Cyber Warfare and Deterrence: Trends and Challenges in Research

Amir Lupovici

In recent years a growing number of researchers have expanded the discussion of deterrence strategy to a host of new threats. Unlike the Cold War era in which the study of deterrence focused primarily on deterrence among nations and superpowers and on nuclear deterrence, recent years – particularly since 9/11 – have seen much research on deterrence strategy in relation to other threats, such as terrorism, rogue states, and ethnic conflicts. These studies share several elements: they are based primarily on an effort to examine the relevance of conditions necessary for successful deterrence, formulated in the context of the Cold War, and to a large degree are policy oriented, particularly regarding the challenges confronting the United States.[1] These same elements dominate the evolving debate on the connection between deterrence and cyber warfare.[2] Much of the research on deterrence strategy and cyber warfare is based on an American perspective. It examines the possibility of successfully implementing the strategy of deterrence in order to prevent cyber attacks, or analyzes the way the US can use cyber warfare in order to deter other threats it faces.[3]

These studies make it clear that the possibility of successful deterrence against cyber attacks is limited with regard to each of the dimensions required for its success: the existence of capability (weapons), the credibility of the threat, and the ability to convey the threatening message to the potential challenger.[4] Nonetheless, there are several elements to consider that under certain circumstances are likely to serve as the basis for successful deterrence even in the realm of cyberspace. This essay surveys the literature and proposes directions for continued research on the topic.

Dr. Amir Lupovici is a lecturer in the Department of Political Science at Tel Aviv University.

The essay begins by presenting the necessary conditions for a successful strategy of deterrence. It then reviews the central claims regarding the difficulties in applying successful deterrence in cyber warfare vis-à-vis each of these conditions. The third part discusses some benefits and shortcomings of certain factors that may strengthen deterrence against cyber warfare. Finally, it highlights the importance of continuing the discussion of deterrence and cyber warfare, indicating a number of directions for future research.

The Conditions for Successful Deterrence

There are different ways in which actors can try to prevent their enemies from taking undesirable action. The strategy of deterrence by punishment is one of the most studied. This type of deterrence has several definitions,[5] with the definition by George and Smoke, whereby deterrence is the ability to persuade a potential enemy that the price it will pay as the result of carrying out the undesirable action will outweigh any possible profit, is among the most commonly used.[6] This type of deterrence differs from deterrence by denial,[7] which is based on the attempt to persuade potential aggressors that they must avoid taking action because they will fail to attain their goals.[8] The concept of deterrence also differs from the concept of compellence, which is based on the use of threats in order to make an enemy undertake an action, whereas the aim of deterrence is to make the enemy avoid taking undesirable action.[9]

A central question regarding the strategy of deterrence by punishment concerns the conditions under which it is likely to be successful, i.e., cause a potential enemy to avoid challenging the defender. The research, developed mostly during the Cold War and dealing with deterrence between the superpowers, focuses on three central conditions: the defender's capabilities, the credibility of the threat, and relaying the threat message to the challenger.

The first essential condition for successful deterrence by punishment is that the defender be able to exact a price from the challenger. It is therefore not surprising that studies in deterrence arose in particular during the nuclear era, as this weapon allowed both sides to make the cost of a future war very clear. Nuclear weapons gave leaders a crystal ball of sorts, allowing them to see the effects of the next big war and thus encourage them to exert caution in their conduct.[10] At the same time, capabilities are

not limited to the non-conventional, as conventional means too may be used to take a toll on the challenger.[11] Moreover, an important part of the capabilities dimension is the means of delivery available to the defender, such as aircraft, missiles, and even roads and vehicles that may play a role in the element of capabilities within the context of deterrence.

A second condition for successful deterrence is the credibility of the threat. In order for the deterrence threat to be effective, the defender must be ready to use the capabilities at its disposal. Various researchers have presented a range of factors that may limit this willingness, e.g., internal or international public opinion, or even the deterrence capabilities of the enemy (the challenger).[12] Common to all these elements is that each in its own way raises the cost of taking action, thereby reducing the actor's credibility in terms of carrying out the threat, if necessary.[13]

The third condition is effective delivery of the messages to the challenger concerning the two previous conditions – capabilities and intentions. In other words, the challenger must be aware of the defender's capabilities and its willingness to use them. Researchers who have developed psychological approaches to deterrence claim that this condition is the most important of all, whereby the perceptions and misperceptions of decision makers directly affect the success of deterrence.[14] In this sense, what matters are neither the capabilities nor the intentions of the defender, rather how they are perceived by the potential challenger.

Finally, because the strategy of deterrence may prevent different types of threats, it is difficult to discuss the conditions for successful deterrence uniformly, as they must be adapted not only to the challenger but also to the type of action the defender is trying to prevent. So, for example, while nuclear weapons may be effective in deterrence against an all-out attack ("general deterrence"), its effectiveness would be lower against more limited types of threats.[15]

Difficulties of Deterrence in Cyber Warfare

Many of the studies analyzing the strategy of deterrence against cyber warfare are based on Cold War theories. Researchers analyzed the central conditions for successful deterrence discussed in the literature: defensive capabilities, the credibility of the threat, and communication, or the ability to transmit the message of capabilities and the credibility of the threat to the challenger. Most researchers believe that an analysis of these conditions

shows that the strategy of deterrence may be expected to fail when applied to threats created by cyber warfare.[16]

Capabilities

Cyber warfare allows weak players to move the confrontation into a sphere in which they can maximize profits while risking little – which makes deterrence harder to establish. In effect, an actor that is more technologically developed is also more susceptible to cyber warfare.[17] In fact, the possibility of retaliation against a weaker player is reduced, and thus the ability to establish a credible threat of deterrence is also lessened. For example, it is very difficult to deter players, especially individuals, who do not own information systems that can be threatened with damage.[18] This challenge also exists in the confrontation with nations with less developed information systems infrastructures, where the possibility of creating an effective threat by means of cyber warfare alone is limited.

Credibility

A second challenge to deterrence against cyber threats relates to the defender's credibility. The defender's vulnerability may limit its willingness to tap its capabilities out of concern that retaliation could lead to escalation. The problem for the defender is that such escalation is liable to be much more dangerous to itself than to the challenger, which in turn is likely to strengthen the challenger's belief that the defender's willingness to act is low.[19] This challenge is further amplified by the fact that cyber warfare entry costs are usually lower for the weaker side.[20] In other words, the cost to the challenger of engaging in cyber warfare is often limited, which further increases the difficulties in presenting and executing the deterrent threat required in order to prevent such action.

Internal as well as international public opinion may limit the credibility of the threat of retaliation because of the nature of cyber warfare. In situations in which it is difficult to establish the identity of the source of the attack,[21] the ability to employ a retaliatory measure likely to cause damage is constrained.[22] A potential challenger may view these constraints as undermining deterrence credibility. In this way a potential aggressor, assessing that the chances of the defender making good on its threats are low because of the damage it is likely to incur as a result, will be more willing to take risks and challenge the defender.

Conveying the Threat

A third problem stems from the defender's difficulty in conveying the message about its capabilities and about the credibility of its response to the challenger. Beyond the fundamental problems regarding each of the dimensions described above, challengers may be not only anonymous but even individuals who often have no identifiable physical address.[23] Libicki, for example, claims that to this day the source of the 2007 attack on the Estonian servers is in question: it is not at all certain that the attack was directed from above by the Russian government, as claimed by many who have analyzed the case.[24] The source of an attack can be another state entity, organizations or individuals operating from within the borders of another state, or organizations or individuals operating from within the targeted state. This situation reflects the frequent blurring between crime, terrorism, and warfare.

Moreover, when speaking of deterrence, it is necessary to identify the challenger in advance, before any challenge takes place, in order to target the deterrent threat. This is a key issue, because deterrence is based on the fact that the potential challenger is aware of the defender's capabilities and its willingness to use them ahead of time. However, if the defender is hard pressed to identify the source of the damage even after the attack, it will certainly find it difficult to do so prior to it. While intelligence capabilities may provide a partial solution, the threat that the defender can envision in most situations is general only, and is meant to cover a relatively broad range of potential challengers that the defender thinks would be likely to attack. However, deterrence is more effective when the threat – even if not completely explicit – is aimed at specific actors rather than at anonymous and undifferentiated sets of actors or types of actors liable to issue a challenge.[25]

Another difficulty directly related to the transmission of messages to the challenger involves the specific platform used.[26] This difficulty is amplified in light of the multiplicity of actors capable of creating threats. Unlike the Cold War era, when enemies were a limited number of known state entities with relatively clear capabilities, the number of possible aggressors has multiplied in the information age, lowering the possibility of presenting stable and credible deterrence.[27] The large number and variety of threats possible in cyber warfare creates an arena in which it is more complex to operate and in which it is not completely clear how or to whom to transmit the deterrent message.

Opportunities for Deterrence in Cyber Warfare

Despite these difficulties, the possibility of successful deterrence in cyber warfare exists, at least in part and under specific circumstances. For example, a number of researchers have stressed that retaliation need not be limited to cyberspace but may be effected by more traditional means. Thus, in the case of a state threatening to act by means of cyber warfare, the deterrent threat towards it may be based on the broadest range of capabilities the defending nation has at its disposal. Different threats, whether economic or military, may be effective in deterring a state enemy using cyber warfare against another state entity. Similarly, against threats posed by individuals or terrorist organizations seeking to use cyber warfare, states may, as proposed by a number of researchers (and also several decision makers), choose means of deterrence that do not require use of cyber capabilities. For example, they can employ threats through the judicial system (internal or international) and through internal security services, as well as use of traditional military threats.[28] As such, if actors assess that they will profit by diverting the confrontation into cyberspace, where they enjoy superiority, the actors under attack that might be attacked are under no obligation to limit the theater to cyberspace and may instead move the confrontation into theaters more convenient to them.

Another measure is deterrence by denial. The benefit inherent in this sort of strategy is that it may be based on defensive measures and thus not only be a means of preventing the enemy from acting but also providing a solution in case the challenger decides to act. Moreover, according to Morgan, making extensive use of various defensive measures may help identify the aggressor and strengthen the ability to take retaliatory action, which in turn strengthens deterrence by punishment.[29] Nonetheless, the challenges of using this strategy lie in overcoming problems similar to those linked to the successful use of deterrence by punishment. In both cases, the low entry cost required of challengers when they engage in cyber warfare remains a central difficulty.

Morgan also suggests that serial deterrence[30] may be useful in confronting cyber warfare threats: "Cyber attacks are very likely to turn out to be manageable primarily through applications of serial deterrence, repeated harmful responses over an extended period, to induce either temporary or eventually permanent suspensions of the most bothersome

attacks or of attacks by the most obnoxious opponents."[31] While this is an original way to confront threats in cyberspace and represents an interesting attempt to use existing concepts in an innovative way, it is not without difficulty. For example, it is unclear whether the enemy can be affected over time by repeated attempts, as these are liable to teach the challenger that the deterrence of the defender is not working (and that therefore the defender needs to engage in the same repetitive actions).[32]

Another problem regarding a strategy based on serial deterrence is exposing the capabilities of the defender. Although this problem is inherent in every form of deterrence in cyberspace (deterrence by punishment or denial), it is particularly acute when what is at issue is deterrence over time, as with the strategy of serial deterrence.[33] In such situations, exposing the offensive capabilities as the consequence of repeated attacks may serve as the basis for knowledge or inspiration for the challenger.[34] Morgan himself has referred to this issue and argues that revealing capabilities is liable not only to provide inspiration to enemies and motivation to attain similar capabilities but is also likely to allow enemies to prepare for a future threat, thereby damaging its measure of effectiveness.[35]

Directions for Further Research

While indeed some scholars have started to suggest new directions for research on deterrence in cyberspace, I would like to point to two main avenues through which cyber deterrence thinking can be further developed. First, research dealing with threats in cyberspace should be sharpened. It seems that there is a growing gap between practice and types of threats in the international arena, and the way in which research in this field examines the strategy of deterrence. This gap exists in other research dealing with deterrence, but it is particularly prominent in the realm of cyberspace, which includes many types of interaction between many different sorts of actors representing various kinds of threats. Therefore it is necessary to expand the discussion about the types of actors, the threats they create, and the ways and challenges of deterring each one. In addition, similar to the broader research relating to the strategy of deterrence, there is a tendency to focus on the deterrence of states against various types of players (e.g., terrorist organizations, rogue states),[36] while an important aspect not given sufficient attention is the deterrence of these actors against the states they seek to challenge. This aspect exists also in cyber warfare

and intensifies the problems of states that must now deal with a much more complex setting than in the past.

Moreover, research on cyber warfare tends to deal with more classical aspects of security, whereas the arena of threats is complex and varied.[37] For example, states are worried about the growing strength of economic players (such as Google) or ideological ones (e.g., individuals seeking to promote government reforms) using cyberspace. Irrespective of whether or not the existing definitions of cyber warfare include interactions with these actors, a considerable contribution could be made by analyzing these relations using theories of deterrence. The concept of the strategy of deterrence might be used, for instance, to study the interactions between Google and China with regard to the implied or direct threats presented by these players to one another in the context of search engine censorship. In this sense, dividing research on deterrence and cyber warfare according to different types of threats (e.g., internet war, cyber terror, cybercrime, cyberwar) and the actors operating them (states, individuals, economic institutions) may be not only more accurate and productive but may also identify the conditions for raising the chances of success of each actor's strategy of deterrence against its enemy.

The second theme that should be expanded is analysis of the traditional literature on the strategy of deterrence in critical and original ways. This has already been done in some of the essays published on the topic. However, it remains to analyze further concepts regarding deterrence strategy already discussed in the literature, such as immediate deterrence,[38] general deterrence, and extended deterrence,[39] and to try to understand the significance and relevance of applying these practices to cyberspace.

Similarly, the concept of ambiguity should be studied. This concept may serve as a framework for practical thinking in confronting the dilemma inherent in the need for revealing capabilities on the one hand,[40] balanced against the concern that the enemy will be able to exploit this exposure to increase its own strength and immunity to attack. Using insights developed in different contexts may provide an interesting foundation for developing ideas on cyberspace ambiguity, not only with regard to intention and willingness to make good on threats but generally with regard to the existence of capabilities. In this respect, it is possible, for example, to analyze the different efforts made by several nations in recent years in the field of cyber warfare. Not only are the means developed by nations

likely to strengthen their strategy of deterrence against these threats, but the very prominence of these efforts may also serve as a deterrent tool. The same is true of the American establishment of a strategic command to manage cyber warfare:[41] it has a range of objectives and functions, but its very reference and prominence allow not just improvements in capabilities but also demonstrate US willingness to invest resources in reducing threats and damage. It may be that stressing the desire to invest in measures of this sort and revealing the scope of the budgets, resources, and manpower dedicated to the subject – even absent a detailed breakdown of the measures acquired and their capabilities – can help increase the credibility of the deterrent message against threats in cyberspace, especially with regard to threats involving high levels of violence on the part of other nations. In other words, a partial revelation of capabilities while maintaining ambiguity about their essence allows for a reduction of the harmful effects described above but also transmits a forceful message. At the same time, one may expect that the low entry threshold for operating in cyberspace, especially in cases of asymmetrical confrontations, will continue to present a challenge to establishment of a strategy of deterrence seeking to prevent threats in this realm.

Conclusion

The research that deals with cyber warfare deterrence discusses primarily the difficulties inherent in deterring enemies from using this strategy. Although deterrence may work under certain circumstances, the problems associated with the defender's capabilities, the defender's willingness to use them, and the defender's ability to convey a message of deterrence to its potential enemy greatly limit the possibility of successful deterrence. Nonetheless, in light of the benefits inherent in the strategy of deterrence in reducing the scope of violence of conflicts, it is important to try to further the research dealing with the connections between deterrence and cyber warfare. This essay has indicated some directions for further thought and development of these ideas. However, as claimed by Morgan, these insights should be applied carefully, because additional empirical knowledge about the essence of cyber warfare is required, in terms of both the damage it can generate and the way in which it may be used.

Notes

1 Amir Lupovici, "The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda," *International Studies Quarterly* 54, no. 1 (2010): 705-32.

2 "Cyber warfare" refers here to a certain type of information warfare, though at times the concept of "information warfare" serves as a synonym for cyber warfare. This type of warfare is based on various attempts to prevent, disrupt, or destroy the enemy's information systems, while protecting the information systems of the defender against similar threats. See Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996): 93-107; Gary F. Wheatley and Richard E. Hayes, Infor*mation Warfare and Deterrence* (Washington, DC: National Defense University Press, 1996), pp. v-vi, 5-6; Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," *Parameters* 26, no. 3 (1996): 83, 86-90. For a review of central concepts in cyber warfare, see Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75-92.

3 On the general tendency of research dealing with cyber warfare and security to analyze policy oriented issues and to minimize the incorporation of broader theoretical dimensions, see Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27, no. 3 (2006): 221-44.

4 This essays use the common terms to describe the actors involved in deterrence strategy: the *defender* – the actor seeking to use the strategy of deterrence in order to prevent undesirable action against it, and the *challenger* – the actor seeking to act against the defender. The sometime usage of the alternative terms – the deterring actor or the deterred actor – is problematic because it assumes the success of the strategy.

5 For an excellent survey of definitions of the concept of deterrence by punishment, see Patrick M. Morgan, *Deterrence Now* (New York: Cambridge University Press, 2003), pp. 1-2.

6 Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), p. 11.

7 Deterrence by denial also differs from the strategy of defense. While there is an overlap, defense seeks to provide a solution to a situation in which the strategy of deterrence has failed, while deterrence by denial seeks to prevent the action by making the challenger understand that it lacks the capacity to execute the action because of the defender's capabilities.

8 Glenn Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 1961). Nevertheless, deterrence by punishment and deterrence by denial may in theory support one another. If a potential challenger is made to realize that not only are its chances for success low but it will also be

required to pay a steep price for aggression, there is a higher chance it will refrain from action.

9 Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966).

10 Albert Carnesale, Paul Doty, Stanley Hoffmann, Samuel P. Huntington, Joseph S. Nye, Jr., and Scott D. Sagan, *Living with Nuclear Weapons* (Cambridge: Harvard University Press, 1983).

11 For a discussion of conventional deterrence, see., e.g., John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983) and Jonathan Shimshoni, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca: Cornell University Press, 1988).

12 For example, it has been claimed that the development of international norms calling for the ban on nuclear weapons and international public opinion in support of this call have weakened the strategy of deterrence because they have raised the cost of their use of them. See T. V. Paul, "Nuclear Taboo and War Initiation in Regional Conflicts," *Journal of Conflict Resolution* 39, no. 4 (1995): 696-717.

13 Various researchers have debated the question of how to increase the credibility of the threat and have even proposed measures to attain this goal, e.g., by means of costly signals. See James Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88, no. 3 (1994): 577–92. Still, some researchers have cast doubt on the effectiveness of some of these measures. For a discussion of the topic, see, for example, Paul Huth, "Reputations and Deterrence: A Theoretical and Empirical Assessment," *Security Studies* 7, no. 1 (1997): 72-99.

14 Morgan, *Deterrence Now*, pp. 15-16.

15 For an excellent survey demonstrating the different types of Israeli deterrence, see Uri Bar-Joseph, "Variations on a Theme: The Conceptualization of Deterrence in Israeli Strategic Thinking," *Security Studies* 7, no. 3 (1998): 12-29.

16 Harknett, "Information Warfare and Deterrence"; Br*uce* D. Berkowitz, "Warfare in the Information Age," in John Arquilla and David F. Ronfeldt, eds., *Athena's Camp: Preparing for Conflict in the Information Ag*e (Santa Monica: RAND, 1997), pp. 183-84; Emily O. Goldman, "Introduction: Security in the Information Technology Age," in Emily O. Goldman, ed., *National Security in the Information Age* (London: Taylor & Francis, 2004), p. 3; John Arquilla. "Thinking about New Security Paradigms," in Emily O. Goldman, ed., *National Security in the Information Age* (New York: Routledge, 2004), pp. 210-13. Morgan reaches similar conclusions, claiming that the different elements affecting the practices of deterrence of the Cold War, based both on this strategy and on supportive measures such as arms control, are less relevant to deterrence in cyberspace, though he does not entirely rule out the possibility of using different types of deterrent strategies in confronting these threats. See Patrick M. Morgan, "Applicability

of Traditional Deterrence Concepts and Theory to the Cyber Realm," in John D. Steinbruner et al., eds., *Proceedings of a Workshop on Deterring Cyberspace* (Washington: National Academies Press, 2010), pp. 55-76. In light of the various limitations regarding the ability to establish deterrence against cyber warfare, it has been proposed – especially for the United States, which is the primary subject of the research – to take alternative measures, such as using defensive means. See Wheatley and Hayes, Infor*mation Warfare and Deterrence*, p. 9, and James Adams, "Virtual Defense," *Foreign Affairs* 80 (2001): 107-12.

17 Harknett, "Information Warfare and Deterrence"; Wheatley and Hayes, *Information Warfare and Deterrence*, p. 9; Berkowitz, "Warfare in the Information Age," pp. 183-84; Martin C. Libicki, *Conquest in Cyberspace* (Cambridge, Cambridge University Press, 2007), p. 272. On societies' vulnerability to electronic attacks, see Ron Deibert, "Circuits of Power: Security in the Internet Environment," in J. P. Singh and James N. Rosenau, eds., *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (NY: SUNY Press, 2002), p. 115. For sensitivity to threats – both external and internal – to information systems, see Martin C. Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica: RAND, 2009), www.rand.org/pubs/monographs/2009/RAND_MG877.pdf. At the same time, for Libicki the scope of threat created by cyber warfare in the present age is neither clear nor certain. According to Libicki, the issue of the scope of damage liable to be created by cyber warfare is a central question at the heart of the debate about the importance of the strategy of deterrence against this type of warfare (*Cyber Deterrence and Cyberwar*, p. 36). For similar reasons having to do with the paucity of available information and the newness of the subject, Morgan cautions against drawing hasty conclusions about the possibilities of deterrence against cyberspace threats, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," pp. 61-62.

18 Libicki, *Cyber Deterrence and Cyberwar*, p. 26.

19 Harknett, "Information Warfare and Deterrence," p. 104.

20 Molander, Riddile, and Wilson, "Strategic Information Warfare," p. 87.

21 For more on the difficulties in identifying the source of cyber warfare attacks, see also Libicki, *Cyber Deterrence and Cyberwar*, pp. 44-45.

22 For more on internal and international public opinion limiting the possibility of using force, thereby affecting the defender's deterrence, see., e.g., Robert Jervis, "Deterrence, Rogue States, and the Bush Administration," in T. V. Paul, Patrick Morgan, and James Wirtz, eds., *Complex Deterrence*: *Strategy in the Global Age* (Chicago: University of Chicago Press, 2009), p. 153.

23 Wheatley and Hayes, Infor*mation Warfare and Deterrence*, p. 9; Harknett, "Information Warfare and Deterrence," p. 104; Berkowitz, "Warfare in the Information Age," pp. 183-84; Anthony Cordesman and Justin Cordesman, *Cyberthreats, Information Warfare, and Critical Infrastructure Protection:*

Defending the US Homeland (Westport: Praeger, 2001), p. 7; and Arquilla, "Thinking about New Security Paradigms," pp. 210-11.

24 Libicki, *Cyber Deterrence and Cyberwar*, pp. 1-3.

25 The reason is that a deterring threat must be adapted to the type of threat and the type of element posing it. Therefore it is important to establish the deterrence in the context of the threat for the specific aggressor. For example, deterrence against a state actor enjoying sovereignty in a particular territory and possessing valuable target differs from a non-state actor and therefore requires the presentation of different types of threats. This issue has in recent years been at the center of an extensive debate in the context of tailored deterrence, particularly in the context of deterring terrorism. For a discussion of the concept, see Jeffrey S. Lantis, "Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice," *Contemporary Security Policy* 30, no. 3 (2009): 469-71. For a discussion of the concept vis-à-vis cyber warfare, see Richard L. Kugler, "Deterrence of Cyber Attacks," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), pp. 331-33, and Lantis, pp. 469-71.

26 Harknett, "Information Warfare and Deterrence," pp. 98-100.

27 Libicki, *Conquest in Cyberspace*, p. 272. For more on the effect of the Revolution in Military Affairs on deterrence and the ability to deter, see Morgan, *Deterrence Now*, pp. 219-24.

28 Hayes and Wheatley, Infor*mation Warfare and Deterrence*, pp. 13, 19-20; Kugler, "Deterrence of Cyber Attacks," p. 328; and in Cordesman and Cordesman, *Cyberthreats, Information Warfare, and Critical Infrastructure Protection* , p. 7.

29 Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," p. 59.

30 Doron Almog uses the similar concept of "cumulative deterrence" with regard to the way to deter terrorist threats not in the cyber arena. See Doron Almog, "Cumulative Deterrence and the War on Terrorism," *Parameters* 34, no. 4 (2004-2005): 4-19.

31 Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," p. 59.

32 Lupovici, "The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda," p. 722.

33 Thus, for example, a challenger is likely to learn about the defensive measures (or be inspired to attain such measures) on the basis of the means used by the actor trying to use deterrence by denial, thereby limiting the ability to deter effectively with this strategy.

34 Similar criticism was raised after the reports about the Stuxnet virus, which reportedly disrupted the systems of the Iranian reactor in Bushehr. The concern presented by a number of information security specialists was that this cyber attack would serve as inspiration not only for what can be

done using such warfare but also that some of the codes of the virus itself were revealed and could conceivably serve various actors in their attempts to damage sensitive infrastructures. See., e.g., "Experts Fear Hackers Can Launch Stuxnet-Like Attacks on Power Plants, Prison Gates," *The Globe and Mail,* October 24, 2011.

35 Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," p. 63.

36 For reference to this issue in the context of information warfare, see, e.g., Goldman, "Introduction: Security in the Information Technology Age," p. 3.

37 For a discussion of the range of these threats, see Tabansky, "Basic Concepts in Cyber Warfare," especially pp. 80, 86-88.

38 A basic distinction existing in the study of deterrence deals with the difference between general deterrence, based on the attempt to prevent the enemy from thinking at all about the possibility of attacking (e.g., as with nuclear deterrence), and immediate deterrence, touching on a situation in which an actor would like to take an action (e.g., move troops) and by using threats the defender dissuades the enemy from taking such action. An important discussion in this context could deal with the meaning of each of these types of deterrence in cyberspace.

39 Libicki, for example, has started to analyze extended deterrence in cyberspace. See Libicki, *Cyber Deterrence and Cyberwar*, pp. 104-6), and it is possible to develop the discussion of theoretical issues discussed in the literature with regard to extended deterrence. For a discussion of the concept of extended deterrence see., e.g., Paul Huth,, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press, 1988).

40 The literature about deterrence stresses that it is necessary to transmit the threat message to the enemy, including the price it will have to pay. Therefore messages about defensive capabilities or revealing capabilities have been noted as important elements in this context.

41 "U.S. Cyber Command Fact Sheet," *US Department of Defense*, May 25, 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf.