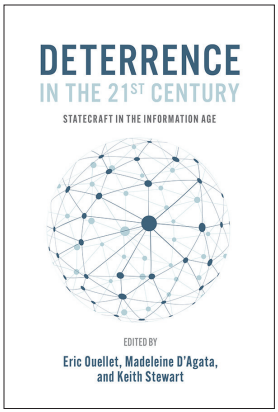
UNIVERSITY OF CALGARY
Press



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

1

Deterrence Is Always about Information: A New Framework for Understanding

Christopher Ankersen

Deterrence works when an adversary refrains from undertaking a particular action for fear of paying too high a price; in other words, it "means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit" (Nye, 2017). It depends on several elements. Much focus is placed on capability (the ability of a party to effect the retaliation), giving a certain material bias to much of contemporary deterrence discourse. Do we have the right "things" (weapons systems, for instance) to be able to deter a potential aggressor? Following this material train of thought, several observers wonder if deterrence can translate from the world of nuclear and conventional statecraft into the information environment. Does deterrence, for instance, work below the threshold of armed attack in the same way it works (or at least appears to work) above that threshold? Can or does deterrence work in the domain of cyber security? If so, does it work the same way that it does in the "real world?"

This material bias, though, blinds us to the fact that deterrence actually operates—has always operated—in the information environment. In addition to, and I argue much more importantly than, the material aspects of deterrence (capability) are the ideational elements of credibility and communication.

While these dimensions are integral to deterrence, what has changed are the operant media through which and with which opponents threaten each other. What this chapter proposes is a framework that treats a variety of different attacks (across both material and ideational dimensions) and, hence, allows for some form of "valuation" to be carried out. Only once such an

appraisal has occurred can any kind of "cost-benefit analysis" (the basis of deterrence) be conducted.

Where deterrence is focused on nuclear weapons, the costs are understood to be catastrophic. Based on the results of the two US atomic attacks on Japan, as well as predictions based on tests and modelling from all nuclear weapon states since then, the notion that there could be an "upside" to nuclear war was not a mainstream opinion (Blair & Wolfsthal, 2019; Waltz, 1981).[1] As Robert Jervis puts it, "the healthy fear of devastation . . . makes deterrence relatively easy" (quoted in Payne, 2011, p. 395).

Of course, deterrence has never solely been about nuclear weapons (Huntington, 1983; Paret et al., 1986). Recently the United States Department of Defense has been moved to adopt a strategy of "integrated deterrence," in which military power is not the only component. In a recent speech Secretary of Defense Austin explained that "Deterrence still rests on the same logic—but it now spans multiple realms, all of which must be mastered to ensure our security in the 21st century" (quoted in Lopez, 2021). The idea is that countries like Russia and China are waging a campaign of hybrid or grey-zone warfare, whereby they aim to disrupt and undermine the status quo, but do so "below the threshold" of armed conflict (Chivvis, 2017; Morris et al., 2019).[2] Accordingly, adversaries use "everything but" in their campaigns: propaganda, agitation, use of proxies, and cyber-attacks are the stock in trade here. The British Ministry of Defence goes so far as to claim that

> old distinctions between "peace" and "war," between "public" and "private," between "foreign" and "domestic" and between "state" and "non-state" are increasingly out of date. Our authoritarian rivals see the strategic context as a continuous struggle in which non-military and military instruments are used unconstrained by any distinction between peace and war (United Kingdom, 2021, p. 22).

By choosing to use "less kinetic" and/or "difficult to attribute" methods, thereby not setting off the tripwire of overt military action, adversaries may prod and probe freely, based on the idea that what they are doing is not worthy of large-scale retaliation. In this sense, such tactics are meant to act as a way of circumventing deterrence by inverting the usual cost-benefit analysis: the

benefits accrued by an adversary operating in the "grey zone" seem too small to warrant the imposition of high costs.

The response from the West to counter and indeed deter such efforts has been, in a word, integration. Secretary Austin explains it thus:

> Integrated deterrence means all of us giving our all. . . . It means that working together is an imperative, and not an option. It means that capabilities must be shared across lines as a matter of course, and not as an exception to the rule. And it means that coordination across commands and services needs to be a reflex and not an afterthought (quoted in Lopez, 2021).

Similarly, the British approach stresses the need

> to create multiple dilemmas that unhinge a rival's understanding, decision-making and execution. This requires a different way of thinking that shifts our behaviour, processes and structures to become more dynamic and pre-emptive, information-led and selectively ambiguous. In essence, a mindset and posture of continuous campaigning in which all activity, including training and exercising, will have an operational end (United Kingdom, 2021, p. 22).

If integration is indeed the key to deterring Chinese and Russian efforts, then it is worth examining where Western thinking and acting are falling short. One such area is that of cyber security. Despite the novelty of the field, as it stands our approach to cyber is highly stovepiped—precisely the opposite of what we are aiming for. Indeed, by fragmenting cyber security we are doing our adversaries' work for them. By focusing only on some kinds of cyber activity and labelling them as attacks while dismissing others merely as hacking, we form an incomplete picture of how our adversaries use cyberspace against us. With only a partial picture, we cannot hope to achieve integrated deterrence.

In this chapter, I propose a new way of understanding cyber security, one that is more comprehensive than is currently the case. Moreover, the proposed framework concentrates not on the sources of cyber-attacks or into whose jurisdiction they might fall. Instead, it focuses on *the effects* of cyber-attacks and allows for several outcomes. Such a framing does two things. First, it

lends itself to an integrated response. Second, and more importantly, it allows for the (re)establishment of deterrence, as it permits an appropriate and holistic accounting of the impact of cyber-attacks, so that a proper "cost-benefit" footing can be set.

My argument unfolds as follows. First I cover the basics of deterrence and how it applies in a world of "hybrid threats," focusing on the fact that deterrence is all about a particular frame of mind. Second, I discuss how security in, of, and from cyberspace interacts with that understanding. As mentioned above, I propose a comprehensive typology for managing cyber threats in this section. Finally, I discuss how such an approach—one centred on intended effects—leads itself to better forms of deterrence.

Deterrence Is a State of Mind

Deterrence is not only about capability. An adversary's decision not to attack is largely ideational, not material. Indeed, "deterrence is a psychological process in which subjective elements such as fear, pressure, and influence inform how calculations are made and decisions are taken. . . . Threat and fear are at the epicentre of deterrence, because deterrence as such is a state of mind" (Filippidou, 2020, p. 14). And while this is not a new observation, it is often forgotten, pushed aside in the pell-mell of calculations and preparations. "Deterrence posits a psychological relationship, so it is strange that most analyses of it have ignored decision makers' emotions, perceptions, and calculations and have instead relied on deductive logic based on the premise that people are highly rational" (Jervis et al., 1985, p. 1). Instead of concentrating on how opponents are thinking, we tend to get sucked directly into discussions of defences and countermeasures, happy to count and plan and prepare. What is more, we dismiss too quickly incidents that we regard as nothing more than vandalism, or espionage, or propaganda, waiting for our enemies to "cross the threshold," where they do "real-world harm." Only then can we conceive that some kind of retaliation is necessary, only then would deterrence be applicable.

The fact that deterrence is more ideational than material means that disinformation plays a large part in it. Convincing an adversary not to attack can be achieved as much through deceit as through defence. This is as true inside the cyber domain as it is outside of it. What is more, though, the cyber domain can be used as a powerful tool for the dissemination of disinformation in the first place. This means that disinformation in the cyber realm

has a double effect. First, it can be used to confuse or deceive an adversary. Following the logic of "garbage in, garbage out," bad information injected into a decision-making process can lead to faulty conclusions on a range of aspects, from intention, to desire effect, and so on. Separately, though, disinformation can be used outside of such a rational process to generate a range of non-rational outcomes, not within the decision-making elites, but among the mass population. Such outcomes might include not only faulty conclusions, but also disbelief and, ultimately, distrust. Instead of aiming for an alternate, rational conclusion, disinformation, then, can be used to create irrational non-conclusions. This may serve to undermine legitimacy, or merely sow confusion and controversy. Either way, it is intended as a means of degrading the bases for action.

Security and Cyberspace

At first blush it may seem foolish to try and impose some form of order to activities taking place in what has been called a consensual hallucination experienced daily by billions of legitimate operators, in every nation (Gibson, 2000). While it is true that cyberspace is a virtual realm, when we analyze it as a field of security, we can and must concentrate on the effects that are generated in and because of it. In that sense, I object to referring to cyberspace as a mere domain. In my use of the term, I want to highlight its multi-dimensionality. If we regard it too narrowly, we may lose sight of what is possible. Such an overly narrow focus can mean that we lose sight of the impact that cyber-attacks have, making it harder to conceive of them as something to be deterred in the first place.

While some have envisioned cyberspace as a realm divorced entirely from the material world, the reality is less tidy. The virtual world is propped up by cables and cords; sitting beside artificial intelligences are networked toaster ovens; its population is made up of flesh-and-blood denizens as well as numeric databases. Any view of security in cyberspace must include all these elements. Only regarding "pure play" digital threats as worthy of cyber-security efforts is a strategy that leads to be being outmanoeuvred by one's opponents. The framework presented here accounts for all sources of harm that might emanate from or across cyberspace, whether they are aimed at hijacking data or tearing up fibre optics. It is this degree of comprehensiveness that allows for a holistic appreciation of the threat landscape, which in turn can enable an integrated approach to deterrence. The end goal is to reduce what Nye (2017)

has labelled the "ambiguity of cyber threats." I contend that such ambiguity is often exploited and indeed exacerbated through the use of disinformation. IP masking, routing through multiple servers, the use of cut-outs, intentionally using technical markers (such as specific types of hardware or lines of code associated with a particular actor or country)—all this is deliberately done to create confusion and doubt as much as it is meant to convince an adversary of a specific, false source of cyber activity.

It is a truism to say that developments in cyberspace are constantly in flux. Future methods of attack may be difficult to predict in their precise technological dimensions. However, by focusing on the intended *effects* of cyber-attacks, this typology allows us to remain undistracted by the details. Asking ourselves, "What do our opponents attend to achieve?" forces us to concentrate on our opponents' goals, what they consider as the benefits in any cost-benefit calculation. In turn, this enables us to note that it is not necessary that a specific attack be restricted to one kind of effect. A single attack might have several different effects, either by design or as a matter of "collateral impact." Indeed, just as arson might be used as a means of disguising a murder, a cyber-attacker might choose to destroy infrastructure as a way to obfuscate the primary focus, which was data collection. Similarly, a cyber incident that appears to have been nothing more than espionage could easily have also provided an adversary with the possibility of creating a "back door" for future exploits, or even delivering a payload that could wreak havoc at a later date. Obfuscation of this kind (disguising one's true intentions) is commonplace, and if we are too quick to categorize incidents as "merely hacks" and not keep an open mind to the possibility of more serious effects, we fall prey to our adversaries' disinformation. What is better, I argue, is to regard every cyber incident as an attack in the first instance, and then proceed to rule out other possibilities based on further information. As such, I propose below a fourfold typology of cyber-attacks.

ATTACKS ON CYBER

Attacks on cyber have infrastructure as their target. Such attacks may be physical or digital, or both. Physical attacks involve the destruction of cables or other hardware. This could involve cutting wires, burning or bombing buildings, or smashing computers, servers, modems, or other physical aspects of the Internet. Digital attacks might not visibly damage or destroy materials, but they could render useless the digital capacity of physical infrastructure

or media through magnetism or moisture, for example. Whether physical or digital, attacks on cyber have the same effect: the destruction of the target.

An example of such an attack on cyber could be similar to what happened to Tonga. While it has not been publicly described as an intentional event, an incident in January 2019 left the island nation without connectivity after "a boat with an anchor . . . dragged the [undersea Internet] cable, or something of this sort" (Westbrook, 2019). A satellite work-around was arranged but provided only one-tenth of the access previously provided by the cable. Repairs took about two weeks.

The impact of such relatively crude attacks is hard to downplay. According to some reports, these cables "carry global business worth more than $10 trillion a day, including from financial institutions that settle transactions on them every second. Any significant disruption would cut the flow of capital. The cables also carry more than 95 percent of daily communications" (Sanger & Schmitt, 2015). The vulnerability of submarine cables has been evident in the North Atlantic since the Russian invasion of Ukraine ("The *Irish Times* view," 2022). The destruction of the Nord Stream 2 underwater pipeline goes to show the ease with which such physical attacks can be carried out, the apparent difficulty involved in definitively determining attribution, and the disbelief that can be generated when competing accounts circulate ("Kremlin eyes object," 2023).

ATTACKS IN CYBER

Attacks in cyber focus on data, attempting to steal or corrupt it. There are myriad ways in which this might be done, ranging from unauthorized access by legitimate users to penetration of networks by outside attackers. There are two main kinds of attacks in cyber. The first seeks to gain information and exploit it. This could take the form of proprietary intellectual property (United States of America, 2021a) or other sensitive information (Sanger, 2020). The second kind of attack in cyber aims not to steal data but to corrupt or deny access to it: ransomware is an example of this kind of attack (Turton & Mehrotra, 2021).

These types of incidents are often regarded as hacks, not attacks, and are dismissed as examples of cyber espionage (Rid, 2012). By not including them as attacks, we aid our adversaries by disaggregating the effects that they are achieving. Indeed, by interfering with the confidentiality and integrity of, as well as access to, information, adversaries can, in effect, generate a form of

disinformation or, alternatively, degrade our ability to counter, or disprove, other disinformation attempts. Labelling such efforts as attacks in cyber allows us to account for their effects. Of course, just as not all physical assaults are politically motivated, care must be taken when deciding whether particular cyber-attacks are the work of criminals, vandals, or state actors. However, these kinds of conclusions should be the fruit of investigations, not prima facie assumptions.

ATTACKS FROM CYBER

Attacks from cyber focus on disconnecting, damaging, or destroying devices that are connected to the Internet. Here the aim is not to steal data, but to disrupt some particular function. By 2025, it is estimated that there will be more than thirty billion connected devices in the Internet of Things (Vailshery, 2022): whether an industrial valve, an airplane, or a hospital, Web-connected devices are vulnerable to attacks from cyber.

These attacks use specially written code to interrupt the normal operations of peripheral devices, whether they are digital or mechanical in nature. The most famous such attack is the now legendary Stuxnet incident from 2011 (Kushner, 2013), which destroyed Iranian nuclear centrifuges. It is worth noting that the Stuxnet attacks involved extremely sophisticated means of generating the impression that no manipulation of the physical controllers was underway. In other words, in addition to the alteration of the intending function of the centrifuges, Stuxnet generated convincing disinformation meant to lull Iranian scientists into believing nothing was amiss. Since Stuxnet, the number of such networked systems has multiplied exponentially, meaning that the global vulnerability to such attacks has likewise ballooned. As Bruce Schneier (2018), a leading cyber-security expert, puts it, hackers can now crash your car, your pacemaker, or your city's power grid. That's catastrophic.

ATTACKS VIA CYBER

If attacks from cyber are the kinds of attacks that come to mind when we think of cyber security involving state adversaries, attacks via cyber are often regarded as "something else." Attacks from cyber do not target physical devices or stored data. Instead, their targets are us: "Disinformation is a tool commonly used by a number of states to sow discord, undermine faith in governing institutions, stoke fear and anxiety, and ultimately achieve certain policy goals" (CSIS, 2020). Given its ubiquitous presence in our lives,

Table 1.1. Effects-Based Cyber Attack Typology

Type of attack	Target	Modality	Effect	Example	Defence mechanism
On cyber	Network	Physical	Disruption/ destruction	Tonga 2019	Critical infrastructure protection (CIP)
In cyber	Data	Digital	Theft/denial/ corruption	OPM 2016	Information assurance (IA)
From *cyber*	Peripheral	Digital	Disruption/ destruction	Stuxnet 2010	CIP/IA
Via cyber	People	Information	Distrust	US election 2016	Resilience/ censorship

the Internet is a key conduit for such disinformation. Social media is particularly useful as a tool for spreading and amplifying false and/or divisive information and has been adroitly used by Russian operatives (Allyn, 2020). Some attacks via cyber have been used directly in conjunction with physical military operations (Sokol, 2019), while others have been used to "soften up" potential targets (Duszyński, 2020). In other cases, whether related to elections or COVID-19 response, the aim is to sow distrust and reduce the ability of societies to co-operate (Barnes, 2021).

Taken together, this framework allows us to better understand how malicious activities in cyberspace work. Rather than simply focusing on "whodunit" (criminals, spies, or hacktivists), it enables us to concentrate on the effects intended and, often, achieved. Such an integrated appreciation of cyber-attacks is important because, "unless statesmen [*sic*] understand the ways in which their opposite numbers see the world, their deterrence policies are likely to misfire; unless scholars understand the patterns of perceptions involved, they will misinterpret the behavior" (Jervis, 1982, p. 57). The British Ministry of Defence asserts that in today's world "our rivals employ an expanding, diverse and largely unregulated set of information tools to influence target audiences' attitudes, beliefs and behaviours. These weapons are increasingly employed above and below the threshold of war. They challenge international norms and restrict our response options. They work in the seams of our institutions, exacerbate societal divisions and prejudices, and lead people to cooperate, wittingly or unwittingly, in the undermining of democracy" (United Kingdom, 2021, p. 6).

Deterring by Defending

Deterrence relies on retaliation, or more correctly, the *threat* of some form of punishment following a transgression. As mentioned above, that clearly entails an element of capability: Is there the means available to retaliate? More so, though, deterrence hinges on the credibility of the threat: Even if means are available, is it believable that an adversary would act on their threats of retaliation? Many observers believe that deterrence is not possible in cyberspace, for this very reason: any attempt at reconstructing the norms and expectations that underpin deterrence in the physical world "fails to consider the unique characteristics of cyberspace" (Fischerkeller & Harknett, 2017). Difficulties surrounding attribution, for instance, make it hard to identify who to punish, for example.

The current approach to cyber security does not focus at all on the intended effects of its potential adversaries. It takes them for granted, labelling only certain kinds of incidents as attacks at all. Instead it proposes a "defend forward" strategy that sees American cyber assets operating persistently "over there" (United States of America, 2018). A number of other countries have also adopted similar strategies, relying on "offensive cyber operations" as a means of disrupting adversary activity, downplaying any kind of connection between that and defence or deterrence (Gold, 2020).

I contend that the notion of cyber uniqueness is often overstated. Yes, the particular details of how some attacks are carried out (through the routing of malicious code, for example) differs from what we see in the non-virtual world; by focusing on the effects of cyber-attacks we can see that, regardless of the way in which those attacks are carried out, it is possible to view them as analogous to other malicious acts, defend against them, and fit them into a deterrence framework. The aforementioned confusion surrounding the Nord Stream attacks are merely one such example.

Defence in cyberspace varies according to the particular threat. As the attack modality varies, so, too, will the means of protection. In the case of attacks on cyber, an approach that prioritizes the protection of critical infrastructure might be best: locking doors, erecting fences, and the like, as a way of preventing unauthorized entry to vulnerable network elements.[3] For attacks in and from cyber, the defences are less physical and more digital in nature, but nonetheless relatively straightforward. Maintaining "good cyber hygiene" (e.g., updating and patching programs, implementing stringent

access-control procedures, eliminating known vulnerabilities, such as obsolete VPNs and the like) may sound simple, but it has proven to be effective (Such et al., 2019). Indeed, many of the largest attacks in and from cyber have hinged on basic cyber hygiene errors, leading to large and long-lasting disruptions (Carnovale & Yeniyurt, 2021; Hemsley & Fisher, 2018; Kushner, 2013). Dissuading attackers through the use of robust defences is itself a form of deterrence, deterrence by denial (Wilner & Wenger, 2021).

Beyond a denial approach, the idea of deterrence by punishment requires "threats of wider punishment that would raise the cost of an attack" (Mazarr, 2018, p. 14). However, if we are too eager to "rule out" attacks and see incidents merely as vandalism, without considering what else might be going on, we undermine our own ability to comprehend what our adversaries are attempting. I contend that 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.

Defending against or deterring attacks via cyber warrants special mention. Although other forms of attack may include elements of disinformation, these attacks rely on disinformation to generate their intended effect. Here defence is extremely difficult because access to the intended target (the population) is often very easy. Indeed, in many countries around the world, including but not restricted to those in the West, social media usage is widespread. In Canada, for instance, there are estimated to be approximately thirty-five million social media users, and that figure is set to grow by over 10 per cent per year between now and 2030 (Dixon, 2023b). What is more, the average user is on social media for over two hours each day (Dixon, 2023a). The level of susceptibility to disinformation via these sources is enormous. What, then, is the best way to guard against such attacks?

One approach, favoured by democracies, is to boost what is called "societal resilience." Sweden, for instance, has created a national Psychological Defence Agency in order to enable its population to recognize and resist propaganda (Sweden, 2023). Such an approach is regarded by some as contributing to deterrence by denial (Braw & Roberts, 2019).

However, there is another route, and that is censorship. This works in a different fashion: rather than inoculating the population to recognize and dismiss potential disinformation, censorship aims at blocking such information from reaching the population in the first place. Originally favoured in autocracies and anocracies, such as China and Thailand, respectively

(Economy, 2018; Human Rights Watch, 2016), it has become a tactic in so-called open societies too. Governments and social media providers have been accused of implementing a variety of forms of censorship, often in the name of limiting disinformation (Goldberg, 2022). As discussed elsewhere in this volume, there is a fine line between defence and paternalism in this regard.

Ultimately, any attempt at developing and deploying an integrated approach to the array of activities that countries such as Russia and China are carrying out as part of a "hybrid warfare" campaign cannot afford to be disjointed. The typology presented here allows a wide range of cyber incidents to be properly understood as attacks, permitting the development of robust defence, and the generation of a deterrent effect.

NOTES

1 It should be noted that Waltz's enthusiasm for the spread of nuclear weapons relies on the fact that states possessing them would themselves be deterred from using such weapons.

2 It is important to point out that both of these terms have a somewhat slippery, polysemic quality that renders their use imprecise. For a discussion, see Janičatová and Mlejnková (2021).

3 See, for instance, United States of America (2021b).

REFERENCES

Allyn, B. (2020, 16 June). Study exposes Russia disinformation campaign that operated in the shadows for 6 years. *NPR*. https://www.npr.org/2020/06/16/878169027/study-exposes-russia-disinformation-campaign-that-operated-in-the-shadows-for-6-

Barnes, J.E. (2021, 5 August). Russian disinformation targets vaccines and the Biden administration. *New York Times*. https://www.nytimes.com/2021/08/05/us/politics/covid-vaccines-russian-disinformation.html

Blair, B., & Wolfsthal, J. B. (2019, 1 August). We still can't "win" a nuclear war. Pretending we could is a dangerous fantasy. *Washington Post*. https://www.washingtonpost.com/outlook/2019/08/01/we-still-cant-win-nuclear-war-pretending-we-could-is-dangerous-fantasy/

Braw, E., & Roberts, P. (2019, 25 March). *Societal resilience as a deterrent*. NATO Science and Technology Organization. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-11.pdf

Carnovale, S., & Yeniyurt S. (Eds.). (2021). *Cyber security and supply chain management: Risks, challenges and solutions*. World Scientific.

Chivvis, C. (2017). *Understanding Russian "hybrid warfare": And what can be done about it*. RAND Corporation. http://www.rand.org/pubs/testimonies/CT468.html

CSIS. (2020, 23 September). *Countering Russian disinformation*. Centre for Strategic and International Studies. https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation

Dixon, S. (2023a, 3 March). Average time spent on social media Canada 2023. *Statista*. https://www.statista.com/statistics/1317217/time-spent-on-social-media-in-canada/

Dixon, S. (2023b, 31 March). Canada: Social media users 2019–2028. *Statista*. https://www.statista.com/statistics/260710/number-of-social-network-users-in-canada/

Duszyński, J. (2020, 11 December). Russian disinformation in Latvia. *Baltic Rim Monitor*. Warsaw Institute. https://warsawinstitute.org/russian-disinformation-latvia/

Economy, E. C. (2018, 29 June). The great firewall of China: Xi Jinping's Internet shutdown. *The Guardian*. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Filippidou, A. (Ed.). (2020). *Deterrence: Concepts and approaches for current and emerging threats*. Springer.

Fischerkeller, M. P., & Harknett, R. J. (2017). Deterrence is not a credible strategy for cyberspace. *Orbis, 61*(3), 381–93. https://linkinghub.elsevier.com/retrieve/pii/S0030438717300431

Gibson, W. (2000). *Neuromancer*. Ace Books.

Gold, J. (2020). *The Five Eyes and offensive cyber capabilities: Building a "cyber deterrence initiative."* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf

Goldberg, J. (2022, 16 September). Opinion: How Ottawa's Internet censorship law will affect you. *Financial Post*. https://financialpost.com/opinion/opinion-how-ottawas-internet-censorship-law-will-affect-you

Hemsley, K., & Fisher, R. (2018). A history of cyber incidents and threats involving industrial control systems. In J. Staggs & S. Shenoi (Eds.), *Critical infrastructure protection xii, IFIP advances in information and communication technology* (pp. 215–42). Springer International.

Human Rights Watch. (2016, 21 December). Thailand: Cyber crime act tightens Internet control. *Human Rights Watch*. https://www.hrw.org/news/2016/12/21/thailand-cyber-crime-act-tightens-internet-control

Huntington, S. P. (1983). Conventional deterrence and conventional retaliation in Europe. *International Security, 8*(3), 32–56. https://www.jstor.org/stable/2538699?origin=crossref

The *Irish Times* view on undersea cables: A strategic threat. (2022, 28 July). *Irish Times*. https://www.irishtimes.com/opinion/editorials/2022/07/28/the-irish-times-view-on-undersea-cables-a-strategic-threat/

Janičatová, S., & Mlejnková, P. (2021). The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political-military discourse on Russia's hostile activities. *Contemporary Security Policy, 42*(3), 312–44. https://doi.org/10.1080/13523260.2021.1885921

Jervis, R. (1982). Deterrence and perception. *International Security, 7*(3), 3–30. http://www.jstor.org/stable/2538549

Jervis, R., Lebow, R. N., & Stein, J. G. (1985). *Psychology and deterrence*. Johns Hopkins University Press. https://muse.jhu.edu/book/74118

Kremlin eyes object found next to Nord Stream pipeline. (2023, 24 March). *Reuters*. https://www.reuters.com/world/europe/kremlin-important-identify-object-found-next-nord-stream-pipeline-2023-03-24/

Kushner, D. (2013, 26 February). The real story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. *IEEE Spectrum*. https://spectrum.ieee.org/the-real-story-of-stuxnet

Lopez, C. T. (2021, 30 April). Defense secretary says "integrated deterrence" is cornerstone of U.S. defense. *DOD News*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/2592149/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/

Mazarr, M. J. (2018). *Understanding deterrence*. RAND Corporation. https://www.rand.org/pubs/perspectives/PE295.html

Morris, L., Mazarr, M. J., Hornung, J. W., Pezard, S., Binnendijk, A., & Kepe, M. (2019). *Gaining competitive advantage in the gray zone: Response options for coercive aggression below the threshold of major war*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2942.html

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://direct.mit.edu/isec/article/41/3/44-71/12147

Paret, P., Craig, G. A., & Gilbert, F. (Eds.). (1986). *Makers of modern strategy: From Machiavelli to the nuclear age*. Princeton University Press.

Payne, K. B. (2011). Understanding deterrence. *Comparative Strategy, 30*(5), 393–427. https://doi.org/10.1080/01495933.2011.624814

Rid, Thomas. 2012. Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Sanger, D. E. (2020, 13 December). Russian hackers broke into federal agencies, U.S. officials suspect. *New York Times*. https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html

Sanger, D. E., Schmitt, E. (2015, 26 October). Russian ships near data cables are too close for U.S. comfort. *New York Times*. https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html

Schneier, B. (2018). *Click here to kill everybody: Security and Survival in a hyper-connected world*. W.W. Norton & Company.

Sokol, S. (2019, 2 August). Russian disinformation distorted reality in Ukraine. Americans should take note. *Foreign Policy*. http://foreignpolicy.com/2019/08/02/russian-disinformation-distorted-reality-in-ukraine-americans-should-take-note-putin-mueller-elections-antisemitism/

Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic cyber hygiene: Does it work? *Computer, 52*, 21–31. https://eprints.lancs.ac.uk/id/eprint/133762/1/cyber_hygiene.pdf

Sweden. (2023, 6 February). *Government taking strong action against disinformation and rumour-spreading campaign*. Government Offices of Sweden. https://www.government.se/press-releases/2023/02/government-taking-strong-action-against-disinformation-and-rumour-spreading-campaign/

Turton, W., & Mehrotra, K. (2021, 4 June). Hackers breached Colonial Pipeline using compromised password. *Bloomberg.* https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

United Kingdom. (2021). *Integrated operating concept 2025*. Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf

United States of America. (2018). *Summary: Department of Defense cyber strategy 2018*. Department of Defense. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_ SUMMARY_FINAL.PDF

United States of America. (2021a, 19 July). Four Chinese nationals working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including infectious disease research. *Justice News*. Department of Justice. https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

United States of America. (2021b, 28 July). National Security memorandum on improving cybersecurity for critical infrastructure control systems. *The White House*. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

Vailshery, L. S. (2022, 6 September). Global IoT and non-IoT connections 2010–2025. *Statista*. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

Waltz, K. N. (1981). The spread of nuclear weapons: More may be better: Introduction. *Adelphi Papers, 21*(171). https://doi.org/10.1080/05679328108457394

Westbrook, T. (2019, 23 January). Severed cable sends Tonga "back to beginning of the Internet." *Reuters*. https://www.reuters.com/article/us-tonga-internet-idUSKCN1PI0A8

Wilner, A. S., Wenger, A. (Eds.). (2021). *Deterrence by denial: Theory and practice*. Cambria Press.