Chapter 20

Cyber Deterrence: The Past, Present, and Future

Stefan Soesanto and Max Smeets

Contents

20.1 Introduction.....	386
20.2 The Past	387
20.3 The Present	391
20.4 The Future	394
20.5 Conclusion	396
References	397

Abstract The question on whether and how deterring an adversary in or through cyberspace is feasible has provoked the minds of scholars and practitioners for decades. Today, cyber deterrence remains a quintessential anchoring concept for the political debates on cyber policy. However, does the concept of deterrence in cyberspace have a future when for almost three decades little to no seemingly feasible practical solutions nor an academic consensus have emerged? The purpose of this chapter is to situate the current debate on cyber deterrence within the historical evolution of deterrence thinking in cyberspace, clarify the existing conceptualizations, and comprehensively discuss whether the concept of cyber deter-

S. Soesanto (✉)

The Risk and Resilience Team, Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland

e-mail: stefan.soesanto@sipo.gess.ethz.ch

M. Smeets

Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland

e-mail: Smeets@ethz.ch

M. Smeets

Center for International Security and Cooperation, Stanford University, Stanford, CA, USA

M. Smeets

Centre for Technology and Global Affairs, University of Oxford, Oxford, UK

© The Author(s) 2021

F. Osinga and T. Sweijts (eds.), *NL ARMS Netherlands Annual Review*

of Military Studies 2020, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_20

385

rence has an analytical future. We argue that the future deterrence debate can move into four directions: increased incorporation of cyber deterrence as an element within the broader international security and contest in a multi-domain world. A deeper focus on the technical aspects of the cyber domain to achieve deterrence effects on the operational and tactical level. A closer analysis of compellence, as the alternative form of coercion. And an exploration of new strategic concepts that seeks to contain and blunt adversarial aggression in cyberspace that stands apart from traditional deterrence thinking.

Keywords Cyber Deterrence • Offensive Cyber Operations • strategy • cyberspace

20.1 Introduction

The question on whether and how deterring an adversary in or through cyberspace is feasible has provoked the minds of scholars and practitioners for decades. The definition of ‘cyber deterrence’ has evolved over time and been conceptually stretched.¹ Today, it remains a quintessential anchoring concept for the political debates on how to deal with the wide-range of cyber threats in general and offensive military cyber operations in specific. But does the concept of deterrence in cyberspace have a future when for almost 30 years little to no seemingly feasible practical solutions nor an academic consensus have emerged?²

The purpose of this chapter is to situate the current debate on cyber deterrence within the historical evolution of deterrence thinking in cyberspace, clarify the existing conceptualizations, and comprehensively discuss whether the concept of cyber deterrence has an analytical future.³

This chapter is logistically structured into three sections. The first section discusses the historical evidence of cyber deterrence literature—also delving into its conceptual origins. The second section looks at the two uses of the term in the present—and identifies six distinct cyber deterrence mechanisms. The third section is about the future of cyber deterrence research. It explains why a deeper understanding of the dynamics of cyber operations is essential for the cyber deterrence concept as a whole. It also explores avenues for new theoretical research that moves beyond the mere idea of traditional deterrence concepts. The chapter culminates with a conclusion that draws out several implications.

¹Indeed, many other cyber terms—and the prefix itself—have suffered the same fate; Sartori 1970; Shires and Smeets 2016.

²For a more extensive discussion on the lack of agreement, see Brantly and Smeets, forthcoming. The general notion is that cyber deterrence below the threshold of armed attack is not working.

³Also, whilst compellence is a potentially more promising form of coercion in cyberspace, this chapter only focuses on cyber deterrence. For broader overviews on coercion and the strategic value of offensive cyber operations, see Borghard and Lonegran 2017; Smeets 2018; Libicki 2012; Byman and Waxman 2001.

20.2 The Past

To map the evolution of deterring an adversary online, it is worth venturing back to the early days of the hacking community. During the 1970s and 80s, phreakers—or phone hackers—used to listen to “the clicks and clunks and beeps and boops” to figure out how the telephone system worked and how they could manipulate it.⁴ Although few underground stories from those hay days have been made public, the most well-known phreaker ‘conflict’ occurred back in 1989—when the Masters of Deception (MoD) went to ‘war’ against the Legion of Doom.⁵ The ‘cyber activity’ of the time could include switching a target’s phone carrier to another carrier; making a target’s phone ring constantly to the effect that the victim had to unhook his phone and leave it unhooked for hours on end; or eavesdropping on and cross-connecting a victim’s phone call (imagine you are calling your parents and suddenly a 911 operator joins the call wanting to know what your emergency is).⁶ During this “gang-war in cyberspace”, as *Wired* called it, deterrence was primarily discussed with a criminology mind-set—though with an ill understanding of seriousness of offense, rehabilitation, recidivism, and above all offender’s motivations and ability to act. Kevin Mitnick spent five years in prison for various ‘cyber crimes’, including eight months in an isolation cell, when he was caught by the FBI in 1995. The reason he received this harsh treatment is because someone convinced the judge he was able to initiate “a nuclear war by whistling on a public telephone”.⁷

Parallel to the end of the phreaking days and the expansion of the World Wide Web, the idea of—what was then called—information warfare, gained increasing traction within the US Department of Defense.⁸ Definition-wise, it was an amalgam ranging from “media wars to electronic combat, and from economic competition to strategic conflict waged against civilian populations”.⁹ In a sense, information warfare then was what hybrid warfare is now. A concept that encompassed everything and was analytically so broad that it is hard to strategize, plan, and act around the term. Early attempts at bringing deterrence thinking into the information warfare discussion, led to the recognition that network defences were overall

⁴Lapsley 2013.

⁵This is an inherently western-biased conception of the emergence of the field. For an early history in the Chinese context (from 1995), see Henderson 2007.

⁶Slatalla and Quittner 1994.

⁷Mitnick 2012.

⁸The term is said to originate in 1970s, when Tom Rona in the Office of Net Assessment was investigating the relationships among control systems (now known as cybernetics). See Keuhl 2002.

⁹In fact, as the Congressional Research Service writes in a report, “Although several official documents now refer to “information warfare” in other countries, [as of 2018] the United States has no formal government definition of IW. The DOD definition of information operations refers only to military operations and does not emphasize the use of cyberspace to achieve nonmilitary strategic objectives”; Wheatley and Hayes 1996, p. iii; Theohary 2018, p. 6.

inadequate and that they needed to be improved to deter anyone. In other words, deterrence was largely equated with better defence.

Through several war-gaming scenarios, the United States Department of Defense (DoD) slowly but surely realized that the US would be unable to simply deter an adversary through defensive measures alone when they themselves were unable to climb their way out of the proverbial glasshouse.¹⁰ Consequently, information warfare turned purely offensive, sparking concepts such as decapitation strikes—whose aim was to sever the linkages between an adversary's political leadership and the mechanisms it utilizes to control its civilian population; and counter command-and-control—which focused on breaking the communication links between an adversary's military leadership and the military assets deployed on the battlefield.¹¹ In essence, adversaries were seen as information hubs and spokes systems whose functioning was dependent upon the continuous information exchange between its parts. Anything from telephone lines, computers, radios, and media outlets were subsequently tagged as cut-off point to break this information flow and thereby weaken and subsequently defeat an enemy through sheer chaos creation.

In 1993, RAND's John Arquilla and David Ronfeldt introduced the concept of 'Netware' in an article titled "Cyberwar is Coming".¹² Netwar was distinctly different from cyberwar. Cyberwar stood in the tradition of counter command-and-control, by focusing on the disruption if not even destruction of adversarial information and communication systems. Its primary goal: tipping the balance on information and knowledge. Netwar by contrast was defined by Arquilla and Ronfeldt as "trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it".¹³ Meaning, pure Netware was a societal-level focused, inherently non-violent, ideational conflict, aimed at disruption rather than destruction. To some degree Netware shared significant overlaps with what was then known as information-based deterrence, that is "turning international opinion against an aggressor, altering his perception of the military correlation of forces in theatre, and fostering instability in his country".¹⁴ However, Netware, as Arquilla and Ronfeldt defined it, was removed from the traditional battlefield and encompassed adversaries as diverse as "transnational terrorists, criminals, and even radical activists".¹⁵ In other words, it also included organized non-state hacker communities. At its core, Arquilla and Ronfeldt viewed an adversary not as one large harmonious network, but numerous smaller ones,

¹⁰Wheatley and Hayes 1996, op cit.

¹¹Also see Broder 1990; Molander et al. 1996.

¹²It should be noted, however, is that it was the Mongol way of warfare from the 12th and 13th century which inspired Arquilla and Ronfeldt to coin the term 'netwar'. See Arquilla and Ronfeldt 1993.

¹³Arquilla and Ronfeldt 1993, op cit, p. 28.

¹⁴Nichiporuk 1999, p. 193.

¹⁵Ronfeldt and Arquilla 1999, p. 352.

each with their own internal stability, interests, and allegiances, that were organized to function as a somewhat coherent unit. The most important aspect of counter-Netware thinking was thus that an adversary could be potentially defeated by targeting the connectivity between and among these smaller networks, to shape how they interacted and behaved differently when disconnected from each other. Defending against a Netware would be inherently difficult, if not impossible, given how deep an adversary will have to penetrate into a target's society. Writing in the late 1990s, Arquila and Ronfeldt therefore concluded that, "it may be that deterrence against netwar will grow problematic, and all that will remain is a choice between either preclusive or depth-oriented defensive schemes. The former applies an ability to provide 'leak-proof' defences, while the latter accepts initial incursions, then aims to expel the intruders or invaders by means of counterattack."¹⁶

Amidst the question of how deterrence might work in the context of this more refined view of information warfare, the term cyber deterrence was forming. In his 1994 Wired piece, James Der Derian coins 'cyber deterrence' talking about the US Army's Desert Hammer VI war game exercise.¹⁷ Far from outlining how an adversary can be deterred in cyberspace, Der Derian's term described the Army's fusing of "media voyeurism, technological exhibitionism, and strategic simulations" to create a hyper digitalized image of US military dominance across the four traditional battlespace domains.¹⁸ Coming out of the aftermath of Desert Storm, which saw the baptism of stealth technology, precision guided ammunition use, and the unprecedented access of embedded journalists, Der Derian's definition made perfect sense. The major problem was that cyber deterrence stood apart from the cyberwar concept, had little to nothing to do with Netware, and only partially captured the logic of information warfare. What Der Derian's definition nonetheless did, was to point out the obvious fact: Deterrence is a mind game.

In 1995, the DoD eventually tasked RAND to explore "the development and achievement of national information warfare goals" in a series of wargames. While the final report by Molander et al. opened up more questions than answers, it does provide a few insights into the early days of cyber deterrence thinking as it is widely understood today. The report summarized the participant's question by noting that;

[first], how will one make retaliatory threats and against whom when there is great uncertainty about the origin of an attack. Second, there is the question of the proportionality of any response when the immediate and collateral damage associated with a particular act of cyberspace retaliation is poorly understood by national decision makers. Third is the potential asymmetry of vulnerability between the United States, its allies, and the potential opponent. [...] All of this points to the prospect that there will be no low-cost and conceptually simple deterrent concept that obviates the need to worry about future cyberspace attacks.¹⁹

¹⁶Ronfeldt and Arquilla 1996, p. 94.

¹⁷Der Derian 1994.

¹⁸Ibid.

¹⁹Molander et al. 1996, p. 38.

By 1996, still very few scholars and practitioners actually thought about deterrence in cyberspace as being feasible. Richard Harknett for example concluded that “the nature of Netware and cyberwar lend themselves to analytical frameworks and a strategic calculus dominated by offense-defence models, rather than by deterrence.”²⁰ Gary Wheatley and Richard Hayes similar observed that “while significant, overall U.S. capability and will do not guarantee deterrence of information attacks.”²¹ It would take another 25 years for this ‘demonstration of will’ to translate into the strategic concept we now call: persistent engagement.

Figure 20.1 provides a historical overview of the journal articles, book chapters, and research reports written on the specific terms ‘cyber deterrence’ and ‘cyberdeterrence’.²² Based on the figure, we can roughly distinguish between three phases in the literature: The early period, stretching from the early 1990s to the DDoS attacks against Estonia in 2007. The advancement period, when publications on cyber deterrence sky-rocketed from 2007 until 2016. And the reflection period, which has seen publications on cyber deterrence drop from its height in 2016 to 2014 levels.²³

²⁰Harknett 1996.

²¹Participants at the 1993 US-Navy sponsored wargame titled ‘Strategic Deterrence and Information Warfare’ even argued that “[high leverage options] work best with other deterrent measures such as presence, force movements (e.g. movements into theater; call up of reserves), and other direct deterrent actions that serve as a demonstration of will”. Wheatley and Hayes op cit, p. 19.

²²Annual JSTOR search results for the terms ‘cyber deterrence’ and ‘cyberdeterrence.’ The terms ‘cyber deterrence’ and ‘cyberdeterrence’ were chosen, due to JSTOR’s search engine ignoring hyphens between two words as well as capitalizations. Meaning, the term ‘Cyber-deterrence’ returns the same search results as ‘cyber deterrence.’ The annual division was attained by searching for the keywords from ex. 2000/01 to 2000/12. The former number denoting the year, the latter the month. Additionally, the search was performed with the ‘access type’ switched to ‘all content’ to capture even those publications JSTOR includes in its search results that are inaccessible through the JSTOR subscription. The methodology has several shortcomings, which, although significant, we deem good enough for the rough estimation of the growth and decline of the usage of the term cyber deterrence/cyberdeterrence. The most obvious shortcoming is that JSTOR treats the search query ‘cyber deterrence’ also a search for the individual terms ‘cyber’ and ‘deterrence.’ Meaning, it returns hits in which both terms are used pages apart. From a statistical point of view this is a problem. From an analytical perspective it is not. Any writings on ‘cyber’ that touch upon ‘deterrence’ even in a different context are worth including. In this case, casting a wider net is more adequate than using a narrow one. The second shortcoming concerns the time lag for newer publications to make their way into the JSTOR database. Meaning the further away the year of publication, the more stable the number of search hits for that year. One could argue that this invalidates our notion of a decrease in the publications on cyber deterrence since 2016. While we do expect a rise in the numbers for the years 2017, 2018, and 2019, we are highly confident—based on the analytical part of this chapter—that these figures will not reach the level of 2016. Time will tell whether we are right. As of this writing we definitely are.

²³Excluding results from unrelated disciplines, such as toxicology, does not significantly alter the search results.

Fig. 20.1 Journal articles, book chapters, and research reports on cyber deterrence, Jan 1990—Dec 2019 (*Source* Soesanto and Smeets)

20.3 The Present

In the aftermath of the DDoS attacks against Estonia, the cyber literature turned into high gear.²⁴ From 2007–2008 onwards, discussion of cyber war has dominated the literature.²⁵ Betz and Stevens note the “popular discourse on cyberwar tends to focus on the vulnerability of the ‘physical layer’ of cyberspace to cyber-attack and the ways in which this may permit even strong powers to be brought to their knees by weaker ones, perhaps bloodlessly.”²⁶ Indeed, Richard Clarke and Robert Knake wrote one of the most widely-read books on cyberwar in 2010—spurring an increase in academic literature—talking about the different ways a cyber-attack could potentially take down the United States power grid.²⁷ More sceptical research was published too, observing a striking absence of destructive cyber-attacks—including the article and book by Thomas Rid pushing back against the cyberwar hype.²⁸

Against this backdrop, it is hardly surprising that cyber deterrence started to receive increased attention. If war and conflict are possible in cyberspace, then

²⁴For a more comprehensive overview of literature topics, see Smeets and Gorwa 2019.

²⁵For key works, see Rid 2012; Gartzke 2013; Liff 2012.

²⁶Betz and Stevens 2011, p. 76.

²⁷Clarke and Knake 2010.

²⁸Rid 2012.

deterrence must be possible or needed as well.²⁹ By 2016, the academic discussion on cyber deterrence peaked with 480 publications that year.³⁰

Today, as a military concept, cyber deterrence has at least three different meanings. First, cyber deterrence can refer to the use of (military) cyber means to deter a (military) attack. Second, cyber deterrence can refer to the use of (military) means to deter a (military) cyber-attack. Third, cyber deterrence can refer to the use of (military) cyber means to deter a (military) cyber-attack. Although not explicitly spelled out, the majority of the existing literature has focused on the latter two conceptions.³¹

Scholars currently disagree to what degree it is generally possible to deter an adversarial cyber-attack. Table 20.1 provides an overview of the distinct positions various scholars have articulated over the past few years.³² Within this table we can roughly distinguish between three groups of scholars. The first group (denoted in the table in light grey) argues that cyber deterrence does not have distinctive problems and therefore works—or occasionally fails—like conventional deterrence. Dorothy Denning, for example, notes that cyberspace “shares many characteristics with the traditional domains,” and thus deterrence can be achieved through existing regimes—e.g. norms and international agreements, better cyber security, and applying the classical deterrence by punishment logic.³³ The second group of scholars (denoted in the table in dark grey) believes that cyber deterrence encompasses a unique set of issues because cyberspace is inherently different from the traditional domains. Solving the deterrence puzzle is thus only be possible if we gain a better understanding of the underlying dynamics at play. Proponents of cyber deterrence—in either the first or second group—tend to discuss one of the following four deterrence logics: (i) Deterrence by denial, (ii) deterrence by punishment, (iii) deterrence by entanglement and (iv) deterrence by—delegitimization.³⁴

First, *deterrence by denial* is essentially synonymous to cybersecurity. At its core, the conceptual idea is that better cybersecurity will decrease the probability of

²⁹Having said this, Martin Libicki—discussing the Estonia DDoS attacks as the opening of his classic book ‘cyberdeterrence and cyberwar’—was quick to note that the “ambiguities of cyberdeterrence contrast starkly with the clarities of nuclear deterrence” and “military cyberdefense is like but not equal to civilian cyberdefense”. Libicki 2009, pp. xii–xvii.

³⁰This paper focuses on academic research in the international relations field, which dominates the discussion on cyber deterrence. There are however several underdeveloped cyber deterrence research silos that have distinctly different views on the topic, such as the field of criminology (tackling cybercrime), psychology (defending against information warfare), intelligence studies (curbing digital espionage), and the computer sciences (mitigating system vulnerabilities and network disruptions).

³¹Denning 2015; Lindsay 2015; Nye 2016/2017; Kello 2017; Tor 2015; Harknett and Nye 2017. Also see William 2017; Harknett and Fischerkeller 2017; Brantly 2018.

³²Discussion and table based on Smeets and Lin 2018a.

³³The scholars note that “Studies of ‘cyber deterrence’ raise as many problems as would be raised by a comparable study of ‘land deterrence’.” Denning 2015.

³⁴For a similar classification, see Nye 2016/2017; for a general description, see the Preface by Osinga and Sweijts in the present volume.

Table 20.1 Overview of arguments on the potential to deter cyber attacks

Scholarship	Arguments
Denning 2015	Same problems for CD as for conventional deterrence. Potential for CD through existing regimes
Gartzke and Lindsay 2015	CD suffers from problems of rationality, attribution, and secrecy. This means we have to instead focus on deception as distinct strategy
Tor 2015	We should move from ‘absolute’ CD to ‘cumulative’ CD, which is restrictive and continuous in nature
Stevens and Muller 2017	(NATO) CD seems to be viable. Yet, it should be viewed as a cumulative process, beyond military
Sulmeyer 2017	CD might be possible in theory. However, we are still unclear what activity to deter, and which tools to use to impose costs
Kello 2017	CD does not work as a strategy, but we should aim for punctuated CD instead: we should not deter individual actions but a series of actions
Healey 2017	CD is still working on the high-end—yet, nations show limited restraint. It is the aspect of ‘constant cyber activity’ which causes problems
Nye 2017	Conventional CD is difficult. Instead, we should focus on deterrence by economic entanglement and norms to overcome barriers
Harknett and Fischerkeller 2017	CD is impossible due to the structure of cyberspace. We need to move away from the deterrence paradigm and consider different forms of strategy
Brantly 2018	Absolute deterrence may not be possible—but a form deterrence as in criminology might be. We need to move away from deterrence only by punishment and denial

(Source Smeets and Lin 2018a, p. 62)

network penetration, and thus influence the cost-benefit calculations of an adversary to the degree that it either disincentivizes an attack or grinds an attacker to halt over time. Second, *deterrence by punishment* seeks to discourage the adversary from attacking, recognizing the costly consequences following their actions outweigh the benefits. We have seen variations of this logic being proposed as well. According to Lucas Kello, instead of trying to deter individual acts, countries should go for punctuated deterrence: “a series of actions that generate cumulative effect, rather than tit for tat response”.³⁵ Third, *deterrence by entanglement* rests on the unresolved discussion in international relations theory on whether state-to-state interdependence mitigates interstate conflict. Fourth, *deterrence by de-legitimization* focuses on the creation of norms and rules for state behaviour in cyberspace, will over time translate into a general principle of restraint, raise the reputational costs of bad behaviour, and shrink the battlespace to only encompass military combatants.

³⁵Kello 2017.

The third group (denoted in the table in white) argues that cyber deterrence is not possible. At least not in the way that the first two groups tend to believe. Jon Lindsay and Erik Gartzke, for example, put forward the idea of a comprehensive deception strategy—both on offense and defence—because the cyber domain is “a global network of gullible minds and deterministic machines.”³⁶ In contrast Harknett and Fischerkeller make the case that the unique characteristics of cyberspace “[demand] a unique strategy, a capabilities-based strategy of cyber persistence,” whose goal it is “to remove the escalatory potential from adversarial action”.³⁷

20.4 The Future

Figure 20.1 suggests that the writing and thinking about cyber deterrence is slowly falling out of fashion among scholars. This could be for at least three reasons: (i) everything has been said already;³⁸ (ii) the concept of deterrence is misapplied in cyberspace, or (iii) other strategic concepts are gaining more prominent attention. Likely a mix of these causes, it is unlikely this trend reverses itself anytime soon. Instead, we expect the debate to fork into four directions, which—although distinct and separate—do not mutually exclude each other.

The first direction will seek to increasingly incorporate cyber deterrence as an element within the broader international security and contest in a multi-domain world. Aaron Brantly for example argued back in 2018 that the main challenge of the future is not to define deterrence in cyberspace, but to “*understand the role digital technologies play in the broader scope of interstate deterrence*”.³⁹ A recently published edited volume of Jon Lindsay and Erik Gartzke on *Cross-Domain Deterrence* has also already moved in this direction. As the scholars write, “cross-domain deterrence is not new today, but its relevance is increasing. Strategic actors have long combined capabilities or shifted domains to make coercive threats or design around them [...] As a larger and more diverse portfolio of tools available for coercion complicates strategic choices, a better understanding of [cross-domain deterrence] becomes a critical asset for effective national security strategizing.”⁴⁰

Given the technical nature of the cyber domain, the second direction will primarily focus on deterrence effects that can be achieved on the operational and tactical level. Currently, there are numerous practical obstacles that hinder scholars

³⁶Gartzke and Lindsay 2015.

³⁷Harknett and Fischerkeller 2017.

³⁸We consider this reason to be least likely given that nuclear deterrence continues to be a prolific research area despite the numerous articles published in the field over the past decades.

³⁹Brantly 2018.

⁴⁰Lindsay and Gartzke 2019, pp. 333–335; also see Futter 2018.

and strategists to explore this route, including: highly classified documents, non-access to cyber operators, and the embryonic stage of existing military cyber organizations. Over time, we expect those hurdles to slowly melt away to the extent that operational and tactical know-how on how cyber operators actually defend, fight, and win in cyberspace will increasingly make its way into open source.⁴¹ Insights into this ground game, will also highly likely lead to a better understanding on how escalation dynamics work in cyberspace and what psychological effects can and cannot be created.

The third direction seeks to shift the attention away from deterrence, towards the other form of coercion: compellence.⁴² Compellence refers to an action that persuades an adversary to stop or change an action. Compellence is conventionally considered to be more difficult. When the actor changes behaviour, there are often reputational costs. In this respect, offensive cyber operations may come with an advantage: “Its effects do not necessarily have to be exposed publicly, which means the compelled party can back down post-action without losing face. More specifically, the compelled actor can deny that the effect was caused by OCC.”⁴³ There are also more opportunities to reverse the effects of cyber operations, which may further encourage compliance.⁴⁴

The final direction will explore strategic concepts that seeks to contain and blunt adversarial aggression in cyberspace that stands apart from traditional deterrence thinking. Persistent engagement is a first step into this direction—a concept also adopted by the US Cyber Command in their 2018 ‘Vision’ document entitled “Achieve and Maintain Cyberspace Superiority”.⁴⁵ Early contours of this concept are found in a 2016 article by Richard Harknett and Emily Goldman, talking about an “offense-persistent strategic environment” in which “the contest between offense and defence is continual [and] the defence is in constant contact with the enemy”.⁴⁶ Harknett and Michael Fischerkeller further refined the idea a year later, arguing that “in an environment of constant contact, a strategy grounded in persistent engagement is more appropriate than one of operational restraint and reaction for shaping the parameters of acceptable behaviour and sustaining and advancing U.S. national interests.”⁴⁷ Underlying this move away from deterrence thinking is a belief that the literature paid too much attention to the ‘the high-and-right’ cyber equivalent to an armed attack—that is, the concept of ‘cyberwar’, ignoring the fact that the actual behaviour of actors in cyberspace has been of a far more nuanced nature. As

⁴¹There is also the opportunity for more game theoretical modeling at this level. For an initial analysis, see Axelrod and Iliev 2014. For an overview, see Smeets and Work 2020.

⁴²Schelling 1966.

⁴³Smeets and Lin 2018a, p. 64.

⁴⁴Ibid.

⁴⁵United States Cyber Command 2018. For a summary, see Harknett 2018. For critical assessments, see Healey 2018; Healey 2019; Smeets and Lin 2018b; Schneider 2019; Smeets 2020.

⁴⁶Harknett and Goldman 2016, p. 15.

⁴⁷Fischerkeller and Harknett 2017, p. 381.

Harknett and Smeets wrote in a 2020 *Journal of Strategic Studies* article, “what has emerged are campaigns comprised of linked cyber operations, with the specific objective of achieving strategic outcomes without the need of armed attack”.⁴⁸

It is also likely we will see the emergence of alternative strategic concepts, beyond persistent engagement. Analysts from European states can be expected to promote ideas that stand in stark contrast to U.S. thinking. While most European states have absorbed early U.S. thinking of cyberspace being a warfare domain and the need for cyber deterrence, European policymakers are uncomfortable with adopting much less discussing persistent engagement, as it is perceived as overly aggressive. Similarly, most European military cyber organizations will not be able to increase their operational capacities to such a degree that they can navigate “seamlessly, globally, and continuously”, as persistent engagement demands. Recognizing these limitations, EU member states will have to fill this strategic vacuum with creative conceptual thinking.

20.5 Conclusion

The purpose of this chapter was to situate the current debate on cyber deterrence within the historical evolution of deterrence thinking in cyberspace, clarify the existing conceptualizations, and comprehensively discuss whether the concept of cyber deterrence has an analytical future. Born in the 1990s, the thinking on cyber deterrence was nurtured by the U.S. Department of Defense in numerous war-gaming exercises. Hitting puberty in the aftermath of the distributed denial-of-service campaign against Estonia in 2007, we showed in this chapter that cyber deterrence matured after Stuxnet and received peak attention from policymakers and academics from 2013 to 2016 during the golden age of ‘cyberwar’ scholarship. Yet, it also became clear that, from 2016 onward, the interest in cyber deterrence started to fade to the extent that it is now intentionally neglected.

We argued that the future deterrence debate can move into four directions: increased incorporation of cyber deterrence as an element within the broader international security and contest in a multi-domain world. A deeper focus on the technical aspects of the cyber domain to achieve deterrence effects on the operational and tactical level. A closer analysis of compellence, as the alternative form of coercion. And an exploration of new strategic concepts that seeks to contain and blunt adversarial aggression in cyberspace that stands apart from traditional deterrence thinking.

In contrast to the evolution of deterrence theory in realspace, which has moved along four (respectively five) distinctive waves, the evolution of cyber deterrence is to some degree schizophrenic. Theory-wise it is still stuck between the first and second wave—due to absence of large empirical datasets and comprehensive case studies. As

⁴⁸Harknett and Smeets 2020, p. 1.

a result, the three groups of scholars outlined in Table 20.1, are still interlocked in a disagreement on the very fundamentals of deterrence thinking in the cyber domain. Meanwhile, mechanism-wise, cyber deterrence is seen as an inherent part of the fourth (detering asymmetric threats) and fifth deterrence wave (resilience and cross-domain integration). To reconcile this schizophrenic approach, scholars and practitioners need to figure out whether cyberdeterrence mechanisms can actually work without having a firm grasp on cyber deterrence theory, and whether cyber deterrence theory is actually based on evidence collected from the cyber domain rather than deduced from known behavioural outcomes in realspace. Answers to these questions will likely be found within the three future directions we have outlined.

References

- Arquilla J, Ronfeldt D (1993) Cyberwar is Coming! *Comparative Strategy*, 12.2:141–165
- Axelrod R, Iliev R (2014) Timing of Cyber Conflict. *PNAS*, 111.4:1298–1303
- Betz D J, Stevens T (2011) Cyberspace and the State: Towards a Strategy for Cyber-Power. *Adelphi Series* 51:424
- Borghard E D, Lonegran S W (2017) The Logic of Coercion in Cyberspace. *Security Studies* 26:3 452–481
- Brantly A, Smeets M (n.d.) Military Cyber Operations. In: McD Sookermany A (ed) *Handbook of Military Sciences*. Forthcoming, Springer
- Brantly AF (2018) The Cyber Deterrence Problem. 2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects. <https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf>. Accessed 14 April 2020
- Broder J M (1990) U.S. War Plan in Iraq: ‘Decapitate’ Leadership: Strategy: The Joint Chiefs believe the best way to oust the Iraqis would be air strikes designed to kill Hussein. <https://www.latimes.com/archives/la-xpm-1990-09-16-mn-1221-story.html>. Accessed 14 April 2020
- Byman D, Waxman M C (2001) *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*. Cambridge University Press, New York
- Clarke R, Knake R (2010) *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins Publishers
- Denning D E (2015) Rethinking the Cyber Domain and Deterrence. *Joint Forces Quarterly* 77:8–15. <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-77/Article/581864/rethinking-the-cyber-domain-and-deterrence/>. Accessed 14 April 2020
- Derian J D (1994) Cyber-deterrence. <https://www.wired.com/1994/09/cyber-deter/>. Accessed 14 April 2020
- Fischerkeller M, Harknett R J (2017) Deterrence is not a credible strategy for cyberspace. *Orbis*, 61:381–393
- Futter A (2018) *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Georgetown University Press, Washington, D.C.
- Gartzke E (2013) The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38.2:41–73
- Gartzke E, Lindsay R J (2015) Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies* 24(3):316–348
- Harknett R J (1996) Information Warfare and Deterrence. *Parameters*, 26:3
- Harknett R J (2018) United States Cyber Command’s New Vision: What It Entails and Why It Matters. *Lawfare*. www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters. Accessed 14 April 2020

- Harknett R, Fischerkeller M P (2017) Deterrence is Not a Credible Strategy for Cyberspace. *Orbis* 61:381–393.
- Harknett R J, Goldman E (2016) The search for cyber fundamentals. *Journal of Information Warfare*. <https://www.jinfowar.com/journal/volume-15-issue-2/search-cyber-fundamentals>. Accessed 14 April 2020
- Harknett R J, Nye J S (2017) Is Deterrence Possible in Cyberspace? *International Security*, 42.2:196–199
- Harknett R J, Smeets M (2020) Cyber campaigns and strategic outcomes. *Journal of Strategic Studies* 1–34
- Healey J (2017) Cyber Deterrence Is Working – So Far. *Cypher Brief*. <https://www.thecipherbrief.com/cyber-deterrence-is-working-so-far>. Accessed 14 April 2020
- Healey J (2018) Triggering the New Forever War, in *Cyberspace*. *Cipher Brief*. www.thecipherbrief.com/triggering-new-forever-war-cyberspace. Accessed 14 April 2020
- Healey J (2019) The implications of persistent (and permanent) engagement in cyberspace, *Journal of Cybersecurity*, 5:1
- Henderson SJ (2007) *The Dark Visitor: Inside the World of Chinese Hackers*. Available from <https://www.lulu.com/shop/scott-henderson/the-dark-visitor-ebook/ebook/product-2420426.html>
- Kello L (2017) *The Virtual Weapon and International Order*. Yale University Press, Yale
- Keuhl DT (2002) Information Operations, Information Warfare, and Computer Network Attack, Their Relationship to National Security in the Information Age. In: Schmitt MS, O'Donnell BT (eds) *Computer Network Attack and International Law*. Naval War College Press
- Lapsley P (2013) *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*. Grove Press
- Libicki MC (2009) *Cyberdeterrence and Cyberwar*. RAND Corporation, Santa Monica, CA p. xii–xvii
- Libicki MC (2012) *Crisis and Escalation in Cyberspace*. RAND Corporation, Santa Monica, CA
- Libicki MC (2012) *Crisis and Escalation in Cyberspace*. RAND Corporation, Santa Monica, CA
- Liff A P (2012) Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35.3:401–428
- Lindsay J R (2015) Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cyber Security*, 1.1:53–67
- Lindsay J R, Gartzke E (2019) *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press
- Mitnick K (2012) *Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker*. Little Brown and Company
- Molander R C, Riddile A S, Wilson P A (1996) *Strategic Information Warfare: The New Face of War*. RAND
- Ney J S Jr. (2016/2017) Deterrence and Dissuasion in Cyberspace. *International Security* 41.3:44–71
- Nichiporuk B (1999) US Military Opportunities: Information-warfare Concepts of Operation. In: Khalizah Z, White J (eds) *The Changing Role of Information in Warfare*. RAND Corporation, p. 193
- Rid T (2012) Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35.1:5–32
- Ronfeldt D, Arquilla J (eds) (1996) Implications for US Doctrine and Strategy. *The Advent of Networks*. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR789/MR789.ch6.pdf. Accessed 14 April 2020
- Ronfeldt D, Arquilla J (1999) What Next for Networks and Networks. In: Ronfeldt D, Arquilla J (eds) *Networks and Networks: The Future of Terror, Crime, and Militancy*. RAND, Santa Monica CA, p. 532. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch10.pdf. Accessed 14 April 2020
- Sartori G (1970) Concept Misinformation in Comparative Politics. *The American Political Science Review*, 64.4:1033–1053
- Schelling TC (1966) *Arms and Influence*. Yale University Press, New Haven

- Schneider JG (2019) Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy. *Lawfare*. <https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy>. Accessed: 14 April 2020
- Shires J, Smeets M (2016) What Do We Talk About When We Talk About ‘Cyber’? SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2860839. Accessed 14 April 2020
- Slatalla M, Quittner J (1994) Gang War in Cyberspace. *Wired*. <https://www.wired.com/1994/12/hacker-4/>. Accessed 14 April 2020
- Smeets M (2018) The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, 12.3:90–113
- Smeets M (2020) U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. *Intelligence and National Security*, 2:444–453
- Smeets M, Gorwa R (2019) Cyber Conflict in Political Science: A Review of Methods and Literature. *SocArXiv Papers*. <https://osf.io/preprints/socarxiv/fc6sg>. Accessed 14 April 2020
- Smeets M, Lin H (2018a) Offensive Cyber Capabilities: To What Ends? In: Minárik T, Jakschis R, Lindström L (eds) 2018 10th International Conference on Cyber Conflict, CyCon X. NATO CCD COE Publications, Tallinn
- Smeets M, Lin H (2018b) What Is Absent From the U.S. Cyber Command ‘Vision’. *Lawfare*. <https://www.lawfareblog.com/what-absent-us-cyber-command-vision>. Accessed 14 April 2020
- Smeets M, Work J D (2020) Operational Decision-making or Cyber Operations: In Search of a Model. *Cyber Defense Review* 95–112
- Stevens T, Muller LP (2017) Upholding the NATO cyber pledge. *Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics*. Norwegian Institute of International Affairs, Policy Brief 5/2017. <https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2442559>. Accessed 14 April 2020
- Summeyer M (2017) Which Cyberattacks Should the United States Deter, and How Should It Be Done? CFR. <https://www.cfr.org/blog/which-cyberattacks-should-united-states-deter-and-how-should-it-be-done>. Accessed 14 April 2020
- Theohary C A (2018) Information Warfare: Issues for Congress. <https://fas.org/sgp/crs/natsec/R45142.pdf>. Accessed 14 April 2020
- Tor U (2015) ‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies*, 40.1–2:92–117
- United States Cyber Command (2018) Achieve and Maintain Cyberspace Superiority. <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>. Accessed 14 April 2020
- Wheatley G F, Hayes R E (1996) *Information Warfare and Deterrence*. NDU Press
- William B D (2017) Meet the scholar challenging the cyber deterrence paradigm. *The fifth domain*. <https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/>. Accessed 14 April 2020

Stefan Soesanto is a Senior Researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

Max Smeets is senior researcher at the Center for Security Studies (CSS) at ETH Zurich. He is also an Affiliate at Stanford University Center for International Security and Cooperation and Research Associate at the Centre for Technology and Global Affairs, University of Oxford, UK.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.