National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

UNCONVENTIONAL DETERRENCE: WHY CYBER WARFARE DEMANDS A NEW APPROACH IN WESTERN DETERRENCE STRATEGY

Commander Christopher Wood

JCSP 45	PCEMI 45
Exercise *Solo Flight*	**Exercice *Solo Flight***
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

UNCONVENTIONAL DETERRENCE: WHY CYBER WARFARE DEMANDS A NEW APPROACH IN WESTERN DETERRENCE STRATEGY

Commander Christopher Wood

INTRODUCTION

Deterrence strategy came to prominence during the cold war; the more recent emergence of a multipolar global order has created renewed interest in deterrence as a means of avoiding or mitigating inter-state conflict. Yet, many of the theories that underpinned earlier iterations of deterrence strategy no longer apply in today's information age. Cold war deterrence was bi-polar and utilitarian: it assumed that leaders would make rational choices of costs and benefits within a strategic environment that was, with hindsight, relatively stable.[1] Today, the rapidly evolving face of inter-state warfare, often described as "hybrid" or "postmodern", is characterized by ambiguity and the emergence of new warfighting dimensions.[2]

Cyber warfare, the focus of this paper, typifies the challenges faced by state actors navigating this technically complex and normatively vague environment. The cyber dimension is characterized by uncertainty of both capabilities and effects, difficulties in attribution, and ambiguity in the interpretation and definition of what constitutes a military attack. The networks that form the battlefield, and which provide the means of delivery for most cyber attacks, are owned by commercial companies and shared with a global community of civilian, commercial, criminal, as well as military, users. There exists an absence of sovereignty, territorial boundaries and norms to inform interstate confrontation. These characteristics provide tempting options for military action short of,

[1] Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004), 5; Richard Ned Lebow, *Avoiding War, Making Peace* (Cham, Switzerland: Palgrave Macmillan, 2018), 65.

[2] Hans-Georg Ehrhart, "Postmodern warfare and the blurred boundaries between war and peace," *Defense & Security Analysis* 33, no.3 (2017): 263.

or perhaps in support of, kinetic attacks; but the potential for misunderstanding, miscalculation, and unintended collateral effects, is significant.

This paper argues that the effective inclusion of cyber capabilities within deterrence strategy is essential in moderating conflict between states. Focussing on state-based threats and responses, it will analyze the development, and sometimes neglect, of deterrence thinking alongside the emergence of the postmodern form of warfare. A behaviourist approach to decision-making will be taken to demonstrate why some assumptions that have underpinned deterrence theory have become invalid. The complex character of postmodern warfare demands that deterrence strategy be applied simultaneously across multiple domains, including cyber, and most likely in a non-linear fashion. Within such a strategy, the actual capability of cyber effects may be relatively modest, but the particular uncertainty they create has the potential to exert a disproportionate influence on the decisions of both the aggressor and the defender.

Whilst theory and strategy are discussed here in parallel, and it is axiomatic that the concepts *should* be mutually supporting, the paper acknowledges Richard Ned Lebow's distinction between, on the one hand, the logic and assumptions of deterrence theory and, on the other hand, discussion of the mechanisms by which this theory is applied in the real world; as Lebow argues, much cold war "theory" falls into the latter category.[3]

THE RISE AND FALL – AND RISE AGAIN – OF DETERRENCE STRATEGY

"Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them."[4] So wrote Bernard Brodie in 1946

[3] Lebov, *Avoiding War, Making Peace,* 65-66.

[4] Bernard Brodie, ed., *The Absolute Weapon* (New York: Harcourt, Brace, 1946), 76.

in his edited book *The Absolute Weapon*. Brodie's analysis was based on the devastating potential of nuclear weapons which, he correctly assumed, would soon be produced in significant numbers by both the United States (US) and the Soviet Union. In the absence of a credible defence against atomic weapons, deterrence could only be achieved by maintaining "the possibility of retaliation in kind."[5] In the context of the bipolar strategic environment, Brodie's logic appeared sound. The development, on both sides, of increasingly powerful thermonuclear weapons and intercontinental ballistic missiles, added further to the destructiveness of nuclear capabilities; whilst the ability to retaliate was ensured by "second strike" capabilities such as ballistic missile-carrying nuclear submarines. A massive first strike nuclear attack now conferred no particular advantage and so it was envisaged that a crisis would escalate incrementally until a nuclear threshold was reached. Herman Kahn conceived these steps as rungs on a ladder: "a linear arrangement of roughly increasing levels of intensity in a crisis." [6] Deterrence was based on the threat of punishment; it elevated the costs of nuclear war beyond those which either power could withstand.

Whether nuclear deterrence prevented direct conflict between the US and the Soviet Union is unknowable,[7] although the nuclear threat did not constrain American intervention in Vietnam[8] nor, later, Soviet adventurism in Afghanistan. Britain's

[5] *Ibid.*

[6] Herman Kahn, *On Escalation: Metaphors and Scenarios* (London, New York: Routledge, 2010), 38. https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=4925868.

[7] Robert P. Haffa, Jr., "The Future of Conventional Deterrence: Strategies for Great Power Competition," *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 98.

[8] General Westmoreland, the US military commander in Vietnam, proposed moving nuclear weapons into the theatre, but was overruled by President Johnson. This President's decision was apparently motivated by a fear of bringing China into a conventional war, rather than by concerns of Soviet or Chinese nuclear retaliation. New York Times, "U.S. General Considered Nuclear Response in Vietnam War, Cables Show," last modified 6 October 2018, https://www.nytimes.com/2018/10/06/world/asia/vietnam-war-nuclear-weapons.html.

possession of nuclear weapons did not deter Argentina from seizing the Falkland Islands and Britain did not threaten to use nuclear weapons in the Islands' recapture. Nevertheless, the strategy of deterrence by nuclear punishment remained dominant to the end of the cold war, underpinned by utilitarian assumptions of costs and benefits, and of linear escalation. Freedman argues that this durability was based on presentational features of nuclear deterrence that enabled (Western) governments to sustain political support for their policies: in particular, that it provided a narrative that made sense of the maintenance of an expensive nuclear arsenal; and that it became "a reflection of institutional inertia" to rationalize any defence procurement or position as contributing to deterrence.[9]

Cold war deterrence strategy contained inherent contradictions. Once it became impossible to think that a nuclear war between the superpowers could result in a victory for either side, it was difficult to view the threat of nuclear escalation as reasonable. Lebow argues that this resulted in a situation where leaders were forced to appear less rational than they really were, in order to maintain the credibility of nuclear deterrence. In doing so, they each came to feel more threatened by the other, and less certain in the robustness of their deterrence strategy. Lebow concludes, "The strategy of deterrence was self-defeating; it provoked the kind of behaviour it was designed to prevent."[10] The credibility of extended deterrence, such as that offered by the US to Western Europe through North Atlantic Treaty Organization (NATO) security guarantees, was even more

[9] Freedman, *Deterrence,* 11-14.

[10] Lebov, *Avoiding War, Making Peace,* 153.

difficult to maintain, since it required that the security of Europe would be achieved by the self-induced destruction of the US.

John Mearsheimer is credited with the incorporation of conventional deterrence into cold war theory. In particular, he argued the utility of deterrence through denial by convincing an adversary that its military goals will not be achieved.[11] Freedman argues that, "In principle, denial is a more reliable strategy than punishment because, if the threats have to be implemented, it offers control rather than continuing coercion."[12] The West could not afford a credible conventional defence during the cold war, so opportunity costs favoured a reliance on nuclear deterrence. However, deterrence through denial is pertinent in considering cyber threats.

Deterrence strategy fell out of favour at the end of the cold war. Freedman argues that this was largely due to circumstances rather than any intellectual challenge to the theory.[13] The US now enjoyed conventional military supremacy, and the means to project this almost anywhere in the world; combined with the rise in threats to its interests from failing states and non-state actors including violent extremist organisations, this led the US (aided by its allies) to adopt a strategy of armed pre-emption, for example the invasion of Iraq in 2003. Russia, despite having inherited most of the Soviet Union's nuclear arsenal, did not seek to constrain such actions. Freedman concludes, "if the USA was to be deterred, it was less likely to be because of some balancing military capability

[11] John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), 15. https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=4799673&query=.

[12] Freedman, *Deterrence*, 39.

[13] *Ibid.,* 21.

than because of the costs and frustrations associated with running territories, such as Afghanistan and Iraq, for which it had acquired some responsibility."[14]

Today, several factors again make deterrence a preferred strategy for the US and its allies. Russia and China pose authoritarian near-peer military challenges, whilst Iran and North Korea seek to develop capabilities that seriously threaten US interests. The strategy of pre-emption has meanwhile proved costly; its twin legacies are a reduction in the public appetite for prolonged overseas commitments, and, through the focus on counter-insurgency operations, a reduction in the American military's competitive technological edge. This strategic multipolarity, and the need for the US military to reprioritize lethality in its Joint Force, are recognized in the 2018 *National Defense Strategy*.[15] The new strategic environment shifts the assessment of costs and benefits compared to the post-cold war period; for example, Russia's intervention has considerably constrained the ability of the Western powers to influence the conflict in Syria.

If the assumption of Western freedom of action in the military-strategic environment has become too costly to maintain, then it follows that there is advantage in deterring some threats at lower cost. Yet, it is clearly not sufficient to dust-off cold war deterrence strategy and apply it in the modern environment because much has changed and the theory has not kept pace. Writing in 2011, James Blackwell argued forcefully that, "Today, our understanding of deterrence has atrophied. In fact, deterrence has been

[14] Freedman, *Deterrence*, 3.

[15] United States Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," Accessed 21 April 2019, http://nssarchive.us/national-defense-strategy-2018/2018-national-defense-strategy-summary/.

incarcerated … as if it were some kind of contagion that requires quarantine."[16] In the next sections, this paper will consider the new threats, capabilities and cognitive theory that require consideration for an effective deterrence strategy today. It does so through a Western perspective, and a focus on the cyber domain.

DETERRENCE THEORY AND THE CHANGING CHARACTER OF WARFARE

When deterrence strategy prevailed during the cold war, the threat of nuclear punishment was foremost. Conventional forces were understood to be armies, navies and air forces, which occupied the lower rungs of Kahn's escalation ladder. Nonnuclear deterrence was based mainly on denial; defeat of one side's conventional forces was a likely prelude to nuclear escalation, so punishment by conventional means received little attention. Today, deterrence must take into account far greater complexity. As Mueller observes, "Conventional deterrence is not simply another name for nonnuclear deterrence."[17] Deterrence must consider non-military means such as economic sanctions, new domains such as cyber, and improved lethality of both nuclear and nonnuclear military forces.

Erhart identifies five key elements of "postmodern warfare": information as a means of exercising power; networks, which increasingly include organisations that combine military and civil means; indirect and covert approaches; new technologies that enable long-range warfare, or which eliminate geographical constraints entirely; and irregular warfare doctrines. Collectively, these elements create a "grey zone" where activities take place that are directed towards an adversary but which do not fall under

[16] James Blackwell, "Deterrence at the Operational Level of War," *Strategic Studies Quarterly* (Summer 2011): 30.

[17] Karl P. Mueller, "Conventional Deterrence Redux: Avoiding Great Power Conflict in the 21st Century" *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 80.

established norms for warlike acts.[18] The term "hybrid warfare" is often used in relation to Russian strategy and perceived as somehow underhand and particularly threatening to democracies;[19] Ehrhart argues the equivalence of concepts popular in the West such as the "Comprehensive Approach" and "Whole of Government Approach."[20] Collectively, these elements add risk and complexity, but also provide opportunities for those who are willing to exploit the lower entry costs and ambiguous attribution of many grey zone activities.

Deterrence is fundamentally an exercise in power, defined by Barnett and Duvall as "…the production … of effects that shape the capacities of actors to determine their circumstances and fate."[21] By focussing on effects, it becomes apparent that a purely utilitarian comparison of costs and benefits for specific actions is not a sufficient basis for effective deterrence. Nye's definition of deterrence recognises the uncertainty of the value of costs and benefits; to him, deterrence means "dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."[22] Thus the ambiguity of the grey zone introduces uncertainty but also provides the means to influence an actor's appreciation of potential costs and benefits of a particular course of action. This line of argument moves away from a view of deterrence as a defence of the status quo, as it became during the bipolar era. The complexity of the modern strategic environment presents new opportunities for deterrence using a broader

[18] Ehrhart, *Postmodern Warfare* …, 264-266.

[19] See, for example, Tad A. Schnafer II, "Redefining Hybrid Warfare: Russia's Non-linear War against the West," *Journal of Strategic Security* 10, no. 1 (2017): 17-31. http://doi.org/10.5038/1944-0472.10.1.1538.

[20] Ehrhart, *Postmodern Warfare* …, 265.

[21] Michael Barnett and Raymond Duvall, "Power in International Politics," *International Organisation* 59, no. 1 (2005): 39.

[22] Joseph S. Nye, Jr, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 45. https://doi.org/10.1162/ISEC_a_00266.

range of means including cyber capabilities, to shape the strategic environment to advantage; this is sometimes described as "coercion" rather than "deterrence" but in the grey zone the difference between the two is less clear-cut.[23] Deterrence can support strategic change and need not be seen as purely reactive or defensive.

FRAMING THE CYBER DETERRENCE SPACE

Cyber, which is characterized by uncertainty and challenges of attribution, spans the full spectrum of Ehrhart's exposition of postmodern warfare. Martin Libicki has argued that cyber capabilities can contribute to a broader deterrence strategy, although their utility is constrained by uncertainty of the consequences of action and retaliation, and by the absence of a deterrence scale for cyber actions to determine what constitutes a reasonable and credible response.[24] The following sections will consider how the difficulty of attribution and general uncertainty of cyber effects may used to advantage in deterrence, whilst promoting the development of norms and other mechanisms to mitigate the most destabilising tendencies.

An analysis of approaches to cyber warfare is complicated by the fact that specific capabilities or, as in the UK case, entire doctrines, are classified.[25] Nye identifies a tendency in Western military circles to define cyber as an environmental domain in the same vein as air, land, maritime and space; however, he argues cyber is also a range of instruments that can be employed across environments and so "it is a mistake to see the cyber realm in isolation."[26] The US Department of Defense defines cyberspace very

[23] Brian M. Mazanec and Bradley A. Thayer, *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* (Basingstoke, England: Palgrave Macmillan, 2015), 30.

[24] James J. Libicki, "Expectations of Cyber Deterrence," *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 45.

[25] UK Cyber Doctrine, Joint Doctrine Publication 0-50, is classified UK Secret.

[26] Nye, "Deterrence and Dissuasion …", 46.

broadly as “the domain within the information environment that consists of the interdependent network of information technology structures and resident data,” including the Internet, communication networks, computer systems and “embedded processors and controllers.”[27] The latter reference invites a clear connection to the Stuxnet attack, widely attributed to (although not acknowledged by) the US, on the Iranian nuclear weapons programme; this targeted a specific type of centrifuge controller and may have been the first cyberattack to cause actual physical destruction.[28] It also highlights official recognition of the threat posed by cyberattack to critical civilian infrastructure.

The rapid growth in the importance of computer networks to society is striking. In 1995, less than half of one percent of the world's population had access to the Internet.[29] At the end of 2018, more than half the global population of 8 billion was online, with the greatest penetration being in Europe and the Americas.[30] Economic and societal dependence on the Internet has introduced new vulnerabilities that may be exploited by hostile states, proxies, criminals and variously-motivated hackers. The magnitude of the threat, particularly the prospect of a nationally-disabling “cyber Pearl Harbor” attack, is difficult to assess. As Libicki observes, “When the potential of cyberattack has been

[27] United States Department of Defense, Joint Doctrine Publication 3-12, *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 8 June 2018), I-1, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[28] Mazanec and Thayer, *Deterring Cyber Warfare* …, 21.

[29] Internet World Stats, “Internet Growth Statistics,” accessed 25 April 2019, https://www.internetworldstats.com/emarketing.htm.

[30] UN News, “Internet Milestone Reached, as More Than 50 Per Cent Go Online: UN Telecoms Agency,” last modified 7 December 2018, https://news.un.org/en/story/2018/12/1027991.

likened to nuclear attack *and* where cyberattacks, as oft observed, have yet to kill anyone, making a credible case for equivalence [of a kinetic attack] ... is fraught."[31]

Defining the parameters of military cyber defence and deterrence is also challenging, potentially including everything from safeguarding critical national infrastructure to prevention of denial of Internet service and even cryptojacking and ransomware attacks.[32] In assessing likely threats as a product of capability and intent, the difference between espionage through Computer Network Exploitation (CNE), and a more serious Computer Network Attack (CNA) may amount only to a few keystrokes.[33] Helpfully, there is a growing body of evidence which indicates that many states regularly engage in cyber warfare; whilst definitive attribution of attacks is rarely achieved, it is possible to discern the boundaries of the emerging battlefield of interstate cyber warfare and, therefore, to frame the position of cyber capabilities within deterrence strategy.

In the public consciousness, Stuxnet remains the most widely known example of interstate cyberattack, but attacks on Estonia in 2007, and Georgia in 2008, offer more likely scenarios for large-scale interstate cyber warfare. In 2007, Estonia experienced a series of coordinated Distributed Denial of Service (DDOS) attacks on Internet and Web-based services. This type of attack aims to disrupt a network or server by overwhelming it with additional malicious traffic, causing the network to slow down.[34] Internet traffic from outside Estonia peaked at 400 hundred times normal levels and involved tens of millions of computers in numerous countries. The DDOS attacks accompanied the

[31] Libicki, "Expectations of Cyber Deterrence," 50.

[32] "Toward a Cyber Deterrence Strategy?", *Endgame* (blog), 21 May 2018, https://www.endgame.com/blog/technical-blog/toward-cyber-deterrence-strategy.

[33] Mazenac and Thayer, *Deterring Cyber Warfare* …, 7.

[34] Cloudflare, "What is a DDoS Attack?" accessed 25 April 2019, https://www.cloudflare.com/en-ca/learning/ddos/what-is-a-ddos-attack/.

Estonian government's removal of a Soviet-era statue in the capital, Tallinn, and therefore Russia is the most likely culprit for these attacks, which represented the first sophisticated DDOS attack against a state.[35] The following year, the former Soviet state of Georgia was subjected to a DDOS attack that significantly disrupted government communications, in conjunction with a Russian military invasion of parts of the country. Although attribution has not been achieved, it is reasonable to assume the attacks were orchestrated by the Russian military.[36] This represents an early example of Russia's hybrid approach in coordinating cyber and other grey zone activities as conventional force multipliers, a strategy replicated in its annexation of the Crimea and infiltration of parts of Eastern Ukraine from 2014 onwards. Such examples demonstrate the most serious military cyber threats and frame the contested space where cyber should contribute to a broader strategy of interstate deterrence.

On a more general level, millions of cyberattacks take place across the information domain every day.[37] The Washington DC-based Center for Strategic and International Studies, in conjunction with the cyber security company McAfee, estimated in 2018 that cyber crime costs the world economy $600 billion annually, around 0.8 percent of global gross domestic product.[38] The Internet also provides a ready means for non-attributable propagation of disinformation and public influence activity, much discussed at present in the context of allegations of Russian influence in President

[35] Mazenac and Thayer, *Deterring Cyber Warfare* …, 18-19.

[36] *Ibid.,* 20.

[37] Nye, “Deterrence and Dissuasion …”, 47.

[38] Center for Strategic & International Studies, “Economic Impact of Cybercrime,” last modified 21 February 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

Trump's election victory,[39] or the Brexit referendum in the United Kingdom.[40] Such ubiquitous, malicious cyber activity cannot realistically be included in a deterrence strategy, even if some of it is conducted by states or their proxies; nevertheless, as discussed further below, it may provide opportunities to strengthen the credibility of a cyber contribution to a more general deterrence strategy.

MAKING CYBER WORK FOR DETERRENCE STRATEGY

Uncertainty of Capabilities and Effects

Unlike kinetic weapons, possession of a cyberattack capability does not indicate an ability to strike at any target within range. Offensive cyber capabilities are specific to their intended target and may take considerable time to prepare. The likely result of an attack, whether or not it will achieve its intended effect, cannot be predicted with the same degree of confidence as for a conventional military action because both the offensive capability, and the defensive cyber capability of the adversary, are uncertain and specific to a particular case.[41] The effects of a conventional military attack are more certain, although such forces may also require significant time to generate and apply desired effects;[42] in this case, however, the buildup of force is visible to the adversary and

[39] The diversity of the means by which Russia is alleged to have interfered in the 2016 presidential election is illustrated by this recent article in the *New York Times* arguing that racial divisions were exploited by a campaign run by a Russian-based Internet research agency: New York Times, "Russian Efforts to Exploit Racial Divisions in 2016 Found Firm Ground in U.S., Report Says," last modified 6 May 2019, https://www.nytimes.com/2019/05/06/us/russia-disinformation-black-activists.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection.

[40] For example, Russian "Internet Trolls" are alleged to have used Twitter to spread divisive information during the UK European Union referendum campaign. The Telegraph, "Russian Trolls Sent Thousands of Pro-Leave Messages on Day of Brexit Referendum, Twitter Data Reveals," last modified 17 October 2018, https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/.

[41] Libicki, "Expectations of Cyber Deterrence," 51.

[42] John Stone, "Conventional Deterrence and the Challenge of Credibility," *Contemporary Security Policy* 33, no. 1 (2012): 113.

so shapes his freedom of decision-making in a way that planning a cyberattack does not. Libicki argues that the threat of punitive cyberattack is less compelling than that of kinetic strike, because cyberattack lacks both immediacy and predictability of effect, whilst cyber in support of kinetic action is unlikely to be a first-order consideration for an adversary because kinetic effects are likely to result in greater damage and are easier to incorporate into the other side's decision-making.[43] Further, the interpretation of a cyberattack attack can be ambiguous: does an apparently minor attack represent a successful demonstration of latent capability, or the failure to realise a more significant intent?[44] The inherent narrowness of cyberattack capabilities, and the absence of an assured general capability to strike through cyber means, implies that the contribution of offensive cyber to a broader strategy of deterrence is likely to remain limited.

Conversely, because of the specificity of cyberattack capability, a small adjustment by the target may have a greater relative effect than if the threat were kinetic.[45] If considering cyber in isolation, this implies than denial may be a more effective deterrence strategy than punishment. However, it should also be borne in mind that a cyberattack does not always require a cyber response. Reflecting the characteristics of postmodern warfare, deterrence strategy can also assume a non-homogenous, non-linear approach. For example, the UK's recent doctrine note, *Deterrence: the Defence Contribution* (the title itself indicates the commitment to the "Whole of Government Approach") states that, "Integration across domains raises potential costs for the adversary and enhances deterrence. For example, a kinetic strike might be conducted …

[43] Libicki, "Expectations of Cyber Deterrence," 46.
[44] Nye, "Deterrence and Dissuasion …", 49.
[45] Libicki, "Expectations of Cyber Deterrence," 54.

in response to a cyberattack… ."[46] For denial to be most effective it must be seen to have worked. This implies a need for better and more public attribution of attacks and the countermeasures employed, and the development of norms to support the deterrence narrative. These aspects are discussed later in the paper.

The Behaviourist Approach to Understanding Decision-Making Under Uncertainty

In either the offensive or defensive cases, a straightforward assessment of costs and benefits of cyberattack is impossible because the potency of the attack, and the effectiveness of the defence, cannot be understood in advance. Instead, as Blackwell has argued, a behaviourist approach that seeks to understand how an adversary is likely to view the balance of these uncertain risks, and how they may respond in different situations, is needed.[47]

In 2002, when few people were thinking about deterrence theory, the behavioural psychologist Daniel Kahneman was awarded the Nobel Prize for Economic Sciences for the advances he and his colleague, Amos Tversky, had made in understanding human decision-making under uncertainty.[48] Kahneman and Tversky's work included a study of utility theory, which underpins economic theory but which they found to be imperfectly applied by real humans. In their 1984 paper *Choices, Values and Frames*, they demonstrated how human subjects making risky decisions (i.e. those where costs and benefits are expressed as probabilities rather than certainties) are prone to overweighting

[46] United Kingdom Ministry of Defence, Joint Doctrine Note 1/19, *Deterrence: the Defence Contribution* (Swindon: Defence Concepts and Development Centre, 2019), 42.

[47] Blackwell, "Deterrence at the Operational Level …", 35.

[48] The Nobel Prize, "The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2002," last modified 9 October 2002, https://www.nobelprize.org/prizes/economic-sciences/2002/press-release/.

of low probabilities and underweighting of high probabilities.[49] Humans are naturally and unconsciously risk-averse in some situations and risk-seeking in others. Applied to a set of concurrent decisions, Kahneman and Tversky demonstrated that “invariance”, the utilitarian assumption that a comparison of costs and benefits should always result in the same judgement, is “psychologically unfeasible”.[50] The consequences for deterrence strategy are clear: leaders cannot be assumed to be rational. This does not mean that actors do not make reasonable decisions, but rather that their judgements do not consistently support their conscious values. The assessment is independent of the type of uncertainty afforded to costs and benefits in the grey zone (Kahneman and Tversky’s subjects were offered choices based on mathematical probabilities); therefore, any theory of deterrence which invites an actor to choose between costs and benefits, however these are presented or implied, cannot assume a rational, utilitarian response.

This non-linear attribution of decision weights is amplified through the “endowment effect”[51] that values what one currently has over what might be gained or lost by a particular decision. This has significant implications for the role of cyber effects in deterrence. For example, it has been argued that threatening a cyber response in place of conventional military action may have the opposite effect to that intended because, “The substitution of something that *might* be painful for something that *would* be painful may *reduce* the overall deterrence posture.”[52] However, whether or not this would actually be the case would depend on the adversary’s perspective of his position and the

[49] Daniel Kahneman and Amos Tversky, “Choices, Values, and Frames,” *American Psychologist* 34 (1984), reproduced in Daniel Kahneman, *Thinking Fast and Slow* (Canada: Anchor, 2013), Appendix B, 439.

[50] *Ibid., 438.*Annex B, 438.

[51] Attributed to Thaler (1980) in Kahneman and Tversky, “Choices, Values, and Frames,” 444.

[52] Libicki, “Expectations of Cyber Deterrence,” 50.

relative value assigned to the gains and losses of action. An actor who is already in a strong position may view the gains of taking action as relatively small compared to the losses associated with the threatened reprisal; their tendency to overweight the smaller, uncertain risk, combined with the fear of a large loss, may make them especially risk-averse and willing to accept an unfavourable settlement. This is not to say that the threat of conventional military punishment would not also be effective; but it would be much more costly to the deterrer. Conversely, as Lebow has argued, a leader in a weaker position, who is driven by vulnerability rather than opportunity, may feel compelled to go to war in search of a large, albeit highly improbable, gain.[53] This analysis illustrates the futility of trying to assign to a leader such as Kim Jong-Un a tag of "rational" or "irrational" as a basis for deterrence. A perspective of gains and losses is more informative than an assessment of costs and benefits, and demonstrates how relatively modest cyber capabilities have potential to be disproportionately influential in some deterrence situations.

Persistence, Norms, Attribution and Entanglement

As demonstrated earlier, it is apparent that many states routinely conduct cyberattacks against their competitors. The relatively low costs of doing so, combined with the minimal risk of positive attribution, provide little disincentive. For this reason, Fischerkeller and Harknett have argued that attempting to deter cyberattack is counter-productive and escalatory since frequent failures of denial can only lead to greater frequency of punishment and the incurred costs associated with this. Instead, they advocate a strategy of "cyber persistence" that is enabled by continual contact and the

[53] Lebow, *Avoiding War, Making Peace,* 82.

versatility in cyberspace to inflict reversable damage without engaging in armed conflict.[54] There are benefits to this approach. Firstly, acknowledging the military inability to deter most cyberattacks encourages commercial and personal users of networks to implement protective cyber measures thus adding resilience generally and mitigating the threat to society of large-scale cyberattack. Secondly, since cyber capabilities can only be demonstrated through successful use, persistence provides credibility; this in turn enables narrow effects to be framed in terms of more general capability that contributes to deterrence overall. Fischerkeller's and Harknett's proposition is therefore useful, although limited by its consideration primarily of the cyber realm. By considering deterrence across multiple dimensions, as discussed earlier, it is still relevant to apply a threat of punishment to deter some cyberattacks; this will be most effective when supported by a normative framework that enables equivalence of cyber and other effects to be determined.

Norms are rules or expectations that are socially enforced; they encourage positive behaviour and discourage negative behaviour.[55] In regular warfare, norms have been legalized and institutionalized, for example through the Geneva Conventions, the United Nations (UN), and the International Criminal Court. Normative considerations can deter by imposing reputational costs that exceed the gains from an attack, and are therefore effective even without the threat of retaliation.[56] Mazanec and Thayer argue for the development of cyber norms, to both limit the use and development of cyber weapons and

[54] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61, Issue 3 (2017): 387-388. https://doi.org/10.1016/j.orbis.2017.05.003.

[55] Oxford Bibliographies, "Norms," last modified 11 January 2018, http://www.oxfordbibliographies.com/view/document/obo-9780199756384/obo-9780199756384-0091.xml.

[56] Nye, "Deterrence and Dissuasion …", 60.

to lower the evidentiary standards for attribution.[57] On the first count, the UN's Group of Government Experts (GGE) on information and telecommunications security declared in 2015 that "a State should not conduct or knowingly support … activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure."[58] However, the GGE's June 2017 session ended without consensus amid fundamental disagreements between states of the right to self-defence and applicability of international humanitarian law in cyber warfare.[59] Thus, it appears that top-down efforts to impose norms in cyberspace are for the moment stalled.

It seems likely that, in the short term, cyber norms will develop more organically, as states move towards a consensus of what is acceptable and what requires an external response. For example, the NATO's Tallinn Manual on the International Law Applicable to Cyber Warfare articulates a view of what constitutes cyberattack, and restates the right of self-defence within this definition;[60] this position must be taken into account by any adversaries and so has the potential to become a normative feature of cyberspace that also informs the "red lines" that could elicit punishment. To be effective, however, an improved ability to enable attribution of cyberattacks is required.[61]

Whilst the application of humanitarian law in cyberspace may be problematical, Stone argues that for Western powers deterrence must uphold the principles of proportionality and discrimination because to do otherwise "would be hypocritical in the

[57] Mazenac and Thayer, *Deterring Cyber Warfare* …, 46-47.

[58] United Nations General Assembly, *Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: UN, 22 July 2015), 2.

[59] Stefan Soesanto and Fosca D'Incau. "The UN GCE is Dead: Time to Fall Forward." *European Council on Foreign Relations* (blog), 15 August 2017, https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

[60] *Ibid.*

[61] Nye, "Deterrence and Dissuasion …", 60.

extreme" and counterproductive in terms of legitimacy and narrative.[62] In accepting such constraints and the asymmetric costs associated with them, Western powers may hope to be seen as "norm entrepreneurs"[63] who can promote the development of accepted cyber behaviour in their interests. However, as Mazanec and Thayer point out, the US reputation as a moral actor in cyberspace was dealt a significant blow by the 2013 Edward Snowden leaks that demonstrated the full range of US offensive cyber activities.[64]

Attribution, as shown by the examples of cyberattack cited earlier, is likely to remain difficult to achieve within established evidentiary standards. Even when the circumstantial link is clear, use of proxies and multiple layers of security mask the true source of an attack. Mazanec and Thayer propose both a lowering of the evidentiary standard and the development of "cyber forensics"[65] to aid attribution, although this represents a technical solution whereas the normative influence it would support is based on a social contract. A technically complicated proof of hostile cyberattack might not be any more convincing to the public than the adversary's flat denial of responsibility.

If attribution is difficult for now, Nye instead introduces the concept of "entanglement". This refers to the interdependencies that exist between all states, and which simultaneously impose costs on both the attacker and the target.[66] Entanglement is effective because it does not rely either on norms or attribution, but rather on the attacker's assessment of broader potential losses associated with action. In the cyber

[62] Stone, "Conventional Deterrence …", 111.
[63] Mazenac and Thayer, *Deterring Cyber Warfare* …, 48.
[64] *Ibid.,* 53.
[65] *Ibid.,* 58.
[66] Nye, "Deterrence and Dissuasion …", 58.

domain, entanglement is inherent in any attack that uses the Internet, which is itself a collection of interdependent servers and communication links. Because the Internet is not constrained by geography, an attack which is targeted at another state may spread unintentionally to affect neutral states, allies, or the attacker itself – a phenomenon known as "blowback". For example, the Stuxnet virus, despite being introduced to a system not connected to the broader Internet, is thought to have infected around 40,000 computers outside Iran.[67]

Entanglement provides a mechanism that influences the behaviour of states without reference to attribution, norms, or threats of punishment or denial. This type of self-restraint is powerful. Whilst the cold war adversaries were not anywhere near as interconnected as all states are today, Lebow argues that "self-deterrence" through the reluctance of states to accept the risks of armed conflict, independent from any action taken by the other side, was a more effective restraint than even nuclear deterrence strategy.[68]

CONCLUSION

Deterrence was seen as a strategy of the cold war and had been neglected since the decline of the Soviet threat. In the meantime, both the character of interstate war and our understanding of human decision-making and risk taking have evolved considerably. This paper has argued for the inclusion of cyber into deterrence strategy in the age of

[67] Mazenac and Thayer, *Deterring Cyber Warfare* …, 6, 20.
[68] Lebow, *Avoiding War, Making Peace,* 8.

postmodern warfare. Deterrence can be effective if it is flexible, multi-dimensional and non-linear; and underpinned by behaviourist rather than utilitarian theory.

In cyber, denial is likely to be effective, whilst punishment is problematic. Actors are likely to be constrained less by norms imposed through developments in international law, than by entanglement and the threat of punishment by cyber or other means. The role of cyber within broader deterrence strategy is likely to be modest, although this paper has identified circumstances where the threat of cyber punishment may have a disproportionate effect at less cost than conventional military means. A credible cyber capability should be demonstrated, and continually developed, through a strategy of cyber persistence that acknowledges the futility of attempting to deter minor attacks and that exploits the inherent fluidity of cyberspace.

However, there are two outstanding elements of an effective cyber deterrence regime that may take some time to implement: attribution and norms. It must be assumed for now that international agreement on these will not be forthcoming. Therefore, if cyber is to be fully incorporated into Western deterrence strategy, either through inclusion in the range of available punishment capabilities, or in determining a scale of equivalence in responding to hostile cyberattacks, then the US and its allies must adhere to a coherent set of norms and attribution standards that limit the capacity of states such as Russia, China, Iran and North Korea to act without consequence.

A larger question may be the extent to which cyber, and other elements of postmodern warfare, benefit authoritarian regimes over democracies. China in particular seeks to insulate itself and its citizens from the broader Internet, whilst adopting an ambivalent attitude towards established international authorities when they do not suit national interests. Meanwhile, there is widespread concern of the security consequences of allowing the Chinese telecommunications giant Huawei to provide equipment for new 5G data networks.[69] Yet, whilst it is easy to argue that China does not have an interest in sharing cyber norms and attribution standards with the Western allies, its transition from challenger to established power may change its evaluation of potential gains and losses in cyberspace.

Russia may also discover that its current isolation, whilst protecting it from entanglement in the cyber domain, does not provide long-term advantage in an interconnected world. This leaves the US to choose between the values it publicly espouses and its conduct to date in cyberspace. The need to incorporate cyber into a deterrence strategy that is coherent with its allies, strongly implies that the US should forego the temptations of unattributable cyberattack and take the lead in developing a normative regime that encourages long-term stability in the interactions between major powers.

[69] BBC News, "Vodafone Denies Huawei Italy Security Risk," last modified 30 April 2019, https://www.bbc.com/news/business-48103430.

BIBLIOGRAPHY

Barnett, Michael, and Raymond Duvall. "Power in International Politics." *International Organisation* 59, no. 1 (2005): 39-75.

BBC News. "Vodafone Denies Huawei Italy Security Risk." Last modified 30 April 2019. https://www.bbc.com/news/business-48103430.

Blackwell, James. "Deterrence at the Operational Level of War." *Strategic Studies Quarterly* (Summer 2011): 30-51.

Brodie, Bernard, ed., *The Absolute Weapon*. New York: Harcourt, Brace, 1946.

Center for Strategic & International Studies. "Economic Impact of Cybercrime." Last modified 21 February 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

China. The Permanent Mission of the People's Republic of China to the United Nations. *Note Verbale CML/17/2009.* (7 May 2009). http://www.un.org/depts/los/clcs_new/submissions_files/mysvnm33_09/chn_2009re_mys_vnm_e.pdf.

Cloudflare. "What is a DDoS Attack?" Accessed 25 April 2019. https://www.cloudflare.com/en-ca/learning/ddos/what-is-a-ddos-attack/.

Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." *Defense & Security Analysis* 33, no.3 (2017): 263-275.

Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, Issue 3 (2017): 381-393. https://doi.org/10.1016/j.orbis.2017.05.003.

Freedman, Lawrence. *Deterrence*. Cambridge: Polity Press, 2004.

Haffa, Robert P. Jr. "The Future of Conventional Deterrence: Strategies for Great Power Competition." *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 94-115.

Internet World Stats. "Internet Growth Statistics." Accessed 25 April 2019. https://www.internetworldstats.com/emarketing.htm.

Kahn, Herman. *On Escalation: Metaphors and Scenarios.* London, New York: Routledge, 2010. https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=4925868.

Kahneman, Daniel. *Thinking, Fast and Slow.* Canada: Anchor, 2013.

Libicki, James J. “Expectations of Cyber Deterrence.” *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 44-57.

Lebow, Richard Ned. *Avoiding War, Making Peace*. Cham, Switzerland: Palgrave Macmillan ,2018.

Mazanec, Brian M. and Bradley A. Thayer. *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace.* Basingstoke, England: Palgrave Macmillan, 2015.

Mearsheimer, John J. *Conventional Deterrence.* Ithaca: Cornell University Press, 1983. https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=4799673&query=.

Mueller, Karl P. “Conventional Deterrence Redux: Avoiding Great Power Conflict in the 21st Century.” *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 76-93.

New York Times. “Russian Efforts to Exploit Racial Divisions in 2016 Found Firm Ground in U.S., Report Says.” Last modified 6 May 2019. https://www.nytimes.com/2019/05/06/us/russia-disinformation-black-activists.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection.

New York Times. “U.S. General Considered Nuclear Response in Vietnam War, Cables Show.” Last modified 6 October 2018. https://www.nytimes.com/2018/10/06/world/asia/vietnam-war-nuclear-weapons.html.

Nye, Joseph S. Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/17): 44-71. https://doi.org/10.1162/ISEC_a_00266.

Oxford Bibliographies. “Norms.” Last modified 11 January 2018. http://www.oxfordbibliographies.com/view/document/obo-9780199756384/obo-9780199756384-0091.xml.

Schnaufer, Tad A. II. “Redefining Hybrid Warfare: Russia’s Non-linear War against the West.” *Journal of Strategic Security* 10, no. 1 (2017): 17-31. http://doi.org/10.5038/1944-0472.10.1.1538.

Stone, John. “Conventional Deterrence and the Challenge of Credibility.” *Contemporary Security Policy* 33, no. 1 (2012): 108-123.

The Nobel Prize. “The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2002.” Last modified 9 October 2002. https://www.nobelprize.org/prizes/economic-sciences/2002/press-release/.

The Telegraph. “Russian Trolls Sent Thousands of Pro-Leave Messages on Day of Brexit Referendum, Twitter Data Reveals.” Last modified 17 October 2018. https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/.

United Kingdom. Ministry of Defence. Joint Doctrine Note 1/19, *Deterrence: the Defence Contribution.* Swindon: Defence Concepts and Development Centre, 2019.

United Nations General Assembly. *Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: UN, 22 July 2015.

United States. Department of Defense. Joint Doctrine Publication 3-12. *Cyberspace Operations.* Washington, DC: Joint Chiefs of Staff, 8 June 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

United States. Department of Defense. “Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge.” Accessed 21 April 2019. http://nssarchive.us/national-defense-strategy-2018/2018-national-defense-strategy-summary/.

UN News. “Internet Milestone Reached, as More Than 50 Per Cent Go Online: UN Telecoms Agency.” Last modified 7 December 2018. https://news.un.org/en/story/2018/12/1027991.