December 2011

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

STRATEGIC FORUM

National Defense University

Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?

by Vincent Manzo

About the Authors

Vincent Manzo is a Research Analyst in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.

Key Points

- Many weapons systems and most military operations require access to multiple domains. These linkages create vulnerabilities that actors can exploit by launching cross-domain attacks; the United States may seek to deter such attacks by threatening cross-domain responses. However, both the U.S. Government and potential adversaries lack a shared framework for analyzing how counterspace and cyber attacks fit into an accepted escalation ladder.
- The real-world effects of attacks that strike targets in space and cyberspace and affect capabilities and events in other domains should be the basis for assessing their implications and determining whether responses in different domains are proportionate or escalatory.
- Development of a shared framework that integrates actions in the emerging strategic domains of space and cyberspace with actions in traditional domains would give decisionmakers a better sense of which actions and responses are expected and accepted in real-world scenarios and which responses would be escalatory. This would support more coherent cross-domain contingency planning within the U.S. Government and deterrence threats that potential adversaries perceive as clearer and more credible.

> *In most real conflicts the potential escalation sequence is more like a ladder that has been bent and twisted out of shape with all sorts of extra and odd protuberances added on, which vitally affect how the conflict does or does not climb it. . . . Controlling escalation will depend crucially on identifying the particular twists and protuberances of that conflict's misshapen ladder.*[1]

Warfare has become even more complicated since Richard Smoke wrote this description of escalation in 1977. The *National Security Space Strategy* describes space as "congested, contested, and competitive," yet satellites underpin U.S. military and economic power. Activity in cyberspace has permeated every facet of human activity, including U.S. military operations, yet the prospects for effective cyber defenses are bleak. Many other actors depend on continued access to these domains, but not nearly as much as the United States.

For this reason, some analysts argue that China's opening salvo in a conflict with the United States would unfold in space and cyberspace. Worst-case scenario assessments conclude that such an attack might render the United States blind, deaf, and dumb almost exclusively through nonkinetic means, although it is unclear how effective attacks in the space and cyber domains would be in an actual military conflict. How do concepts such as escalation, deterrence, and proportionality apply in such a context? What "odd protuberances" would counterspace and cyber attacks create in an escalation ladder? What are the salient thresholds for cross-domain attacks? And what exactly does *cross-domain* mean? This paper explores these questions using the illustrative example of a hypothetical U.S.-China conflict because both countries

possess diverse strategic capabilities that span air, land, sea, space, and cyberspace.

Defining Cross-domain: Platforms or Effects?

Cross-domain is an ambiguous term. U.S. doctrine identifies land, air, and sea as domains. Recent U.S. national security policy and strategy documents recognize space and cyberspace as distinct domains as well.[2] Assuming that all five are strategic domains, there are at least two different ways an action could cross domains.

cross-domain attacks enable an actor to utilize its strengths and exploit an adversary's vulnerabilities

Cross-domain could be defined according to the platform from which an actor launches an attack and the platform on which the target resides. Destroying a satellite with a ground-launched antisatellite (ASAT) missile is a cross-domain attack, whereas destroying one with a co-orbital ASAT (for example, a maneuverable satellite) is not. Striking a surface ship with a conventional air-launched cruise missile is a cross-domain attack, whereas an attack on the same target with a sea-launched cruise missile (SLCM) is not. Defining *cross-domain* by platforms demonstrates that cross-domain operations are not new. Air attacks on naval forces, naval attacks on air forces, and attacks from both domains on ground forces are common in modern warfare. Indeed, in many instances, a cross-domain operation might simply be the most expedient option. As an example, a nation under attack by SLCMs might, for a variety of reasons, be able to attack the adversary's naval assets more quickly with aircraft than with submarines and surface ships.

This definition might be too simplistic. Most U.S. military forces on land, in the air, and at sea make use of cyber and space assets, and most complex missions integrate contributions from multiple domains. One could even argue that a precision conventional strike is a cross-domain attack, regardless of whether the attacking platform and target are in the same domain, if it utilizes satellites and computer networks. By the same reasoning, characterizing a cyber attack—as opposed to cyber exploitation—against U.S. military computer networks as single-domain is misleading. If successful, such an attack would have important cross-domain effects: it would undermine the air, ground, or naval forces that depend on the degraded computer networks. These indirect effects in other domains are often the primary purpose of cyber attacks.[3] The same logic applies to attacks with co-orbital ASATs; even if the platforms are in the same domain, the effects are cross-domain.

Thus, *cross-domain* can also be defined according to the effects of an operation. Under this approach, an attack is cross-domain if its intended consequences unfold in a different domain than its target. This definition illuminates that inter-domain relationships (our own and our adversary's) create strategic vulnerabilities.[4] For example, U.S. precision conventional strike operations depend on access to multiple domains. A potential adversary might be incapable of destroying U.S. aircraft or nuclear-powered cruise missile submarines, but it might be able to attack the space and cyber assets that enable these platforms to destroy targets. This appears to be the logic underlying China's interest in counterspace and cyber attacks: such attacks shift the conflict to domains where China's offensive forces have an advantage over U.S. defenses, thereby altering U.S. capabilities in domains (air and sea, for example) where China would otherwise be at a disadvantage.[5] This cross-domain approach would be ineffective if U.S. air, sea, and ground forces did not depend heavily upon space and cyber assets. Without this link, China would be unable to translate U.S. vulnerability in space and cyberspace into an operational impact in other domains. Cross-domain attacks thus enable an actor to best utilize its strengths and exploit an adversary's vulnerabilities in some instances. Reports that the United States considered launching a cyber attack at the start of North Atlantic Treaty Organization operations in Libya suggest that the U.S. military

also perceives cross-domain attacks as useful for exploiting adversary vulnerabilities.[6]

Cross-domain Operations and Deterrence

These definitions highlight the fact that military actors frequently cross domains. Indeed, U.S. military posture is inherently cross-domain: U.S. offensive and defensive weapons are distributed across air-, sea-, and ground-based platforms; space and cyber assets are ubiquitous in U.S. military operations and engender advantages in other domains; and it is highly unlikely that future U.S. conflicts will unfold exclusively within one domain. From this perspective, U.S. deterrence is inherently cross-domain too: when the United States threatens to respond to actions that endanger U.S. and allied interests, it threatens, albeit implicitly in most cases, cross-domain responses. The platforms the United States employs, the targets it attacks, and the effect of the attack might be in different domains and might differ from the domains utilized in and affected by the adversary's initial attack.

By the same logic, the United States traditionally deters attacks in general, without distinguishing between attacks that cross domains and those that do not. Naval attacks on naval forces are not inherently more or less dangerous than air attacks on naval forces. The United States attempts to deter both, and the means, target, and scale of the U.S. response to either would depend on the effects of the attack and U.S. objectives rather than the domains involved.

Thus, the United States deters attacks, regardless of whether the attacks cross domains, by threatening responses that will likely cross domains and differ from the initial attack. Given that cross-domain deterrence is neither new nor rare, the real question underlying recent interest in the topic is: How can the United States mitigate vulnerabilities that stem from its dependence on space and cyberspace? Both are offense-dominant domains where U.S. defenses are inadequate and policymakers are uncertain about how to credibly threaten to impose costs on aggressors and deny benefits of attacks. Although potential adversaries depend on space and cyberspace less than the United States does, this does not explain why threats to respond to counterspace and cyber attacks in other domains are considered less credible than cross-domain responses to air, land, or sea attacks.

Shared Framework for Assessing Proportionality and Escalation in Space and Cyberspace

A concept Thomas Schelling explored in *Arms and Influence* is a useful starting point for answering these questions. Schelling argued that deterrence threats are more comprehensible to potential adversaries, and thus more credible, if they are proportionate with and connected to the actions they are intended to deter:

countries lack a shared framework for interpreting how counterspace and cyber attacks fit into an escalation ladder

> *There is an idiom in this interaction, a tendency to keeps things in the same currency, to respond in the same language, to make the punishment fit the character of the crime. . . . It helps an opponent in understanding one's motive, and provides him a basis for judging what to expect as the consequences of his own actions . . . the direct connection between action and response helps to eliminate the possibility of sheer coincidence and makes one appear the consequence of the other.*[7]

Of course, such communication requires that countries interpret military actions and reprisals similarly—in other words, that they communicate through a shared idiom of action.

Schelling also acknowledged that breaking a pattern of behavior (that is, escalation) might be necessary in some circumstances "to catch an adversary off balance, to display unreliability and dare the adversary to respond in kind." Even then, however, a shared understanding of limits, norms, and expected responses creates a necessary

frame of reference by which actors distinguish between proportionate and escalatory behavior: "Breaking the rules is more dramatic, and communicates more about one's intent, precisely because it can be seen as a refusal to abide by rules."[8]

The idiom of military action was never as coherent, communicable, and universally recognized in reality as it is in Schelling's prose. Nevertheless, during the Cold War, there was a generally accepted escalation ladder from conventional to chemical and biological to nuclear weapons. Within a conventional conflict, there has been an understanding that escalation can occur by broadening the geographical area of fighting, expanding the targets attacked (for example, shifting from narrow military to broader societal targets), and increasing the intensity of violence (for example, using more bombs per sortie or shifting to more destructive conventional weapons). The salient thresholds differ in every conventional conflict.

Unfortunately, countries lack a shared framework for interpreting how counterspace and cyber attacks fit into an escalation ladder. Competition and vulnerability in space and cyberspace are new relative to land, air, and sea. Countries have less experience fighting wars in which space and cyberspace are part of the battlefield. Unlike conventional and nuclear weapons, experts are less certain about the precise effects of attacks in these domains.[9] For these reasons, a widely shared framework for judging how counterspace and cyber attacks correspond with interactions in other domains and, more broadly, with political relations between potential adversaries during peacetime, in crises, and in wars does not yet exist. Without one, decisionmakers will have difficulty distinguishing between proportional and escalatory attacks and reprisals that cross from traditional strategic domains into these newer ones and vice versa.

the absence of a shared framework undermines deterrence and increases the potential for miscalculation

The absence of a shared framework within the U.S. strategic community complicates effective cross-domain contingency planning. Developing coherent, effective, and usable options for responding to attacks in space and cyberspace requires that military planners in the different Services and combatant commands possess similar assumptions about cross-domain proportionality and escalation. For example, Principal Deputy Under Secretary of Defense for Policy James Miller testified that U.S. responses to counterspace attacks "could include necessary and proportional responses outside of the space domain."[10] Yet there are a variety of types of counterspace attacks and even more potential nonspace targets for U.S. reprisals. A common framework would help planners determine which "nonspace" responses best correspond with counterspace attacks of varying scope and severity.

The absence of a shared framework between the United States, allies, and potential adversaries undermines deterrence and increases the potential for miscalculation. Effective deterrence requires that U.S. officials influence potential adversaries' perceptions of the likely consequences of the actions the United States wishes to deter. The United States might threaten to respond to a particular type of attack in space or cyberspace by employing different capabilities against different targets in other domains. Such threats, however, are less likely to resonate as credible with potential adversaries if they do not understand U.S. assumptions about how domains are linked and why a particular response is a logical and proportional reaction to the initial attack.

As an example, imagine the United States threatened to respond to ASAT attacks on U.S. intelligence, surveillance, and reconnaissance (ISR) satellites with attacks against the adversary's air defense network. The logic underlying this policy is that the United States might employ ISR aircraft over the adversary's territory to compensate for the lost satellites. Attacks on the air defense network would be necessary to en-

sure that the aircraft could effectively penetrate the country's airspace. This policy is proportional because the United States is restoring its lost ISR capability, thereby denying the benefits of the ASAT attack. However, the U.S. response would be different from the adversary's attack. Instead of responding in space, the United States would attack targets on or around the adversary's homeland. To further complicate the situation, the United States might use conventional weapons to destroy the air defense network even if the initial ASAT attack was nonkinetic. Without a shared framework, potential adversaries might consider this deterrence threat illogical and therefore not credible. If deterrence failed, they might perceive such a U.S. response as arbitrary and escalatory. Even with a shared framework, they may still consider this response as escalatory, but they would also understand it to be a likely consequence of employing ASATs against the United States before authorizing an attack.

To be clear, a shared framework would not and could not prescribe set actions for every imaginable scenario. Rather, it would define a generic escalation ladder, a tacit or loosely defined code of conduct that would give decisionmakers a better sense of which actions and responses are expected and accepted in real-world scenarios and which would cross thresholds that escalate the situation. This would pave the way for more coherent cross-domain contingency planning within the U.S. Government and U.S. deterrence threats that potential adversaries perceive as clearer and more comprehensible and credible. The United States would also have a better understanding of the calculus of potential adversaries in their efforts to deter U.S. actions. Cultivating such a shared framework is a constructive goal for the future because deterrence, crisis management, and escalation control would be easier if different countries interpreted proportionality, connectedness, and escalation similarly. Engaging the U.S. strategic community in a thorough dialogue on these issues is the first step toward achieving this goal. Forming a deterrence working group of regionalists, functionalists, and legal experts might be a fruitful approach to starting this conversation.

What would be the basis for assessing counterspace and cyber attacks in a shared framework? Must responses to kinetic attacks also be kinetic to be proportional? Is a kinetic response to a nonkinetic attack always escalatory? Can a cyber attack be proportional to a cruise missile strike? How do officials compare attacks that strike targets in some domains and affect capabilities and events in other domains? Counterspace and cyber attacks can vary widely in intensity, from the equivalent of a tap on the shoulder to a fist in the face. Clearly, the mere act of extending the conflict into these domains is an insufficient metric for evaluating attacks and calibrating responses. Rather, the real-world effects of such attacks, both within the domain of the attack and in other domains, should determine whether they are escalatory and which responses would be appropriate.

Variables in a Shared Framework

Cultivating a shared framework between potential adversaries for assessing effects and formulating appropriate responses is difficult regardless of how many domains are involved. U.S. and foreign officials interpret events through different prisms. Cultural differences, contrasting strategic objectives, differences in force structure and doctrine, and differing strengths and vulnerabilities can cause decisionmakers in the United States and other countries to reach different conclusions about proportionality and escalation.[11] This challenge is not new, but the uncertainties in emerging strategic domains discussed in the previous paragraphs might exacerbate it.

Imagine that China interferes with U.S. satellites via nonkinetic means (laser-dazzling or jamming) during a military crisis that has yet to escalate into an armed conflict. The United States might attempt to undermine China's ability to attack U.S. satellites, perhaps by scrambling its space-tracking data through a cyber attack. One could argue that this response is proportional because it is limited to systems that China is already employing

against the United States and does not cross the kinetic threshold. On the other hand, one could argue that attacking in a new domain is escalatory, opening the door to reprisals and counterreprisals in cyberspace and other domains. Would Chinese officials distinguish between attacks on military computer networks and computer networks that support the regime's domestic security operations? If not, they might interpret this "proportional" response as an existential assault, especially if they believe that U.S. cyber attacks will cause collateral damage to computer networks other than the one targeted.

actions that are escalatory during crises might be proportionate in limited wars and underwhelming responses as the scope and intensity of a conflict increase

What if the initial Chinese ASAT attack is kinetic? Would U.S., allied, and Chinese officials perceive a nonkinetic response against China's space tracking capability as weak even if it succeeded in protecting U.S. satellites? On the other hand, would kinetic attacks on the ASAT weapons China is employing be proportional? Or would crossing the geographic threshold (assuming the targets are on mainland China) make this response escalatory? One could argue that a symmetrical response—a kinetic attack on a Chinese satellite—is proportional. However, if satellites play a smaller role in Chinese military operations, one could also argue that such a response is less than proportionate because it does not impose comparable operational costs on China.[12]

The balance between offense and defense in these domains will also influence perceptions of effects, escalation and proportionality, and optimal deterrence strategies. For example, if offense continues to dominate in space and cyberspace and potential adversaries want to attack U.S. assets in these domains precisely because they are the U.S. military's "soft underbelly," U.S. stakes in any conflict would grow exponentially after such attacks occur because the effects in other domains would be profound. As a result, U.S. officials might feel pressure to take preemptive action prior to such an attack, or they might take risks to quickly terminate a conflict and punish the adversary in its aftermath. The linkage between vulnerabilities in space and cyberspace and the effectiveness of U.S. capabilities in other domains that makes U.S. satellites and computer networks high-value targets also makes the threat of a strong reprisal more credible: it would be proportionate to the effects of the attack. Conveying this to potential adversaries would be a central component of a deterrence strategy. Emphasizing this link might even enhance the credibility of the U.S. commitment to retaliate.

Alternatively, the United States might become capable of denying adversaries the benefits of attacks in these domains through cyber defenses and substituting terrestrial assets for satellites. In this case, U.S. deterrence strategy would strive to convince potential adversaries that they cannot affect U.S. ground, air, naval, and nuclear forces by attacking satellites and computer networks. Such a message might make U.S. threats to respond offensively appear disproportionate and less credible, but this would be a worthwhile tradeoff if the United States developed a defensive advantage in space and cyberspace.

Decisionmakers will also perceive attacks in space and cyberspace differently depending on the context. Attacks on military satellites and computer networks might be expected and accepted once a conventional war has started. But similar attacks might trigger a conventional conflict if they occur prior to hostilities, when both countries want to prevent a crisis from escalating into a war but are concerned about being left blind, deaf, and dumb by a first strike in space and cyberspace. Proportionality and escalation are relative concepts: actions that are escalatory during crises might be proportionate in limited wars and underwhelming responses as the scope and intensity of a conflict increase.

A related issue is whether U.S. reactions to cyber exploitation during peacetime would affect deterrence in

crises. Though the technology and operations of cyber exploitation and cyber attacks are similar, the goals and effects are different: exploitation extracts information from computers and networks without authorization; attacks destroy, degrade, or alter them to achieve effects in other domains.[13] But news outlets frequently describe incidents of cyber exploitation against the U.S. Government as cyber attacks and evidence of an ongoing war in cyberspace.[14] Conflating these operations contributes to the impression that U.S. deterrence has already failed. Potential adversaries might conclude that U.S. threats to respond to cyber attacks in other domains lack credibility based on how the United States reacted to previous exploitation operations. This perception might affect how they calculate risks and benefits of cyber attacks in crises. How can U.S. officials publicly convey that cyber exploitation and attacks pose different threats and require different responses, especially given the overlap between the two? Emphasizing that the real-world effects of attacks and exploitation differ might be a first step toward establishing a threshold between the two. This message would reinforce that deterrence has not failed because the effects of exploitation in cyberspace have not yet warranted U.S. military responses in other domains. It clarifies the types of actions that the United States is attempting to deter.

Some strategists may conclude that proportionate counterspace and cyber responses are impossible because escalation control in these domains is too difficult. There are an "infinite number of scenarios that are neither indicative of a minor harassing incident of jamming nor strategic attack" in space and cyberspace.[15] Assessing the effects of such attacks and choosing appropriate responses amid the stress and confusion of a military crisis might be difficult. U.S. and foreign officials likely will have differing views about the severity of nonkinetic disruptions that defy easy categorization, and the obstacles to developing a common framework might be too formidable. Furthermore, the effects of sophisticated attacks on satellites and computer networks might be indiscriminate and too difficult to predict. In this case, a deterrence strategy could emphasize that limited counterspace and cyber attacks carry an intolerable risk of misperception, miscalculation, and unintended escalation. Evoking "threats that leave something to chance," U.S. officials could credibly argue that they are uncertain about what they would do because such attacks would involve "a process that is not entirely foreseen . . . reactions that are not fully predictable . . . decisions that are not wholly deliberate . . . events that are not fully under control."[16] Of course, expressing trepidation about unintended escalation could backfire. Adversaries may conclude that threatening such attacks would yield U.S. concessions.

Conclusion

Many weapons systems and most military operations require access to multiple domains (land, air, sea, space, and cyberspace). These linkages create vulnerabilities that actors can exploit by launching cross-domain attacks; the United States may seek to deter such attacks by threatening cross-domain responses. Yet both the U.S. Government and potential adversaries lack a shared framework for analyzing how concepts such as proportionality, escalation, credibility, and deterrence apply when capabilities in space and cyberspace not only enable operations in other domains but also are part of the battlefield. The real-world effects of attacks that strike targets in space and cyberspace and affect capabilities and events in other domains should be the basis for assessing their implications and determining whether responses in different domains are proportionate or escalatory.

Integrating actions in the emerging strategic domains of space and cyberspace with actions in traditional domains in a clear escalation ladder would be a first step toward more coherent cross-domain contingency planning within the U.S. Government. Communicating this framework to potential adversaries would contribute to more effective deterrence and crisis management.

Notes

[1] Richard Smoke, *War: Controlling Escalation* (Cambridge: Harvard University Press, 1977), 252.

[2] See Department of Defense (DOD), *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 33–34, 37–39;

The White House, *National Security Strategy* (Washington, DC: The White House, May 2010), 22; DOD, *National Security Space Strategy* (Washington, DC: DOD, January 2011); The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011); DOD, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: DOD, July 2011).

[3] A 2009 National Research Council report defined *cyber attacks* as deliberate actions that "alter, disrupt, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks," whereas cyber exploitation is extracting information from computer systems or networks without authorization. The report demonstrates that the intended effects of cyber attacks occur in other domains: "Direct or immediate effects are effects on the computer system or network attacked. Indirect or follow-on effects are effects on the systems and/or devices that the attacked computer system or network controls or interacts with, or on the people that use or rely on the attacked computer system or network. . . . the indirect effect is often the primary purpose of the attack." National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 80.

[4] For more on inter-domain relationships and vulnerability, see Mark E. Redden and Michael P. Hughes, *Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?* INSS Strategic Forum 259 (Washington, DC: National Defense University Press, October 2010).

[5] For a discussion of the role of space, counterspace, and cyber capabilities in China's military strategy, see David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, DC: National Defense University Press, 2011), chapter 3; James Dobbins, David C. Gompert, David A. Shlapak, and Andrew Scobell, *Conflict with China: Prospects, Consequences, and Strategies for Deterrence* (Santa Monica, CA: RAND, 2011), 5–7; Office of the Secretary of Defense, *Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2010* (Washington, DC: DOD, August 2010), 22–37; Jan Van Tol with Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, *AIRSEA Battle: A Point-of-Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), 17–47; Roger Cliff et al., *Entering the Dragon's Lair: Chinese Anti-Access Strategies and their Implications for the United States* (Santa Monica, CA: RAND, 2007), 51–60.

[6] For reports of U.S. debates about launching a cyber attack against Libya, see Eric Schmitt and Thomas Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, October 18, 2011, and Ellen Nakashima, "Pentagon Officials Had Weighed Cyberattack on Gaddafi's Air Defenses," *The Washington Post*, October 18, 2011.

[7] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 146–149.

[8] Ibid., 150–151.

[9] For a discussion of expert uncertainty surrounding intended and cascading effects of cyber attacks, see National Research Council, 121–128.

[10] James N. Miller, testimony for the House Armed Services Committee, Subcommittee on Strategic Forces, March 2, 2011.

[11] For a theoretical/historical study of the causes and implications of doctrinal differences in U.S.-China relations, see Christopher P. Twomey, *The Military Lens: Doctrinal Differences and Deterrence Failure in Sino-American Relations* (Ithaca: Cornell University Press, 2010).

[12] This example demonstrates that symmetrical and asymmetrical responses to attacks in space and cyberspace are not synonymous with proportionate and escalatory responses; however, since symmetrical responses attack the same type of target with the same type of weapon in the same domain as the initial attack, it likely would be easier for different countries to reach similar assessments about whether such responses are proportionate or escalatory. Assessing asymmetric responses against targets in the same domain as the initial attack—which might attack the same type of target with different types of weapons, different types of targets with the same type of weapon, or different types of targets with different types of weapons—might be more difficult. Assessing asymmetric responses against targets in different domains than the attack would likely be the most difficult because it requires a shared standard for determining equivalencies across domains.

[13] National Research Council, 149–152.

[14] For example, Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race," *Bloomberg Businessweek*, July 20, 2011.

[15] Susan J. Helms, "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain," *Air Force Space Command High Frontier* 7, no. 1 (November 2010), 14.

[16] Schelling, 95.

Acknowledgments

This Strategic Forum benefited greatly from discussions with and comments by Elaine Bunn and Phillip Saunders, from comments by peer reviewers CAPT Mark Redden and Col Michael Hughes, and feedback from a presentation for the Office of the Secretary of Defense for Policy.

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

The Center for Strategic Research within the Institute for National Strategic Studies provides advice to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and unified combatant commands through studies, reports, briefings, and memoranda. The center conducts directed research and analysis in the areas of strategic and regional studies and engages in independent and leading-edge research and analysis in related areas.

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

NDU Press

The Strategic Forum series presents original research by members of NDU as well as other scholars and specialists in national security affairs from the United States and abroad. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Defense Department or any other agency of the Federal Government. Visit NDU Press online at www.ndu.edu/press.

Nicholas Rostow
Director
Center for Strategic Research

Hans Binnendijk
Director
INSS

Phillip C. Saunders
Director of Studies
Center for Strategic Research