TNO innovation for life

The Hague Centre for Strategic Studies

HCSS SECURITY

Cross Domain Deterrence and Hybrid Conflict

Tim Sweijs and Samo Zilincik

The Hague Centre for Strategic Studies

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

Cross Domain Deterrence and Hybrid Conflict

HCSS Security
The Hague Centre for Strategic Studies

ISBN/EAN: 9789492102706

Authors: Tim Sweijs and Samo Zilincik
December 2019

Design: Mihai Eduard Coliban (layout) and Constantin Nimigean (typesetting).

The Hague Centre for Strategic Studies
info@hcss.nl
hcss.nl

Lange Voorhout 1
2514EA
The Hague
The Netherlands

HCSS SECURITY

Cross Domain Deterrence and Hybrid Conflict

Tim Sweijs and Samo Zilincik

Table of contents

Executive Summary

In this era of rapid technological, social, economic and political change, increasing interstate competition and swift strategic innovation, hybrid strategies have become part and parcel of contemporary statecraft. Thus far, Western liberal democracies have not been able to effectively counter the hybrid strategies of other actors. In fact, these actors have seized the strategic initiative by synergistically deploying a variety of instruments of influence across different domains. The approaches of liberal democracies towards these strategic innovations has been largely *reactive* rather than *proactive* in nature. Liberal democracies have had trouble articulating effective strategies and the process of designing new postures to address a salient form of contemporary conflict is still in its early stages. This paper argues that deterrence can be an important component of such a posture, although the emergence of new strategic challenges necessitates the evolution and adaptation of traditional concepts of deterrence. If deterrence-by-punishment and deterrence-by-denial may have been appropriate in dealing with the threat of a nuclear attack or the large-scale conventional invasion of the North German Plain by the Soviet Union, contemporary challenges require novel forms of deterrence. The potential role of deterrence in countering hybrid activities requires a better understanding of the utility of different concepts of deterrence applied to different single domains *and* across different domains, which needs to build on an emerging body of literature on cross domain deterrence (CDD). This paper reviews the rise of CDD in the context of deterrence theory as a concept that has been developing over the past few years but predominantly in a military context, and it argues that CDD is applicable also to hybrid domains. It then turns to four problems and four arguments posited against the feasibility of deterrence against hybrid threats by liberal democracies related to *attribution*, *proportionality*, *signaling* and the *nature of liberal Western democracies*. In reviewing and refuting these arguments, it adduces insights concerning the use and utility of CDD against hybrid threats and identifies the prerequisites for deterrence to play a role in an overall strategic posture to deal with cross domain hybrid activities.

Attribution capabilities are rooted in a combination of robust situational awareness, contextual understanding, political willingness, and a legal framework that stipulates the level of evidence necessary for attribution. This underscores the need for liberal democratic governments to maintain robust monitoring capabilities to expose hybrid actions in a timely fashion, in combination with a vigorous research and analysis infrastructure to understand the geopolitical context underlying these actions.

It also requires tackling larger legal questions associated with how to share sensitive information on attribution with parliament that is necessary for democratic oversight, as well as under which conditions attribution is considered legitimate from within a legal perspective. Whether political leadership will muster the will to perform attribution is another question all-together. All things equal, however, political willingness is likely to be greater if these issues are actively addressed.

Developing standards of proportionality in the service of deterrence is certainly complicated, yet it is not impossible. Liberal democratic governments should develop options of what they deem inappropriate behavior and what they consider to be proportionate responses across different domains in the service of deterrence. The development of responses will also contribute to the establishment of new norms of behavior, if such norms are developed, and communicated not only reactively but also proactively. The level of detail at which these options should be formulated may be subject to debate (as an opponent may venture precisely clear just below that threshold) and should merit further attention.

Part of the signaling effort is to share the menus containing options with allies, as well as with adversaries. Successful signaling entails the synchronization of communication efforts at the political, strategic, and tactical level in a consistent manner. In addition to streamlining communication efforts in strategies, doctrines and verbal messages, it also requires that liberal democratic governments showcase their capabilities to adversaries and have clear guidelines when transgressions will be punished at the tactical level. Such a coordinated effort is instrumental in creating a shared understanding of the rules of the game which underlies a deterrent-based relationship.

Finally, liberal democracies are not inherently incapable of developing hybrid capabilities. In fact, liberal democracies have been actively engaging in hybrid activities in the past, sometimes outside but more often within the purview of democratic checks and balances within their systems. However, the legal framework framing hybrid options in the service needs further development. At the national level, it requires consideration of the legal framework associated with civilian, military and other actors in terms of roles, prerogatives and responsibilities. This should be analyzed through the lens of intelligence collection and the freedom to operate within and outside of one's own borders. Moreover, the legal status of cyber measures requires closer examination in order for measures to be developed and implemented in the service of deterrence. At the international level, it will be necessary to develop new regimes that codify appropriate measures and countermeasures to which actors can commit, and thereby shape escalation dynamics. Overall, it is time to seize back the strategic initiative, and start taking hybrid deterrence seriously.

1. Introduction[1]

The use and utility of deterrence has been garnering renewed interest from policymakers, strategists and scholars in recent years. Deterrence refers to the practice, the process or the situation in which one state relies on the prospect of harm to persuade an opponent not to engage in certain specified behaviour.[2] By now, it is widely acknowledged that traditional concepts of nuclear and conventional deterrence that were developed and implemented during the second half of the twentieth century, no longer suffice in today's strategic environment.[3] Even seasoned Cold War warriors, such as Henry Kissinger, already argued a decade ago that "the end of the Cold War made the doctrine of mutual Soviet-American deterrence obsolete."[4] Although nuclear and conventional deterrence remain important components of great power strategic postures,[5] the emergence of new strategic challenges necessitates the evolution and adaptation of traditional deterrent concepts. Both state and non-state actors increasingly draw on a broader range of coercive instruments to hurt adversaries against the backdrop of an assortment of technological, social, economic and geopolitical macro trends that have made new forms of power and influence projection across different domains possible. Revisionist powers engage in *gray zone* conflicts "in the no man's land between peace and war" in "a pattern of state rivalry that can substitute for traditional military aggression", which nonetheless allows them to "achieve gradual but decisive results."[6] This has become a particularly pernicious

[1] This paper has been presented at the Oxford Changing Character of War Symposium, Pembroke College, 29 June 2019. The research for this paper has been undertaken in the context of a multi-annual research project on hybrid conflict of The Netherlands Organisation for Scientific Research (TNO) which receives funding from the Dutch Ministry of Defence. The authors would like to thank Frank Bekkers, Paul Ducheine, Rick Meessen, Frans Osinga, Christopher Painter, and Rob de Wijk.

[2] For a variety of definitions and subtle differences in their conceptualization, see Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security.* First Edition (Princeton: Princeton University Press, 1961). Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword*, Revised edition (New Haven, CT: Yale University Press, 2008). Alexander George and Richard Smoke, *Deterrence in American Foreign Policy* (New York: Columbia University Press, 1974). Patrick M. Morgan, *Deterrence: A Conceptual Analysis*, 2nd edition (Beverly Hills, Calif: SAGE Publications, Inc, 1983). Michael Mazarr et al., *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression* (RAND Corporation, 2018).

[3] See for example Mariarosaria Taddeo, 'The Limits of Deterrence Theory in Cyberspace', *Philosophy & Technology* 31, no. 3 (1 September 2018): 339–55. and Martin C Libicki, 'Expectations of Cyber Deterrence', *Strategic Studies Quarterly* 12, no. 4 (2018): 44–50.

[4] George P. Shultz et al., 'A World Free of Nuclear Weapons', *Wall Street Journal*, January 2007, sec. Opinion.

[5] Conventional and nuclear deterrence for instance feature as a core tenet of the January 2018 Trump Administration Defense Strategy, and their merits continue to be debated in popular outlets read by military and foreign policy professionals, see Strategic Forum on National and International Security, 'Strategic Studies Quarterly Special Edition', *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 1–135.; and Andrew F. Krepinevich, 'The Eroding Balance of Terror', January 2019.

[6] Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Arlington: Strategic Studies Institute, 2015).

problem for Western policymakers, who have found themselves neither prepared nor equipped to deal with important contemporary challenges including Russia's invasion of Ukraine (2014); Russia's concerted campaign to manipulate the information sphere in the US and Europe (from 2016 onwards);[7] foreign sponsored assassinations on European soil by Russia and Iran (Skripal UK, 2018[8]; Iran in the Netherlands, 2015 and 2017[9]); as well as persistent cyber intrusions for sabotage and espionage (which make it into the public news only in case of escalation with considerable real world damage) by various actors including China (PLA Unit 61398, 2013[10]), the DPRK (Wannacry, 2017[11]), and again Russia (NotPetya, 2017[12]). It has been convincingly argued that such activities in the gray zone are conceived and executed as part of so-called hybrid strategies implemented by these actors to achieve their political objectives.

1.1 Hybrid Conflict, Hybrid Threats, Hybrid Challenges

The term *hybrid* originated in the military sphere and was initially employed with reference to hybrid warfare. Its original purpose was to describe the simultaneous employment of regular and irregular forces and tactics within one combat theatre.[13] Gradually, the meaning of the term evolved to suit the purposes of various stakeholders. Hybrid warfare transformed in everyday policymaker parlance into hybrid conflict featuring hybrid threats, in order to denote a spectrum of objectionable activities ranging from non-violent to violent ones in both the military and the civil domain.[14] One formal definition of hybrid threats now espoused by the European Centre of Excellence for Countering Hybrid Threats thus asserts:

> "The term hybrid threat refers to an action [...] whose goal is to undermine or harm the target by influencing its decision-making [...] Activities can take place, for example, in the political, economic, military, civil or information domains."[15]

[7] Committee on Foreign Relations, 'Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security' (United States Senate, January 2018). See also National Intelligence Council, 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', January 2017.

[8] Jay Elwes, 'The Skripal Assassination: What Is Putin Thinking?', March 2018.

[9] Raf Sanchez, 'Iran Hired Criminals to Assassinate Dissidents in the Netherlands, Dutch Government Claims', *Telegraph*, January 2019.

[10] David Cohen, 'The Growing Spotlight on China's Cyber Activities', The Diplomat, accessed 15 June 2019.

[11] Ellen Nakashima and Philip Rucker, 'U.S. Declares North Korea Carried out Massive WannaCry Cyberattack', *Washington Post*, December 2017, sec. National Security.

[12] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED', August 2018.

[13] Frank G Hoffman, 'Conflict in the 21st Century: The Rise of Hybrid Wars' (Arlington: Potomac Institute for Policy Studies, December 2007).

[14] Ofer Fridman, *Russian 'Hybrid Warfare': Resurgence and Politicization* (Oxford: Oxford University Press, 2018).

[15] Center of Excellence, 'What Is Hybrid CoE?', Hybrid CoE, accessed 15 June 2019.

NATO, similarly, has articulated a formal definition of what it designates as hybrid threats, which it understands to be those "posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."[16] NATO member states have therefore launched euphemistically-named Counter Hybrid Threat Units to identify, formulate, and coordinate cross domain responses.[17] These newly established units seek not only to defend against hybrid threats but also to deter adversaries from engaging in hybrid activities in the first place. An important question that these units therefore confront concerns the role of deterrence within an overall strategic posture to deal with hybrid, cross domain challenges.

1.2 Deterring Hybrid Challenges

The traditional deterrence scholarship has identified various conditions or factors which contribute to the success of nuclear and conventional deterrence.[18] These factors include a clearly delineated demand of the action the opponent is expected *not* to execute combined with a credible threat of the costs it will incur should it decide to go ahead. The credibility of the threat rests on the ability and willingness of the deterrer to carry out the threat (deterrence-by-punishment) or by making the action itself prohibitively costly (deterrence-by-denial). Moreover, it should be clear, when these demands are not met, which requires transparency (instead of opaqueness) and the ability to attribute actions to a transgressing actor. This is partly related to the fact that an opponent may employ *salami tactics* and violate the terms of the deterrent demands in a real but minor way such that it is seemingly disproportionate for the deterrer to carry out their threat.[19] Furthermore, the deterrer should also be able to communicate credible assurances of the benefits that the opponent will receive if they refrain from certain behaviour. The demand, the threat, as well as the assurances need to be clearly and consistently communicated to the opponent, as deterrence can be understood as successful or unsuccessful only in reference to the decision of the receiving party.[20] The deterrer, therefore, needs to understand their opponent and adjust their signaling strategy accordingly. An important question is whether deterrence can be useful in the context of hybrid challenges. Given the increased salience of hybrid threats in interstate strategies, we argue that the role of deterrence in this context requires closer examination.

[16] NATO, 'Capstone Concept for the Military Contribution to Countering Hybrid Threats', 2010, 2,

[17] See for example the Counter Hybrid Unit in the Netherlands Ministry of Defense in 2018; and The European Centre of Excellence for Countering Hybrid Threats in Finland.

[18] Thomas C. Schelling, *The Strategy of Conflict*, 2nd ed. (Cambridge ; New York: Harvard University Press, 1990). Snyder, *Deterrence and Defense*. Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004). Mazarr et al., *What Deters and Why*.

[19] Schelling, *Arms and Influence*, 66–69.

[20] Morgan, *Deterrence*, 18–19.

The potential role of deterrence in countering hybrid activities requires a better understanding of the utility of different concepts of deterrence applied to different single domains *and* across different domains, which brings us to an emerging body of literature on cross domain deterrence (CDD). This requires not just greater synergy between deterrence strategies across these different domains, as most of the scholarship in the area of hybrid conflict and CDD attests to, but first and foremost close attention to the mechanisms through which hybrid deterrence is supposed to work in the first place. It may also require new forms of deterrence than were prevalent in the traditional nuclear and conventional domains. Fortunately, a lot of interesting and innovative work has been produced on single domain deterrence, for instance with respect to cyber and non-state actor deterrence, that can be drawn upon.

1.3 Objective and Structure of this Paper

In bringing deterrence "back to reality",[21] the overall research agenda is fairly straightforward. This paper reviews the rise of CDD in the context of deterrence theory, a concept that has been developing over the past few years but predominantly in a military context and argues that CDD is applicable also to the hybrid domain. It then turns to problems associated with deterrence in the hybrid domain and develops the argument that deterrence can work against hybrid threats *in theory* but that *in practice* favouring conditions for effective deterrence need to be met.[22] The body of work and collection of evidence is considerably limited on this, however, both due to a dearth of systematic studies and because many of these domains are evolving rapidly as an outcome of technological progress and strategic innovation. A combination of a deductive and an explorative approach is therefore warranted. This paper is structured as follows: in the next section it defines CDD situating its emergence in the context of the larger evolution of deterrence theory over the past seventy years and identifies relevant insights that can be applied in the context of hybrid conflict. It then reviews and refutes four arguments that posit that deterrence cannot work in the hybrid domain. On that basis, it adduces insights concerning the use and utility of CDD against hybrid threats and identifies the prerequisites for deterrence to play a role in an overall strategic posture to deal with cross domain hybrid activities.

[21] Aaron Brantly, 'Back to Reality: Cross Domain Deterrence and Cyberspace' (Boston: Virginia Tech, 2018).2018 On this point, see also Shannon Carcelli and Erik A. Gartzke, 'The Diversification of Deterrence: New Data and Novel Realities', in *Oxford Research Encyclopedia of Politics*, 26 September 2017.

[22] George and Smoke, *Deterrence in American Foreign Policy*.

2. From Deterrence to Cross Domain Deterrence

The practice of deterrence, despite appearing as a strategic studies concept only in the mid-twentieth century, appears much earlier in the recorded history of *homo sapiens* with records going back as early as the 8th millennium B.C.[23] Despite its historical prevalence, the concept and its underlying logic was only explicitly formulated in Western strategic thinking at the beginning of the Cold War. From then onwards, four successive waves of scholarship examining the concept from different angles are distinguished.[24] The first wave came in the direct wake of the invention of the atomic bomb in the mid-1940s, with scholars considering its effects on international stability.[25] The second wave, which followed more than a decade afterwards, gave birth to a body of rational deterrence theory, which focused on the game theoretic foundations of deterrence and relied principally on formal theorems and deductive reasoning.[26] The third wave emerged a decade later when authors started examining these insights both in case studies and with quantitative research methods.[27] During that third wave, psychological and decision-making perspectives increasingly complemented the rational actor perspective that was still characteristic of the first two waves.[28] In the 1990s and the 2000s, after the end of the Cold War, a fourth wave appeared with work focusing on asymmetric deterrence especially in the context of the question how to deter terrorists.[29] These four waves reflected important methodological and substantive orientations of the field, as well as strategic concerns of the day. New security challenges thus forced professionals and scholars to rethink

[23] Claudio Cioffi-Revilla, 'Origins and Age of Deterrence: Comparative Research on Old World and New World Systems', *Cross-Cultural Research* 33, no. 3 (1999): 257. See also Raoul Naroll, *Military Deterrence in History;: A Pilot Cross-Historical Survey*, First Edition edition (Albany: State University of New York Press, 1974).

[24] Michael Quinlan, 'Deterrence and Deterrability', *Contemporary Security Policy* 25, no. 1 (April 2004): 11–17.

[25] Robert Jervis, 'Deterrence Theory Revisited', ed. Alexander George and Richard Smoke, *World Politics* 31, no. 2 (1979): 289–324.

[26] Daniel Ellsberg, 'The Theory and Practice of Blackmail', Product Page (Washington: RAND Corporation, 1968),. Schelling, *The Strategy of Conflict*. Schelling, *Arms and Influence*. Herman Kahn, *On Escalation: Metaphors and Scenarios* (Santa Barbara: Praeger, 1965).

[27] George and Smoke, *Deterrence in American Foreign Policy*. Glenn H. Snyder and Paul Diesing, *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises* (Princeton: Princeton University Press, 1977). Barry Blechman and Stephen S. Kaplan, *Force without War: U.S. Armed Forces as a Political Instrument* (Washington: Brookings Institution Press, 1978).

[28] Robert Jervis, *Perception and Misperception in International Politics*, New edition (Princeton: Princeton University Press, 2017). Robert Jervis, 'Deterrence and Perception', *International Security* 7, no. 3 (1982): 3–30. Richard Ned Lebow and Janice Gross Stein, 'Rational Deterrence Theory: I Think, Therefore I Deter', *World Politics* 41, no. 2 (1989): 208–24.

[29] Jeffrey W. Knopf, 'The Fourth Wave in Deterrence Research', *Contemporary Security Policy* 31, no. 1 (1 April 2010): 1–33.

and adapt traditional concepts and explore new ones, such as the concept of "complex deterrence" to describe and capture an

> "ambiguous deterrence relationship, which is caused by fluid structural elements of the international system to the extent that the nature and type of actors, their power relationships, and their motives become unclear, making it difficult to mount and signal credible deterrent threats in accordance with the established precepts of deterrence theory."[30]

The circumspect description of complex deterrence obfuscates the fact that the focus continued to be on the deterrence of various types of actors rather than on the much broader spectrum of coercive activities employed by these actors across multiple domains, often in synergistic ways. The shift from complex deterrence to CDD took place in the US late under the Bush administration in the 2000s.[31] The first papers explicitly dedicated to this topic were written,[32] and seminars were held to explore the intricacies and requirements of CDD, leading to an emerging, if still small, body of scholarship on CDD.[33]

While the concept as such may have been new, initially it seemed a classic case of old wine being served in new bottles. After all, CDD was practiced in earlier times too, albeit across a smaller number of military domains. King Mallory, for instance, observes in *New Challenges in Cross-Domain Deterrence*, that "during the Cold War, military strategists primarily focused on deterrence of a Warsaw Pact conventional or nuclear attack that would take place in Europe on land, in the air, and at sea."[34] Vincent Manzo writes in *Deterrence and Escalation in Cross-domain Operations* that "the United States deters attacks, regardless of whether they cross domains, by threatening responses that will likely cross domains and differ from the initial attack."[35] Similarly, Christopher Buckley, in *Building "Space" into Multi-Domain Deterrence Strategy*, argues for the essential continuity and unity of (cross-domain) deterrence, claiming that any deterrence is still deterrence regardless of the specific domains employed for its exercise.[36] He finds that "deterrence policy and strategy are concepts too big to be constrained in a single domain," and observes that the US

[30] T. V. Paul, 'Introduction', in *Complex Deterrence: Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago: University of Chicago Press, 2009), 8.

[31] Carcelli and Gartzke, 'The Diversification of Deterrence'.

[32] James A. Lewis, 'Cross-Domain Deterrence and Credible Threats' (Center for Strategic and International Studies, 2010).

[33] A Cross-Domain Deterrence Seminar was held at the Lawrence Livermore National Laboratory, annually since 2014. Paul, 'Introduction'.

[34] King Mallory, 'New Challenges in Cross-Domain Deterrence', Product Page (Santa Monica: RAND Corporation, 2018).

[35] Vincent Manzo, 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?', *Strategic Forum*, 2011, 3.

[36] Christopher Buckley, 'Building "Space" into Multi-Domain Deterrence Strategy', *Airpowerstrategy* (blog), 2 December 2018.

has already been practicing deterrence across domains for decades.[37] Robert Vince agrees in *Cross-Domain Deterrence* that CDD constitutes nothing new in strategic practice, but argues that it is necessary to develop new theory to understand its many nuances.[38]

Various definitions of CDD are offered in the literature that all converge on the notion that cross domain deterrence involves the use of threats in one domain to counter activities in other domains. With some exceptions, most of the work examines either explicitly or implicitly deterrence across military domains with the inclusion of cyber and space. Jon Lindsay and Jiakun Zhang, for instance, observe that cross-domain deterrence "extends classical deterrence by investigating how threats in one domain can be countered by unlike capabilities in another."[39] In the 2019 volume *Cross-Domain Deterrence: Strategy in an Era of Complexity,* Erik Gartzke and Jon R. Lindsay define cross domain deterrence as "the use of threats in one domain, or some combination of different threats, to prevent actions in another domain that would change the status quo."[40] The volume brings together an assortment of interesting and timely contributions on cross-domain deterrence, yet, similar to previous work, it continues to predominantly address military cross-domain deterrence. Breach, in *Binary Thinking in a Complex World* follows Gartzke and Lindsay, defines CDD as "the use of unlike means for the political ends of deterrence."[41] Scouras et al. similarly focus on military domains conceiving of cross-domain deterrence as "making retaliatory threats from one domain to prevent attacks from another."[42] Dawkins, in *Rising Dragon*, defines cross-domain deterrence as "the ability for the weapons or tools of power from one domain to be used to deter the weapons or tools of power in another domain."[43] Vince, however, parts from this more limited interpretation and defines CDD in a more precise, yet less restricted fashion, as "the act of deterring an action in one domain, where the domains are defined as land, under the land, at sea, under the sea, in the air, in space, and in cyberspace, and may use economic sanctions and other diplomatic and political tools."[44] Mallory also approaches the topic from within a slightly broader perspective in his 2018 piece *New Challenges in Cross-Domain Deterrence*. He examines challenges for deterrence across different settings including

[37] Buckley.

[38] Robert J. Vince, 'Cross-Domain Deterrence Seminar Summary Notes', Government & Nonprofit (Livermore: Center for Global Security Research, May 2015), 3–12.

[39] Jon R Lindsay and Jiakun Jack Zhang, 'Information Infrastructure: Cyberspace, Outer Space, and the U.S.-China Security Relationship', (2014).

[40] Jon R Lindsay and Erik Gartzke, 'Introduction: Cross-Domain Deterrence, From Practice to Theory', in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik A. Gartzke and Jon R. Lindsay (Oxford: Oxford University Press, 2019), 6.

[41] A. Breach, 'Binary Thinking in a Complex World: The Failure of NATO Deterrence since 1994 and Implications for the NATO Readiness Action Plan' (Fort Leavenworth: School of Advanced Military Studies, 2017), 4.

[42] James Scouras, Edward Smyth, and Thomas Mahnken, 'Cross-Domain Deterrence in US–China Strategy', 2017.

[43] James C. Dawkins, 'Rising Dragon: Deterring China in 2035': (Fort Belvoir, VA: Defense Technical Information Center, 12 February 2009), 12.

[44] Vince, 'Cross-Domain Deterrence Seminar Summary Notes', 3.

hybrid warfare, explaining that the latter can also encompass non-military means.[45] He defines successful cross-domain deterrence as a state

> "when an opponent has no incentive to initiate or escalate conflict at any given intervention or escalation threshold in any given domain of warfare—both vertically and horizontally within that domain and laterally into one or more additional domains of warfare."[46]

Vertical escalation revolves around the intensity of power exercised in one specific domain of conflict.[47] Horizontal escalation has commonly been used to refer to the expansion of escalation in other geographical domains, but can also describe escalation to non-traditional domains.[48] Because a horizontal escalation ladder is added to the vertical escalation ladder, the picture becomes significantly more complex.[49] It is generally considered that China and Russia have developed cross domain deterrence concepts. Chase and Chan, for instance, in *China's Evolving Approach to 'Integrated Strategic Deterrence'*, argue that Chinese understanding of cross domain deterrence includes "a multidimensional set of military and non-military capabilities that combine to constitute the "integrated strategic deterrence" posture required to protect Chinese national security interests."[50] While the authors also draw attention to the importance of non-military instruments of power, they stress that it is military power potentially exercised through several domains that is at the core of Chinese cross domain deterrence.[51] Qui, in *China's Science of Military Strategy*, examines Chinese thinking about deterrence across multiple domains, explaining that it rests upon a combination of nuclear, conventional, information, space, and civilian forces.[52] Adamsky, in *Cross-Domain Coercion*, argues that the Russian theory of cross-domain deterrence and compellence is inherently intertwined, is still evolving and is being tested in the contemporary strategic practice.[53] He views Russian cross-domain deterrence as being composed of three intertwined concepts: traditional nuclear deterrence; non-nuclear (conventional) deterrence relying mostly on precision-guided missiles and special forces; and informational deterrence in cyberspace. In practice, this results in "uninterrupted informational deterrence waged

[45] Mallory, 'New Challenges in Cross-Domain Deterrence', 11–12.

[46] Mallory, 7.

[47] For the original work, see Kahn, *On Escalation: Metaphors and Scenarios*.

[48] Forrest E Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica: RAND Corporation, 2008). One of the authors of this paper has applied this notion to escalation to non-military domains, see Tim Sweijs et al., *Back to the Brink: Escalation and Interstate Crisis* (The Hague: HCSS, 2016), 39–40.

[49] One of the authors of this paper has argued in an earlier study that crisis management in this context thus hinges on "the ability and flexibility to escalate (and de-escalate) both vertically and horizontally." see Sweijs et al., *Back to the Brink: Escalation and Interstate Crisis*, 58.

[50] Michael S. Chase and Arthur Chan, 'China's Evolving Approach to Integrated Strategic Deterrence', Product Page (Washington: RAND Corporation, 2016), vii. Chase, M. S. and Chan, A.. 2016. *China's Evolving Approach to 'Integrated Strategic Deterrence'*. Santa Monica, CA: RAND Corporation, vii.

[51] Chase and Chan, vii.*Ibid*, vii.

[52] Mingda Qiu, 'Cross-Domain Concepts in the 2013 Edition' (La Jolla: UCSD, September 2015), 13.

[53] Dmitry Adamsky, 'Cross-Domain Coercion: The Current Russian Art of Strategy' (Security Studies Center, 2015), 10, 41–43.

on all possible fronts against all possible audiences, augmented by nuclear signaling, and supplemented by intrawar coercion [...]."[54] The ultimate purpose of this kind of deterrence is "to deescalate, or dissuade the adversary from aggression, and impose Russia's will, preferably with minimal violence."[55] Russian deterrence, compared to the Western concept, has three unique characteristics. It is inherently cross-domain and universal because "it seeks to deter all types of security threat with the use of all means available."[56] It is also continuous, as it takes place both during war and peace, and blurs the distinction between deterrence and coercion, because it does not stop once hostilities break out.[57]

Many authors therefore emphasize the need for greater cross domain integration within an overall deterrence posture both because of the emergence of new warfighting domains and because of the closer synchronization of war fighting instruments in these domains. Thus, James Lewis, in *Cross-Domain Deterrence and Credible Threats*, argues that "deterrence in space or cyberspace cannot be domain limited and will require threats in other domains, such as saying that an attack on our satellites could lead to an attack on terrestrial targets."[58] In a similar vein, Mallory asserts that "because war in space and cyberspace cannot be limited to the boundaries of a single geographic theatre of military operations, military leaders and analysts have increasingly chosen to highlight the need to deter potential adversary aggression within and across all five domains of military activity."[59] Craig Wuest too, in *Multi-Domain Deterrence*, contends that responses to the complex issues of contemporary security "should be considered and weighed in the multi-domain context."[60] As Erik Gartzke and Jon Lindsay sum it up, "increasing complexity in the entire portfolio of means now available now appears to necessitate the refinement of deterrence as both a military and political process."[61]

Yet, CDD comes with an assortment of challenges. These include challenges associated with the credibility of threats, proportionality and the complexity of signaling in CDD, as well as issues related to escalation control.[62] Dawkins argues that a fundamental issue with CDD is the challenge of making the retaliatory threat credible in the eyes of the challenger.[63] Deterrent threats are more likely to be perceived as credible if they are considered proportionate. Thus, threatening nuclear attack as a response to cyber espionage is not likely to be perceived as credible.

[54] Adamsky, 'Cross-Domain Coercion', 37.
[55] Adamsky, 37.
[56] Kristin Ven Bruusgaard, 'Russian Strategic Deterrence', *Survival* 58, no. 4 (3 July 2016): 17.
[57] Bruusgaard, 18.
[58] Lewis, 'Cross-Domain Deterrence and Credible Threats', 3.
[59] Mallory, 'New Challenges in Cross-Domain Deterrence', 6.
[60] Craig Wuest, 'Multi-Domain Deterrence Table Top Exercise Summary' (Livermore: Lawrence Livermore National Laboratory, January 2018), 13.
[61] Lindsay and Gartzke, 'Introduction: Cross-Domain Deterrence, From Practice to Theory', 24.
[62] Jacquelyn Schneider, 'Cyber and Cross-Domain Deterrence' (2018).
[63] Dawkins, 'Rising Dragon', 12.

Responses in different domains will therefore need to convey not only different levels but also different types of force. Of course, what is deemed proportionate and therefore appropriate is likely to change over time. Israeli air-strikes from early May 2019 at cyber hackers from Hamas may well be a harbinger of a new development of cross domain retaliation, which in turn, may modify interpretations of appropriateness.[64]

A fundamental problem here remains that each individual domain has a particular logic of escalation and these logics may not be inherently symbiotic. The challenge of signaling is that signals in each of the domains are of such a different character that it proves difficult to synchronise them into one clear but also credible message. The domains and the forces which can be employed in each of them are so dissimilar that their synergistic use proves to be very complex, as both military and foreign policy practitioners have experienced in recent years. For example, during the Obama administration, the US government struggled to devise an appropriate response to Russian interference in the country's elections.[65] European governments experienced similar challenges as they were not ready to formulate responses to Russian disinformation campaigns.[66] Similarly, debates about how to respond to Chinese espionage, and whether such a response should be proportional or asymmetric, are ongoing in Western capitals.[67] Shawn Brimley therefore argues in *Promoting Security in Common Domains* that "cross-domain deterrence dynamics will constitute a core analytic issue for the U.S. defence, diplomatic, and intelligence community, particularly as shifts in the actual or perceived balance of power in sea, air, space, and cyberspace become more opaque."[68] He therefore observes that it is vital to develop a far better understanding of "how to control escalation dynamics" in several domains.[69]

At the same time, the issue of escalation management is not seen as inherently unsolvable, although the recommendations that are put forward are thus far generic in nature. Manzo proposes the development of a shared framework for interpreting how attacks in all domains "fit into an escalation ladder".[70] One of the authors of this paper has therefore pointed previously towards the need to create "a joint [...] grammar with the opponent, that is aimed at establishing a shared understanding

[64] Erica D. Borghard and Jacquelyn Schneider, 'Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal.', *Washington Post*, 9 May 2019.

[65] Jason Healey, 'Not The Cyber Deterrence the United States Wants', *Council on Foreign Relations* (blog), June 2018.

[66] Mason Richey, 'Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation', *Asia Europe Journal* 16, no. 1 (March 2018): 101–13.

[67] See for example James Lewis, 'Responding to Chinese Espionage', *Center for Strategic and International Studies* (blog), November 2018. See also Adam Segal, 'The Code Not Taken: China, the United States, and the Future of Cyber Espionage', *Bulletin of the Atomic Scientists* 69, no. 5 (September 2013): 38–45. For an overview of various possible responses, see Sico van de Meer and Frans Paul van der Putten, 'US Deterrence against Chinese Cyber Espionage' (The Hague: Netherlands Institute of International Relations, 2015).

[68] Shawn Brimley, 'Promoting Security in Common Domains', *The Washington Quarterly* 33, no. 3 (July 2010): 129,.

[69] Brimley, 129.

[70] Manzo, 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?', 4.

of the meaning and the significance of actions across different domains."[71] Juarez, in *Cross-Domain Deterrence*, suggests that successful CDD can include some combination of five distinct strategies: counter-force (attacking the types of assets that launch the attack), counter-value (attacking high value targets of the opponent), tit for tat (attacking a target of similar value), denial (denying the opponent to attack oneself), and ambiguity (being ambiguous about one's response).[72] Lewis recommends to effectuate CDD, promoting stigmatisation, improving defence, establishing common norms, declaring constraint on traditional military instruments, and improving signaling.[73] Stigmatisation involves "the creation of a credible international norm that says some forms of attack (in space or cyberspace) run counter to accepted international behavior."[74] Improving defences revolves around strengthening defences in addition to boosting resiliency in order to diminish the expected benefits of offensive actions, and therefore, change the cost calculation of the adversary. The establishment of common norms also shapes the decision-making process of actors because they affect their cost calculus associated with counter responses following exposure of their actions. Declared constraint is important because it contributes to assuaging the fear of potential adversaries of US intentions to use capabilities, thereby decreasing the chance of spiral dynamics. Signals, finally, encompass a wider range of messages and moves, which include, but are not limited to, "implicit warnings created by changes in force status or readiness posture, concern over opponent behavior, by developing tacit understandings on 'redlines' and thresholds, by implicit or explicit understandings among potential opponents, and by public statements about intentions."[75] Though all these recommendations specifically concern the cyber domain, their applicability transgresses the boundaries of this domain, due to their broad scope. Denning argues in *Rethinking the Cyber Domain and Deterrence* that in order to develop a better understanding of deterrence across domains, we need to focus more on specific kinds of attacks and their effects rather than using domain specific approaches per se.[76] His argument is therefore that we should approach deterrence in the cyber domain just as we approach deterrence in other domains, focusing on the particular actions rather than on the domain. In other words, there should be no one "cyber" deterrence, since there is no "land" or "naval" deterrence.[77] Rather we should single out particular attacks worth deterring, as is the case with the deterrence of nuclear attack, which in its means of delivery and its consequences transfers across the domains. Denning argues that there are at least two possible avenues on how to approach this issue: either by developing categorical classes for

[71] Sweijs et al., *Back to the Brink: Escalation and Interstate Crisis*, 60.
[72] A. Juarez, '2015 Cross-Domain Deterrence Seminar Summary Report', 2016, 6.
[73] Lewis, 'Cross-Domain Deterrence and Credible Threats', 4.
[74] Lewis, 4.
[75] Lewis, 4.
[76] Dorothy E. Denning, 'Rethinking the Cyber Domain and Deterrence', *Joint Force Quarterly* 7, no. 2 (2015): 15.
[77] Denning, 11–12.

groups of weapons; or by utilising already established regimes for deterrence of particular levels of hostile activities.

This review of recent research suggests that CDD offers relevant insights for deterring hybrid challenges, even if traditional understandings of deterrence need to be updated and complemented, and a number of factors that complicate deterrence across these different domains needs to be addressed.

3. Deterrence by Democracies in a Hybrid Context

Doubts have been raised about whether deterrence can be of value in the prevention of hybrid activities, since a combination of factors complicate deterrence through punishment, at the same time deterrence-through-denial is considerably more complicated in new domains such as cyber and space that are often characterised as offense dominant.[78] Generally speaking, four arguments are put forward against deterrence being of much use against hybrid challenges. These arguments, which evolve around problems associated with attribution, proportionality, signaling, and liberal democratic values, are discussed below.

3.1 Attribution in Hybrid Deterrence

The opaqueness of hybrid activities typically complicates any deterrent efforts which benefit from transparency and clarity.[79] After all, only if actions can be observed by the deterrer and attributed to a particular actor, is it possible - relying on backwards inductive logic - to deter that actor from taking that action in the first place. Hybrid conflict challengers, it is said, can easily circumvent any red lines laid down by the deterrer and rely on plausible deniability for cover.[80] Examples that are sometimes pointed at include both the Russian government's denial that *green little men* invading the Crimean peninsula were Russian,[81] chemical attacks on UK soil, cyberattacks on critical US infrastructure of various origins, and a variety of attempts to manipulate the information domain in various European countries and in North America. But both for traditional and new domains that argument does not necessarily seem to hold up. In fact, as we have seen in many of these cases, the perpetrator either could have been identified or was in fact identified. In other words, attribution took place.

[78] For a nuanced take see Rebecca Slayton, 'What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment', *International Security* 41, no. 3 (January 2017): 72–109.

[79] Dave Johnson, 'Russia's Approach to Conflict - Implications for NATO's Deterrence and Defence' (Rome: NATO Defense College, Research Division, April 2015).

[80] Sugio Takahashi, 'Development of Gray-Zone Deterrence: Concept Building and Lessons from Japan's Experience', *The Pacific Review* 31, no. 6 (2018): 787–810. Jahara Matisek, 'Shades of Gray Deterrence: Issues of Fighting in the Gray Zone', *Journal of Strategic Security* 10, no. 3 (October 2017): 1–26. Michael J. Mazarr, 'Strugle in the Gray Zone and World Order', *War on the Rocks* (blog), December 2015.

[81] Heidi Reisinger and Aleksandr Golts, 'Russia's Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defence' (Rome: NATO Defense College, Research Division, 2014). Andrew Radin, 'Hybrid Warfare in the Baltics', Product Page (Santa Monica: RAND Corporation, 2017).

Despite Putin's denial that the *green little men* invading the Crimean Peninsula were Russian, this was not - or should at least not have been - hard to verify for Western military intelligence services. In the Skripal chemical attacks on British soil in March 2018, the UK government announced within eight days that the toxin was of Russian provenance, and the perpetrators were identified and charged later that year. Attribution in the cyber domain poses more challenges.[82] As Joseph Nye explains:

> "If [..] attackers do use the Internet, they can mask the point of origin behind the flags of several remote servers, which can be located in a variety of jurisdictions. They can use nonstate actors as proxies and create false flags. ... Moreover, knowing the true location of a machine is not the same as knowing the ultimate instigator of an attack."[83]

The problem of attribution is further compounded by the multiplicity of actors in the cyber domain.[84] At the same time, other experts argue that technological advances, increased expertise and accumulated experience render attribution increasingly possible. Cross triangulation of the digital footprints, the geographical origin, the tradecraft of the attack, as well as of the motivation in a wider geopolitical context, means that attribution in cyber space no longer poses an insurmountable obstacle.[85] While Western governments admit that attribution is not always easy, it is a challenge that they are intent on taking on, and tackling with increasing success in most high profile cyber cases in recent years.[86] Both in the case of Non-Petya,[87] Wannacry,[88] Russia's hacking of the DNC,[89] but also in the case of Russia's manipulation of the information sphere,[90] perpetrators were identified, even if it there was a time lag in some instances between the event and the attribution. In fact, the number of cases of successful attribution by the West has been growing steadily over recent years. It is increasingly recognised that attribution is not a black or white phenomenon but that it is better to conceive of attribution as a spectrum. It is therefore suggested that attribution is "what states make of it".[91] Brandon Valeriano and Ryan Manes

[82] Martin C Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 43.

[83] Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security* 41, no. 3 (January 2017): 44–71.

[84] Libicki, *Cyberdeterrence and Cyberwar*, 43.

[85] Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities* (Oxford: Oxford University Press, 2015), 10. See the guide to cyber attribution specifying general indicators and examples of successful attribution Office of the Director of National Intelligence, 'A Guide to Cyber Attribution', September 2018.

[86] Alex Younger, 'MI6 "C" Speech on Fourth Generation Espionage' (London: UK government, December 2018). US Department of Defense, 'National Cyber Strategy of the United States of America' (US DoD, September 2018). Ministerie van Defensie, 'Defensie Cyber Strategie 2018', publicatie, 12 November 2018,. National Cyber Security Center, 'Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed', *NCSC* (blog), October 2018.

[87] Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED'.

[88] Nakashima and Rucker, 'U.S. Declares North Korea Carried out Massive WannaCry Cyberattack'.

[89] Huib Modderkolk, 'Dutch agencies provide crucial intel about Russia's interference in US-elections', de Volkskrant, January 2018.

[90] See Adrian Chen, 'The Agency', *The New York Times*, 2 June 2015,. Andrew Weisburd, Clint Watts, and J. M. Berger, 'Trolling for Trump: How Russia Is Trying to Destroy Our Democracy', *War on the Rocks* (blog), November 2016.

[91] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *The Journal of Strategic Studies* 38, no. 1–2 (2015): 7.

also emphasise that attribution should not be overblown, because it is possible to identify the motivations behind the attacks, just as in other domains.[92] This pragmatic approach recognises that perfect attribution is not always necessary for deterrence to work even if problems associated with attribution in this domain may "slow and blunt its deterrent effects."[93] Yet, as Nye articulates, "despite the [..] difficulty of obtaining prompt, high-quality attribution that would stand up in a court of law, there is often enough attribution to enable deterrence."[94]

More generally, attribution, especially in democracies, is sometimes hindered by the dual challenge of compiling sufficient evidence to satisfy parliament and the general public, while avoiding leaking critical information about operational assets to adversaries.[95] This dual-headed challenge was apparent in the earlier mentioned Skripal affair. Here, the UK government sought to persuade both its own population as well as those of allies that Russia was responsible for the attempted assassination, while it had to be careful not to share too much information in order to not endanger its intelligence sources. Challenges associated with the plausible deniability of covert action are thus transformed into problems associated with the willingness to acknowledge these actions.[96] The growing importance of private cyber security companies in the attribution sector is also relevant in these regards because it makes attribution possible without governments having to expose classified information. While covert actions are moving on the spectrum from totally opaque in the direction of reasonably identifiable, the decision to acknowledge those actions lies not only with the aggressor but also with the deterring party. Effective attribution will continue to depend on improved situational awareness through the implementation and effective use of technology; on a better understanding of the broader context in which these actions take place and on stronger political willingness and corresponding legal frameworks to attribute actions based on more stringent public support. The point is that governments can try and create these conditions provided they channel appropriate technological, institutional and political resources to this endeavour in the service of hybrid deterrence.

3.2 Proportionality in Hybrid Deterrence

The breadth and scope of the hybrid spectrum - which judging from the EU and NATO definitions essentially encompasses every instrument of state influence - complicates the a priori identification and matching of proportionate responses from

[92] Valeriano and Maness, *Cyber War versus Cyber Realities*, 10.
[93] Nye, 'Deterrence and Dissuasion in Cyberspace', 68.
[94] Nye, 51.
[95] Florian J Egloff and Andreas Wenger, 'Public Attribution of Cyber Incidents' (Center for Security Studies, 2019).
[96] Rory Cormac and Richard Aldrich, 'Grey Is the New Black: Covert Action and Implausible Deniability', *International Affairs* 94, no. 3 (May 2018): 493.

actions in one domain to other domains, which is vital to sustaining deterrence.[97] The lacklustre response of the Obama administration to Russia's interference in the 2016 elections, as it grappled with devising an appropriate but also proportional cross domain response with an eye to deterring Russia from future interference, is representative in these regards.[98] Proportionality is typically much more straightforward if applied in the same domain. As Thomas Schelling so elegantly explained back in the 1960s, this is because:

> "there is an idiom in this interaction, a tendency to keeps things in the same currency, to respond in the same language, to make the punishment fit the character of the crime..."[99]

Yet, despite being more complex, it is not impossible that in time deterrers are able to devise a list of circumscribed behaviours and threats stipulating which retaliatory actions are considered proportional - and therefore appropriate - to deal with which types of actions. This entails first and foremost developing a shared framework of reference that delineates the relationship between activities in different domains. Such a framework ties proportionality to the costs of actions rather than to their specific domains and would facilitate the earlier mentioned currency conversion across different domains. Diplomatic sanctions can then be explicitly used to deter cyber hacking or cyber sabotage operations to avert deliberate external manipulation of the information domain. Creating a list of options, which is then related to specific actions or behaviour *ex ante* rather than *ex post* as a response, is therefore conducive to deterrence.

Both in Europe and in the US, initiatives are being developed to establish a diverse pool of cross domain options. In the EU, this happens in the context of a framework for a "joint EU diplomatic response", called "the cyber diplomacy toolbox" to deal with "malicious cyber activities of varying in scope, scale, duration, intensity, complexity, sophistication and impact."[100] While the policy paper envisages cross domain measures, and thereby marks a first step, it does not however, talk about those measures being used in service of deterrence. The US government through the Department of State has launched its cyber deterrence initiative which will seek to develop a portfolio of instruments, measures and guidelines in the service of cyber deterrence that will allow the US government to synchronise deterrent efforts in

[97] David Whetham, '"Are We Fighting Yet?" Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?', *The Monist* 99, no. 1 (January 2016): 55–69.

[98] Healey, 'Not The Cyber Deterrence the United States Wants'.

[99] Schelling, *Arms and Influence*, 147.

[100] Council of the European Union, 'Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions' (Council of the EU, May 2017). Council of the European Union, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities' (Council of the EU, June 2017).

cyber space with relevant actors within the US government and with its allies.[101] The initiative is in line with calls of other experts, who argue that CDD options should be much further elaborated and implemented.[102] Other recommendations include the recalibration of risk tolerance (being more risk-acceptant and hence pro-active), the development of a clear and credible signaling posture based on demonstrations of capabilities, intentions and immediate responses in the service of deterrence.[103]

These recommendations are relevant because the development of options in itself does not suffice for a stable situation of deterrence to develop. Parallel to this effort, a shared framework needs to be established to both set and understand the rules guiding interaction. In that sense, it may be instructive to use the analogy of a game. Games have rules. The rules define what can and cannot be done, they describe the instruments and methods which are and are not allowed, and they give rise to expectation patterns.[104] Actors participating in a game together set the rules that shape their behaviour, which over time evolves into standard norms shaping interactions. In the context of deterrence during the Cold War, it took the Soviet Union and the US considerable time and significant effort to create a set of rules undergirding their interaction, and, more specifically, work out the prerequisites for deterrence. Even if these rules were certainly subject to change, they thus consciously sought and found a set of fundamental pillars underlying conventional and nuclear deterrence.[105]

Three further refined concepts of deterrence are relevant in the development of such rules in a hybrid context, namely: *tailored deterrence*; *punctuated deterrence;* and *cumulative deterrence*. *Tailored deterrence* targets the specific vulnerabilities of the target.[106] *Punctuated deterrence* involves the clear delineation of a red line based on a specifically defined amount of damage rather than on the type of activity.[107] Finally, *cumulative deterrence* conceptualises deterrence as a continuous, longer term process in which a one-off transgression does not spell failure but adversarial behaviour is shaped by the deterrer in a concerted effort.[108]

[101] US Department of State, 'Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats', May 2018. Eileen Donahoe et al., 'Establishing International Norms and Agreements to Prevent Election Interference', in *Securing American Elections*, ed. Michael McFaul (Stanford: Cyber policy Center, 2019), 62.

[102] Herbert Lin, Chris Painter, and Andrew Grotto, 'Deterring Foreign Governments from Election Interference', in *Securing American Elections* (Stanford: Cyber policy Center, 2019), 66–67.

[103] Lin, Painter, and Grotto, 65–66.

[104] See van Creveld, who elaborates this analogy at greater length in the context of war, Martin van Creveld, *More on War* (Oxford: Oxford University Press, 2017), 49.

[105] See Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: Palgrave Macmillan, 2003). See also Marc Trachtenberg, *A Constructed Peace: The Making of the European Settlement 1945-1963* (Princeton: Princeton University Press, 1999).

[106] Michael Johnson and Terrence K. Kelly, 'Tailored Deterrence Strategic Context to Guide Joint Force 2020', *Joint Force Quarterly* 74, no. 3 (2014): 22–29.

[107] Lukas Kello, *The Virtual Weapon and International Order* (Yale: Yale University Press, 2017), 197.

[108] Uri Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence' 40, no. 1–2 (2015): 95.

In sum, like in CDD, devising proportionality in a hybrid context is complex yet not impossible. Rather, it is both necessary and possible to develop threats of proportionate responses across different domains in the service of deterrence. This will also help set new norms of behaviour specifically in the context of deterrence if they are developed and applied not only reactively but also proactively. Relevant insights can be gleaned from more recent deterrence literature, which considers more refined concepts of deterrence in particular domains. In addition to the issue of developing such a framework, there exists the issue of how to signal capabilities in that arena, which is a topic we will turn to now.

3.3 Signaling in Hybrid Deterrence

Signaling is a vital component of deterrence. It is through signaling that actors are able to convey their ability as well as their willingness to execute a deterrent threat, which in turn allows for the development of the rules that shape the interaction between the participants, as discussed in the previous section. Signaling, however, is considerably more complicated in the hybrid domain for two principal reasons. First, it is typically harder to communicate - although certainly not impossible - to an opponent the possession of hybrid capabilities which can be used to impose punishment.[109] After all, conveying the number of intercontinental ballistic missiles with nuclear warheads deployed to an opponent with whom you have agreed on the use of technical national means of verification is easier than, let's say, the number of clickbots one possesses on Twitter.[110] Second, it is harder to qualify and quantify the effect of the use of hybrid capabilities which may be, from a terror point of view, less immediately visible and less able to instil fear on decision-makers and spur them into action. After all, the distorting, and often creeping, effects of the malign use of clickbots on the health of a democratic discourse and their ability to sway elections, is harder to quantify than the blast radius of a medium yield nuclear weapon.[111]

These two issues can be addressed in a process of repeated interaction in which the parties signal what capabilities they have, what behaviour they deem undesirable, and how they assess the effects of certain actions. Signaling of capabilities and of the will to use these capabilities, can be done through a wide spectrum of means and involves both words and actions. Moreover, signaling can and, as we have learned from the deterrence literature, is done most effectively when done consistently at the political, the strategic, and the tactical level.

[109] Taddeo, 'The Limits of Deterrence Theory in Cyberspace', 352.

[110] Although working out the logic and the operational requirements underlying Mutual Assured Destruction (MAD), also took considerable effort over the course of an extended period of time. See Freedman, *The Evolution of Nuclear Strategy*.

[111] For a discussion about the different qualities of violent and non-violent instruments of power, see, Lukas Milevski, *Grand Strategy Is Attrition* (Carlisle: Strategic Studies Institute, 2019).

At the political level, this involves public and private communication by the political leadership about the set of behaviours that the offender is expected not to engage in and the type of responses it will be met with. It also involves the establishment of norms to stigmatise such behaviour. At the strategic level it involves the publication of strategies and doctrines specifically outlining which set of behaviours are undesirable and laying down the potential consequences of such actions with counter options.[112] The resulting menu of options can be shared both with adversaries but also with allies in order to shape and set the rules of interaction in support of deterrence.[113]

It also involves symbolic demonstrations of the ability to execute an action in particular domains so that the opposing actor is aware of the fact that the deterrer possesses the ability to punish it. Russia, for instance, showcased its cyber capabilities not just to Ukraine but also to European states and the US with its cyberattack on Ukraine's power grid when it shut off the electricity supply of over 250,000 Ukrainian citizens in December 2015.[114] At the tactical level, signaling hinges on actually carrying out operations to not only demonstrate the ability to punish but also to factually punish the opponent for their transgressions in the context of punctuated deterrence, which involves immediate push back against the individuals and systems involved in the act of transgression. A case that is described as an example of successful application of deterrence signaling at multiple levels was the US orchestrated campaign to deter Chinese economic espionage, which was consistently brought up by the Obama administration at multiple levels, both publicly and privately, as being unacceptable. This was stigmatised through the building of international norms against espionage, and complemented with actual concrete disruptive measures implemented against the military units (e.g., Unit 61398) that were thought to be behind the economic espionage.[115] The competition of nerves lasted almost two years and culminated in 2015 at the summit of the presidents of both countries, where the Chinese side backed down as a consequence of clear signaling of both resolve and capability by the Obama administration.[116] After the incident, the Chinese attempts at espionage dropped considerably. Signaling in the service of hybrid deterrence may therefore be slightly more complicated but certainly not impossible. It entails the synchronisation of words and acts at multiple levels in a consistent manner in order to communicate undesirable behaviours and the costs associated with such behaviours as well as the capabilities and willingness to impose these costs, to communicate and thereby create a joint understanding of the rules of the game.

[112] Even if there can be some room for ambiguity as to what transgression of which specific thresholds leads to which consequences, in order to avoid a situation in which an opponent implements *salami tactics* and/or deliberately stops just below specific thresholds. See also the conclusion of this paper.

[113] We thank Christopher Painter for that suggestion, interview in The Hague on 18 June 2019.

[114] Andy Greenberg, 'How an Entire Nation Became Russia's Test Lab for Cyber War', *Wired* (blog), June 2017.

[115] Brantly, 'Back to Reality: Cross Domain Deterrence and Cyberspace'. Chris Painter, 'Deterrence in Cyberspace' (Barton: Australian Strategic Policy Institutute, 2018), 3–4 . Nye, 'Deterrence and Dissuasion in Cyberspace', 65–66.

[116] Aaron Brantly, 'Conceptualizing Cyber Deterrence by Entanglement', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 5 April 2018), 18–19.

3.4 Liberal Democracies and Hybrid Deterrence

It is sometimes asserted that decision-makers of liberal democracies may be less inclined to openly use coercive instruments in non-traditional domains, because they feel constrained by liberal-democratic norms which proscribe the use of hybrid activities.[117] They may also be more vulnerable to external hybrid activities. One reason for the alleged disadvantage of liberal democracies in the hybrid domain, in contrast to authoritarian regimes, is that they cannot streamline the efforts of military, media, and business entities.[118] Unity of action is further undermined by the existence of a plethora of diverging interests. In this context, Peter Pomerantsev finds the way the UK approaches Chinese investments illustrative arguing that "the money men at the Treasury were delighted; the moral men in the media appalled by the United Kingdom selling out on human rights; and the military men worried by Chinese penetration of British energy and telecommunications infrastructure."[119] Liberal democracies, precisely because of the transparent nature of their political systems, it is argued, cannot operate in the gray zone.[120]

Yet, even a cursory glance at hybrid activities conducted by the US as well as European powers in the past, renders clear that this is simply untrue.[121] During the Cold War era, the US used its special forces combined with non-violent instruments of power to achieve regime change in several states in Latin America. Western states used hybrid strategies to undermine the Soviet Union in the context of the Cold War.[122] Also today, liberal democracies use a wide spectrum of coercive activities against a variety of opponents such as China, Iran, North Korea and Russia - in the economic, cyber and covert realm. The liberal and democratic character of Western polities does not proscribe the use of coercive activities as a response to hostile actions. In fact, many activities are either allowed by Western constitutions and international law or not explicitly outlawed. Sanctions authorised by collective international bodies, such as the UN, are considered to be legal and legitimate means for coercion including deterrence.[123] The legal basis for such actions is rooted in Articles 39 and 41 of the UN Charter.[124] Article 39 states that the Security Council of the UN identifies threats and makes recommendations about

[117] Christopher S Chivvis, 'Hybrid War: Russian Contemporary Political Warfare', *Bulletin of the Atomic Scientists* 73, no. 5 (August 2017): 21. Peter Pomerantsev, 'Brave New War', *The Atlantic*, December 2015.

[118] Rod Thorton and Manos Karagiannis, *The Journal of Slavic Military Studies* 29, no. 3 (August 2016): 345–47. Pomerantsev, 'Brave New War'.

[119] Pomerantsev, 'Brave New War'.

[120] Pascal Brangetto and Matthijs A. Veenendaal, 'Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations' (International Conference on Cyber Conflict, Tallin: NATO CCD COE Publications, 2016), 125.

[121] With another of George Kennan's famous memos explicitly acknowledging this George Kennan, 'Policy Planning Staff Memorandum', May 1948.

[122] Thomas McCormik, *America's Half-Century: United States Foreign Policy in the Cold War and After* (Maryland: Johns Hopkins University Press, 1995).

[123] Syed Ali Akhtar, 'Do Sanctions Violate International Law?', *EPW* 54, no. 17 (April 2019): 1–4. See also the nuanced assessment of Sturchler of the role of threats of force in international law, Nikolas Struchler, *The Threat of Force in International Law* (Cambridge: Cambridge University Press, 2007).

[124] The UN, 'Charter of the United Nations', 1945.

appropriate measures.[125] Article 41 specifies that measures taken cannot involve violence and it explicitly mentions economic sanctions and diplomatic isolation as preferable instruments of choice.[126] Western states also increasingly impose economic sanctions outside of these international institutions, such as for instance the EU sanctions targeted at Russian banks, and energy and defence companies from 2014 onwards, and US sanctions against Iran dating back many decades. Even if the legal status of economic sanctions pursued unilaterally by individual states is controversial, it is part and parcel of everyday statecraft.[127] In the cyber domain, states have formulated laws that often allow for the use of cyber instruments in the service of deterrence in order to protect national security.[128] The deployment of intelligence services and special forces is also permissible within the legal framework of liberal democracies as long as they fall within the purview of a system of democratic checks and balances. Other coercive activities are not explicitly allowed, although they are not prohibited either. States are allowed to take broadly defined countermeasures in response to breaches of international law. These should fulfil three conditions: they should seek to coerce the opponent to either halt, reverse or abstain from an action, rather than to punish them; they should be proportionate to the initial transgression; and they should not involve the use of violence.[129] Depending on the specific context, cyber operations may fill all the three criteria.[130]

In short, there is nothing inherent in the nature of liberal democracies that makes them inherently ill-suited to develop hybrid deterrent options, neither in theory nor in practice. Still, it is necessary to further develop the legal framework for hybrid deterrence that is to be applied, both domestically and internationally. Domestically, the changing character of competition requires closer cooperation between civilian, military as well as public sectors across different domains, which in some arenas requires both extension and refinement of the legal framework. The legal status of various actions in cyber space requires closer scrutiny which similarly requires an extension and refinement of legal frameworks so that options of actions can be used in the service of deterrence. Internationally, it may require new rules that stipulate appropriate measures and countermeasures that, through their codification of severity thresholds for legitimate action and response, shape escalation dynamics. Overall, however, the conclusion seems justified that liberal democracies have considerable leeway in developing options in the service of hybrid deterrence.

[125] The UN, 39.

[126] The UN, 41.

[127] See Jana Ilieva, Aleksandar Dashtevski, and Filip Kokotovic, 'Economic Sanctions in International Law', *UTMS Journal of Economics* 9, no. 2 (March 29): 210.

[128] For the case of the US, see Nakashima and Rucker, 'U.S. Declares North Korea Carried out Massive WannaCry Cyberattack'.

[129] Joyce Hakmeh and Harriet Moynihan, 'Can State Cyber Attacks Be Justified under International Law?', World Economic Forum, April 2018. And also Joyce Hakmeh and Harriet Moynihan, 'Offensive Cyberattacks Would Need to Balance Lawful Deterrence and the Risks of Escalation', Chatham House, March 2018,. See also the nuanced assessment of Sturchler of the role of threats of force in international law, Struchler, *The Threat of Force in International Law*.

[130] Hakmeh and Moynihan, 'Can State Cyber Attacks Be Justified under International Law?'

4. Conclusion

In this era of rapid technological, social, economic and political change increasing interstate competition and swift strategic innovation, hybrid strategies have become part and parcel of contemporary statecraft. Thus far, Western liberal democracies have not been able to effectively counter the hybrid strategies of actors. In fact, these actors have seized the strategic initiative by synergistically deploying a variety of instruments of influence across different domains. The approaches of liberal democracies towards these strategic innovations has been largely *reactive* rather than *proactive* in nature. Liberal democracies have had trouble articulating effective strategies and the process of designing new postures to address a salient form of contemporary conflict is still in its early stages. This paper has started from the premise that the role of deterrence in countering hybrid threats should not be neglected because deterrence can be an important building block of a proactive approach towards dealing with hybrid threats.

The small body of CDD literature that has emerged over the last decade provides relevant insights for hybrid deterrence too. These relate to the inherently cross domain nature of hybrid deterrence and the increased demand for synergetic approaches; the role of grammars that lay down actions and appropriate counter reactions that shape and subsequently set the rules for horizontal and vertical escalation; as well as issues associated with signaling, so that perceptions and positions can be exchanged which are conditional for the development of a shared framework and understanding so that a situation of stable deterrence can emerge. At the same time, the overwhelming focus on military CDD in that literature necessitates further elaboration and refinement of CDD. The wider spectrum of threats across a greater variety of domains in hybrid conflict requires a broader range of deterrent concepts to address them.

This paper then turned to how these insights can be usefully applied to CDD in a hybrid context by considering four arguments posited against the feasibility of deterrence against hybrid threats by liberal democracies related to attribution, proportionality, signaling and the nature of liberal Western democracies. In reviewing and refuting these arguments, it not only highlighted the role of deterrence, but also identified areas that need further attention for deterrence to be an important component of counter hybrid responses.

Attribution capabilities are rooted in a combination of robust situational awareness, contextual understanding, political willingness, and a legal framework that stipulate the level of evidence necessary for attribution. This underscores the need for liberal democratic governments to maintain robust monitoring capabilities to expose hybrid actions in a timely fashion, in combination with a vigorous research and analysis infrastructure to understand the geopolitical context underlying these actions. It also requires tackling larger legal questions associated with how to share sensitive information on attribution with parliament that is necessary for democratic oversight, as well as under which conditions attribution is considered legitimate from within a legal perspective. Whether political leadership will muster the will to do attribution is another thing. All things equal, however, political willingness is likely to be greater if these issues are addressed.

Developing standards of proportionality in the service of deterrence is certainly complicated, yet it is not impossible. Liberal democratic governments should develop options of what they deem inappropriate behaviour and what proportionate responses across different domains in the service of deterrence. This will also contribute to the establishment of new norms of behaviour, if such norms are developed and communicated not only reactively but also proactively. The level of detail at which these options should be formulated may be subject to debate (because otherwise an opponent may venture precisely clear just below that threshold) and should merit further attention.

Part of the signaling effort is to share the menus containing options with allies but also with adversaries. Successful signaling entails the synchronisation of communication efforts at political, strategic, and tactical level in a consistent manner. In addition to streamlining communication efforts in strategies, doctrines and verbal messages, it also requires that liberal democratic governments showcase their capabilities to adversaries and have clear guidelines when transgressions will be punished at the tactical level. Such a coordinated effort is instrumental in creating a shared understanding of the rules of the game which underlies a deterrent relationship.

Finally, liberal democracies are not inherently incapable of developing hybrid capabilities. In fact, liberal democracies have been actively engaging in hybrid activities in the past, sometimes outside but more often also within the purview of democratic checks and balances within their systems. Yet, the legal framework framing hybrid options in the service needs further development. At the national level, it requires consideration of the legal framework associated between civilian, military and other actors in terms of roles, prerogatives and responsibilities in terms of intelligence collection, and the freedom to operate within and outside of one's own borders. At the international level, it will be necessary to develop new regimes that codify appropriate measures and countermeasures to which actors can commit, and thereby shape escalation dynamics. Overall, it is time to take hybrid deterrence seriously and seize back the strategic initiative.

5. Bibliography

Adamsky, Dmitry. ‘Cross-Domain Coercion: The Current Russian Art of Strategy’. Security Studies Center, 2015. http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

Akhtar, Syed Ali. ‘Do Sanctions Violate International Law?’ *EPW* 54, no. 17 (April 2019): 1–4.

Blechman, Barry, and Stephen S. Kaplan. *Force without War: U.S. Armed Forces as a Political Instrument*. Washington: Brookings Institution Press, 1978.

Borghard, Erica D., and Jacquelyn Schneider. ‘Israel Responded to a Hamas Cyberattack with an Airstrike. That’s Not Such a Big Deal.’ *Washington Post*, 9 May 2019. https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/.

Brangetto, Pascal, and Matthijs A. Veenendaal. ‘Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations’, 113–26. Tallin: NATO CCD COE Publications, 2016.

Brantly, Aaron. ‘Back to Reality: Cross Domain Deterrence and Cyberspace’. Boston: Virginia Tech, 2018. https://vtechworks.lib.vt.edu/bitstream/handle/10919/85386/Brantly-Back2Reality-APSA-DRAFT.pdf?sequence=1&isAllowed=y.

———. ‘Conceptualizing Cyber Deterrence by Entanglement’. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 5 April 2018. https://papers.ssrn.com/abstract=2624926.

Breach, A. ‘Binary Thinking in a Complex World: The Failure of NATO Deterrence since 1994 and Implications for the NATO Readiness Action Plan’. Fort Leavenworth: School of Advanced Military Studies, 2017.

Brimley, Shawn. ‘Promoting Security in Common Domains’. *The Washington Quarterly* 33, no. 3 (July 2010): 119–32. https://doi.org/10.1080/0163660X.2010.492725.

Bruusgaard, Kristin Ven. ‘Russian Strategic Deterrence’. *Survival* 58, no. 4 (3 July 2016): 7–26. https://doi.org/10.1080/00396338.2016.1207945.

Buckley, Christopher. ‘Building “Space” into Multi-Domain Deterrence Strategy’. *Airpowerstrategy* (blog), 2 December 2018. http://www.airpowerstrategy.com/2018/12/01/space-deterrence/.

Carcelli, Shannon, and Erik A. Gartzke. ‘The Diversification of Deterrence: New Data and Novel Realities’. In *Oxford Research Encyclopedia of Politics*, 26 September 2017. https://oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-745.

Center of Excellence. ‘What Is Hybrid CoE?’ Hybrid CoE. Accessed 15 June 2019. https://www.hybridcoe.fi/what-is-hybridcoe/.

Chase, Michael S., and Arthur Chan. ‘China’s Evolving Approach to Integrated Strategic Deterrence’. Product Page. Washington: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1366.html.

Chen, Adrian. ‘The Agency’. *The New York Times*, 2 June 2015. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Chivvis, Christopher S. ‘Hybrid War: Russian Contemporary Political Warfare’. *Bulletin of the Atomic Scientists* 73, no. 5 (August 2017): 316–21.

———. ‘Understanding Russian “Hybrid Warfare”: And What Can Be Done About It’. Santa Monica: RAND Corporation, March 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

Cioffi-Revilla, Claudio. ‘Origins and Age of Deterrence: Comparative Research on Old World and New World Systems’. *Cross-Cultural Research* 33, no. 3 (1999): 239–64.

Cohen, David. ‘The Growing Spotlight on China’s Cyber Activities’. The Diplomat. Accessed 15 June 2019. https://thediplomat.com/2013/02/chinas-cyber-problem/.

Committee on Foreign Relations. ‘Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security’. United States Senate, January 2018.

Cormac, Rory, and Richard Aldrich. ‘Grey Is the New Black: Covert Action and Implausible Deniability’. *International Affairs* 94, no. 3 (May 2018): 477–94.

Creveld, Martin van. *More on War*. Oxford: Oxford University Press, 2017.

Dawkins, James C. ‘Rising Dragon: Deterring China in 2035’: Fort Belvoir, VA: Defense Technical Information Center, 12 February 2009. https://doi.org/10.21236/ADA539881.

Defensie, Ministerie van. ‘Defensie Cyber Strategie 2018’. Publicatie, 12 November 2018. https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018.

Denning, Dorothy E. ‘Rethinking the Cyber Domain and Deterrence’. *Joint Force Quarterly* 7, no. 2 (2015): 8–15.

Donahoe, Eileen, Toomas Ilves, Chris Painter, Sergey Sanovich, Larry Diamond, Andrew Grotto, and Megan Metzger. ‘Establishing International Norms and Agreements to Prevent Election Interference’. In *Securing American Elections*, edited by Michael McFaul, 57–62. Stanford: Cyber policy Center, 2019.

Egloff, Florian J, and Andreas Wenger. ‘Public Attribution of Cyber Incidents’. Center for Security Studies, 2019. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse244-EN.pdf.

Ellsberg, Daniel. ‘The Theory and Practice of Blackmail’. Product Page. Washington: RAND Corporation, 1968. https://www.rand.org/pubs/papers/P3883.html.

Elwes, Jay. ‘The Skripal Assassination: What Is Putin Thinking?’, March 2018. https://www.prospectmagazine.co.uk/world/the-skripal-assassination-what-is-putin-thinking.

European Council of the European Union. ‘Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions’. Council of the EU, May 2017. https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

———. ‘Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities’. Council of the EU, June 2017. http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

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

———. *The Evolution of Nuclear Strategy*. New York: Palgrave Macmillan, 2003.

Fridman, Ofer. *Russian ‘Hybrid Warfare’: Resurgence and Politicization*. Oxford: Oxford University Press, 2018.

George, Alexander, and Richard Smoke. *Deterrence in American Foreign Policy*. New York: Columbia University Press, 1974.

Greenberg, Andy. ‘How an Entire Nation Became Russia’s Test Lab for Cyber War’. *Wired* (blog), June 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

———. ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED’, August 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hakmeh, Joyce, and Harriet Moynihan. ‘Can State Cyber Attacks Be Justified under International Law?’ World Economic Forum, April 2018. https://www.weforum.org/agenda/2018/04/can-offensive-cyber-attacks-be-justified-under-international-law/.

———. 'Offensive Cyberattacks Would Need to Balance Lawful Deterrence and the Risks of Escalation'. Chatham House, March 2018. https://www.chathamhouse.org/expert/comment/offensive-cyberattacks-would-need-balance-lawful-deterrence-and-risks-escalation.

Healey, Jason. 'Not The Cyber Deterrence the United States Wants'. *Council on Foreign Relations* (blog), June 2018. https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants.

Hoffman, Frank G. 'Conflict in the 21st Century: The Rise of Hybrid Wars'. Arlington: Potomac Institute for Policy Studies, December 2007.

Jervis, Robert. 'Deterrence and Perception'. *International Security* 7, no. 3 (1982): 3–30. https://doi.org/10.2307/2538549.

———. 'Deterrence Theory Revisited'. Edited by Alexander George and Richard Smoke. *World Politics* 31, no. 2 (1979): 289–324. https://doi.org/10.2307/2009945.

———. *Perception and Misperception in International Politics*. New edition. Princeton: Princeton University Press, 2017.

Johnson, Dave. 'Russia's Approach to Conflict - Implications for NATO's Deterrence and Defence'. Rome: NATO Defense College, Research Division, April 2015.

Johnson, Michael, and Terrence K. Kelly. 'Tailored Deterrence Strategic Context to Guide Joint Force 2020'. *Joint Force Quarterly* 74, no. 3 (2014): 22–29.

Juarez, A. '2015 Cross-Domain Deterrence Seminar Summary Report', 2016. https://doi.org/10.2172/1238236.

Kahn, Herman. *On Escalation: Metaphors and Scenarios*. Santa Barbara: Praeger, 1965.

Kello, Lukas. *The Virtual Weapon and International Order*. Yale: Yale University Press, 2017.

Kennan, George. 'Policy Planning Staff Memorandum', May 1948. http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

Knopf, Jeffrey W. 'The Fourth Wave in Deterrence Research'. *Contemporary Security Policy* 31, no. 1 (1 April 2010): 1–33. https://doi.org/10.1080/13523261003640819.

Krepinevich, Andrew F. 'The Eroding Balance of Terror', January 2019. https://www.foreignaffairs.com/articles/2018-12-11/eroding-balance-terror.

Lebow, Richard Ned, and Janice Gross Stein. 'Rational Deterrence Theory: I Think, Therefore I Deter'. *World Politics* 41, no. 2 (1989): 208–24. https://doi.org/10.2307/2010408.

Lewis, James. 'Responding to Chinese Espionage'. *Center for Strategic and International Studies* (blog), November 2018. https://www.csis.org/analysis/responding-chinese-espionage.

Lewis, James A. 'Cross-Domain Deterrence and Credible Threats'. Center for Strategic and International Studies, 2010. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100701_Cross_Domain_Deterrence.pdf.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

Lin, Herbert, Chris Painter, and Andrew Grotto. 'Deterring Foreign Governments from Election Interference'. In *Securing American Elections*, 63–70. Stanford: Cyber policy Center, 2019.

Lindsay, Jon R, and Erik Gartzke. 'Introduction: Cross-Domain Deterrence, From Practice to Theory'. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Erik A. Gartzke and Jon R. Lindsay, 1–26. Oxford: Oxford University Press, 2019.

Lindsay, Jon R, and Jiakun Jack Zhang. 'Information Infrastructure: Cyberspace, Outer Space, and the U.S.-China Security Relationship'. 2014. http://quote.ucsd.edu/deterrence/files/2014/10/APSA-La-Jolla-Presentation.pdf,.

Mallory, King. 'New Challenges in Cross-Domain Deterrence'. Product Page. Santa Monica: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE259.html.

Manzo, Vincent. 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?' *Strategic Forum*, 2011.

Matisek, Jahara. 'Shades of Gray Deterrence: Issues of Fighting in the Gray Zone'. *Journal of Strategic Security* 10, no. 3 (October 2017): 1–26. https://doi.org/10.5038/1944-0472.10.3.1589.

Mazarr, Michael. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Arlington: Strategic Studies Institute, 2015. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303.

Mazarr, Michael, Arthur Chan, Alyssa Demus, Bryan Frederick, Alireza Nader, Stephanie Pezard, Julia Thompson, and Elina Treyger. *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression*. RAND Corporation, 2018. https://doi.org/10.7249/RR2451.

Mazarr, Michael J. 'Strugle in the Gray Zone and World Order'. *War on the Rocks* (blog), December 2015. https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/.

McCormik, Thomas. *America's Half-Century: United States Foreign Policy in the Cold War and After*. Maryland: Johns Hopkins University Press, 1995.

Meer, Sico van de, and Frans Paul van der Putten. 'US Deterrence against Chinese Cyber Espionage'. The Hague: Netherlands Institute of International Relations, 2015. https://www.clingendael.org/sites/default/files/pdfs/Deterrence%20against%20Chinese%20Cyber%20Espionage%20policy%20brief%20-%20Clingendael%20September%202015.pdf.

Milevski, Lukas. *Grand Strategy Is Attrition*. Carlisle: Strategic Studies Institute, 2019.

Modderkolk, Huib. 'Dutch agencies provide crucial intel about Russia's interference in US-elections'. de Volkskrant, January 2018. https://www.volkskrant.nl/gs-b4f8111b.

Morgan, Forrest E, Karl P Mueller, Evan S Medeiros, Kevin L Pollpeter, and Roger Cliff. *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica: RAND Corporation, 2008.

Morgan, Patrick M. *Deterrence: A Conceptual Analysis*. 2nd edition. Beverly Hills, Calif: SAGE Publications, Inc, 1983.

Nakashima, Ellen, and Philip Rucker. 'U.S. Declares North Korea Carried out Massive WannaCry Cyberattack'. *Washington Post*, December 2017, sec. National Security. https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html.

Naroll, Raoul. *Military Deterrence in History;: A Pilot Cross-Historical Survey*. First Edition edition. Albany: State University of New York Press, 1974.

National Cyber Security Center. 'Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed'. *NCSC* (blog), October 2018. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

National Intelligence Council. 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

NATO. 'Capstone Concept for the Military Contribution to Countering Hybrid Threats', 2010. https://www.act.nato.int/the-countering-hybrid-threats-concept-development-experiment.

Nye, Joseph S. 'Deterrence and Dissuasion in Cyberspace'. *International Security* 41, no. 3 (January 2017): 44–71. https://doi.org/10.1162/ISEC_a_00266.

Office of the Director of National Intelligence. 'A Guide to Cyber Attribution', September 2018. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

Painter, Chris. 'Deterrence in Cyberspace'. Barton: Australian Strategic Policy Institutute, 2018. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-05/Deterrence%20in%20cyberspace_0.pdf?JtY9WhXLd53pCnni2U5PiHr8ikcPMC5I.

Paul, T. V. 'Introduction'. In *Complex Deterrence: Strategy in the Global Age*, edited by T. V. Paul, Patrick M. Morgan, and James J. Wirtz, 1–30. Chicago: University of Chicago Press, 2009.

Pomerantsev, Peter. 'Brave New War'. *The Atlantic*, December 2015. https://www.theatlantic.com/international/archive/2015/12/war-2015-china-russia-isis/422085/.

Qiu, Mingda. ‘Cross-Domain Concepts in the 2013 Edition’. La Jolla: UCSD, September 2015. http://deterrence.ucsd.edu/_files/Chinas%20Science%20of%20Military%20Strategy%20Cross-Domain%20Concepts%20in%20the%202013%20Edition%20Qiu2015.pdf.

Quinlan, Michael. ‘Deterrence and Deterrability’. *Contemporary Security Policy* 25, no. 1 (April 2004): 11–17. https://doi.org/10.1080/1352326042000290470.

Radin, Andrew. ‘Hybrid Warfare in the Baltics’. Product Page. Santa Monica: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1577.html.

Reisinger, Heidi, and Aleksandr Golts. ‘Russia’s Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defence’. Rome: NATO Defense College, Research Division, 2014.

Richey, Mason. ‘Contemporary Russian Revisionism: Understanding the Kremlin’s Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation’. *Asia Europe Journal* 16, no. 1 (March 2018): 101–13. https://doi.org/10.1007/s10308-017-0482-5.

Rid, Thomas, and Ben Buchanan. ‘Attributing Cyber Attacks’. *The Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

Sanchez, Raf. ‘Iran Hired Criminals to Assassinate Dissidents in the Netherlands, Dutch Government Claims’. *Telegraph*, January 2019. https://www.telegraph.co.uk/news/2019/01/08/iran-hired-dutch-criminals-assassinate-iranian-dissidents-netherlands/.

Schelling, Thomas C. *Arms and Influence: With a New Preface and Afterword*. Revised edition. New Haven, CT: Yale University Press, 2008.

———. *The Strategy of Conflict*. 2nd ed. Cambridge ; New York: Harvard University Press, 1990.

Schneider, Jacquelyn. ‘Cyber and Cross-Domain Deterrence’. U.S. Naval War College, 2018. http://nsiteam.com/social/wp-content/uploads/2018/05/Cyber-CDD-Schneider.pdf.

Scouras, James, Edward Smyth, and Thomas Mahnken. ‘Cross-Domain Deterrence in US–China Strategy’, 2017. https://www.jhuapl.edu/Content/documents/CrossDomainWeb.pdf.

Segal, Adam. ‘The Code Not Taken: China, the United States, and the Future of Cyber Espionage’. *Bulletin of the Atomic Scientists* 69, no. 5 (September 2013): 38–45. https://doi.org/10.1177/0096340213501344.

Shultz, George P., William J. Perry, Henry A. Kissinger, and Sam Nunn. ‘A World Free of Nuclear Weapons’. *Wall Street Journal*, January 2007, sec. Opinion. https://www.wsj.com/articles/SB116787515251566636.

Slayton, Rebecca. ‘What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment’. *International Security* 41, no. 3 (January 2017): 72–109. https://doi.org/10.1162/ISEC_a_00267.

Snyder, Glenn H. *Deterrence and Defense: Toward a Theory of National Security.* First Edition. Princeton: Princeton University Press, 1961.

Snyder, Glenn H., and Paul Diesing. *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises*. Princeton: Princeton University Press, 1977.

Strategic Forum on National and International Security. ‘Strategic Studies Quarterly Special Edition’. *Strategic Studies Quarterly* 12, no. 4 (Winter 2018): 1–135.

Struchler, Nikolas. *The Threat of Force in International Law*. Cambridge: Cambridge University Press, 2007.

Sweijs, Tim, Frank Bekkers, Stephan Spiegeleire, and Willem Oosterveld. *Back to the Brink: Escalation and Interstate Crisis*. The Hague: HCSS, 2016.

Taddeo, Mariarosaria. ‘The Limits of Deterrence Theory in Cyberspace’. *Philosophy & Technology* 31, no. 3 (1 September 2018): 339–55. https://doi.org/10.1007/s13347-017-0290-2.

Takahashi, Sugio. ‘Development of Gray-Zone Deterrence: Concept Building and Lessons from Japan’s Experience’. *The Pacific Review* 31, no. 6 (2018): 787–810.

The UN. ‘Charter of the United Nations’, 1945. https://treaties.un.org/doc/publication/ctc/uncharter.pdf.

Thorton, Rod, and Manos Karagiannis. *The Journal of Slavic Military Studies* 29, no. 3 (August 2016): 331–51.

Tor, Uri. '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence' 40, no. 1–2 (2015): 92–117.

Trachtenberg, Marc. *A Constructed Peace: The Making of the European Settlement 1945-1963*. Princeton: Princeton University Press, 1999.

UK Government. 'National Cyber Security Strategy 2016-2021', 2016. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf.

US Department of Defense. 'National Cyber Strategy of the United States of America'. US DoD, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

US Department of State. 'Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats', May 2018. https://www.state.gov/s/cyberissues/eo13800/282011.htm.

Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities*. Oxford: Oxford University Press, 2015.

Vince, Robert J. 'Cross-Domain Deterrence Seminar Summary Notes'. Government & Nonprofit. Livermore: Center for Global Security Research, May 2015. https://www.slideshare.net/LivermoreLab/summary-notes-47797997.

Weisburd, Andrew, Clint Watts, and J. M. Berger. 'Trolling for Trump: How Russia Is Trying to Destroy Our Democracy'. *War on the Rocks* (blog), November 2016. https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

Whetham, David. '"Are We Fighting Yet?" Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?' *The Monist* 99, no. 1 (January 2016): 55–69.

Wuest, Craig. 'Multi-Domain Deterrence Table Top Exercise Summary'. Livermore: Lawrence Livermore National Laboratory, January 2018. https://cgsr.llnl.gov/content/assets/docs/Wuest_Multi-Domain_Deterrence_Table_Top_Exercise_Summary-January-2018.pdf.

Younger, Alex. 'MI6 "C" Speech on Fourth Generation Espionage'. London: UK government, December 2018. https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage.

The Hague Centre for Strategic Studies

info@hcss.nl

hcss.nl

Address:
Lange Voorhout 1
2514EA
The Hague
The Netherlands