posted to the Royal Military College (RMC) as an assistant professor. At RMC, Dr. Porter conducted research in army culture, instrument psychometric assessment, and psychological operations. His academic experience also includes appointments as an associate professor at St. Mary's University and a senior lecturer at York St. John University in the United Kingdom.

Ron Schleifer is a senior lecturer at the School of Communication of Ariel University of Samaria, Israel, and is a renowned authority on psychological warfare. His books and articles deal with psychological warfare and the Arab-Israeli Conflict. He taught at the IDF Command College, and lectures and trains defence organizations on issues of information warfare both in Israel and abroad.

Anthony Seaboyer is director of the Centre for Security, Armed Forces and Society at the Royal Military College of Canada, where he teaches political science, political philosophy, and political geography. He is a senior lecturer at the Peace Support Training Centre teaching adversary information exploitation and information weaponization. At the Centre for Philosophy and AI Research of the Friedrich-Alexander Universität, he researches the effects of government AI exploitation for influence operations. He is a regular guest commentator on national security for CTV News Channel and a contracted national security commentator for the CBC News Network. His research focuses on national security regarding information warfare, AI for influence operations, social influence, psychological warfare, persuasion, social media exploitation, armed non-state actors, as well as the effects of the weaponization of information and AI on democracies.

Minqian Shen is a PhD candidate at Queen's University. He works in the Attitudes and Persuasion Lab under Dr. Leandre Fabrigar. His research focuses on attitude structure, the role of vocal properties in persuasion, and attitude measurement. Minqian holds a bachelor of science with a specialization in psychology from the University of Toronto and a master's of science in social psychology from Queen's University. His master's thesis focused on the structure and sequencing of information and its effects on persuasion. He is interested in the application of social psychology theory to practical domains of society and industry. Minqian's other interests include teaching, having taught statistics courses at Saint Lawrence College.

Anne Speckhard, PhD, is director of the International Center for the Study of Violent Extremism. She serves as adjunct associate professor of psychiatry at Georgetown University School of Medicine and an affiliate in the Center for Security Studies, Georgetown University. She has interviewed over 800 terrorists and violent extremists, as well as their family members and supporters around the world, including in western Europe, the Balkans, Central

Asia, the former Soviet Union, and the Middle East. Over the past five years, she has conducted in-depth psychological interviews with 273 ISIS defectors, returnees, and prisoners, and 16 al Shabaab cadres (as well as family members and ideologues,) studying their trajectories into and out of terrorism, and their experiences inside ISIS and al Shabaab.

Keith Stewart works at Defence Research and Development Canada's Toronto Research Centre. In a thirty-year career that has included periods in private industry and government service, he has focused on human-centric research issues, including influence operations, human elements of military command, and human error in high-hazard environments. He has worked previously on theoretical analysis of command approach, an examination of non-technical interoperability in the command and control of multinational forces, and an investigation of organizational structures in net-enabled organizations.

Joseph Szeman is a political studies and history graduate of Queen's University at Kingston, where he has conducted research on the strategic culture of middle powers, cyber operations, and deterrence and coercion in cyberspace.

Alex Wilner is an associate professor at the Norman Paterson School of International Affairs, Carleton University, Canada. His research explores the nexus between deterrence and emerging security considerations and domains. His books include *Deterrence by Denial* (co-edited with Andreas Wenger, Cambria Press, 2021), *Deterring Rational Fanatics* (University of Pennsylvania Press, 2015), and *Deterring Terrorism* (co-edited with Andreas Wenger, Stanford University Press, 2012). His articles have been published in top-ranked journals, including *International Security*, the *Journal of Strategic Studies*, and *Security Studies*. His scholarship has been awarded nearly $2 million in funding, including a SSHRC Insight Development Grant (2016–17), a SSHRC Insight Grant (2020–5), and a Government of Ontario Early Researcher Award (2021–6) for his cyber-deterrence project; two IDEaS grants (2018–21) and several Department of National Defence MINDS grants (2019, 2020) in support of his AI-deterrence project; and a major Mitacs grant (2020–2) and MINDS Collaborative Network grant to explore Canadian defence and emerging technology.

INDEX

Note to reader:
Names using the definite article *al* are indexed under the subsequent letter in the term, e.g. al Qaeda appears under Q, not A.
t denotes an in-text table.

Able Archer (1983), 55
Abu Ali Express (blogger), 174
Abu Ibrahim. *See* al Qaisi, Zuhir
action, pre-emptive, 25, 50, 57, 106, 108, 155, 202, 253, 255–57, 259, 337, 340. *See also* information environment
active measures, 3, 12, 85, 163, 165–66. *See also* KGB; Russia, information operations of
Agardh-Twetman, Henrik, 72
Ahrar al Sham, 279
Alaska, 51
Aleppo, 281
Almog, Doron, 153
al Aloul, Ibrahim, 146
alternative facts, 3, 13
alternative narratives, 73, 296, 345
American Psychological Association, 275
Amidror, Yaakov, 155–56
anocracy, 33
Antalya, 283
Antifa, 287–88
anti-Semitism, 193, 249, 290
anxiety, 30, 169, 237, 239, 245, 247–51, 259–61, 288, 332; anxiety/uncertainty management (AUM) theory, 250; economy and, 271; public health and, 271
Argentina, 213, 215
Armstrong, Michael, 158
artificial intelligence, 27, 167, 199
Aryan Nations, 288
Aryan Resistance Movement, 289
ASEAN. *See* Association of South East Asian Nations (ASEAN)
al Assad, Bashar, 269, 278
Association of South East Asian Nations (ASEAN), 226
asymmetric warfare, 68, 172, 194, 219
attacks, kinetic, 41–42, 164, 175, 197, 302. *See also* attacks, non-kinetic
attacks, non-kinetic, 86, 197, 302, 333
attitude measurement, 305–321, 322nn1–3, 344; affect-misattribution procedure (AMP), 314–15, 317, 321; direct/explicit measures, 305; error choice technique (EC), 309–10, 317, 321; evaluative priming (EP), 312–14, 317; implicit association task (IAT), 311–15, 317; indirect/implicit measures, 304, 306–311, 316–20; lost e-mail technique (LET), 307–308; lost letter technique (LLT), 307–309, 319–20; standardized behavioural assessment, 309, 320
Austin, Lloyd, 24–25
Australia, 128, 173, 177, 213, 215, 229, 277
autocracy, 33, 72, 241
al Awlaki, Anwar, 279

al Baghdadi, Abu Bakr, 294
Baghouz, 280, 282, 284, 294
Balkans, wars in (1990s), 53
ballistic missile defences (BMD), 56; NATO-Russia collaboration and, 56–57
Baltic, the, 87, 89, 92, 94, 203
Batyuk, Vladimir, 42
BBC. *See* British Broadcasting Corporation (BBC)
Belgium, 53, 173, 177
Bellingcat, 174, 341

belonging, need for, 237, 239–41, 244–46, 248, 250, 253, 259–61, 285, 293, 296, 298, 332. *See also* tribes/tribalism
Bensouda, Fatou, 154
Berlin, 45; Berlin Wall, fall of, 327
Biden, Joe, 156. *See also* United States
Bing, 133
Black Lives Matter, 260
blackmail, 87, 91
Blair, Bruce, 49
Blood and Honour, 294
Bloomberg, 127
BMD. *See* ballistic missile defences (BMD)
Bolton, John, 170
booby traps, 149–52. *See also* Hamas
border walls, 249
Bosnia, 53
bots, bot networks, 90, 97–100, 102, 192. *See also* propaganda; Twitter
Brazil, 213
Breaking the ISIS Brand Counter Narrative Project, 296
Brennan, John, 105
Brinkel, Theo, 72–75
British Broadcasting Corporation (BBC), 135, 342
Brooker, Guy, 171
Bucharest,291
Bulgaria, 342
Bulletin of the Atomic Scientists, 8
Bystrov, Mikhail, 99

Cambridge Analytica, 102, 241
Cambridge University Press, 130. *See also* China, information warfare of
Canada, 1, 5, 71, 81–82, 213, 215, 229, 268, 277, 283, 285, 287, 291, 304, 311–14, 328; Atlantic Canada, 295; China, threat from, 226; conspiracy theories in, 8; cyber capabilities of, 226–27; cyberspace, position in, 225; cyber threats to, 225–28; far right in, 269–71, 284–92, 294–95, 297–98; far right in rural areas, 295; functional engagement, candidate for, 227–28; functional principle, use of, 224–25, 227; internationalism of, 226; Iran, threat from, 226; ISIS, members of and, 278–84, 296–97; jihadis and, 267–69, 270, 273, 278–84, 293, 297; multilateral groups, participation in, 226; North Korea, threat from, 226; racism in, 8; Russia, threat from, 226; Sikhs in, 7; terror list of, 294; Toronto, 18, 267–68, 279; values of, 106; violent extremism in, 201, 267–68, 271, 273, 279, 284, 295, 297; white supremacists in, 269, 273, 284–92. *See also* Canada, Government of; Canadian Armed Forces (CAF); Canadian Security Intelligence Service (CSIS); COVID-19; disinformation, Canada and; foreign terrorist fighters (FTFs); middle powers
Canada, Government of, 9, 106; *Anti-Terrorism Act*, 294; Bill C-11 and, 9; Bill C-59 (*An Act Respecting National Security Matters*) and, 227; *Consumer Privacy Protection Act*, 9; Critical Elections Incident Public Protocol, 200; defence policy of (2017, *Strong, Secure, Engaged*), 227; *Elections Modernization Act* (2019), 199; narrative strategy of, 106; National Cyber Threat Assessment (2020), 226; *National Security Act* (2017), 203; *Personal Information and Data Protection Tribunal Act*, 9. *See also* Canadian Indo-Pacific Strategy; Digital Charter (Canadian Federal government policy)
Canadian Anti-Fraud Centre, 328–29
Canadian Armed Forces (CAF), 9, 106, 226; disinformation, response to, 10–11; EFP in Latvia and, 10, 201; influence operations and, 301, 303–304, 315, 319, 321. *See also* radicalization
Canadian Incidents Database, 267
Canadian Indo-Pacific Strategy, 15
Canadian Liberty Net, 288–89
Canadian Security Intelligence Service (CSIS), 6, 9, 199, 226, 294; *CSIS Public Report 2020*, 6–7
cancel culture, 238, 242, 260
Capitol riot (January 2021), 5, 247, 271–72, 294; conspiracy theories and, 272; role of disinformation in, 5
Caucasus, 280
CCP. *See* Chinese Communist Party (CCP)
censorship, 31*t*, 33–34, 91, 97, 120, 128–29, 132, 172, 177, 330, 345n2. *See also* China, People's Republic of; Israel; Russia
Central Intelligence Agency (CIA), 105
C4ISR. *See* command, control, communications, computers,

intelligence, surveillance, and reconnaissance (C4ISR)
China Daily, 133
China, information warfare of, 120, 131–34, 171, 217; academia and, 127–28; Cambridge University Press and, 130–31; categories of, 120; Central Propaganda Department (CPD) of, 126–27; definitions of, 123; "informationalization", 120–25, 330; information operations, 120–21; cyber warfare, 120, 124; computer network operations, 120, 127; electronic warfare, 120, 124; foreign media/video game companies, purchases of, 130; hacking and, 129–30; intellectual property theft and, 122, 217; international audiences, messaging for, 130, 133; journalists, use of, 126; legal warfare, 120; media (tv/radio), use of, 121, 126; non-official media and, 126; proxies, use of, 126; psychological operations, 120; Russia, cooperation with, 135–36; space-based operations, 120, 124; state media and, 126. *See also China Daily*; COVID-19, Chinese disinformation about; *Global Times*; People's Liberation Army (PLA); propaganda; social media; WeChat; Weibo
China, People's Republic of, 1, 7, 9, 24–25, 40–41, 48, 57, 122, 200, 211–12, 216, 220, 226, 229, 302, 329–30, 343, 349–50; anti-Asian hysteria and, 8; Canadian official view of, 15; censorship in, 33–34, 120, 128–29, 132, 330, 345n2; Central Military Commission of, 123; corruption in, 125; COVID-19, exploitation of, 136; Djibouti, base in, 125; foreign media organizations/journalists, treatment of, 127; "Golden Shield" (firewall) of, 129, 340; "Great Firewall of China" (firewall), of 330, 345n2; "Historic Missions for the New Phase of the New Century" (2004), 123; independent media, elimination of, 128; India, relationship with, 52; Ministry of Industry and Information Technology of, 124; National Strategy for Informationalization Development for 2006 to 2020 (2005), 123; Seventeenth Party Congress of, 124; Sixteenth Party Congress of, 123; society, weaponization of, 125–26; Tenth Five-Year Plan of (2001–2005), 123; war as constant, view of, 41, 330. *See also* China, information warfare of; Chinese Communist Party (CCP); COVID-19, Chinese disinformation about; hacks, hacking; *People's Daily*; People's Liberation Army (PLA); Shanghai Cooperation Organisation; Taiwan; Ukraine
China Quarterly, 130–31
Chinese Communist Party (CCP), 121, 330; information, perception of, 122
Christianity, 288, 291
Church of the Creator, 291
CIA. *See* Central Intelligence Agency (CIA)
Citizen Lab (University of Toronto), 7
Clausewitz, Carl von, 44, 165
Clinton, Bill, 345n2
Clinton, Hillary, 86–87, 98, 101–105; QAnon and, 272. *See also* hacks, hacking; Russia, information operations of
Cohen, Eli, 173
Cold War, 1, 11–12, 39–42, 44–46, 48–49, 51–52, 57, 63–64, 75, 176, 194, 224, 243, 330, 334, 340; general deterrence and, 40, 52, 67; inevitability of war, belief in, 47; peace/war boundary and, 41; SIOP and, 49. *See also* cyber weapons; deterrence, nuclear; propaganda
Combat 18, 294
command and control systems, civil-military, 50
command, control, and communications, 49, 54, 56. *See also* command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); nuclear command, control, and communication (NC3)
command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) 41, 337. *See also* United States; weapons, nuclear
Commonwealth, The, 226
Communications Security Establishment (CSE), 9, 199; defensive cyber operations of, 202; offensive cyber operations of, 227
communications, strategic, 10, 83–84, 105–108, 195, 201, 339–41
compellence, 63, 66–68, 196, 204
conflict termination, 56

conspiracy theories, 4, 8, 87, 103, 133–34, 271–72, 332. *See also* Canada; Capitol riot (January 2021); jihadis; QAnon; white supremacists
Council of Europe, 216
Council on Foreign Relations, 211
counter-intelligence, 84
counter-narratives, 7, 17, 107, 197, 201, 275, 296, 339. *See also* alternative narratives
counter-radicalization, 17
counterterrorism 67–68, 73, 175, 243, 267, 273, 292, 297, 334. *See also* social media
COVID-19 1, 7–8, 31, 175, 248, 250, 260, 271–72, 274; anti-Asian feelings and, 271; bioweapon origins and, 169, 272; Canadian political establishment and COVID-19, 272; disinformation about, 5–6, 8–10, 131–35, 168, 193, 272, 328; fraud, financial losses caused by, 328–29; hate crimes and, 271; as "infodemic", 169; origins of, 1, 6, 8; Trump administration and, 119; US origin, rumours about, 132–33; vaccines against, 5, 170; Wuhan Seafood Market and, 132. *See also* COVID-19, Chinese disinformation about; Department of National Defence (DND); radicalization; Russia
COVID-19, Chinese disinformation about: attacks on credibility of other countries, 131; Canada, attacks on, 133; censorship and, 132; evolution of, 134–36; deaths, disinformation about, 136; foreign diplomats, role of, 132; Foreign Ministry, role of, 132; Fort Detrick, rumours about, 133; image of China as proactive and, 131–36; international audiences, messaging for, 132–33, 135; as largest global contributor to COVID disinformation, 119, 131; messaging, volume of, 134; nature of virus, rumours about, 132; news of outbreaks, suppression of, 131–32; role of officials in, 131; Russia, cooperation with, 135; United States, attacks on, 132–35; vaccine safety, attacks on, 5, 119, 132; viral origins, disinformation about, 6, 8, 14, 131–34; West, attacks on, 132–35; western social media content and, 132–36; Wuhan and, 132–33
CPI. *See* Harvard Belfer Center Cyber Power Index (CPI)
crisis management, 44–51, 335; communication, disruption of, 48–49; cyber-attacks, effect of, 48–52; disinformation during, 49–50, 54; messaging and, 45; nuclear crisis management, 39–40, 44, 49–52, 54, 335–37; signalling and, 44; time pressures and, 45–47, 49–50
Cruz, Ted, 98
Cryptic Studios, 130
CSE. *See* Communications Security Establishment (CSE)
CSIS. *See* Canadian Security Intelligence Service (CSIS)
Cuba, 46, 50. *See also* Cuban Missile Crisis
Cuban Missile Crisis, 12, 14, 46, 50–51
cyber-attacks, 25, 32, 46, 54, 86, 167, 169, 174, 180, 193, 203, 321, 338; attacks from cyber, 30, 31*t*; attacks in cyber, 29–30, 31*t*; attacks on cyber, 28–29, 31*t*, 32, 175, 342; attacks via cyber, 30–31, 31*t*, 33; attributes of, 43*t*; data attacks, 29–30; effects/impact of, 25–26, 28–34; falsely detected attacks and, 46; infrastructure attacks, 28–29, 55; Internet, attacks on, 30; NC3, attacks on, 40–42, 44, 46–50, 54, 57; obfuscation during, 28, 49–51; psychological effects of, 51; range of, 43; typology of, 28–31, 31*t*, 43*t*; undetected attacks and, 46; vulnerabilities to, 172. *See also* crisis management; disinformation, Canada and; hacks, hacking; Russia, information operations of; TV5 Monde, cyber-attack on; Ukraine; weapons, nuclear
cyber-bullying, 332
cyber defence, 195, 199–200, 223, 226, 343
cyber diplomacy, 223, 226
cyber escalation, 218, 228
cyber espionage, 29, 71, 211, 217, 223–24, 227
cyber-nuclear relationship, 40–43, 43*t*, 46–50, 333. *See also* crisis management
cyber operations, 32, 42, 54, 165, 197, 211, 213, 216–23, 226–29, 331, 337; defensive, 202, 227; offensive/aggressive, 32, 42, 202, 222, 226–27
cyber persistence, 213, 218–19; functional engagement and, 223–24, 229; interconnectedness and, 219; persistent

engagement and, 223, 229, 343; theory of, 223, 228–29. *See also* cyberspace; middle powers; United States Cyber Command (USCYBERCOM)
cyber reconnaissance, 124
cyber resilience, 165, 343; defined, 165, 180
cyber security, 23, 25, 30, 96, 180, 216; approaches towards, 25, 32; cyber hygiene and, 32–33; deception and, 40, 42; D5 and, 40; liberal states and, 216. *See also* cyber-nuclear relationship; information security
cyber sovereignty, 216
cyberspace, 26–28, 31, 57, 197, 216–22, 225–29, 243, 329; ambiguous/multidimensional nature of, 27–28; deterrence, practicality of in, 32; environment of, 211; illiberal ideas of, 220; international law and, 216–17; operational domains, impact on, 211; persistent engagement, strategy of, 197, 213, 221–22; stability/instability of, 216, 220, 225, 227–29; tacit bargaining and, 218–21, 223–24, 229. *See also* Canada; norms, cyber; United States; United States Cyber Command (USCYBERCOM)
cyber-stalking, 332
cyber verification, 42
cyber warfare, 44, 48, 84, 120, 125, 168. *See also* China, information warfare of; Hamas; cyber-attacks
cyber weapons, 41; arms control and, 42–43; Cold War era and, 42, 50; D5 abilities and, 41

DC Leaks, 89, 102
DDOS. *See* distributed denial of service attacks (DDOS)
deception, deception campaigns, 40–42, 84, 120, 154, 167, 172, 176, 189, 321
deepfakes, 167, 201, 241, 251
de-escalation, 54–56, 156
defectors, 273, 276, 278, 344
Defence Research and Development Canada (DRDC), 2, 11
degrade, deny, disrupt, destroy, deceive (D5), 41, 47, 49. *See also* cyber security; cyber weapons; nuclear command, control, and communication (NC3)
democracy, 5, 33, 72, 191, 241, 301–302; efforts to undermine, 6, 8, 31, 72, 81–82, 105, 164, 193; promotion/defence of, 106–108; values of, 6, 83, 106, 296. *See also* polarization/division; tribes/tribalism
Democratic Congressional Campaign Committee, 87, 96. *See also* hacks, hacking
democratic deterrence (concept), 204
Democratic National Convention, 87. *See also* hacks, hacking
Democratic Party (US), 96, 102
democratic suasion (concept), 191, 204–205
Denmark, 173, 177, 213
Department of National Defence (DND), 1–2, 9, 11, 106, 199, 201; COVID-19 pandemic and, 9–10; disinformation, response to, 9–11; Public Affairs office of, 9. *See also* Defence Research and Development Canada (DRDC)
Department of Public Safety (Canada), 199, 201
de-programming, 292
de-radicalization, 12, 75, 286, 290. *See also* counter-narratives; de-programming; disengagement
deterrence: capabilities for, 23, 26, 32, 257, 341–42; civil, 197; classical ideas about, 11–12; communication, importance of, 23, 333, 335–36; cost-benefit analysis and, 24–26, 66, 196–97; credibility, importance of, 23, 32, 333, 336; defined, 164, 190; denunciation, as form of deterrence, 72; economic, 197–98, 203; evolution of, 63–65, 190; fear, role of, 11; function of, 23; illusion of, 197; information and, 40, 197; information operations and, 40, 58; integrated deterrence, policy of, 24–25; kinetic, 144, 197; as means to counter disinformation, 3, 11, 13, 32, 329; non-kinetic, 68, 197; normative costs and, 202, 204; norms and, 70–71, 197, 202, 334–35; passive measures and, 12; perceived risk and, 39, 333; political, 153–54, 197, 203; psychology of, 26–27, 63, 197, 334–35; punctuated/cumulative nature of, 198; retaliation, reliance on, 32; scholarship of, 63–69, 73, 243; theory-to-policy transition of, 75. *See also* identities; terrorism; tribes/tribalism; trust. *See also* individual categories of deterrence
deterrence by counter-narrative, 197

deterrence by de-legitimization, 13–14, 65–66, 68–75, 197, 202, 334, 345; different views of, in scholarship, 73–75
deterrence by denial, 12, 15, 33, 57, 68–69, 73–75, 190, 195–96, 200–201, 204, 243, 254–57, 273, 295–98, 333, 338, 340, 344; strategic, 195; technical, 195. *See also* resilience; tribes/tribalism
deterrence by entanglement, 197, 202
deterrence by punishment. *See* deterrence by retaliation
deterrence by retaliation, 12–13, 33, 57, 67–69, 73, 190, 196, 202, 243, 254, 257–58, 335. *See also* tribes/tribalism
deterrence, nuclear, 11–12, 14, 24, 39, 41, 43*t*, 44, 54, 57, 144, 165; US attacks on Japan (1945), influence of, 24
deterrence theory, 63–68, 73–75, 190, 193–98, 243, 254, 332, 334; waves of, 63–66, 68, 194; first wave, 63, 65; second wave, 63, 65; third wave, 63–64; fourth wave, 64–65, 73, 194, 252–53; fifth wave, 65, 68, 73, 194
D5. *See* degrade, deny, disrupt, destroy, deceive (D5)
dictators, dictatorships, 121, 241, 272
Digital Charter (Canadian Federal government policy), 9
Digital Citizen Initiative (awareness campaign), 8
digital footprints, 319
digital literacy, 2, 339
disengagement, 286, 289–90, 297
disinformation, Canada and: academic research on, 6; costs, imposition of, 201–203; cyber-attacks, capability of, 203; education/awareness and, 200; foreign retaliation and, 15; international cooperation and, 199–200, 202; monitoring and, 201; normative costs and, 202, 204; policy on, 14–15, 329; public information about, 6–7, 15; quarantine concentration camps, disinformation about, 7; resilience and, 199–202, 340, 343; responses to, 191, 198–205; scope of, 7–8; securitization of disinformation and, 201; societal resilience and, 200. *See also* Communications Security Establishment (CSE); social media
disinformation (general): asymmetry and, 16, 168, 172, 174, 217, 219; computational propaganda and 4; critical thinking and, 173, 175, 195, 339; cyber domain/realm and, 26–28; definitions of, 2–6, 87, 191–93; education and, 2, 195, 338–39, 344–45; far right and, 5, 8; global nature of, 179; harm caused by, 1; laundering of, 193–94; rumours and, 3; terrorists/disinformers, similarities and differences between, 13–14; trolls and, 90. *See also* disinformation, Canada and; misinformation
disinformation, Internet and, 1, 3–4, 7, 31, 54, 92–95, 167. *See also* social media
disinformation, strategic, 54, 189–90, 193–99, 202–204, 343
distributed denial of service attacks (DDOS), 86
DND. *See* Department of National Defence (DND)
Doorn, Cees van, 73, 75
doxing, 286–88
DRDC. *See* Defence Research and Development Canada (DRDC)

echo chambers, 105, 191, 242
Egypt, 147–48, 151, 157, 287
8Chan, 271
elections and election interference, 1, 31, 93–94, 224, 228, 238, 328; Canadian election (2019), 6, 8, 200; European elections (2017), 81; French election (2019), 86; Israel and, 171; North Carolina, problems in (2016), 95; Russian election (2012), 96; US Presidential election (2016), 6, 81–82, 87, 90, 93–105; vote tampering and, 94–95; voter fraud and, 101; voter suppression and, 101–102. *See also* Elections Canada; hacks, hacking; Internet Research Agency (IRA); Russia, information operations of; social media; United States Cyber Command (USCYBERCOM)
Elections Canada, 199
electronic warfare (EW), 55, 84, 120, 124
Empire, Roman, 349
Epic Games, 130
escalation, 39–40, 44–45, 52–53, 56, 72, 144, 147, 218, 220, 222, 228, 246, 338, 345;

escalation control, 52, 56; nuclear, 243. *See also* cyber escalation; de-escalation
Escape Hate Counter Narrative Project, 296
espionage, 26, 28; commercial, 226; economic, 217. *See also* cyber espionage
Estonia, 94, 176. *See also* Russia
Ethiopia, 152, 279
European Council on Foreign Relations, 153
European Parliament, 153
European Union, 5, 107, 152–53, 196, 200, 217, 277; General Court of, 153; Hamas and, 153. *See also* Council of Europe
EW. *See* electronic warfare (EW)
extremism, 201, 267–68, 271, 273, 279, 282, 284, 292–95, 297–98, 332; countering, 273, 284, 292, 295–96, 298; far right, 82, 200, 243, 269–70, 273, 288, 294–95; jihadis/Islamists, 243, 273, 282, 293, 297; online content and, 271–72, 292, 296; recruitment into, 271, 273, 292–93, 295–96, 298; social media, 271; white supremacist, 270, 273, 294–95, 297. *See also* Canada; far right; ISIS (Islamic State); propaganda; terrorism; white supremacists

Facebook, 90, 97–104, 179, 192, 242, 247, 260, 271, 290, 298, 318
fact-checking, 4, 176, 195
fake news, 3, 13, 89–90, 97, 107, 168, 173, 199, 241, 244
false information, 3, 86, 192, 329
far left, 13
far right, 5, 8, 13, 81, 89, 200, 243, 269–73, 275, 284–98; alcohol and, 289–90, 293; music and, 270, 285, 288, 293; underestimation of, 269, 293. *See also* Canada; Islamophobia; Neo-Nazis; Proud Boys; social media; white supremacists
FBI. *See* Federal Bureau of Investigation (FBI)
Federal Bureau of Investigation (FBI), 96
Finland, 176
First Lebanon War, 171
First World War, 45, 52
Fischerkeller, Michael, 219–20
Five Eyes, 217, 226–27
5G networks, 7, 128; conspiracies about, 170
Floyd, George, 246
Foreign Intelligence Advisory Board (US), 55–56
foreign terrorist fighters (FTFs), 268, 293; Canadian FTFs, 268–69, 273, 278–84; motivations of, 268–69, 278–79, 281–82, 284. *See also* ISIS (Islamic State)
Formosa. *See* Taiwan
4chan, 271
France, 94, 226
Freeland, Chrystia, 200
Freeman Centre for Free Communication (Harvard), 169–70
FSB, 43
FTFs. *See* foreign terrorist fighters (FTFs)
functional engagement. *See* Canada; cyber persistence; middle powers
functional principle. *See* Canada; middle powers

Gab, 271
Gates, Bill, 249
Gaza Reconstruction Mechanism (GRM), 150–51
Gaza Strip, 143–44, 147–48, 154, 156–59, 351; anti-tunnel barrier along, 157; Jabalia, 148; Kerem Shalom crossing, 148; Khan Yunis, 148, 157; Rafah, 148; Shati, 148; Sufa crossing, 148; tunnels in, 143, 145–51, 154, 157–58. *See also* Gaza Reconstruction Mechanism (GRM); Hamas, 7 October 2023 attack of
genocide, 239, 251. *See also* identicide
George, Alexander L., 47
Georgia, 53, 55, 86, 94. *See also* Russia
Gerasimov, Valery, 302. *See also* Russia
Germany, 53, 94, 226
Get Cyber Safe (awareness campaign), 8
Giddens, Anthony, 247–49
Gilad Shalit, abduction of, 143, 148–49
Glazebrook, George, 213
Global Affairs Canada, 9–11, 199–200; international partnerships of, 200
globalism, 242, 260
globalization, 171, 237, 243, 248, 260, 331
Global Times, 130–31, 133
Google, 96, 100, 133, 179
Greatest Story Never Told, The (documentary), 272
GRM. *See* Gaza Reconstruction Mechanism (GRM)
Group of Governmental Experts, 217
GRU, 95–96. *See also* hacks, hacking

G7, the, 199, 216, 226; G7 Rapid Response Mechanism 199–200
G20, the, 216, 226
Guccifer 2.0. *See* hacks, hacking
gullibility, 5

Haaretz, 175
hacks, hacking, 29, 42–43; Black Shadow (Iran), 174; Cozy Bear (Russia), 96; Democratic Congressional Campaign Committee and, 96; Democratic National Committee hack (Hillary Clinton campaign, 2016), 42–43, 86–87, 94–97; French election campaign (Emmanuel Macron, 2019), 86; Guccifer 2.0, 43; Shirbit insurance company, attack on, 174; US Department of Defense and, 96; US Internal Revenue Service and, 95; US Joint Chiefs of Staff and, 95; US Office of Personnel Management and, 129–30; US State Department and, 95; VR Systems, hack of, 95. *See also* China, information warfare of; Russia, information operations of; spearphishing
Hajin, 280
Halutz, Dan, 153
Hamas, 143–56, 331, 336; air capability of, 145–46, 351; army of, 146; booby traps, use of, 150, 152; civilian casualty figures and, 154–55; cruelty of, 351; cyber warfare and, 175; deterrence of Israel and, 144, 150–58, 336, 351–52; disinformation campaigns of, 144, 152, 155, 336, 351; drones and, 145–46; humanitarian supplies, use of, 151; incendiary attacks of, 145, 148, 151, 156; Iran, links with, 147; Izz ad-Din al Qassam Brigades of, 148; Jerusalem terror attack (2001) and, 148; jihadi groups, rivalry with, 158; Kibbutz Ein Hashlosha, attack on, 149; Kibbutz Erez, attack on, 149; Kibbutz Netiv HaAsara, tunnel at, 149; Kibbutz Nir Am, attack on, 149; Kibbutz Sufa, attack on, 149; kidnappings and, 143, 148–49; Mengistu, Avera, disappearance of, 152; naval forces of, 146–47, 351; Nukhba, elite unit of, 146–47, 154; psychological warfare and, 145, 149, 159; restraint, view of, 155, 159; rocket attacks of, 143, 147, 151, 155–56, 158–59; smuggling and, 148; tunnels of, 143, 145–51, 154, 157–58; warnings to Israel, 143–44. *See also* European Union; Gaza Strip; Gilad Shalit, abduction of; Hamas, 7 October 2023 attack of; Israel; missiles/rockets; Popular Resistance Committees
Hamas, 7 October 2023 attack of, 351–52; brutality of, 351; ISIS, comparison with, 351
Hammerskins, 290
hardening, 67, 223, 338–39
Harvard Belfer Center Cyber Power Index (CPI), 226–27
Hatay, 279
hate speech, 4, 193
Heathrow Airport, 153
Hebrew, 172, 179
Heritage Front, 291–92
Hezbollah, 16, 173, 331, 351
Hirschmann, Albert, 212
hoaxes, 4, 87, 89, 272
Ho Chi Minh, 13
Holocaust, 285
Huawei, 128
human rights, 6, 71, 106
Hungary, 249; Hungarian language, 342
Hussein, Saddam, 12, 336
hybrid threats/warfare, 26, 34, 72, 94, 163–65, 182, 194–96, 201, 226; defined, 166–67, 205n1. *See also* asymmetric warfare; Russia

IAF. *See* Israeli Air Force (IAF)
ICC. *See* International Criminal Court (ICC)
ICS/SCADA. *See* industrial control systems/supervisory control and data acquisition (ICS/SCADA)
Idaho, 288
identicide, 238–39, 241, 251–52, 258, 260; defined 251; as precursor to genocide 251
identities, 69, 192–93, 197, 238–42, 244, 247–54, 258–61, 284, 286, 290, 308–309, 332, 344; autobiographical narratives and, 239, 242, 245–46, 251, 260–61; construction of, 242, 252–53; deterrence and, 253; false/stolen, 99–100; gender, 278; Islamic, 278; loss of, 243; self-identity, 247, 249–50; weaponization of, 239, 241. *See also* identicide
IDF. *See* Israel Defence Forces (IDF)

incels, 258, 270, 297
India, 7, 52. *See also* China
Indochina, 13
industrial control systems/supervisory control and data acquisition (ICS/SCADA), 228
influence operations, 84, 96, 165, 167–68, 172–73, 175, 177–78, 180–81, 301–304, 315, 319, 320–21, 322n1, 334, 338–39. *See also* Canadian Armed Forces (CAF); social media
information environment, 2, 9, 23, 41, 65, 70–75, 90, 157, 178, 190, 193, 203, 238, 301, 327–45; behavioural norms within, 70–71, 334–35; changes in, 327, 343; geographic boundaries and, 225, 329, 343; pre-emptive actions in, 340
information inoculation, 2, 164–65
information operations, 40, 58, 81–108, 165, 238, 241, 329–30, 339–41; countering, 105–108; definitions of, 192. *See also* deterrence; Russia, information operations of
information pollution, 3, 90
information security, 123, 128, 216; illiberal states and, 216
information warfare. *See* China, information warfare of; information operations; Iran; Israel Defence Forces (IDF); People's Liberation Army (PLA); Russia, information operations of; social media; Soviet Union
Instagram, 90, 97–98, 100, 246
integrated tactical warning and attack assessment (ITW/AA), 46
intellectual property theft, 122, 217, 228. *See also* China, information warfare of; cyber espionage; espionage
intelligence, military, 43, 95, 148
International Criminal Court (ICC), 144, 154
international order, 212, 215–18, 220, 225; conflict between liberal/illiberal states over 218, 220
Internet, 1, 3–4, 9, 84, 93, 97, 104–105, 107, 130, 165–67, 176, 178, 181, 228, 238, 240–41, 244, 246, 283, 301–302, 317–19, 321, 329–30, 340–41; attacks on, 28–30; Internet of Things, 30; recruitment and, for terrorism/far right, 270–71, 274, 276–77, 283, 285, 292, 298; sock-puppet websites, 87, 107; tribalism and, 240, 246; usage of, in different countries, 244; Web 2.0, 327. *See also* disinformation, Internet and; ISIS (Islamic State); radicalization
Internet Research Agency (IRA), 90, 97–105, 221; criminality and, 100; Project Lakhta and, 98–99; Translator Project and, 98; US Presidential election interference (2016) and, 97–105. *See also* Bystrov, Mikhail; social media; United States Cyber Command (USCYBERCOM)
Iraq, 12, 150, 277, 281, 290, 293, 312; jihadis in, 268, 276, 281; Kurdish autonomous region of, 150; Nineveh Plains of 150; weapons of mass destruction and, 12
Iraq-Iran War, 171
Iran, 1, 9, 147, 155, 164, 200, 211–12, 220, 226, 302, 329; bots, use of, 173; cyber deniability and, 173; deterrence of, by Israel, 164; disinformation campaigns and, 170, 173; influence operations and, 173; information operations of, 170–71; Israel, actions towards, 171, 173; nuclear weapons and, 56; proxies, use of, 164, 173, 331, 351; Stuxnet and, 30; US view of (2018), 170. *See also* hacks, hacking; Hamas; Hezbollah; propaganda; social media
Iron Curtain, 330
ISIS (Islamic State), 69, 102, 149–50, 158, 164, 168–70, 179, 248, 267–68, 273–84, 293, 297, 351; attacks carried out by former adherents, 268; Caliphate and, 273, 278, 282–83, 293–94, 296; *emni* (intelligence) of, 268, 282; Internet, role of in recruitment, 274, 276–77; recruitment of foreign members, 268–69, 273–74; resurgence of, 193; torture and, 282; *wilaya* of, 293; women and, 275–77, 282, 293–94. *See also* al Baghdadi, Abu Bakr; Breaking the ISIS Brand Counter Narrative Project; Canada; Hamas, 7 October 2023 attack of; propaganda; radicalization; social media
Islam, 74, 269, 271, 278–79, 281–84, 287, 296–97; converts to, 283; *hijrah*, 269; shariah law and, 69, 101, 287; Shia Islam, 170; Sunni Islam, 293; *takfir* ideology, 278, 284. *See also* identities; Islamophobia; ISIS (Islamic State)
Islamic Jihad, 158
Islamic State. *See* ISIS (Islamic State)

Islamophobia, 101, 193, 269, 271
Israel, 143–56, 227, 329, 331, 336, 351; arrest of officials, threats of, 153–54; Border Police of, 156; border walls of, 249; censorship and, 172, 177; Coordinator of Government Activities in the Territories and, 151; deterrence against Hamas and, 144–45, 151, 159; drones of, 145–46; Emergency Protection Regulations (British Mandate) and, 177; farmers in, 145, 156–57; Iron Dome system of, 145; Kibbutz Ein Hashlosha and, 149; Kibbutz Erez and, 149; Kibbutz Netiv HaAsara and, 149; Kibbutz Nir Am and, 149; Kibbutz Sufa and, 149; Kibbutz Zikim and, 147; LahavOr (Light Blade) system of, 156; Ministry of Agriculture and Rural Development and, 156; Ministry of Defence and, 156; Ministry of Finance and, 156; Ministry of Foreign Affairs, 151; National Cyber Security Directorate of, 171, 177–78, 183n1; 916th Division of, 147; Palestinian prisoners, release of, 148; Press Ordinance (British Mandate) and, 177; Prime Minister's Office of, 171; reputation, attacks on, 152–54; resilience as deterrence, 168, 174, 182; settlement policy of, 154; Shayetet, 13 147. *See also* anti-Semitism; Iran; Israel Defence Forces (IDF); Israel, operations of
Israel Defence Forces (IDF), 143–44, 147–50, 154–55, 158, 171; information operations and, 171–72, 175; public legitimacy/trust of, 171–72, 177; Spokesperson's Unit of, 171; training and, 178. *See also* Israeli Air Force (IAF); Israel, operations of
Israeli Air Force (IAF), 147
Israel, operations of: Cast Lead (2008–2009), 143, 153, 155, 171; Grapes of Wrath (1996), 171; Guardian of the Walls (2021), 143, 154–56, 158; Protective Edge (2014), 143, 147, 150, 154; Pillar of Cloud (2012), 171; Returning Echo (2012), 144
Italy, 53
ITW/AA. *See* integrated tactical warning and attack assessment (ITW/AA)
Itzkovich, Nahum, 156–57

Jabhat al Nusra, 280
Jaish al Muhajireen wal Ansar, 280
Japan, 24, 128, 213, 217
Jenkins, Brian, 167
Jerusalem, 143, 158–59; East Jerusalem, 154. *See also* terrorism
Jervis, Robert, 24, 47
jihad, 278–79; digital jihad, 294
jihadis, 267–73, 278–84, 293, 295, 297; conspiracy theories and, 271; criminality and, 270. *See also* Canada; Iraq; Syria
Jones, Alex, 272
Judaism, 177, 285–86, 288–90. *See also* anti-Semitism

Kahane, Rabbi, 288
Kennedy, John. F., 46, 50–51
Kenya, 280
KGB, 3, 166, 169. *See also* FSB
Khomeini, Ayatollah, 170
Khrushchev, Nikita, 46, 51
Kotev, Guy, 177
Kruglanski, Arie, 293
Kuijck, Christina van, 74–75
Kuwait, 283

Laing, R. D., 247
Latvia, 10–11; Canadian embassy in, 10, 201; NATO Enhanced Forward Presence (EFP) in, 10, 201. *See also* Canadian Armed Forces (CAF); Russia
Levi, Ron, 74
liberalism, 4–5; efforts to undermine, 5, 8, 13; trust in, 5, 164, 172. *See also* cyber security; cyberspace; democracy; information security; international order; tribes/tribalism; trust
Libicki, Martin, 51
Life After Hate, 286, 289
Lithuania, 176
Liu Xiaobo, 129
Live Journal, 90
Livni, Tzipi, 153
logic bombs, 55
Long, Jerry Mark, 68–70, 75
Lovatt, Hugh, 153

McGill University 269
McInnes, Gavin, 270
Macron, Emmanuel, 86. *See also* hacks, hacking
mainstream news media, 7, 92, 103, 237
Malaysia, 213, 215

malware, 86, 91, 95, 221; NotPetya, 217
Marcus Aurelius, 349
Martin, Paul, 272
martyrdom, 150, 258
Mayadeen, 280
Menzies Lyth, Isabel, 249
Mexico, 249
middle powers, 211–13, 220, 223, 229; Canada as middle power, 213, 224–25, 229; characteristics of, 213–16; functional engagement and, 223–24, 229; functional principles and, 224–25; global/international order, place in, 215–16; influence of, 215; list of, 213–14; as low-risk/high-payoff cyber targets, 225, 229; persistent engagement and, 223–24; theoretical perspectives on, 214–15; vulnerabilities of, 223. *See also* norms, cyber
Minassian, Alek, 270
Mishpacha, 155
misinformation, 3, 39, 87, 163, 174, 176, 191–92, 199–201, 243–44, 272, 328, 339; different from disinformation, 192, 329
missiles/rockets, 14, 41, 46, 48, 55–56, 143, 147, 151, 155–56, 158–59; Grad rockets, 143; Jupiter ballistic missiles, 46; Pershing II ballistic missiles, 55; Qassam rockets, 143. *See also* submarines, nuclear ballistic
Moonshot CVE, 272
Mordechai, Yoav, 151
Morsi, Mohamed, 157
Mossack Fonseca, 98
Mosul, 149–50
Mubarak, Hosni, 157
Munich, 330
Muslim Brotherhood, 143, 157. *See also* Hamas
mutually assured destruction, 11

Nagasaki, nuclear attack on (1945), 54
National Institute of Standards and Technology, 165, 180
National Socialist Black Metal, 289–90
NATO. *See* NATO Association of Canada; North Atlantic Treaty Organisation (NATO)
NATO Association of Canada, 7–8; Centre for Disinformation Studies at, 7
naturalistic decision making (NDM), 337–38; "satisficing" and, 337
Navalny, Aleksei, 97
NC3. *See* nuclear command, control, and communication (NC3)
NDM. *See* naturalistic decision making (NDM)
Neo-Nazis, 270, 294. *See also* Blood and Honour; Combat 18
Netanyahu, Benajmin, 155–56
Netherlands, The, 53, 213, 215, 226, 229
New York Times, 127; *Caliphate* (podcast), 268
Nigeria, 213
Nord Stream 2 pipeline, 29, 32
norms, behavioural, 70–71, 249. *See also* deterrence; information environment; norms, cyber
norms, cyber, 205n2, 212–13, 216–21, 223, 226, 228–29; middle powers and, 212, 224, 226, 228–29; multilateral efforts to enforce, 212–13, 216–18, 222–23, 228–29
North Atlantic Treaty Organisation (NATO), 10, 46, 53, 56, 81, 107, 165, 190, 196, 200, 217, 226, 304, 333; doctrine, review of (2010), 54; expansion of, 349; nuclear alliance, characterized as, 54; Tallinn Manual of, 216; threat to Russia, characterized as, 81; *See also* Able Archer (1983); ballistic missile defences (BMD); Latvia
North Korea, 48, 200, 211, 226, 302, 343
Norway, 213, 215
nuclear command, control, and communication (NC3), 40, 42, 57; deception of, 46; D5 effects on, 51; disinformation and, 49, 53, 57–58; trustworthiness of, 48. *See also* cyber-attacks; Russia; United States
nuclear crisis management. *See* crisis management

OAS. *See* Organization of American States (OAS)
Obama, Barack, 42
Olmert, Ehud, 155
ontological security/ontological security theory (OST), 237–38, 241–42, 244, 247–52, 260
open-source intelligence technologies (OSINT), 174–75, 180, 341
Order, The, 288
Organization of American States (OAS), 226

OSCE. *See* Organization for Security and Co-Operation in Europe (OSCE) 226
Osinga, Frans, 65
OSINT. *See* open-source intelligence technologies (OSINT)
OST. *See* ontological security/ontological security theory (OST)
othering, 237, 248

Palestine, 249
Palestinian Authority, The, 150–51
Pamment, James, 72
Panama Papers, 98. *See also* Putin, Vladimir
Paris, 170
Parler, 247
paternalism, 34
patience, strategic, 44
Payne, Keith B., 45
pedophilia, 179
People's Daily, 132
People's Liberation Army (PLA), 121–23, 128; information warfare training centre of, 123–24; Strategic Support Force (SSF) of, 124
persistent engagement. *See* cyber persistence; middle powers; United States
Peshmerga, 149
P5 (nuclear establishment), 52
PGS. *See* prompt global strike (PGS)
PhotoDNA, 179
PLA. *See* People's Liberation Army (PLA)
pluralism, 82, 242
Podesta, John, 87, 96. *See also* hacks, hacking
Poland, 248; Law and Justice Party in, 248; Polish language, 342
polarization/division, 90, 93, 101, 103, 182, 191, 193, 245, 272
Popular Resistance Committees, 144
populism, 17, 237–38, 242, 245–46, 248, 260
Portland (Oregon), 285
post-traumatic stress disorder (PTSD), 283, 286, 290
Prigozhin, Yevgeny, 99; Concord Management and Consulting and, 99; Putin, relationship with, 99. *See also* Wagner Group
Privy Council, 9
Project Implicit, 316
prompt global strike (PGS), 56. *See also* United States
propaganda, 24, 26, 33, 87, 89, 91–93, 97, 100, 120–21, 163, 329, 339, 341, 345; bots and, 99–100; Chinese, 8, 120, 122, 126, 130–31, 330; Cold War and, 1; computational, 4; countering, 335, 339–40; extremists and, 269, 292, 295; Iranian, 170; ISIS and, 280–82, 293–94; rehabilitation of term, 339, 345n3; resistance to, 33, 73; Russian, 89, 91–93, 97, 99, 107, 166, 168
Proud Boys, 269–70, 286–88, 294–95
proxies, 4, 6, 24, 66, 85, 89, 91, 126–27, 163–64, 167, 173, 329, 331, 351. *See also* China, information warfare of; Iran; Russia, information operations of
pseudo-science, 4
Psychological Defence Agency (Sweden), 33
psychological operations (PSYOPS), 84, 120, 145, 149, 159, 301, 303–304, 309. *See also* attitude measurement; China, information warfare of; Hamas
PSYOPS. *See* psychological operations (PSYOPS)
PTSD. *See* post-traumatic stress disorder (PTSD)
Putin, Vladimir, 42, 81, 83, 96, 98, 101, 105, 349; disinformation, use of, 53, 101; nuclear threats of, 53; Panama Papers and, 98; West, approach to, 81–82. *See also* Prigozhin, Yevgeny; Russia, information operations of

al Qaeda, 64, 69–70, 74–75, 158, 248, 267, 279, 293; adherents/recruits of, 69–70; violence of, 69, 71
al Qaisi, Zuhir, 144
QAnon, 260, 272; international following of, 272. *See also* Clinton, Hillary
Quebec, 7

racism, 8, 247, 285, 290–92. *See also* Canada; white supremacists
radicalization, 64, 68, 75, 268, 270, 297–98, 303, 332; Canadian Armed Forces members and, 290; COVID-19, impact of, 271–72; Internet, role of and, 270–71, 273, 276–93, 296, 298, 344; reciprocal radicalization, 293; Three N model and, 293. *See also* counter-radicalization; de-radicalization
Radio Free Europe, 330
Radio Liberty, 330

RAND Corporation, 167, 274
ransomware, 29
Raqqa, 280, 283–84
RCMP. *See* Royal Canadian Mounted Police (RCMP)
recruitment into extremist groups. *See* Internet; ISIS (Islamic State); social media; terrorism
Reddit, 271, 318
Reimer, Ofek, 71
Reporters without Borders, 126
resilience, 5, 11, 31*t*, 42, 68, 143, 157, 164–65, 168, 174–82, 191, 194–96, 199, 203–205, 335, 338–40, 343–44; defined, 165, 180, 195; deterrence by denial, link with, 72, 190, 195, 333, 338, 340. *See also* cyber resilience; disinformation, Canada and; Israel; resilience, societal
resilience, societal, 2, 33, 73–74, 195, 200. *See also* disinformation, Canada and
retaliation, 12–13, 15, 23–24, 26, 32, 52, 56–57, 67, 240, 243, 253, 331; in nuclear conflict, 14, 43*t*, 52, 56, 67, 328. *See also* deterrence by retaliation
revenge porn, 179
Reyhanli, 279
Riot Games, 130
risk society, idea of, 249
Romania, 342
Rossiya Segodnya, 92. *See also* Simonyan, Margarita Simonova
Royal Canadian Mounted Police (RCMP), 9, 199, 201
RT, 89–92, 100, 126. *See also* Simonyan, Margarita Simonova
Rubio, Marco, 98
Russia, 1, 6–7, 9, 12, 24–25, 34, 40–41, 44, 48, 52, 56–57, 81, 164, 200, 211–12, 216, 220, 226, 229, 329, 349–50; censorship in, 91; disinformation about EFP in Latvia, 10, 201; disinformation about origin of COVID-19, 6–7, 135; disinformation about vaccine safety, 5, 170; Estonia, information attack on (2007), 94; Georgia, war with (2008), 53, 55, 86, 94; Gerasimov Doctrine, use of, 168; hybrid warfare, use of, 94, 168–69; intelligence services of, 6–7; Kremlin and, 97; military doctrine of, 53–54; NC3 networks and, 42; nuclear arsenal of, 41–42, 53; Putin regime of, 81–84, 88, 94, 97–98, 106, 108; security threats to, 81; strategic aims of, 81–82; war as constant, view of, 41, 85, 105, 108, 330; West, approach to, 81–83, 97, 108. *See also* ballistic missile defences (BMD); FSB; GRU; hacks, hacking; KGB; Putin, Vladimir; Russia, information operations of; Russian Security Council; social media; Soviet Union; terrorist attacks
Russia, information operations of, 81–107, 171, 217, 329–31; academia, influence over, 92; active measures and, 85; black outlets and, 89, 93, 331; bots, use of, 90, 93, 97, 99; China, cooperation with, 135–36; countering, recommended methods of, 105–108; cyber-attacks, use of, 86; different elements of, 84; disinformation, use of, 87, 97–98, 105–107; domestic audiences, messaging for, 91–93, 98; Donald Trump, support for, 98, 101–105, 302; election interference and, 81–82, 86–87, 90, 93–105, 221; emotional responses and, 88–89, 102; ethnic/social communities, targeting of, 101–103; as first element of, engagement with enemy, 84; grey outlets and, 89, 93, 331; hacking and, 86–87, 94–97; Hillary Clinton, attacks on, 98, 101–105; HIV/AIDS, disinformation about, 169; importance of in Russian military planning, 83; influence agents, use of, 91, 93; information-psychological type of, 84; information-technical type of, 84, 86; international audiences, messaging for, 89, 91–93, 97–98; malware, use of, 217; media (tv/radio), use of, 84, 91–93; proxies, use of, 89, 91, 331; reflexive control practices and, 85; trolls and, 85, 90–93, 97–101; truth, manipulation of/attack on, 87–89; West, attacks on and, 83–84, 92, 97–98, 105–108; white outlets and, 89, 93. *See also* bots, bot networks; Internet Research Agency (IRA); propaganda; Rossiya Segodnya; RT; social media; Sputnik News; Ukraine; VKontakte
Russian Security Council, 42

St Petersburg, 45, 90
St Petersburg University, 98

Sanders, Bernie, 98
Saudi Arabia, 279
Sawyer, John, 74
scapegoating, 248–49
Schneier, Bruce, 30
Schugart, Ian, 106
SDF. *See* Syrian Democratic Forces (SDF)
Second Lebanon War, 171
Second World War, 108, 224, 243, 327
Security and Intelligence Threats to Elections (SITE) Task Force, 9, 199; composition of, 9
Serbia, 53
settler colonialism, 239
Shabtai, Yaakov, 156
Shanghai Cooperation Organisation, 216
Sherif, Muzafer, 245; experiments of, 245–46
Simonyan, Margarita Simonova, 92
Sinai, 147, 150, 157
single integrated operational plan (SIOP), 49. *See also* Cold War
SIOP. *See* single integrated operational plan (SIOP)
situational awareness, 40, 46, 336–38
Six Day War, 155
social justice, 2, 242, 260
social media, 3, 6–7, 31, 33, 92, 167, 176, 178–79, 181, 189, 191, 238, 244, 270, 294, 297–98, 301, 316–18, 327, 329, 341, 349; #AlleyesonISIS hashtag and, 169; censorship and, 34, 297–98; Chinese information operations/disinformation campaigns and, 121, 131–36; counterterrorism and, 292; election interference and, 94–95, 97–101; fake accounts and, 97, 99, 173, 181, 339; far right and, 270–71, 297–98; influence operations and, 302; Internet Research Agency (IRA) and, 99–105; Iran and, 170, 173; ISIS, use of 169, 175, 276; personality assessment and, 319; regulation, attempts at, by Canada, 202; recruitment and, for terrorism/far right, 270, 292; Russian information operations/disinformation campaigns and, 7, 31, 84, 86–93, 97–105; super-spreaders and, 175; terrorists, use of, 270, 277; tribes/tribalism and, 246, 260; usage of in Canada, 33; as way to influence foreign audiences, 85. *See also* COVID-19, Chinese disinformation about; names of individual social media companies
Soros, George, 249
South Africa, 215
South Korea, 213
Soviet Union, 40, 51–52, 55, 84–85, 166, 176, 243, 336, 345n1; demise of, 52; information operations of, 330, 339–40; nuclear arsenal of, 41–42
Spain, 94, 213
spearphishing, 86, 95–96
SPSS data-analysis software, 276
Sputnik News, 89–92
Stanford University, 176
Stein, Janice Gross, 74
Stein, Jill, 102
Stop AAPI Hate, 260
Stormfront, 285
Stuxnet, 30, 57. *See also* Iran
submarine cables, 29
submarines, nuclear ballistic, 49
Sudan, 280
suicide, 69, 71, 150, 158, 283–84, 287, 294
Sukumar, Arun, 217
Sun Tzu, 163
Sweden, 33, 213. *See also* Psychological Defence Agency (Sweden)
Sweijs, Tim, 65, 71, 74, 204
Switzerland, 277
Syria, 99, 268, 274, 277, 279–81, 296, 351
Syrian Democratic Forces (SDF), 279–80, 284, 293–94; Camp al Hol of, 294

tacit bargaining. *See* cyberspace
Taiwan, 14, 122; as target of Chinese information campaigns, 122; "Voice of the Strait" radio and, 122
Tamimi, Ahlam, 148
Tel Aviv, 143, 158–59
Telegram, 174–75, 280
terrorism, 16, 64, 68–69, 167, 256, 258, 267; deterrence and, 66–70, 73, 75; leadership decapitation and, 258; recruitment and, 69, 74, 270–77, 282–83, 286, 290, 292–93, 295, 297–98, 302–303. *See also* Canada; counterterrorism; social media; terrorist attacks; war on terror. *See also* names of individual terrorist groups
terrorist attacks: Malaysian Airlines Flight, 17 73, 75, 174, 341; Jerusalem (2001), 148; 9/11 12, 64, 267, 297, 327; Toronto van attack (2018), 270

Thailand, 33
Tonga, 29
Toronto, 284, 286–87, 289, 292
toxic masculinity, 286
transparency, 9, 42, 177, 197, 200, 350
treaties and agreements, nuclear: New START, 53, 56; Nunn-Lugar agreement, 42; Russo-American agreement (June 2013), 42
tribes/tribalism, 237–40, 242–46, 249, 290; asymmetry and, 244; belonging and, 237, 239–41, 244–46, 248, 250, 253, 259–61; cross-national structures and, 256; defined, 237, 239, 243; destruction of, 258–59; deterrence and, 252–61; deterrence by denial and, 255–57; deterrence by punishment (retaliation) and, 257–60; digital, 237–38, 242–44, 247, 252–61; engineered, 237, 241–42, 246–47, 250, 261; liberal democracies and, 238; organic, 237, 242, 246, 258, 260; routines/routinization and, 237, 242, 260–61; US political tribalism, 245. *See also* Internet; social media
Trinidad, 281
Trojan Horses, 55
trolls, trolling, 4, 85, 90–91, 97–98, 100, 244; honeypots, use of, 91; troll farms/factories, 90, 97. *See also* bots, bot networks; disinformation (general); Russia, information operations of
Trudeau, Justin, 272
Trump, Donald, 98, 101–105, 200, 247–48; impact of, on far right, 269; influence campaigns and, 302. *See also* COVID-19; Russia, information operations of
trust: 176–77; deterrence and, 350; in liberal government/institutions, 2, 5, 164, 173, 189, 193, 195, 200, 335, 343; undermining of, 164. *See also* Israel Defence Forces (IDF)
truth: concept of, attacks on, 83–84, 87, 106; defence of, 106, 108, 200; disinformation and, 152, 166, 349; identifying, 89; manipulation, of 87; post-truth era, 3, 167; value of, 167. *See also* Russia, information operations of
Turkey, 53, 213, 215, 277, 279, 281
TV5 Monde, cyber-attack on, 217
Twitter, 90, 96–102, 104, 133, 136n3, 169, 174, 179, 192, 244, 246–47, 283, 318; bots and 99–100

Ukraine, 1, 10, 92, 168, 341; Chinese support for Russia and, 125, 135; Crimea, annexation of (2014), 94, 97, 125, 168; cyber-attacks on, 168, 217; Russia information operations and, 86, 168; invasion of (2022–), 1, 14, 29, 42, 53, 55–57, 94, 99, 125, 221, 349. *See also* United States Cyber Command (USCYBERCOM)
UN. *See* United Nations
United Kingdom, 81, 94, 128, 153, 226–27, 277, 304; Brexit vote of (2016), 81, 248; deterrence, interpretation of, 196. *See also* United Kingdom Ministry of Defence
United Kingdom Ministry of Defence, 24–25, 31
United Nations (UN), 150, 202, 213, 216, 226
United Nations High Commissioner for Refugees, 154
United States, 5, 8, 10–11, 14, 40, 44, 48, 51, 55, 57, 86, 90–91, 94, 165, 169, 173, 177, 217, 226, 228–29, 244, 256, 268, 277, 285, 295, 311–12, 336; Biden administration of, 8; Bush (George W.) administration of, 56; C4ISR systems of, 41; Congress of, 103; cyberspace, effort to gain advantage in, 220–23; Kennedy administration of, 12; military superiority vis-à-vis Russia, 53–54; Muslim travel ban and, 248–49; NC3 system of, 40, 43; nuclear arsenal of, 41–42, 53; Obama administration of, 56; PGS plans and, 56; Second Amendment rights and, 256; threat to Russia, characterized as, 81; White House, 87. *See also* COVID-19, Chinese disinformation about; Foreign Intelligence Advisory Board (US); United States Cyber Command (USCYBERCOM); United States Department of Defense; United States National Command Authority; United States State Department

United States Cyber Command (USCYBERCOM), 220–222; *Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority*, 221–22; Cyber National Mission Force teams of, 221; elections, defense of, 221; Internet Research Agency, exposure of, 221; persistent engagement, strategy of, 221–22, 229, 343; Ukraine, partnership with, 221
United States Department of Defense, 24, 87, 96, 166; Joint Chiefs of Staff of, 87, 95. *See also* hacks, hacking
United States Global Engagement Center, 199
United States Information Agency 339–40
United States Internal Revenue Service 95. *See also* hacks, hacking
United States National Command Authority 49
United States Office of Personnel Management 129–30. *See also* hacks, hacking
United States State Department, 87, 95. *See also* hacks, hacking
US Alliance for Securing Democracy, 200
USCYBERCOM. *See* United States Cyber Command (USCYBERCOM)
U-2 reconnaissance aircraft, 51

Vancouver, 281, 288
Vienna, 45
Vietnam War, 149
Virilio, Paul, 182
VKontakte, 90
Voice of America, 342
Volksfront, 285
VUCA (acronym: volatile, uncertain, chaotic, and ambiguous), 349–50

Wagner Group, 99
Wall Street Journal, 101
war on terror, 12, 267
Warsaw Pact, 55
Warsaw Summit (2016), 165
Washington Post, The, 135
WeChat, 132
Weibo, 129
West Bank, 154
weapons, nuclear, 24, 34n1, 39–41, 258; air-delivery and, 53; C4ISR and, 41; cyber-attack and, 41; deployment (geographical) of, 53–54; disabling of, by cyber-attack, 48; first strikes and, 39, 42, 52, 55–57; intercontinental, 53; international arsenals and, 41–42; non-strategic, 53; rogue states and, 52; tactical, 53–54; warning systems and, 50. *See also* Iran; missiles/rockets; treaties and agreements, nuclear
weapons of mass destruction (WMDs), 12. *See also* Iraq; weapons, nuclear
WhatsApp, 169
white supremacists, 269–70, 273, 275, 284–92, 294–97; alcohol and, 289–90, 293; conspiracy theories and, 271; emboldened by far right politicians, 294–95; music and, 270, 285, 288, 293; white replacement theory, 290; women and, 291–92. *See also* Aryan Nations; Canada; Canadian Liberty Net; Church of the Creator; Escape Hate Counter Narrative Project; Hammerskins; Heritage Front; Life After Hate; National Socialist Black Metal; Order, The; Stormfront; Volksfront
Wiggle, Mikael, 204
WikiLeaks, 89, 96, 102
Williams, Russell, 10
WMDs. *See* weapons of mass destruction (WMDs)
World Health Organization, 8, 132, 134, 136, 169, 176
Wrong, Hume, 224–25

Yaalon, Moshe, 153
YNABers, 260
YouTube, 98, 100, 192, 287, 318–19

Zilincik, Samuel, 71, 74, 204

The information age has opened a new front of adversarial statecraft. The past decades have seen the rise and refinement of conflict enacted in the world of information, with tactics including seeding disinformation, the theft of sensitive data, confusing or obscuring public opinion to forward specific goals, and beyond. *Deterrence in the 21st Century* asks how, and if it is indeed possible, to deter an enemy in the realm of information warfare.

Setting the stage with an overview of key concepts of deterrence in the information age, the book presents new conceptual approaches and their possible applications. Bringing together some of the most respected analysts working today, *Deterrence in the 21st Century* looks beyond the technical aspects of the use of information and disinformation as adversarial statecraft to seek new avenues to deter the undermining of institutions and societies.

Treating deterrence as a concept, a policy, a social challenge, and a series of practical solutions, *Deterrence in the 21st Century* presents theoretical approaches, conceptual analysis, empirical research, and content analysis. This is a thorough, thoughtful, and expert analysis of one of the most difficult and essential security challenges of our time.

ERIC OUELLET is a full Professor at the Royal Military College of Canada in Defence Studies, teaching to mid and senior level officers at the Canadian Forces College. He is founder and director of the Centre for Institutional Analysis of Armed Forces, and has been involved in numerous international collaborative research projects on military matters.

MADELEINE D'AGATA received her PhD in psychology in 2017. From 2017 to 2022, she was a Defence Scientist at Defence Research and Development Canada. Dr. D'Agata has published over 60 reports. In 2022 she deployed to Chief, Professional Conduct and Culture and is a Senior Policy Advisor.

KEITH STEWART works at Defence Research and Development Canada's Toronto Research Centre. In a 30-year career, which has included periods in private industry and government service, he has focused on human-centric research issues, including influence operations, human elements of military command, and human error in high hazard environments.

UNIVERSITY OF CALGARY
Press

press.ucalgary.ca