9 Uncertainty and the study of cyber deterrence

The case of Israel's limited reliance on cyber deterrence

Amir Lupovici

Challenges and threats in the cyber domain create many uncertainties for actors – uncertainty about the threat environment as well as about the effectiveness of their means to address these challenges. International relations scholars have long pointed to a number of dynamics that are highly affected by uncertainty, including the security dilemma (e.g. Roe 2004: 9–16; Rathbun 2007). But certain characteristics of the cyber domain can aggravate these difficulties, such as the fragmentation of authority, the lack of accountability, and the tempo and scope of technological developments (Dunn Cavelty and Wenger 2020; Egloff 2020).

The uncertainty policymakers face in crafting strategies and assessing their effectiveness has also become a fundamental challenge for scholars trying to trace, understand, and explain dynamics in the cyber domain. As Dunn Cavelty and Wenger (2020: 20) argue:

A case in point is the lack in public transparency and trusted knowledge about the perpetrators behind most cyber incidents. Although the number of public attributions of cyber incidents by states and threat intelligence firms has been on the rise, both types of actors have political and economic reasons not to fully disclose their evidence.

(see also Egloff 2020: 61)

The uncertainties around the cyber domain thus exacerbate scholars' ability to explore the practices, behavior, and strategies of the various actors involved. For example, scholars who develop databases of cyber conflicts cannot determine whether their data encompass all the main incidents (Valeriano and Maness 2014: 351).¹ Similarly, scholars exploring the cyber security dilemma are less certain about the means each opponent holds and develops. Scholars (as well as practitioners) are uncertain not only about the capabilities of state actors involved, but also about the means of non-state actors, including advanced technological firms (Dunn Cavelty and Wenger 2020: 23). Furthermore, these uncertainties are aggravated by rapid changes in technology that states and non-state actors alike try to acquire. This arms race is rapid, and the efficiency of the means the actors develop is not fully understood² by either the involved actors or scholars. While

how to use an emerging technology is almost always in question (i.e., nuclear weapons as a means of deterrence or of war-fighting), the facts that the changes are rapid and that non-state actors are involved in acquiring and potentially using these technologies make it even more challenging.

These challenges are thus an obvious obstacle to studying specific strategies, such as cyber deterrence.³ First, studying cyber deterrence is a challenge because scholars have difficulty identifying and tracing situations of deterrence success⁴ as well as situations of deterrence failure (Lupovici 2020). Second, many scholars have emphasized the attribution problem as a great challenge for cyber deterrence success, limiting the ability to issue a credible deterrence threat (see in Morgan 2010; Lupovici 2011; Stevens 2012: 149–53).⁵ While this challenge is not necessarily unresolvable for deterrence actors⁶ – and so should not prevent them from successfully employing cyber deterrence strategies (e.g. Nye 2017) – it may pose an insurmountable challenge for scholars, who have much less access to this kind of information. Given these two problems, scholars who study cyber deterrence have difficulty getting the required empirical information on cyber incidents. Their access to information about deterrence failure and success is limited, and even if they gain knowledge about a case of cyber attack, they may have difficulty attributing the source of the attack. These problems seriously limit the ability to establish arguments about deterrence strategy, especially regarding the conditions under which it works or fails.

It seems from this perspective that the uncertainties created by cyber technology, the rapid changes in technology, and the fragmentation of authority all challenge the scholarly exploration of cyber security. Nonetheless, I argue that these uncertainties should not discourage scholars, but rather might lead them to adapt their research questions, adopt additional methods, and shift their empirical focus. Each of these challenges prompts thinking in directions to minimize or bypass the limitations around studying interactions in the cyber domain. For example, uncertainties and rapid changes in technology mean scholars should focus on shifts over longer segments of time. Even if technology is changing quickly, the impact of this on strategies and doctrines lags. This focus has two important implications. First, it is a more feasible goal: not only does it provide an anchor that decreases uncertainties given the vast amount of information on past strategies and behavior, but it also allows us to limit the challenge of rapid changes. How technology is translated into policy leaves more traces, especially as strategies like deterrence require strategic communication with opponents (i.e., issuing threats). Second, the impact of technologies on strategies and actor behavior is mediated through social attributes.⁷ Therefore, scholars can compare new policies and strategies with past ones and explore whether and how they resonate with them.

Focusing on how a new technology enters into doctrines and strategies raises various questions. Some can be developed and answered through interpretative approaches, by looking at the constraints and opportunities the social context creates for actors relying on new technologies. This helps in conducting comparisons, but also in examining specific characteristics of the technology that allow or limit shifts from past types of behavior. For example, rather than exploring

how a strategy is effective or not effective (i.e., under what conditions a strategy works) given the limitations of uncertainties and rapid changes, scholars can also direct their research toward questions about the strategy's adoption. Among other things, scholars can explore how actors come to adopt a strategy and adapt it to address challenges of the cyber domain, or alternatively how they refrain from adopting it. Elaborating on these issues leads to questions about how technological impetus is embedded in actors' narratives, strategic culture, and identities, and how adopting a certain strategy fits or challenges international norms.

In order to illustrate this research conduct and its merit, I briefly discuss the Israeli cyber deterrence strategy and the limited extent of its adoption. Focusing on the adoption of the strategy – rather than on the more uncertain questions about deterrence success – demonstrates a way to address key challenges in studying cyber security given the uncertainties and rapid changes discussed above. As I elaborate below, studying Israel's adoption of deterrence strategy directs our attention to how it fits Israel's strategic culture and identities. This, in fact, presents a puzzle. While deterrence is a prominent Israeli strategy, cyber deterrence strategy has so far not been fully adopted. Understanding the social context raises important questions that the rapid technological changes do not prevent us from asking and answering.

Israel (cyber) deterrence

It is beyond the space limits of this chapter to discuss all relevant methodological aspects or fully explore the case. Rather, this discussion aims to demonstrate the methodological solutions presented above by focusing on Israel's cyber deterrence strategy. Despite Israel's reliance on deterrence strategies vis-à-vis various kinds of threats, Israel, unlike for example the United States,⁸ has still not adopted an explicit cyber deterrence strategy. However, since the second decade of the 2000s, there has been growing support for adopting such strategy by key Israeli officials.

Deterrence is a prominent strategy in Israel. While this strategy has emerged from different strategic rationales since the 1950s (Yaniv 1987: 72; Levite 1989: 27–35; Bar 1990: 54; Evron 1994: 40, 42–3; Tal 2000: 51; Cohen 2010: 35–6, 77), it continues to be a dominant Israeli strategy, and it is endorsed by both the political and military elites (Yaniv 1987; Evron 1994: 40–1; Levite 1989: 25, 47; Bar-Joseph 2001: 2). Furthermore, over the years the Israeli deterrent strategy has been developed and adapted to address different kinds of threats (Bar-Joseph 1998).

For Israel, practicing deterrence fulfils not just physical security needs, but also identity-related needs. As Lupovici (2016b) suggests, Israel holds a deterrer identity. A deterrer identity is when an actor internalizes a *deterrence role* that it is attached to and through which it perceives how it needs to act in the international arena.⁹ The manifestation of the Israeli deterrer identity is evident in how Israel perceives threats, responds to them, and justifies certain policies. From Israel's perspective, lack of violence is deterrence success, while eruption of violence is

deterrence failure. Israel prioritizes deterrence strategy and practices over other strategies to the extent that deterrence has become an aim itself: the goal in various situations has been defined (and securitized) in terms of enhancing or restoring the Israeli deterrent posture. Given the high status of deterrence in Israel, policymakers can mobilize support for different policies, pointing to their alleged contribution to the deterrent posture (Lupovici 2016b: 55–8).

However, this discussion on the prominence of Israeli deterrence strategy intensifies the puzzle of the state's limited adoption and employment of deterrence in the context of cyber security challenges. Given the prominence of deterrence in Israel's strategic thinking, one would expect that Israel would be eager to adopt a cyber deterrence strategy to address these challenges. The fact it has not developed a clear cyber deterrence strategy is a phenomenon that requires explanation. While fully explaining this behavior is beyond the scope of this chapter, I argue that focusing on the period of the early 2010s shows how Israel has started to adopt cyber deterrence strategy. This dynamic can be understood as part of a broader strategization of cyber security. On the one hand, Israel gives more attention to these practices; on the other hand, the strategization of cyber security is limited, reflecting the limited adoption of cyber deterrence practices.

The strategization of cyber security in Israel

There are a number of indications of changes in how cyber (in)security is seen in Israel. These highlight the similarities of some aspects of cyber security to traditional security issues. These include changes (1) on an institutional level, (2) in the view of cyber as a strategic domain, and (3) in how cyber insecurities are narrated.

Initial efforts to develop a cyber doctrine at the national level are evident in Israel's attempts to solidify its cyber defense. Especially since the early 2000s, Israel has endeavored to protect and regulate the information security of various bodies, including critical infrastructures, private companies, and financial organizations (Even and Siman-Tov 2012: 76–9; Baram 2013: 28–9; Tabensky and Ben Israel 2015: 35–41). It made further efforts during the 2000s to strategize cyber security. A key development was the attempt in August 2011 to integrate national cyber defense by establishing a new body – the Israeli National Cyber Bureau (INCB) (Adamsky 2017: 115). This body has four departments: security, civilian, intelligence and situation assessment, and organization and policy. In addition, it operates a control room (Baram 2013: 35). According to Even and Siman-Tov, establishing this body was significant in that it was the first strategic organ whose scope of activity is defense at the national level (Even and Siman-Tov 2012: 67–8, see also Government Decision 3611, August 2011). As Tabensky and Ben Israel (2015: 52) further clarify, the main task of the INCB is “drafting comprehensive national cyber strategy”. They suggest that evidence of this move to a strategy was hinted in a talk given by Evyatar Matania, who then served as the head of the INCB, in which he emphasized the need of Israel to move from “defense” to “security” (Tabensky and Ben Israel 2015: 52).

Cyber security was further strategized with the establishment of the Israeli National Cyber Directorate (INCD), following a government decision from February 2015. This body is the “highest national authority for strategic cyber policy planning, for the regulation of its operational execution across the government, and for building cyber capabilities for the short, medium, and long term” (Adamsky 2017: 120; see also Government Resolution 2444, 2.15.2015; Even et al. 2016; Orbach 2015; Adamsky 2017: 116, 120).

A brief review of these modifications reveals that Israel went through a process in which policymakers tried to strategize cyber security and centralize the defense of critical infrastructures from cyber threats. Nonetheless, as Baram (2013: 32) suggests, while Israel is a leading cyber power, its capabilities were not reflected in the forming of a cyber strategy or, more specifically, “in the institution of a regular strategy or in a clear statement of an official course of action. It appears that Israel has yet to formulate a strategy in this field”.¹⁰ In a similar way, although an increasing number of Israeli policymakers and practitioners acknowledge that cyber is a critical aspect of war, not all institutional changes that aimed to reflect this acknowledgment were employed. Foremost, key officials referred directly to cyber space as a domain of warfare parallel to traditional spaces. For example, in 2009, IDF Chief of Staff Gabi Ashkenazi defined cyber space as “a strategic and operative domain of warfare” (Even and Siman-Tov 2012: 79). Likewise, in 2012 Netanyahu declared, “Today cyber is part of the battlefield ... This is not tomorrow’s warfare, it is already here today” (qtd. in Keinon 2013). These views are reflected in a document drafted by IDF’s Operations Directorate, which defines cyber space as another battlefield, like land, sea, and airspace (Katz 2012).

Nonetheless, it should also be noted that while key officials ordered the establishment of a new branch – the cyber branch (albeit not a cyber command, as for example in the United States) (Cohen 2015) – it is still not operative (Cohen 2017). Recent years have seen increasing indications not only of attempts to strategize cyber security, but also of seeing it in terms of more traditional security challenges. While there is little public discussion of these issues, some key Israeli political leaders have used analogies clearly demonstrating that they think of cyber security in terms of more traditional security challenges and responses. For example, Prime Minister Netanyahu argued that Israel needs “a cyber Iron Dome”.¹¹ As he claims, “For this purpose, I established the National Cyber Directorate a year ago and it has been working to block these attempts [cyberattacks] by developing what I would call a ‘digital Iron Dome’” (qtd. in Hirsch and Gattegno 2012). Netanyahu repeated this analogy several times, including mentioning Iran and its proxy, Hezbollah, as a main source for cyberattacks on Israel that requires this “iron dome” (e.g., Prime Minister Office 2012; see also in Keinon 2013).¹²

While these claims echo the previous assertion that defense was a key aspect in the formation of Israel’s cyber security thinking (and strategy), they also provide a clear analogy of the traditional security aspects (Haber and Zarsky 2017: 153–4). As emphasized by Eviatar Matania, who then served as the director general of Israel’s National Cyber Directorate, Israel needs to develop a “digital equivalent of the Iron Dome” (Solomon 2017). This analogy reflects both the kind of threat

(cyber threat is the same as the “traditional” rocket threat) and how the threat should be dealt with (by the government).

Israel’s limited reliance on cyber deterrence

I argue that the limited adoption of cyber deterrence in Israel during the early 2010s reflects and is part of the limited strategization of cyber security in Israel. While there seems to have been increasing acknowledgment of the need for cyber deterrence, it was adopted only to a limited extent. Both the adoption of the strategy and the limited nature of its adoption are evident in two main manifestations of this strategy.

The first can be inferred from the cyber operations Israel conducted against the Iranian and Syrian nuclear programs. In these cases, cyber means were used, albeit in different ways. Experts have pointed to these incidents as Israeli attempts to establish cyber cumulative deterrence based on the actual use of force. For example, Tor (2017: 6) noted regarding Stuxnet that although its effectiveness in damaging the Iranian nuclear program is not entirely clear, “Stuxnet may still have had an effect in demonstrating capability and intent” and thus can be examined in the context of deterrence. Likewise, Tabensky and Ben Israel (2015: 68) refer to these two incidents – Stuxnet and the attack on the Syrian reactor – to suggest that if Israel relied on cyberattacks in these operations, “it attests to the high maturity of technology, doctrine, and organisation of the IDF” and thus had a deterrent effect.

The use of cyber capabilities in attempts to create future deterrence fits the strategy of cumulative deterrence that Israel practices in other domains, and it accords with Israel’s reliance on creating deterrence through the actual use of force (Bar-Joseph 1998: 156–7; Almog 2004–5). Nonetheless, not only is the effectiveness of this type of deterrence open to question,¹³ but, more importantly, how Israel has used it – if it has used it at all – also demonstrates the limited way Israel has adopted this strategy and adjusted it to cyber space, as it is a deterrent threat only in a very indirect and implicit way.

The second manifestation is the increasing number of Israeli policymakers, including key politicians such as Prime Minister Netanyahu, who make the point that Israel should adopt a cyber deterrence strategy. Netanyahu asserted that cyber warfare is

cloudy and unknown. The ability to achieve balance in the cyber realm is much harder and is *dependent on combination of defense and deterrence*. The fact that the source of attack is often anonymous challenges the ability to create a balance of deterrence, and we should pay attention to that.

(qtd. in Ben-Yosef 2011, my emphasis and my translation)

This statement clearly demonstrates the limited nature of Israel’s adoption of cyber deterrence strategy. While he acknowledges the need to establish such a

strategy, Netanyahu's statement emphasizes the strategic challenge of creating it and the need to combine it with another strategy (defense). Nonetheless, he does highlight the need to develop a cyber deterrence strategy, an emphasis that was absent from previous statements in this regard.

This need to acquire a cyber deterrence strategy is evident in statements of other key practitioners, for example, Major-General Amos Yadlin, who then served as the head of IDF's Military Intelligence Directorate. According to him, cyber security poses important questions that should be publicly discussed. These questions concern, among other things, "the essence of deterrence that would prevent war in cyber space" (Yadlin 2009, my translation).

Some have even made more explicit the connection between how they perceive cyber security on the one hand and cyber deterrence on the other. For example, at the beginning of a talk he gave in 2012, Minister of Defense Ehud Barak suggested that cyber is another domain of warfare. According to him, "to the security equation, along with land, sea, air and space we need to add cyber as a new dimension". He concluded his talk by stating that in the vagueness created by cyber capabilities, "leadership is required to show the way as to how to do the right thing for Israel and to *establish a deterrent balance* and act effectively in this new world" (Barak 2012, my emphasis and translation). Barak, thus, connects viewing cyber as a traditional domain of security with adopting cyber deterrence strategy.

Likewise, in January 2012, Deputy Foreign Minister Danny Ayalon called for the adoption of a declared cyber deterrence strategy, justifying it with reference to American cyber deterrence strategy, which is based on an explicit threat of retaliation as presented above. According to him, "[T]he US has announced that any attack on its cybernetic space would be considered a declaration of war and that it would go as far as firing missiles to respond to such an attack. This is a good criterion for us all". Furthermore, as evident with this reference, Ayalon sees cyberattacks as a more traditional means of violence – constituting acts of war (Curiel 2012).

To conclude these points, this discussion demonstrates the limited extent to which Israel has adopted a cyber deterrence strategy. While it marks a shift from the silence on cyber deterrence of previous years, the adoption of this strategy demonstrated by these manifestations is relatively limited. The first emphasizes deterrence through the actual use of cyberattacks but concerns only an implied cyber deterrence strategy. The second – the acknowledgment of the need to develop a cyber deterrence strategy – also demonstrates the limitation, as it mainly concerns the need to adapt Israel's capabilities and doctrine to allow issuing a cyber deterrent threat; it is not about recognizing the existence of this strategy or actually issuing such threats.

Conclusion

This chapter aims to demonstrate the feasibility of addressing the methodological challenges of studying cyber (security) given the uncertainties that surround it. One direction offered is to focus on the adoption and employment of a

strategy – and not only on its effectiveness, as most scholars do. I briefly demonstrated these ideas by studying Israel's limited and gradual adoption of a cyber deterrence strategy and how it fits Israel's traditional security practices.

The suggested methodological solutions used in this chapter illustrate that while uncertainties, rapid changes, and fragmentation of authority can constrain the research, they also provide opportunities to develop, think about, and adapt various methods and alternative focuses for research on cyber security. Employing interpretative approaches is another direction that could be developed to explore other aspects of cyber security affected by these challenges.

Furthermore, constructivist research is also highly promising, specifically in studying uncertainties and rapid technological changes (Rathbun 2007: 549–52). Scholars not only can examine whether and how adopted strategies fit states' identities and narratives but can explore the discourse around these strategies: for example, how these strategies are presented, mediated to the public, and justified. These directions provide many opportunities for scholars given both the data and information to which such findings can be compared and given that we can trace such changes evident in the public sphere, despite challenges concerning secrecy.

More traditional methods and directions can also be used to address these challenges in studying cyber security. For example, rapid technological change means that past technologies quickly become obsolete. From a methodological perspective, this means that information about former technologies will become available more quickly than in the past. While the result is that scholars are limited in analyzing the most advanced technologies, scholars can be satisfied with empirical focus on “older technologies” – which, given the rapid changes, may be the advanced technologies of only five years ago.

Similarly, the fragmentation of authority, while enhancing uncertainties in studying different aspects of cyber security, also provides an opportunity. Scholars can focus on non-state actors not only as targets of state actors' strategies but also as strategists themselves. For example, in addition to examining how states attempt to deter non-state actors, scholars can explore how non-state actors issue deterrent threats to different kinds of actors (Wilner 2020: 29; Lupovici 2019).

The discussion of the Israeli case also carries some important implications. One crucial issue is how the understanding of the cyber domain (and the social constructions of it) affects how policymakers develop strategies and adapt old strategies, such as deterrence, to this domain. In explaining this behavior, scholars can contrast this policy with the strategies of other countries that adopt more explicit cyber deterrence strategy, such as the United States (see in Wilner 2020).

Another promising direction concerns tracing changes in the adoption of cyber deterrence over time. A key juncture point is May 2020. As published in the international media, Israel retaliated against targets in Iran following an Iranian cyber-attack on water infrastructures in Israel (e.g., Warrick and Nakashima 2020). This case is significant for several reasons. First, Israeli sources officially acknowledged the Iranian attack. Second, and more importantly, the publication of Israeli retaliation as well as other statements made by Israeli officials, such as Minister of Defense Naftali Bennett, was interpreted as the indication of Israel's tendency

to send deterrent messages for the Iranians (Siman-Tov and Evan 2020).¹⁴ If this interpretation is correct, this marks a shift in Israeli policy toward deterrence by the actual use of force, which aptly fits traditional Israeli deterrence practices in general, as discussed above. Indeed, there is still some ambiguity in the Israeli policy. Nonetheless, this case may turn out to be a significant point where Israeli cyber deterrence is made more explicit.

These changes also demonstrate the fertility of the suggested methodological solution. The seeming change in Israeli behavior invites various kinds of questions. For example, we can ask whether strategic incentives required Israel to shift its policy, or whether the change was due to perceptions of specific policy-makers – such as Bennett, who was about to leave office as a new Israeli government was established. Alternatively, these shifts can be explained by tracing the changes in how the cyber domain is understood or constructed. This is especially important if we acknowledge that messages are delivered not only to international audiences, such as the Iranians, but also to domestic audiences, such as the Israeli public. Targeting domestic audiences may become especially important in the search for legitimacy in how cyber security is understood and in how to address challenges actors face in this domain.

Acknowledgments

The author would like to thank the Interdisciplinary Cyber Research Center at Tel Aviv University for supporting this research.

Notes

- 1 This, for example, is less of a problem when studying traditional conflicts and attacks, where, while scholars might debate over the details, they face much less difficulty obtaining the information about these incidents.
- 2 Compare, for example, debates over the degree to which quantum computers challenge international security (e.g., Lindsay 2020; 2022).
- 3 While there is a debate over what “cyber deterrence” is (see Lupovici 2016a), for the purposes of this project I adopt the view (endorsed by many scholars) that cyber deterrence (by punishment) is a strategy that aims to dissuade a putative challenger from attacking a state’s cyber infrastructures or from attacking the state with cyber means by threatening to retaliate should such an event would occur (Stevens 2012: 149–52; see also Lupovici 2016a: 324–6).
- 4 The traditional assertion is that deterrence success cannot be easily traced because scholars cannot observe it – unlike deterrence failure, where there is an observable incident. The challenge, therefore, is that the scholarship is biased toward studying situations of deterrence failure, where scholars can more easily establish causal arguments (Achen and Snidal 1989: 161; Lebow and Stein 1990: 336, 347; Sauer 2016: 49).
- 5 Scholars argue that because the putative challenger knows that the defender actor will find it difficult to identify the source of attack, the challenger will estimate that the retaliation cannot be employed.
- 6 Scholars make three main points about the limitations of this challenge. First, the identity of a challenger can be deduced from the context – for example, in cases of cyberattack during a conflict between two actors or through the use of traditional intelligence capabilities (Kugler 2009: 310, 317–8; Kello 2013: 17–8). Second, as technology pro-

gresses, actors have better tools to identify the source of attack, including better forensic means to attribute cyberattacks (Rid and Buchanan 2015). Third, it is not only cyber technology per se but also international norms that limit retaliation when actors cannot fully identify the source of attack. However, international norms may change over time (Lupovici 2016a: 330–1).

- 7 Nonetheless, it should be noted that scholars debate to what extent society determines how technology develops and should be used (“social constructivism”) or the technology determines actors’ behavior (“technological determinism”) (e.g., Fritsch 2011; Manjikian 2018).
- 8 For an excellent review of US cyber deterrence strategy, see Wilner (2019). In this respect, as far as I know Israel has never issued a direct threat as the United States did, according to which any cyberattack against it would lead to a retaliation with all the means it holds – both cyber means and kinetic means (e.g., Department of Defense Cyber Policy Report 2011: 2).
- 9 Israel’s adoption and reliance on this strategy can be also explained by certain Israeli-Jewish narratives and identities, including the Israeli-Jewish victim identity. This narrative provides the context through which Israel interprets and magnifies threats, encouraging the need to use force and take active measures to prevent another Holocaust (Waxman 2006: 49; Bar-Tal 2001: 612–5; Barnett 2013: 37–47; see also Sucharov 2005: 31).
- 10 This does not mean that Israel lacks any strategic thinking regarding cyber security. A number of issues have gained much attention in the attempt to form a strategy, such as the legal aspect of cyber security and Israel’s attempt to shape new global norms of cyber security. However, this is less evident in more “traditional” security aspects that are related to the formation of a strategy, as well as in the operation of the different relevant bodies.
- 11 Iron Dome is a missile defense system Israel developed to intercept rockets.
- 12 Interestingly, the former Minister of Defense, Ehud Barak, also implied the connections between cyber threats and the threat of rockets (see in Cohen and Yaron 2012).
- 13 For critical discussion on the effectiveness of creating deterrence through the actual use of force, see Mercer 1996; Press 2005: 22–4, 147–8; Tang 2005; and Lupovici 2016b, but also see Rid 2012. Furthermore, in the cyber domain this is even more problematic, since revealing capabilities may allow a putative challenger to acquire means to neutralize the defender’s capabilities (see also Libicki 2007: 271–2).
- 14 As emphasized by Siman-Tov and Evan, Bennett stated on May 18, 2020, “We must increase political, economic, military, and technological pressure, and act in other dimensions as well. It can be done” (Bennett, in Siman-Tov and Evan 2020).

References

All links checked on August 23, 2021.

- Achen, H. C., and Snidal, D. (1989). Rational Deterrence Theory and Comparative Case Studies. *World Politics*, 42(2): 144–169.
- Adamsky, D. (2017). The Israeli Odyssey toward Its National Cyber Security Strategy. *The Washington Quarterly*, 40(2): 113–127.
- Almog, D. (2004–5). Cumulative Deterrence and the War on Terrorism. *Parameters*, 25(4): 4–19.
- Bar, M. (1990). *Red Lines in Israel’s Deterrence Strategy*. Tel Aviv: Ma’arachot (in Hebrew).
- Barak, E. (2012, June 6). A Keynote Address by Minister of Defense Yuval Na’man. Workshop for Science, Technology and Security. [Video]. YouTube. Retrieved from: <https://www.youtube.com/watch?v=doGiu556ZWQ> [in Hebrew].