NRC Prize for Cyberdeterrence Scholarship

Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences
Policy and Global Affairs
National Research Council

March 11, 2010

In a world of increasing dependence on information technology, the prevention of cyberattacks on a nation's important computer and communications systems and networks is a problem that looms large. Given the demonstrated limitations of passive cybersecurity defense measures (that is, measures taken unilaterally by an organization to increase the resistance of an information technology system or network to attack), it is natural to consider the possibility that deterrence might play a useful role in preventing cyberattacks against the United States and its vital interests.

At the request of the Office of the Director of National Intelligence, the National Research Council (NRC) is undertaking a project entitled "Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy." The project is aimed at fostering a broad, multidisciplinary examination of strategies for deterring cyberattacks on the United States and the possible utility of these strategies for the U.S. government. As part of this project, the responsible committee is issuing a call for papers that address questions relevant to this broad topic.

To stimulate work in this area, the NRC is offering one or more monetary prizes for excellent contributed papers that address one or more of the questions of interest described in the section below entitled "Questions of Interest" in this call for papers.

The NRC strongly encourages prospective authors of such papers to submit a paper abstract of 500 words or less by April 1, 2010. If the NRC deems the abstract to be of sufficient quality, the author may be invited to submit a first draft paper by May 21, 2010. Based primarily on its evaluation of the draft paper, an author may be invited to participate in a workshop on June 10-11, 2010 in Washington DC to discuss his or her paper. (In some cases, some amount of travel support for the workshop may be available, but the NRC cannot guarantee that all workshop invitees will receive such support.) After June 11, 2010 and whether or not the author has attended the workshop, the author should revise the paper as appropriate and provide a final draft by July 9, 2010.

Authors not wishing to submit abstracts and intermediate drafts must submit their final draft by July 9, 2010.

Any paper submitted by July 9, 2010—whether or not an abstract or a first draft was submitted earlier and whether or not the author was present at the workshop—will be eligible for prize consideration. In accordance with the recommendations of the cognizant committee, the National Research Council reserves the right to award zero, one, or more prizes for contributed papers. Winners (if any) will be notified by July 23, 2010; however, the award of a prize or prizes is contingent on the paper's successful passage through the NRC review process, in which authors of papers are expected to modify their papers in accordance with a peer review process that will take place after submission.

An individual prize is $1000, and prizes will be awarded to papers rather than to individual authors (that is, a group of authors awarded a prize will share the prize). Prize-winning papers will be published by the National Research Council in the fall of 2010.

The National Research Council reserves the right to make all decisions regarding acceptance or publication of submitted material, and its decisions are final.

Prospective authors may find useful background in the NRC report entitled *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* available at http://www.anagram.com/berson/absnrcoiw.html in PDF and http://www.nap.edu/catalog.php?record_id=12651 in hard copy. Also, the site located at http://sites.nationalacademies.org/CSTB/CurrentProjects/CSTB_054995 is expected to host an additional relevant report by March 31, 2010.

Paper requirements

All versions of a paper (that is, drafts and final submissions) must be between 4,500 and 7,500 words in length, and conform to the style guide (URL below). In addition, the final submission of a paper must be accompanied by a signed release form (URL below) certifying that:

(a) the submitted paper is original to the author(s); and
(b) the submitted paper is previously unpublished.

In the event that any given paper is not published by the NRC, all rights to the paper will revert to the author(s).

Style guide:
http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_056220.pdf

Release form:
http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_056221.pdf

The Cognizant Committee

The committee roster and biographies of committee members can be found at http://www8.nationalacademies.org/cp/committeeview.aspx?key=49157.

Information About the National Research Council

The National Research Council (NRC) functions under the auspices of the National Academy of Sciences (NAS), the National Academy of Engineering (NAE), and the Institute of Medicine (IOM). The NAS, NAE, IOM, and NRC are part of a private, nonprofit institution that provides science, technology and health policy advice under a congressional charter signed by President Abraham Lincoln that was originally granted to the NAS in 1863. Under this charter, the NRC was established in 1916, the NAE in 1964, and the IOM in 1970. The four organizations are collectively referred to as the National Academies.

The mission of the NRC is to improve government decision making and public policy, increase public education and understanding, and promote the acquisition and dissemination of knowledge in matters involving science, engineering, technology, and health. The institution works to inform policies and actions that have the power to improve the lives of people in the United States and around the world.

Questions of Interest

The broad themes described below (lettered A-H) are intended to constitute a broad forward-looking research agenda on cyberdeterrence. Within each theme are a number of elaborating questions that are illustrative of those that the committee believes would benefit from greater exploration and analysis. Thoughtful research and analysis in these areas would contribute significantly to understanding the nature of cyberdeterrence.

A. Theoretical Models for Cyberdeterrence

1. Is there a model that might appropriately describe the strategies of state actors acting in an adversarial manner in cyberspace? Is there an equilibrium state that does not result in cyber conflict?

2. How will any such deterrence strategy be affected by mercenary cyber armies for hire and/or patriotic hackers?

3. How does massive reciprocal uncertainty about the offensive cyberattack capabilities of the different actors affect the prospect of effective deterrence?

4. How might adversaries react technologically and doctrinally to actual and anticipated U.S. policy decisions intended to strengthen cyberdeterrence?

5. What are the strengths and limitations of applying traditional deterrence theory to cyber conflict?

6. What lessons and strategic concepts from nuclear deterrence are applicable and relevant to cyberdeterrence?

7. How could mechanisms such as mutual dependencies (e.g., attacks that cause actual harm to the attacker as well as to the attacked) and counterproductivity (e.g., attacks that have negative political consequences against the attacker) be used to strengthen deterrence? How might a comprehensive deterrence strategy balance the use of these mechanisms with the use of traditional mechanisms such as retaliation and passive defense?

B. Cyberdeterrence and Declaratory Policy

8. What should be the content of a declaratory policy regarding cyberintrusions (that is, cyberattacks and cyberintrusions) conducted against the United States? Regarding cyberintrusions conducted by the United States? What are the advantages and disadvantages of having an explicit declaratory policy? What purposes would a declaratory policy serve?

9. What longer-term ramifications accompany the status quo of strategic ambiguity and lack of declaratory policy?

10. What is the appropriate balance between publicizing U.S. efforts to develop cyber capabilities in order to discourage/deter attackers and keeping them secret in order to make it harder for others to foil them?

11. What is the minimum amount and type of knowledge that must be made publicly available regarding U.S. government cyberattack capabilities for any deterrence policy to be effective?

12. To the extent that a declaratory policy states what the United States will not do, what offensive operational capabilities should the United States be willing to give up in order to secure international cooperation? How and to what extent, if at all, does the answer vary by potential target (e.g., large nation-state, small nation-state, subnational group, and so on)?

13. What declaratory policy might help manage perceptions and effectively deter cyberattack?

C. Operational Considerations in Cyberdeterrence

14. On what basis can a government determine whether a given unfriendly cyber action is an attack or an exploitation? What is the significance of mistaking an attack for an exploitation or vice versa?

15. How can uncertainty and limited information about an attacker’s identity (i.e., attribution), and about the scope and nature of the attack, be managed to permit policy makers to act appropriately in the event of a

national crisis? How can overconfidence or excessive needs for certainty be avoided during a cyber crisis?

16. How and to what extent, if at all, should clear declaratory thresholds be established to delineate the seriousness of a cyberattack? What are the advantages and disadvantages of such clear thresholds?

17. What are the tradeoffs in the efficacy of deterrence if the victim of an attack takes significant time to measure the damage, consult, review options, and most importantly to increase the confidence that attribution of the responsible party is performed correctly?

18. How might international interdependencies affect the willingness of nations to conduct certain kinds of cyberattack on other nations? How can blowback be exploited as an explicit and deliberate component of a cyberdeterrence strategy? How can the relevant feedback loops be made obvious to a potential attacker?

19. What considerations determine the appropriate mode(s) of response (cyber, political, economic, traditional military) to any given cyberattack that calls for a response?

20. How should an ostensibly neutral nation be treated if cyberattacks emanate from its territory and that nation is unable or unwilling to stop those attacks?

21. Numerous cyberattacks on us and our allies have already occurred, most at a relatively low level of significance. To what extent has the lack of a public offensive response undermined the credibility of any future U.S. deterrence policy regarding cyberattack? How might credibility be enhanced?

22. How and to what extent, if at all, must the United States be willing to make public its evidence regarding the identity of a cyberattacker if it chooses to respond aggressively?

23. What is the appropriate level of government to make decisions regarding the execution of any particular declaratory or operational policy regarding cyberdeterrence? How, if at all, should this level change depending on the nature of the decision involved?

24. How might cyber operations and capabilities contribute to national military operations at the strategic and tactical levels, particularly in conjunction with other capabilities (e.g., cyberattacks aimed at disabling an opponent's defensive systems might be part of a larger operation), and how might offensive cyber capabilities contribute the deterrence of conflict more generally?

25. How should operational policy regarding cyberattack be structured to ensure compliance with the laws of armed conflict?

26. How might possible international interdependencies be highlighted and made apparent to potential nation-state attackers?

27. What can be learned from case studies of the operational history of previous cyberintrusions? What are the lessons learned for future conflicts and crises?

28. Technical limitations on attribution are often thought to be the central impediment in holding hostile cyber actors accountable for their actions. How and to what extent would a technology infrastructure designed to support high-confidence attribution contribute to the deterrence of cyberattack and cyberexploitation, make the success of such operations less likely, lower the severity of the impact of an attack or exploitation, and ease reconstitution and recover after an attack? What are the technical and nontechnical barriers to attributing cyberintrusions? How might these barriers be overcome or addressed in the future?

D. Regimes of Reciprocal/Consensual Limitations

29. What regimes of mutual self-restraint might help to establish cyberdeterrence (where regimes are understood to include bilateral or multilateral hard-law treaties, soft-law mechanisms [agreements short of treaty status that do not require ratification], and international organizations such as the International Telecommunications Union, the United Nations, the Internet Engineering Task Force, the Internet Corporation for Assigned Names and Numbers, and so on)? Given the difficulty of ascertaining the intent of a given cyber action (e.g., attack or exploitation) and the scope and extent of any given actor's cyber capabilities, what is the role of verification in any such regime? What sort of verification measures are possible where agreements regarding cyberattack are concerned?

30. What sort of international norms of behavior might be established among like-minded nations collectively that can help establish cyberdeterrence? What sort of self-restraint might the United States have to commit to in order to elicit self-restraint from others? What might be the impact of such self-restraint on U.S. strategies for cyber conflict? How can a "cyberattack taboo" be developed (perhaps analogous to taboos against the use of biological or nuclear weapons)?

31. How and to what extent, if any, can the potency of passive defense be meaningfully enhanced by establishing supportive agreements and operating norms?

32. How might confidence-building and stability measures (analogous to hotline communications in possible nuclear conflict) contribute to lowering the probability of crises leading to actual conflict?

33. How might agreements regarding nonmilitary dimensions of cyberintrusion support national security goals?

34. How and to what extent, if at all, should the United States be willing to declare some aspects of cyberintrusion off limits to itself? What are the tradeoffs involved in foreswearing offensive operations, either unilaterally or as part of a multilateral (or bilateral) regime?

35. What is an act of war in cyberspace? Under what circumstances can or should a cyberattack be regarded as an act of war?[1] How and to what extent do unique aspects of the cyber realm, such as reversibility of damage done during an attack and the difficulty of attribution, affect this understanding?

36. How and to what extent, if any does the Convention on Cyber Crime (http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm) provide a model or a foundation for reaching further international agreements that would help to establish cyberdeterrence?

37. How might international and national law best address the issue of patriotic hackers or cyber patriots, recognizing that the actions of such parties may greatly complicate the efforts of governments to manage cyber conflict?

E. Cyberdeterrence in a Larger Context

38. How and to what extent, if at all, is an effective international legal regime for dealing with cyber crime a necessary component of a cyberdeterrence strategy?

39. How and to what extent, if at all, is deterrence applicable to cyberattacks on private companies (especially those that manage U.S. critical infrastructure)?

40. How should a U.S. cyberdeterrence strategy relate to broader U.S. national security interests and strategy?

F. The Dynamics of Action/Reaction

[1] The term “act of war” is a colloquial term that does not have a precise international legal definition. The relevant terms from the UN Charter are “use of force,” “threat of force,” and “armed attack,” although it must be recognized that there are no internationally agreed-upon formal definitions for these terms either.

41. What is the likely impact of U.S. actions and policy regarding the acquisition and use of its own cyberattack capabilities on the courses of action of potential adversaries?

42. How and to what extent, if at all, do efforts to mobilize the United States to adopt a stronger cyberdefensive posture prompt potential adversaries to believe that cyberattack against the United States is a viable and effective means of causing damage?

G. Escalation Dynamics

43. How might conflict in cyberspace escalate from an initial attack? Once cyber conflict has broken out, how can further escalation be deterred?

44. What is the relationship between the onset of cyber conflict and the onset of kinetic conflict?

45. What safeguards can be constructed against catalytic cyberattack? Can the United States help others with such safeguards?

H. Collateral Issues

46. How and to what extent do economics and law (and regulation) affect efforts to enhance cybersecurity in the private sector? What are the pros and cons of possible solution elements that may involve (among other things) regulation, liability, and standards-setting that could help to change the existing calculus regarding investment strategies and approaches to improve cybersecurity? Analogies from other "protection of the commons" problem domains (e.g., environmental protection) may be helpful.

47. What are the civil liberties implications (e.g., for privacy and free expression) of policy and technical changes aimed at preventing cyberattacks, such as systems of stronger identity management for critical infrastructure? What are the tradeoffs from a U.S. perspective? How would other countries see these tradeoffs?

48. How can the development and execution of a cyberdeterrence policy be coordinated across every element of the executive branch and with Congress? How should the U.S. government be organized to respond to cyber threats? What organizational or procedural changes should be considered, if any? What roles should the new DOD Cyber Command play? How will the DOD and the intelligence community work together in accordance with existing authorities? What new authorities would be needed for effective cooperation?

49. How and to what extent, if any, do private entities (e.g., organized crime, terrorist groups) with significant cyberintrusion capabilities affect any

government policy regarding cyberdeterrence? Private entities acting outside government control and private entities acting with at least tacit government approval or support should both be considered.

50. How and to what extent are current legal authorities to conduct cyber operations (attack and exploitation) confused and uncertain? What standards should govern whether or not a given cyber operation takes place? How does today's uncertainty about authority affect the nation's ability to execute any given policy on cyberdeterrence?

Research contributions in these areas will provide greater value if they can provide concrete analyses of the offensive actors (states, criminal organizations, patriotic hackers, terrorists, and so on), motivations (national security, financial, terrorism), actor capacities and resources, and which targets require protection beyond that afforded by passive defenses and law enforcement (e.g., military and intelligence assets, critical infrastructure, and so on).