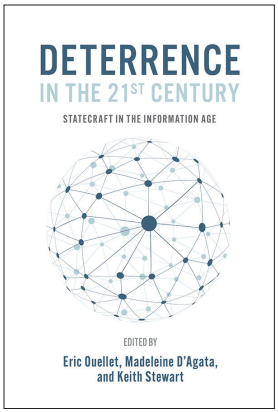
UNIVERSITY OF CALGARY
Press



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

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

ISBN 978-1-77385-404-5

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

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

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

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

3

Deterrence by De-legitimization in the Information Environment: Concept, Theory, and Practice

Alex Wilner

Deterrence theory has expanded a great deal over the past twenty years. The core, overarching logic of deterrence—manipulating an adversary's behaviour—remains the same, but the way in which manipulation might be accomplished, and the context in which deterrence might be applied, has broadened in scope and breadth. New approaches to deterrence, including the development and testing of novel frameworks and theories alongside novel empirical observation, have followed. Some scholars have concluded that deterrence scholarship has entered the "early stages of a . . . fifth wave" (Sweijs & Osinga, 2020, p. 525). The wave analogy is an apt one (Knopf, 2012; Wilner, 2018a). It helps situate deterrence theory's "classic" origins—the first wave—at the beginning of the Cold War within the context of American supremacy, emerging American-Soviet bipolarity, and nuclear weapons development. That short, vibrant period of analysis gave way to the second wave by the 1950s, with a focus on preserving the nuclear balance and great power status quo; game theory applications, scenario constructs, and some of deterrence theory's central concepts (e.g., rationality, punishment, denial, compellence) followed suit. By the mid-1970s, deterrence's third wave was marked by an emphasis on empirical study, testing the concepts and theories proposed over the past decades. New observations were added too, with an eye on the role decision making, human cognition and psychology, and conventional weaponry had on challenger-defender relations. A great flourishing of new

ideas that stemmed, in part, from outside the traditional constructs of international relations theory emerged during this wave.

Without dipping into counterfactuals, third wave dynamics and scholarship might have continued had the Cold War itself not ceased. With the bipolar contest ending, the very engine driving deterrence theory also slowed to a crawl. A fallow period followed during the 1990s. The peace dividend of that era left little room for deterrence, which had proven some of its worth by having simply kept the Cold War cold, but whose primary focus on great power rivalry, high-stakes military engagement, and nuclear standoff sat uncomfortably within the emerging (and short-lived) "end of history" paradigm. Only the terrorist attacks of 11 September 2001 sparked renewed interest in deterrence. While the immediate and short-term response to al Qaeda's attack on the United States was a heavy dose of deterrence skepticism, the previous period of relative theoretical neglect gave way to an incredible renaissance (Wilner, 2015b). Deterrence's fourth wave, a golden era of creative thought that spanned the disciplines of political science, IR and security studies, criminology and psychology, terrorism and intelligence studies, and computer science and engineering, brought fresh thinking on all fronts, deterrence theory, empiricism, and policy included. As I noted in a 2015 article, the fourth wave of deterrence scholarship included applications on a

> variety of sub-state and non-state security concerns, like insurgency, terrorism, radicalization, organized transnational crime, cyber insecurity, and piracy. More traditional inter-state security dilemmas, stemming from "rogue" regimes, nuclear and missile proliferation, and recent advances in missile technology and defense, have also been added to the deterrence agenda. Coercive processes, like punishment, denial, delegitimization, dissuasion, and inducement—as well as concepts like extended deterrence and cumulative deterrence—are likewise being explored in new and exciting ways. . . . Today, we are, as a community of scholars and practitioners, thinking up new ways to expand and apply deterrence theory to emerging and evolving security environments. (Wilner, 2015a, p. 439)

This rejuvenation was welcomed by academics and practitioners alike, paving the way for new and novel research into and applications of deterrence that

went well beyond the traditional and narrow boundaries of state centricity, physical domains, strategic weapons, and military engagement.

Whether, where, and exactly how deterrence skipped into a fifth wave is still up for debate. As in previous periods of transition, more research and time will tell. Certainly, today's deterrence scholarship shares hallmarks of previous waves, including a preference for all-domain observations (from space to cyberspace), an inclination toward trans-disciplinarity (from social to hard sciences), and a penchant for multi-level analysis (from supra-state to individual). But as Tim Sweijs and Frans Osinga posit, contemporary fifth wave deterrence research relies on "more general theorising based on the examination of the dynamics of particular cases." It is both exploratory and empirical in nature, they continue, crosses between civilian (i.e., safety) and military (i.e., security) applications, rests "inside and outside of war," reflects a "non-status quo orientation," and addresses the coercive impact of novel and emerging technologies (Sweijs & Osinga, 2020, p. 525).

Two further observations, both of which resonate with this volume, are warranted. First, the wave analogy as applied to deterrence scholarship from the 1950s onward captures the way in which deterrence itself has perpetually responded to its evolving external environment. Deterrence follows the times, responds to its milieu, shifts its focus as needed, and expands where it might. Deterrence has a knack for reorienting itself around what matters most, from preventing nuclear war among great states (first and second wave), to coercing a myriad of conventional (third wave) and non-state challengers (fourth wave), to manipulating behaviour across the spectrum of domains against the backdrop of novel technology (fifth wave) (Wilner & Babb, 2020). Deterrence never goes stale because it never stops moving. Second, this particular chapter, nestled as it is within this particular volume, is itself a reflection of fifth wave deterrence scholarship. The very topic contributors have been tasked to explore—deterrence in the information environment (IE)—is very much an emerging concern that emanates from the evolving structural and technological environment. Deterrence, once again, has been called up to explore whether and how coercion might be refashioned for proper application within the IE. My contribution to this volume sets out to rethink and reapply *deterrence by de-legitimization*—a theory I first developed in 2011 vis-à-vis ideologically motivated violent non-state actors—in the context of statecraft within the IE (Wilner, 2011; Wilner 2014). That exercise is

speculative in nature, theoretically oriented, crosses multiple disciplines, speaks to emerging security and societal concerns, and spans two waves of deterrence research.

The chapter is presented in four sections. Having situated the chapter within the larger constructs of deterrence research in this introduction, I turn in the second section to a brisk overview of the causal building blocks of deterrence and compellence. The third section introduces the logic of de-legitimization, as it was first applied to deterring terrorism. The fourth section updates this approach, adapting and broadening the concept and framework of de-legitimization for wider application to deterrence in the IE. The fifth section, functioning as the chapter's conclusion, suggests avenues for further research on the topic of deterrence by de-legitimization in the IE.

Deterrence Theory: Foundational Principles

At its most fundamental, deterrence is ultimately about using a combination of threats to shape an adversary's behaviour in a way that meets your own objective. It entails convincing another to forgo an action you would rather they not pursue. Compellence, a related term and concept, flips this around: it entails manipulating an adversary (or ally) in order to induce it to conduct an action it might otherwise not have pursued. Deterrence avoids unwanted behaviour; compellence induces desired behaviour. In both situations at least two actors are involved: a defender deters or compels a challenger with some form of threat. In other scenarios, a third actor is also involved in the calculus. In extended (and triadic) deterrence, for instance, a threat targeting a challenger is meant to protect or induce a change in behaviour in a third party, proxy, or partner (Wilner, 2018b). In all cases of deterrence and compellence (and coercion too, which subsumes both terms), regardless of how many actors are involved, a defender attempts to change a challenger's behaviour by altering its cost-benefit calculus. All behaviour, deterrence theory speculates, is based on an actor's (near) rational calculation of the benefits of action (what might be gained or achieved), and the costs of action (what might be lost or harmed). Importantly, then, deterrence and compellence weigh on a challenger's strategic choice—they retain the option to acquiesce to a coercive threat or not, and to tailor their behaviour accordingly. Vanquishing an adversary strips a challenger of its agency: it cannot behave in a particular way because it has lost the ability and choice to do so. Defeat is not deterrence, it is the imposition of demands; it leaves a challenger with no option to behave in any

other particular way. In sum, then, deterrent or compellent successes acquire a desired outcome by changing (not forcing) behaviour.

Besides these logical constructs, deterrence theory also includes several other prerequisites (Wilner, 2020). First, a challenger's level of rationality must suffice to turn some combination of threats into a change in behaviour. Second, challengers and defenders must share—to some degree and under some condition—a preference for non-violence and inaction; if a desire to hurt the other is the only shared and common attribute, then deterrence is left with little ground to function. Third, threats and behavioural expectations must be communicated to a challenger in some way, such that it can absorb information, weigh its response, and shape its behaviour. Fourth, defenders should retain a perceived capability to act as they threaten, and illustrate a resolve to do so if and when required. And fifth, coercive interactions work best against a known adversary; anonymity in either physical or digital space complicates how deterrence is communicated and carried out.

Most deterrent and compellent relationships are dictated by either a promise of a punishment or a promise of a denial. Deterrence by punishment—also referred to as deterrence by retaliation—works by threatening to harm something the challenger values. The measure, here, is to add to an adversary's perceived cost—threats of retaliation make an unwanted behaviour more costly by promising some form of pain (e.g., military retaliation, sanctions, censure) if and when the behaviour is carried out. Cold War deterrence was heavily reliant on this form of deterrence: war between the great powers was deterred by a threat of (mutual) nuclear retaliation. Besides nuclear exchanges, however, punishment strategies have been a bedrock of other, emerging deterrence-by-punishment calculations, including in deterring terrorism and deterring cyber conflict (Wenger & Wilner, 2012; Wilner, 2020). Threats of denial, the second of the two processes at hand, functions by reducing the expected (or perceived) benefits an adversary seeks to gain by its (unwanted) action (Wilner & Wenger, 2021). Deterrence by denial, long the purview of conventional deterrence scholarship but largely overshadowed by punishment strategies and nuclear threats during the Cold War, raises the cost of action by stripping away desired gains. In counterterrorism, for instance, hardening defences against violent attack raises the cost of conducting an attack by lowering the probability an adversary will accomplish what it set out to do. By raising the bar toward failure, deterrence by denial raises the perceived cost of an action. In sum, then, punishment deters through fear

of pain, denial deters through promises of failure. While punishment and denial make up the bulk of the literature (and practice) of deterrence across all domains of warfare and conflict within the five waves of scholarship, a third coercive process—deterrence by de-legitimization—that weighs on an adversary's normative or ideological perspective has recently been proposed and developed. The following section provides an in-depth review of the coercive logic of de-legitimization, as it was first developed for application in deterring terrorism.

De-legitimization in Counterterrorism: Narratives, Motivations, and Behaviour

The expansion of deterrence theory beyond traditional state-centric interactions by fourth and fifth wave scholars led to a broadening of coercion to include non-kinetic deterrents and compellents that rely on inducements, rewards, and reassurance, and denial, resilience, and mitigation. These processes are particularly attuned to the unique challenges (e.g., asymmetry, non-state characteristics, and attribution dilemma) of deterring terrorists and other non-state actors, along with deterring cyber conflict. A third, particularly unique, cluster of research on non-kinetic coercion sought to explore the use of normative and narrative constraints and de-legitimization to shape and change behaviour (Bar, 2011; Brinkel, 2017; Doorn & Brinkel, 2020; Duchein et al., 2017; Jenkins, 2010; Kitzen & Kuijck, 2020; Kuijck, 2017; Lantis, 2009; Lepgold, 1998; Sawyer, 2021; Stein & Levi, 2021; Sweijs & Zilincik, 2020; Wilner, 2012).

In my award-winning 2011 article "Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism," as well as in the 2014 article "Delegitimizing al-Qaida: Defeating an 'Army Whose Men Love Death,'" co-authored with Jerry Mark Long, I took a first stab at building a theory of deterrence by de-legitimization for counterterrorism that tackles and taps into terrorism's ideological, political, and religious rationales and motivations (Wilner, 2011; Long & Wilner, 2014). From a coercive or deterrence perspective, the objective of de-legitimization, I suggested in 2011, "is to reduce the challenger's probability of achieving his goals by attacking the legitimacy of the beliefs that inform his behavior" (Wilner, 2011, p. 26). Research on terrorism, radicalization, and political violence has found that while terrorist organizations appear to have few normative qualms regarding the use of indiscriminate (and often brutal) violence, they nonetheless

base their activities, expectations, and goals on a set of principles informed by particular ideological, and in some cases socio-religious, belief structures. Terrorism is not just violence, but violence with meaning. Al Qaeda, ISIS, and other religiously inspired militant groups, for instance, may rely on suicide tactics to achieve their goals, but they also take the time and effort to legitimize suicide's use by pointing to, relying on, and interpreting religious decrees that seem to justify its use under particular conditions. Suicide is largely considered a sin by Islamic law; to employ it, terrorist organizations like al Qaeda must illustrate how and why it is nonetheless acceptable. Without this justification in place, suicide is simply illegitimate, and those supporting its use risk tarnishing their credentials as purported adherents of religious law. "Al-Qaida loses," Long and I wrote in 2014, "when its violent excesses are devoid of narratological meaning; when its behavior is deemed offensive and illegitimate by its audience; when its terrorism is judged as mere thuggery, intimidation, and baseless murder" (Long & Wilner, 2014, p. 150).

Applying coercion to this interplay of belief, justification, and action entails identifying forms of leverage that question, debate, and even ridicule the rationales, narratives, and goals informing violent behaviour. "Strengthening and disseminating opinions, positions, and information that contradicts the legitimization of terrorism," I concluded in 2011, "might deter or compel individuals contemplating and/or taking part in violence along with the socio-religious groups that facilitate terrorist efforts" (Wilner, 2011, p. 26). Without question, deterrence by de-legitimization, as described here, rests well beyond the traditional scope of deterrence, yet it nonetheless shares deterrence theory's core requisites of changing behaviour by choice and weighing on an adversary's cost-benefit calculus. The difference is that unlike punishment and denial in deterring terrorism, de-legitimization pivots on the ideas that motivate militancy. It represents an emerging third branch of deterrence scholarship: instead of defenders threating pain or denying objectives, a challenger's behaviour is manipulated by targeting the rationales that motivate and guide it.

As Long and I note in our 2014 article—which includes a deep empirical exploration of al Qaeda's reliance on meta-narratives to shape an adherent's identity, attract and recruit supporters, sanitize its violence among a larger audience, and provide a unique lens for interpreting contemporary and historical events—"the aim is to delegitimize [the group's] narrative, targeting and degrading the ideological motivation that guides support for and

participation in terrorism" (Long & Wilner, 2014, p. 130). De-legitimization's causal logic holds that it should be possible to raise the costs of participating in terrorism by targeting the religious, ideological, normative, and/or cultural rationales and interpretations that groups, leaders, and individuals use to condone and participate in violence. "Stripping away that justification," Long and I argue, "by using the same logic, language, and related cultural inputs that are used to legitimize violence may resonate with individuals, groups, and communities contemplating involvement with al-Qaida" (Long & Wilner, 2014, p. 152). The organization's narrative, in other words, is exploitable. More precisely, if al Qaeda's message loses its credibility, the organization loses adherents, a cost to the group and its leadership. "Fear of narrative collapse," Long and I conclude, "or of adverse reaction among active and would-be supporters, or of popular backlash among their primary audience might manipulate some militant leaders," changing their expectations and group behaviour along the way (Long & Wilner, 2014, p. 153).

While de-legitimization was originally explored, developed, and tested with an eye to deterring terrorism, violent radicalization, and political violence, applying it to other domains of contemporary conflict is a worthy endeavour and should prove feasible. What follows, then, is a speculative account of how deterrence by de-legitimization might itself be broadened and expanded to deter unwanted behaviour by would-be challengers and aggressors in the IE.

De-legitimization in the Information Environment: Norms, Discreditation, and Resilience

Three avenues for applying the logic and theory of de-legitimization to the malicious exploitation of the IE present themselves. They each rest within a specific level of analysis, either at the international level, at the group and/or individual level, or within the ideational level (i.e., having to do with knowledge, truth, and ideas). What follows is a description of each of these distinct applications.

First, at the international and multilateral level, deterrence by de-legitimization as applied to the IE might begin with the establishment of norms of behaviour within the IE itself. Norms relate to deterrence in at least two ways: they help identify acceptable or common behaviour within a domain, delineating what is perceived as legitimate among those active within it, and (perhaps more importantly) norms help establish and communicate the

behavioural bar or red lines against which subsequent threats of punishment rest. In the former case, as Tim Sweijs and Samuel Zilincik note, norms convince "potential transgressors not to engage" in certain acts by "presenting them with the prospect of social costs" (Sweijs & Zilincik, 2020, pp. 148–9). At times, norms of behaviour can eventually cultivate taboos too, which help bolster moral restraint and inform more deeply held behavioural expectations in geopolitics, as in the case of the non-use of chemical, biological, radiological, and nuclear weapons in both peace- and wartime (Tannenwald, 2017). Similar norms (and fledgling taboos) are being established for cyber conflict, especially in the realm of attacks on critical civilian infrastructure and economic cyber espionage (McKeown & Wilner, 2020; Wilner, 2020). For developing deterrence by de-legitimization in the IE, Canada should start by exploring the establishment of norms with like-minded states, allies, and traditional partners, building on already established norms of behaviour emanating from other domains, including those Canada and a variety of other nation-states already express and adhere to (e.g., against targeting civilians; limiting collateral damage; respect for human rights). Eventually enshrining these norms in some form of international agreement, accord, or statute will help solidify their widespread use and passive acceptance, and will, as described above, provide a measure against which collective threats of punishment can be used to convince the few remaining transgressors not to carry out unwanted infractions. In sum, challengers to the norm will be averse to conducting certain types of behaviour within the IE because of moral clarity and conviction (de-legitimization) and/or out of fear of international condemnation, censure, and punishment.

Second, deterrence by de-legitimization in the IE might be applied at the group and individual levels. The general idea is to discredit the individuals, leaders, or groups that use the IE maliciously. Just as al Qaeda and its leadership can be targeted with de-legitimization for their fatuous interpretation of religious texts relating to suicide, violence, and wanton bloodshed, all the while dressing themselves in religious and pious garb, those intent on leveraging the IE for harm can be the target of de-legitimization, discreditation, and ridicule. Emerging research has found, for instance, a link between the information domain, the voluntary and strategic disclosure of intelligence by state officials, and the de-legitimization (and coercion) of adversaries. Ofek Riemer's work on recent Israeli public disclosures and "performative use" of intelligence suggests that officials use the tactic to "draw global attention to

violations of international regimes and norms"; the release of sensitive information and intelligence is "yet another instrument capable of inflicting damage on [an] opponent without using force or risking escalation" (Reimer, 2021, pp. 572–3).

Other scholars, like James Pamment and Henrik Agardh-Twetman, speak of "denunciation" as a form of deterrence in the information space, which involves censuring an adversary using "rhetoric, symbolism, and even humour/memes," in hopes of "damaging its reputation" (Pamment & Agardh-Twetman, 2019, p. 131). From a perspective of de-legitimization, a range of potentially embarrassing intelligence and information—collected and released by state, non-state, and non-profit organizations alike—can be publicized to help undermine and discredit a challenger bent on weaponizing aspects of the IE. As an illustration, defenders might identify, call out, and publicize embarrassing (and potentially costly) contradictions in a challenger's misuse of the IE. A semi-autocratic regime, for example, that uses democratic principles to shield itself against domestic complaints and political opposition, all the while targeting democratic principles in other countries with dis/misinformation spread through the information domain, should be openly ridiculed, loudly and often ("Repression in Putin's Russia," 2021). Hiding behind the veil of democracy domestically while undermining democracy internationally through the IE is a contradiction worth publicizing and de-legitimizing. In a similar vein, undermining an autocrat's purported support for global and domestic anti-corruption norms by showcasing their offshore misdemeanours and accumulated wealth (Hoskins & Shchelin, 2018), and glitzy domestic assets (Amos, 2017), might have a similar effect—that of de-legitimizing their claims while simultaneously punishing their actions.

Third, deterrence by de-legitimization in the IE might be applied at the level of ideas within a defender's (rather than challenger's) collective mindset. The proposition is as lofty as it sounds but nonetheless makes intuitive sense. The goal is to diminish a target society's susceptibility to certain forms of information warfare by augmenting its ideational and collective resilience, thus denying an aggressor the potency and value of the tactic and de-legitimizing its use along the way. Theo Brinkel, for instance, writes of providing Western societies with the tools they need to "mentally arm themselves against . . . ideological threats," such that a "resilient society enhances overall mental deterrence" against hybrid threats, including those stemming from the IE (Brinkel, 2017, p. 19). Opening society up to public debate about "common

values and objectives," Brinkel continues, not only builds social capital and societal trust, but strengthens a society's "sense of purpose," helping it "win the hearts and minds of [its] own population" (p. 20). Brinkel, writing with Cees van Doorn, further argues that "credibility . . . veracity, consistency and respect for the truth" are the natural societal counterweights to malicious propaganda and disinformation campaigns, and work to "enhance . . . deterrence by delegitimization" (Doorn & Brinkel, 2020, p. 371). Brinkel and van Doorn go on to illustrate how the 2020 trial, held publicly in the Netherlands, of Russian and Ukrainian nationals suspected of having had a hand in the 2014 destruction of Malaysian Airlines Flight 17 (in which 193 of the 298 passengers killed were Dutch) serves "to deter by delegitimization as every single detail disclosed [during the trial] will discredit the alternative narratives that Russian actors have issued" (p. 378) about the disaster. This societal resilience, borne by doubling down on democratic ideals, principles, and values, counters and neuters the utility of malicious IE activity.

Next Steps for De-legitimization: Theory and Application

This chapter has sought to expand the notion and nature of deterrence in and through the IE by expanding de-legitimization beyond the context from which it originally stemmed (i.e., deterring terrorism) and importing it for use in the IE. That exercise has been inherently speculative. And despite making modest gains by suggesting how and where de-legitimization fits into the rubric of deterrence in the IE, much more research and thinking is needed. By way of conclusion, what follows are three avenues for further refinement of de-legitimization in terms of theory, empiricism, and practice.

First, the concept of deterrence by de-legitimization—in and outside the IE—is still rather fuzzy. It is not yet clear, for instance, whether and how de-legitimization links back to punishment and denial. My original intention (later shared with my co-author Long) when proposing the term for application in counterterrorism was to delineate a third branch of deterrence theory, one that asserted itself in the realm of ideas, emotions, and desires. Unlike punishment and denial, which threaten pain and loss in the physical and cyber domains, de-legitimization functions at a different level altogether, "targeting what terrorists believe rather than what they value or want" (Long & Wilner, 2014, p. 128). And yet several fourth and fifth wave scholars of deterrence have since made a strong case for thinking of de-legitimization as a form and function of denial, or punishment—or both. De-legitimization

is not a separate branch of coercion, they argue, but an extension of existing deterrence logic.

Consider these various examples. Using social psychology, the logic of persuasion, and actor and audience analysis, Christina van Kuijck illustrates, for instance, that de-legitimization threatens an adversary by "taking away their (potential) support"—a form of denial—by preventing "friendly and neutral audiences . . . from consenting or recognising" the challenger (Kuijck, 2017, p. 200). Similarly, Brinkel's formulation surmises that social and societal resilience deters by de-legitimization by denying would-be aggressors the fertile ground upon which their malicious narratives can thrive (Brinkel, 2017). Janice Gross Stein and Ron Levi, using a criminological perspective of deterrence and a focus on "social sanctions," argue that "delegitimation . . . is increasingly important as one of the deterrence-by-denial strategies in governments' repertoires" (Stein & Levi, 2021, p. 59). Conversely, Sweijs and Zilincik's notion of "social and psychological costs" links de-legitimization to punishment (Sweijs & Zilincik, 2020). And John Sawyer's development of dissuasion by denial posits that de-legitimization is naturally Janus-faced:

> Contrary to the treatment by some scholars [Wilner included], efforts to delegitimize an ideology, key individuals or an organization fit more appropriately within [an] offensive logic rather than a distinct sub-type of deterrence. However, efforts to delegitimize a specific behavior, like targeting civilians, are well within the domain of influence. . . . For example, efforts to undermine the appeal of al Qaeda by citing its perversions of Islamic doctrine aim to restrict the recruitment pool generally, while efforts to delegitimize al Qaeda by citing the large number of Muslims killed in their attacks aim to force a behavioral change away from indiscriminate violence. Admittedly, these two forms of delegitimization may be difficult to disentangle because perceptions about actors and their actions, intentions and environments are generally not independent. (Sawyer, 2021, p.103)

I interpret these conceptual contradictions as a good sign. A healthy, constructive debate on the meaning and theory of deterrence by de-legitimization should be taken as evidence of growth, expansion, and the accumulation of knowledge. As de-legitimization acquires more attention from disparate

scholars working across different domains and disciplines, including vis-à-vis the IE, conceptual delineation will continue to sharpen, paving the way for a more nuanced understanding of de-legitimization theory and a more precise approach to empirical evaluation.

Second, on this notion of empirical evaluation, a next step in bolstering and advancing research on deterrence by de-legitimization in the IE is to test it across the spectrum of conflict and warfare. Very little empirical work on the subject has yet to be pursued or published: Long and I (2014) provide a qualitative assessment of de-legitimization at the group (i.e., militant) level, using al Qaeda as a single case study; van Kuijck (2017) offers some empirical insights on deterrence by de-legitimization in countering radicalization and de-radicalization; and van Doorn and Brinkel (2021) explore de-legitimization against the case of Russian disinformation surrounding the 2014 Malaysian Airlines Flight 17 disaster. These are the rare examples. Much more hard-nosed, original, qualitative, quantitative, and interdisciplinary empirical research is needed on the subject of deterrence by de-legitimization, teasing apart how and why it works to deter behaviour across the domains of conflict. This empirical research could tap into and repurpose observations previously made in other fields of study, including from strategic culture, criminology, and terrorism studies, but it should also seek to uncover new and novel ground within information warfare and cyber security.

Third and finally, part of the reason deterrence theory has remained relevant for over seventy years is that it rarely sits irrelevantly within the ivory tower. Rather, concepts, frameworks, and theories of deterrence are regularly applied in practice, to policy, doctrine, strategy, and tactics. Deterrence's theory-to-policy transition occurred throughout the Cold War, for instance, at a time when ideas about coercive communication and extended deterrence were put into practice rather quickly and smoothly. Something similar, though in a more limited fashion, is happening today with ideas stemming from recent research on deterrence by denial, terrorism deterrence, and cyber deterrence. Scholars should eventually strive to do something similar with their work on deterrence by de-legitimization. Once concepts have been further refined and specific frameworks developed and tested across various domains of conflict, de-legitimization should be translated for real-life application, put to use for deterring unwanted behaviours within and beyond the information environment. Only then will de-legitimization truly leave its mark within the study and practice of deterrence.

REFERENCES

Amos, H. (2017, 31 August). Putin "holiday mansion" revealed by Russian opposition leader. *The Guardian*. https://www.theguardian.com/world/2017/aug/31/putin-holiday-mansion-revealed-russian-opposition-leader-alexei-navalny

Bar, S. (2011). God, nation, and deterrence: The impact of religion on deterrence. *Comparative Strategy, 30*(5), 428–52. https://doi.org/10.1080/01495933.2011.624808

Brinkel, T. (2017). The resilient mind-set and deterrence. In P. A. L. Ducheine & F. P. B. Osing (Eds.), *Winning without killing: The strategic and operational utility of non-kinetic capabilities in crises* (pp. 19–38). Asser Press.

Doorn, C., & Brinkel, T. (2021). Deterrence, resilience, and the shooting down of Flight MH17. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 365–83). Asser Press. https://doi.org/10.1007/978-94-6265-419-8_19

Duchein, P., van Haaster, J., & van Harskamp, R. (2017). Manoeuvring and generating effects in the information environment. In P. A. L. Ducheine & F. P. B. Osing (Eds.), *Winning without killing: The strategic and operational utility of non-kinetic capabilities in crises* (pp. 155–79). Asser Press.

Hoskins, A., & Shchelin, P. (2018). Information war in the Russian media ecology: The case of the Panama Papers. *Continuum Journal of Media & Cultural Studies, 32*(1), 1–17. DOI:10.1080/10304312.2017.1418295

Jenkins, B. M. (2010, 26 May). Internet terror recruitment and tradecraft: How can we address an evolving tool while protecting free speech? [Testimony]. *U.S. House of Representatives Subcommittee on Intelligence, Information Sharing, and Risk Assessment of the Committee on Homeland Security*, 111th Congress, 2nd session. https://www.congress.gov/event/111th-congress/house-event/LC7021/text?s=1&r=114

Kitzen, M., & van Kuijck, C. (2020). All deterrence is local: The utility and application of localized deterrence in counterinsurgency. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 287–310). Asser Press. https://link.springer.com/chapter/10.1007/978-94-6265-419-8_15?error=cookies_not_supported&code=e3550a0b-4075-4a66-a422-deac6f8d36b9

Knopf, J. (2012). Terrorism and the fourth wave in deterrence research. In A. Wenger & A. Wilner (Eds.), *Deterring terrorism: Theory and practice* (pp. 21–45). Stanford University Press.

Kuijck, C. (2017). Delegitimising the adversary: Understanding actor and audience analysis as a tool to influence and persuade. In P. A. L. Ducheine & F. P. B. Osing (Eds.), *Winning without killing: The strategic and operational utility of non-kinetic capabilities in crises* (pp. 195–220). Asser Press. https://link.springer.com/chapter/10.1007/978-94-6265-189-0_11?error=cookies_not_supported&code=55e9fbaa-10ef-4740-aeeb-c18c7ede1dbb

Lantis, J. (2009). Strategic culture and tailored deterrence: Bridging the gap between theory and practice. *Contemporary Security Policy, 30*(3), 467–85. DOI:10.1080/13523260903326677

Lepgold, J. (1998). Hypotheses on vulnerability: Are terrorists and drug dealers coercible? In L. Freedman (Ed.), *Strategic coercion: Concepts and cases* (pp. 136–45). Oxford University Press.

Long, J. M., & Wilner, A. (2014). Delegitimizing al-Qaida: Defeating an "army whose men love death." *International Security, 39*(1), 126–64. https://direct.mit.edu/isec/article-abstract/39/1/126/12287/Delegitimizing-al-Qaida-Defeating-an-Army-Whose

McKeown, R., & Wilner, A. (2020). Deterrence in space and cyberspace. In T. Juneau, P. Lagassé, & S. Vucetic (Eds.), *Canadian defence policy in theory and practice* (pp. 399–416). Palgrave.

Pamment, J., & Agardh-Twetman, H. (2019). Can there be a deterrence strategy for influence operations? *Journal of Information Warfare, 18*(3), 123–35. https://www.jstor.org/stable/26894685

Riemer, O. (2021). Politics is not everything: New perspectives on the public disclosure of intelligence by states. *Contemporary Security Policy, 42*(4), 554–83. https://doi.org/10.1080/13523260.2021.1994238

"Russia's new era of repression." (2021, 12 November). *The Economist*. https://www.economist.com/interactive/repression-in-putins-russia/

Sawyer, J. (2021). Dissuasion by denial in counterterrorism: Theoretical and empirical deficiencies. In A. Wenger & A. Wilner (Eds.), *Deterring terrorism: Theory and practice* (pp. 97–122). Cambria Press.

Stein, J. G., & Levi, R. (2021). The social psychology of denial: Deterring terrorism. In A. Wenger & A. Wilner (Eds.), *Deterring terrorism: Theory and practice* (pp. 65–96). Cambria Press.

Sweijs, T., & Osinga, F. (2020). Conclusion: Insights from theory and practice. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 503–30). Asser Press. https://doi.org/10.1007/978-94-6265-419-8_26

Sweijs, T., Zilincik, S. (2020). The essence of cross-domain deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 129–58). Asser Press. https://link.springer.com/chapter/10.1007/978-94-6265-419-8_8

Tannenwald, N. (2007). *The nuclear taboo*. Cambridge University Press.

Wenger, A., & Wilner, A. (Eds.). 2012. *Deterring terrorism: Theory and practice*. Stanford University Press.

Wilner, A. (2011). Deterring the undeterrable: Coercion, denial, and delegitimization in counterterrorism. *Journal of Strategic Studies, 34*(1), 3–37. https://doi.org/10.1080/01402390.2011.541760

Wilner, A. (2012). Apocalypse soon? Deterring nuclear Iran and its terrorist proxies. *Comparative Strategy, 31*(1), 18–40. https://doi.org/10.1080/01495933.2012.647539

Wilner, A. (2015a). Contemporary deterrence theory and counterterrorism: A bridge too far? *NYU Journal of Law and Politics, 47*, 439–62. https://heinonline.org/HOL/LandingPage?handle=hein.journals/nyuilp47&div=24&id=&page=

Wilner, A. (2015b). *Deterring rational fanatics*. University of Pennsylvania Press.

Wilner, A. (2018a). The dark side of extended deterrence: Thinking through the state sponsorship of terrorism. *Journal of Strategic Studies, 41*(3), 410–37. https://doi.org/10.1080/01402390.2017.1284064

Wilner, A. (2018b). Political realism and terrorism—the logic of deterrence: Using mid-range theories to save political realism from itself. In R. Schuett & M. Hollingworth (Eds.), *The Edinburgh companion to political realism* (pp. 540–53). Edinburgh University Press.

Wilner, A. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies, 43*(2), 245–80. https://doi.org/10.1080/01402390.2018.1563779

Wilner, A., & Babb, C. (2020). New technologies and deterrence: Artificial intelligence and adversarial behaviour. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 401–17). https://link.springer.com/chapter/10.1007/978-94-6265-419-8_21

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