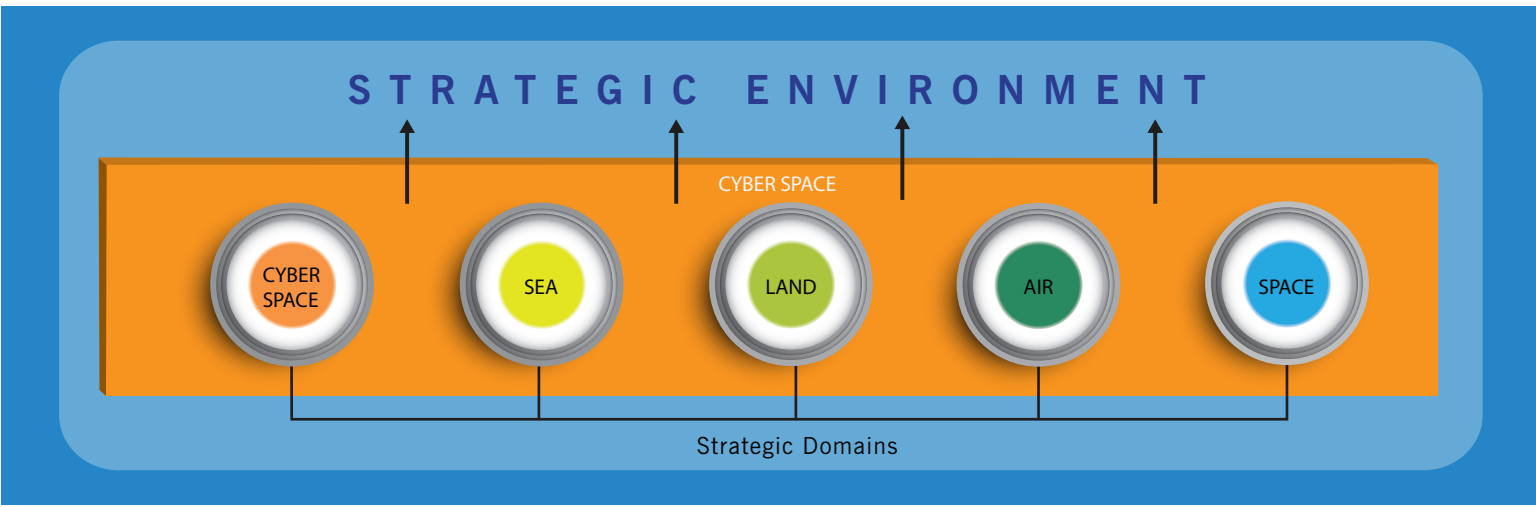
IBM Center for
The Business of Government

Strengthening
Cybersecurity Series

Defining a Framework for Decision Making in Cyberspace



Dighton Fiddner
Indiana University of Pennsylvania

Strengthening Cybersecurity Series 2015

Defining a Framework for Decision Making in Cyberspace

Dighton Fiddner
Indiana University of Pennsylvania

IBM Center for
The Business of Government

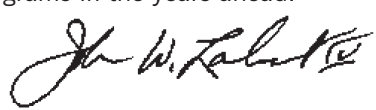
On behalf of the IBM Center for The Business of Government, we are pleased to present this report, *Designing a Framework for Decision Making in Cyberspace,* by Dighton Fiddner, Indiana University of Pennsylvania.

This report is the product of a group of experts, which was convened by the Department of Computer Science at the Indiana University of Pennsylvania (IUP). IUP brought together an interdisciplinary panel of experts in national security, international relations, foreign policy, information system network and security, public policy, and computer science. These experts participated in two collaborative roundtable meetings during the first six months of 2014.

The results of the roundtable discussions, as well as other research conducted by the author, are presented in this report. The report makes a series of recommendations for leaders to consider in developing a greater understanding of cyberspace, including the value of a broad and commonly accepted definition to help guide management actions in cyberspace. The panel of experts found that a better definition of cyberspace was needed, as well as an increased understanding of the concept of "strategic domains."

Recent events demonstrate that global cyber activity is becoming ever-more prevalent as an issue for governments to address. Accordingly, we hope that cyberspace decision makers will find this report to be helpful as they manage and make decisions about cyberspace programs in the years ahead.

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com



John Lainhart
Partner for Cybersecurity
IBM Global Business Services
john.w.lainhart@us.ibm.com

ABOUT THE RESEARCH PROJECT

This report is intended to provide cyberspace decision makers with a more comprehensive, clearer description of cyberspace, which they can use to manage and make decisions about cyberspace programs to improve government's effectiveness in this critically important area. The report offers an assessment and recommendations focused on the unique characteristics of cyberspace, which were initially designed without much focus on security or risk management. Improving the definition of cyberspace will improve current understanding of how to address cyber issues strategically, as well as how, when, and what tools decision makers should use to respond to cyber events.

The Computer Science Department at Indiana University of Pennsylvania (IUP) initiated this project with the support of the IBM Center for the Business of Government. The project brought together an interdisciplinary panel of experts in national security, international relations, U.S. foreign policy, information system network and security, public policy, and computer science. They were asked to apply their individual and collective expertise to develop an integrated understanding of strategic decision making for cyberspace activities. (For a list of roundtable participants, see the Appendix.)

The panel of experts met in two collaborative roundtable meetings, during which participants deliberated on a series of questions to frame and inform the issue. The second roundtable's questions were derived from and informed by the findings of first panel's deliberations. This allowed the researchers to further the goal of defining, describing, and explaining problems that hinder successful management in cyberspace, now that cyberspace is an integral part of the security environment.

Each roundtable was videotaped for reference, archival purposes, and possible future use as edited, digital instructional material.

The report summarizes the roundtables and adds context based on the roundtable participants' experience and research into cyberspace. The following sections present:

- A general discussion of the need to define cyberspace as a tool to help government manage cyber activity more effectively, both directly and across traditional strategic domains of land, sea, air, and space.
- A taxonomy of the range of cyber threats for which effective responses can be framed, using context created by the definition of cyberspace and determining consideration of cyberspace as a separate strategic domain.
- A set of recommendations for government to consider in deciding whether to adopt the proposed definition and implement an effective framework that can help frame cyberspace management in a security context.

GOALS OF THE RESEARCH PROJECT

First, roundtable participants wrestled with the lack of an accepted definition of cyberspace. This stems, in part, from how the perspectives of "technologists," who focus on the hardware that operates the systems, differs from those of "information scientists," who focus on both information and software. Cyberspace decision making and strategy transcend the technical realm and incorporate multiple conditions, as do other national and enterprise security issues, necessitating solutions that extend beyond a purely technical environment. Therefore, roundtable discussions addressed multiple dimensions of cyberspace, including individuals, organizations, and interrelated physical and cognitive components that involve information collection, processing, dissemination, or action.

The roundtables next addressed the notion of cyberspace as a strategic domain (see definition below). Traditionally, strategic domains have been divided into four categories: land, air, sea, and space. The participants concluded that cyberspace is best defined as a fifth, separate, and independent strategic domain that is structured and operates differently than the other four traditional domains. But

participants also acknowledged that cyberspace encompasses the other four strategic domains and, as such, can have a direct causal and catalytic effect on activity that occurs within them. In addressing cyberspace's impact for government, decision makers across all dimensions must understand both specific risks and threats within the cyberspace domain and its relationship to the broader strategic environment.

In taking this approach to devising a definition for cyberspace, roundtable participants had to address the lack of a definition for "strategic domain." The researchers referred to strategic domain as a sphere of activity, concern, or function.[1] Strategists have traditionally found that an activity, concern, or function could occur in four separate, independent domains (land, sea, air, and space). Based on the assessment that cyberspace provides a fifth domain in which an activity, concern, or function can occur, roundtable participants defined cyberspace as:

> A man-made global strategic domain, dimension of national power, and instrument of the dimension of national power within the information environment, consisting of the interdependent network of information technology infrastructures and resident data—including the Internet, telecommunications networks, computer systems, and embedded processors and controllers—for the production and use of information by individuals and organizations.

1. The author thanks Colonel Matthew C. Molineux, USAF. director, Aerospace Studies and the Eisenhower Series College Program, U.S. Army War College, for his diligent research to identify the lack of a definition and work to provide the one used here.

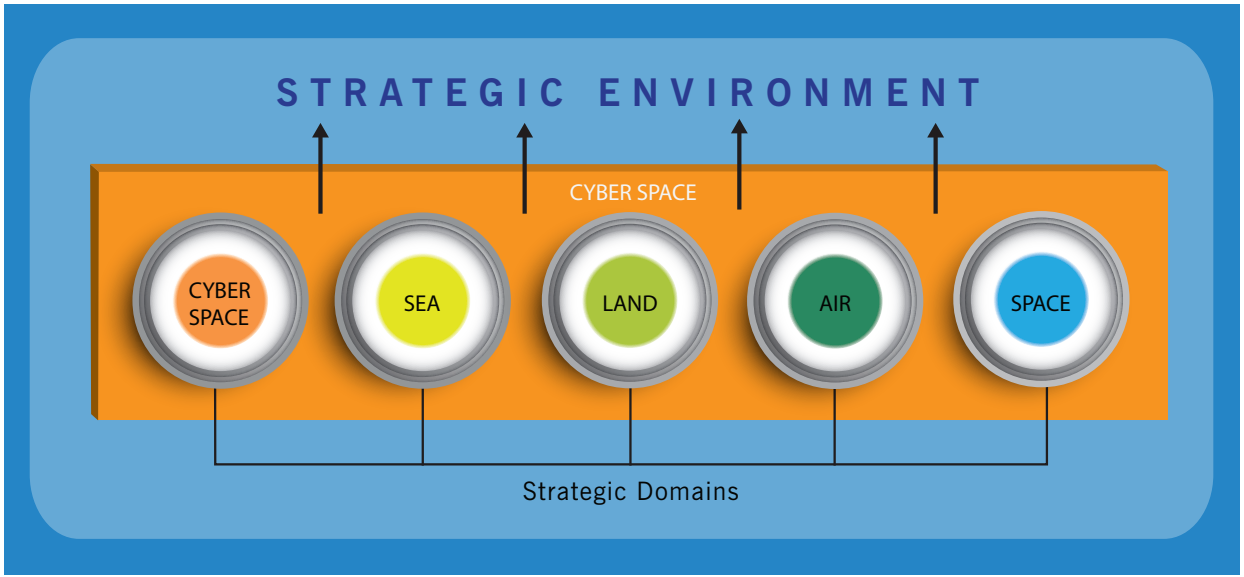
Cyberspace, like the other four domains, can independently serve as the locus of activity, concern, or function, and each could trigger an activity, concern, or function in the other domains. Figure 1 presents the five strategic domains.

In addition, cyberspace as a strategic domain has three unique properties:

- Has no physical boundaries, which means cyberspace permeates the entire strategic environment
- Occupies the same space as the other four domains
- Can generate activity as a dimension and instrument of national power. This means that actions in cyberspace can:
  - Occur solely in the cyberspace domain
  - Move to one or more of the other traditional domains
  - Simultaneously affect activity in one or more of the other domains, either through human activity or through automation

Unlike the air, sea, land, or space strategic domains, cyberspace is not geographically constrained. Much like the space strategic domain, cyberspace is a global common good; no one country controls space, but instruments of national power can exist within the domain. In addition, unlike the other strategic domains, cyberspace simultaneously occupies the space of the other strategic domains, such that cyberspace can be part of the others' extent. As a result, activity within cyberspace can have a direct causal and catalytic effect on activity in the other strategic domains. It is an *uber* strategic domain that can involve the other four domains.

Figure 1: Strategic Domains



Note: Cyberspace is a separate, independent domain that permeates the entire strategic environment and also encompasses the other strategic domains.

Cyberspace also brings together cyber and physical spheres of activity. The threat vector and the response in cyberspace could come from either the cyber or physical sphere. This has tremendous implications that impact how government manages and makes decisions involving cyberspace.

As mentioned above, the roundtables also found that cyberspace shares the characteristics of both a dimension and instrument of national power. As a **dimension** of national power, a nation can leverage cyberspace as it does any other strategic dimension, using it to persuade, entice, coerce, deter, or compel an entity to act in a certain fashion. As an **instrument** of national power, cyberspace includes key components, such as:

- Interdependent networks of information technology infrastructures and resident data, including the Internet
- Telecommunications networks
- Computer systems, especially software[2]
- Embedded processors and controllers[3]

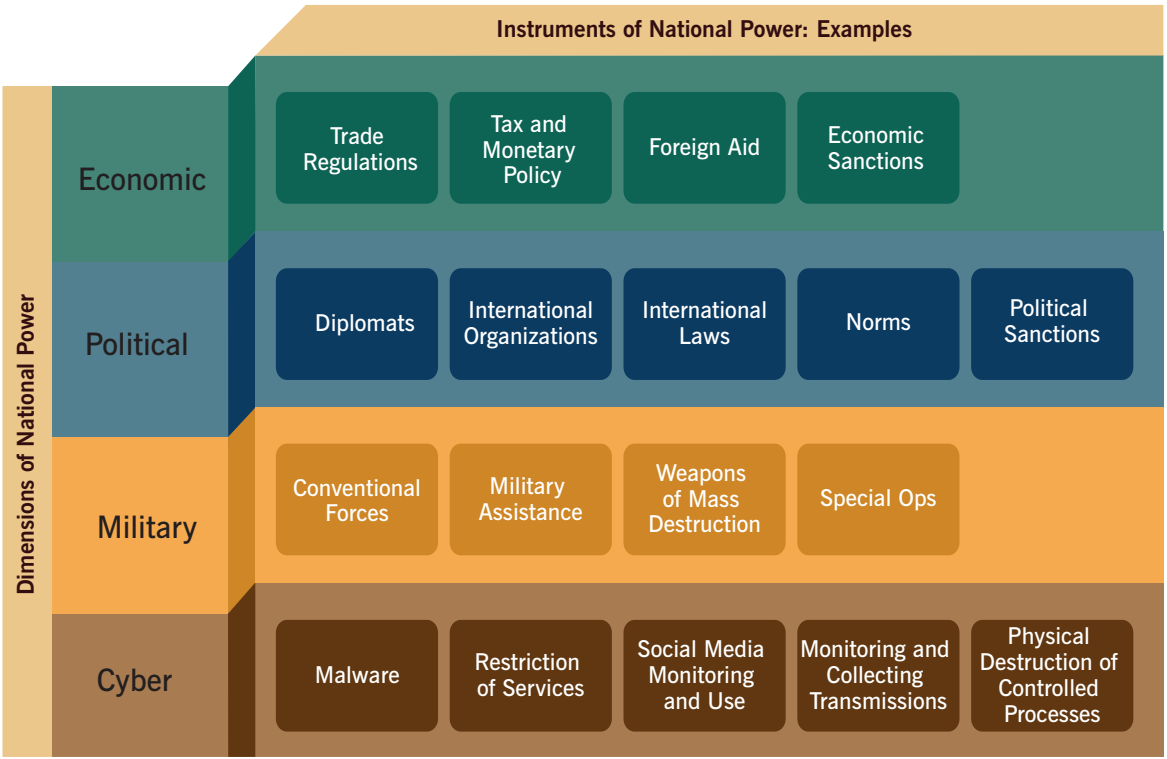
This conceptualization of cyber instruments is analogous to examples of the other dimensions of national power displayed in the chart below. Figure 2 presents the four dimensions of national power and provides examples of each.

Because cyberspace is man-made and already in place, government decision makers must work within the existing cyber environment. This is of concern because certain properties or characteristics of cyberspace were deliberately designed without a specific focus on security or risk management. These properties include its network topography, which inherently introduces risk into cyber activities. This reinforces the need for a commonly accepted framework that defines cyberspace, so that risks can be addressed within a relevant context.

2. Computers (or software) are automatically now constructing malware independently without intervention by humans (National Public Radio 2013).

3. U.S. Joint Pub 3-13 – Information Operations considers cyberspace one of 14 different information-related capabilities (instruments of national power) that contribute to information operations.

Figure 2: Dimensions and Instruments of National Power



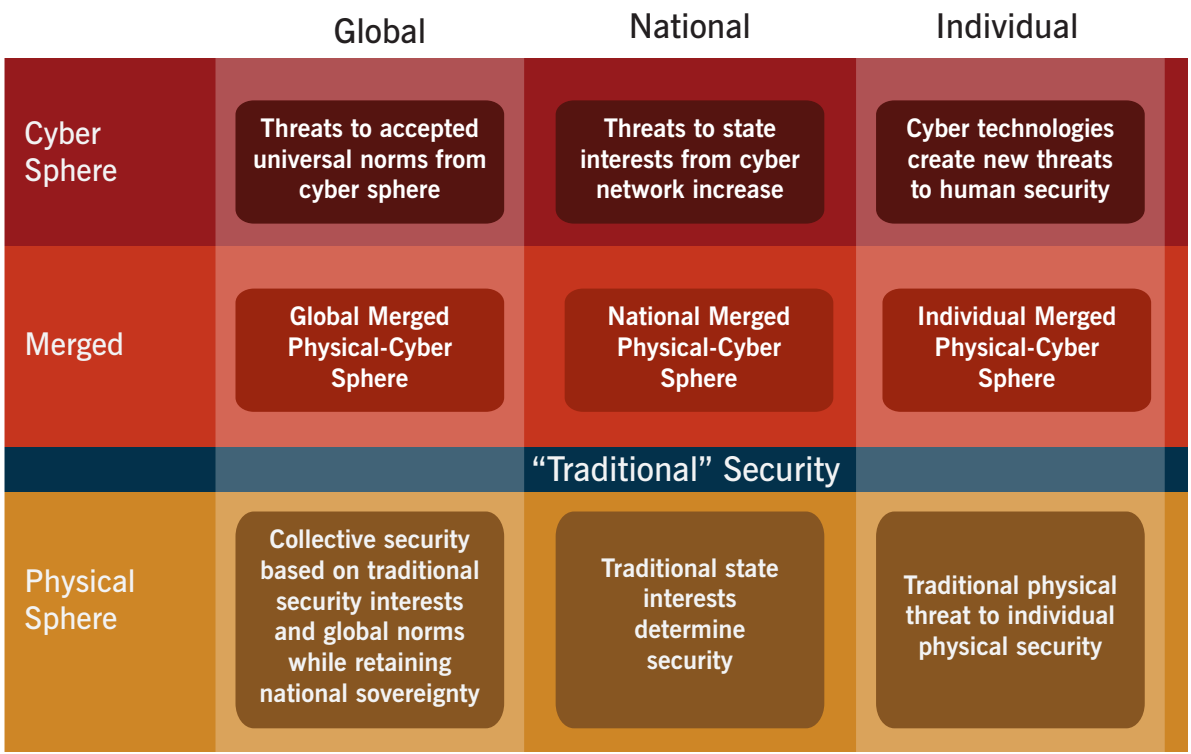
INTRODUCTION

The properties discussed in the previous section magnify the impact of cyberspace threats. Threats that begin in cyberspace now can jeopardize any level of security (personal, collective, and national), and can lead to a wide range of possible response options. In contrast, traditional security threats and responses emanate from the same sphere of interaction—for example, in the traditional physical sphere of interaction, a response would most likely have come from the same sphere from which the initial threat emanated.

Figure 3 includes horizontal rows that represent the sphere of interaction (cyber, physical, or merged cyber-physical), and vertical columns that show activity at differing levels of physical or economic security (individual, national, and global). The framework in Figure 3 was inspired by discussions from the roundtables. The framework is intended to describe threats in cyberspace, based on the context set out by the group's definition of that term as discussed in the previous section.

The following discussion addresses each component of the cyber-threat-and-response framework. The scenarios reinforce the need to develop a strategic context for managing activities in cyberspace—in which specific, general and collateral impacts and their scope, as well as attribution, can vary widely and change rapidly, posing challenges for legitimate actions by government. Using the context set out by the roundtables and described earlier in the report, and the recommendations presented in the next section, government can enhance its ability to make effective decisions about how best to address a wide range of cyber threats.

Figure 3: Threat Vectors



CYBER SPHERE OF INTERACTION

The initial threat vector involves cyberactivity in the cyber sphere.

Global Cyber Sphere (Top left square)
A threat to cybersecurity could take the form of a risk to global cyberinfrastructure or a violation of globally accepted norms of content. Response to this threat in the cyber sphere would usually be constrained to that sphere, which could consist of removing the links to offending cyber sites. Additional responses, such as issuing a warning to remove harmful content from servers or shutting down services, could be implemented if the initial response(s) was not successful in deterring or stopping the threat. This threat vector can also move to the physical sphere of interaction through some action (e.g., unwarranted release of names of people—be they innocent bystanders or people who hold sensitive and undisclosed positions, thereby jeopardizing personal, organizational, national security or other collective groups' security). In such scenarios, a response could still occur within the cyber sphere of interaction; one example would be to degrade the perpetrator(s)' cyberinfrastructure.

Nation-State Cyber Sphere (Top center square)
Threats in this sphere of interaction emanate from the cyber sphere and the response would also occur primarily within the cyber sphere, but these could be combined with threats from the physical sphere. Strategy for this vector does not involve information deterrence alone, whether in cyberspace or with other forms of information. Timothy Thomas wrote "informatized warfare can increase its deterrent power capable of achieving strategic objectives when combined with nuclear deterrence capabilities"(Thomas, forthcoming). Actions in this space may also leverage conventional deterrence, space deterrence, and information deterrence as a "cocktail" for use in future conflicts.

Practitioners in the nation-state sphere of interaction view cyberspace as asymmetric, in which cyber conflict, economic actions, a domestic or international public information campaign, or other measures, supplement large-scale military activities that may be unavailable or simply not usable (n.d.). Most behavior in this sphere is driven by the belief that information superiority is becoming a key component of national power.

As a result, states and other participants can aggressively probe and enter global cyber sphere networks to gain a competitive advantage in economics, business, military, and political bargaining for strategic reasons; for example by conducting strategic reconnaissance to "win victory before the first battle" by mapping the opponent's digital "terrain" (Thomas, forthcoming). Strategic digital reconnaissance will provide knowledge of the digital "landscape" to permit more effective military activity. In this context, proactive responses in cyberspace can be a preferred strategy for winning a cyber conflict (Thomas, forthcoming). Such actions seek to damage or disrupt the critical nodes that comprise the material and technical foundation of the opponent's cybersystem.

Individual Cyber Sphere (Top right square)
The individual threat vector is completely in the cyber sphere and involves a violation of individual cyberinfrastructure of globally accepted norms regarding content that is published in cyberspace. The response would initially be confined to the cyber sphere of interaction, but could migrate to the physical sphere if the desired result is not achieved through cyber sphere response(s).

PHYSICAL SPHERE OF INTERACTION ("TRADITIONAL" SECURITY)

The physical sphere of interaction—the traditional focus of security concerns—addresses the physical or economic well being of the individual, formal organization, or state. Traditional security threats come from within the physical sphere and response was and often is delivered in that sphere as well, but the cyber sphere can be used to augment a physical sphere response.

Global Physical Sphere (Bottom left square)
International security often involves activities in the global, physical sphere. States collaborate to enforce an accepted global norm, which is typically also in their own interest. Although primarily physical, instruments of the cyber dimensions of national power are increasingly being used in conjunction with physical military instruments and other dimensions of national power to provide an even greater comparative advantage.

National Physical Sphere (Bottom center square)
This sphere represents the historical, realist notion of national security: a state acting within the physical sphere of interaction for its own self-interest, generally employing the military dimension of national power. Activity within the cyber sphere of interaction can greatly enhance both the physical sphere's initial instruments of military power, as well as any subsequent activity.

Individual Physical Sphere (Bottom right square)
People who live in dangerous areas and desire physical safety and the basic necessities of life often turn to anyone who can provide them. Although the cyber sphere of interaction could be involved, both the principal threat and response generally reside in the physical sphere of interaction. When authorities do not provide safety for those in jeopardy, unofficial groups might emerge to provide a physical (or cyber) response.

MERGED PHYSICAL-CYBER SPHERE OF INTERACTION

In the global merged sphere, the threat to a specific level of security—and a potential response—could initially appear from either the cyber or physical sphere of interaction. Any subsequent risks could arise from any or all spheres. In this scenario, it becomes difficult to locate in which sphere activity is most prominent. Of course, there is always the potential for a physical threat to the cyber infrastructure. The physical-cyber merged sphere seems to be the perfect example of cyberspace's ability to impact the four traditional strategic domains, encompassing many aspects of cyber and physical spheres.

Global Physical-Cyber Sphere (Middle left square)
The risk in the global-merged physical-cyber sphere of interaction may initially be strategic, economic, or political (involving reconnaissance and intelligence gathering), leading to more direct action in the future. Alternatively, information derived from reconnaissance conducted by governments, embassies, research firms, trade and commerce, aerospace, military installations, energy providers, or critical infrastructures could include geopolitical data for use by nations or be traded underground and sold

to the highest bidder (Holden, forthcoming). A collective response would generally fall in the cyber sphere—but if the risk and loss of data were serious enough to jeopardize vital interests, then the response could move to the physical sphere.

National Physical-Cyber Sphere (Middle center square)
This sphere of interaction represents an integrated merging of the traditional dimensions of national power (political, economic, military, etc.) with the cyber dimension. Countries now view use of the cyber dimension of national power as a supplement to the other more traditional dimensions of power. They may use any and all interchangeably to achieve their preferred outcome(s) as a normal course of action, with the cyber dimension used to directly attack command and control and weapons systems and indirectly to disrupt various civilian functions. Cyber activity can also be used independently to damage objects in the physical sphere.

Individual Physical-Cyber Sphere (Middle right square)
This sphere of interaction involves actions in cyberspace that jeopardize individual physical or economic security and lead to cyber and physical responses. Initial response is generally through the cyber sphere, but can migrate to the physical if the desired outcome is not forthcoming through cyber activity. Vigilantism (or digilantism, the cyber equivalent of vigilantism) might occur in the cyber and physical spheres of interaction absent an appropriate, effective response from recognized authorities; this could also occur in the other two individual levels of security (cyber and physical).

GENERAL CONSIDERATIONS

Response management in cyberspace could prove to be much more problematic than it was during the Cold War because of cyberspace's ontology, and its complex threat and response vectors— especially when definitive attribution of activity is difficult because the perpetrator strives to go undetected. However, managing security in cyber space is not a narrow technical challenge; it involves fundamental issues of politics and strategy, nation-state relations, bargaining, and escalation dynamics and control. An understanding of the technological domain and strategic environment is imperative to developing effective responses to deliberate threats to cyber infrastructures.

Without a solid conceptual foundation, a cyberconflict would pose significant management challenges. Even with more comprehensive scenario development and contingency planning, there is strong potential for miscalculations and misunderstandings that provoke an out-of-control escalatory spiral, absent a commonly understood definitional framework to help frame strategic and tactical choices.

The roundtables did not attempt to resolve the debate over the internal ontology of cyberspace. Such an attempt would have taken the group's attention away from the impact of a definition for cyberspace informing strategic choices by government. Rather, roundtable participants tried to clarify the structures of the strategic environment within which cyberspace exists and operates.

Understanding the role of cyberspace in the strategic environment is crucial to making optimal decisions about cyberactivity, especially during a crisis. The roundtable discussions revealed that cyberspace is a more complex strategic domain than the other four strategic domains (air, land, sea, and space), and therefore demands more complex response calculations. Cyberspace is a separate independent strategic domain, much like the traditional four domains, while at the same time encompassing those four domains. This fact presages significant difficulty for strategic planners and decision makers who seek to accurately identify the true locus of the threat, attribution of the perpetrator, time available to respond, and response options. The roundtable participants recommend that government

decision makers be flexible and adaptable, and approach solutions with open minds within an agreed-upon strategic framework.

RECOMMENDATIONS

Recommendation One: The federal government should agree on a definition of cyberspace. The roundtables believe that cybersecurity management would be more effective and efficient if the term were more clearly defined. Such a definition could replace the one now used by the Department of Defense in Joint Publication. 1–02: *DOD Dictionary of Military and Associated Terms.*[4] Based on roundtable discussions, the following definition is recommended:

> Cyberspace is a man-made global strategic domain, dimension of national power, and instrument of the dimension of national power within the information environment, consisting of the interdependent network of information technology infrastructures and resident data—including the Internet, telecommunications networks, computer systems, and embedded processors and controllers—for the production and use of information by individuals and organizations.

This definition incorporates all of the aspects of cyberspace (functions, components, and uses). Roundtable participants found the recommended definition to be both comprehensive and practical.

4 "[A] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (U.S. Department of Defense 2011).

Considerations Regarding the Proposed Definition of Cyberspace in a Security Context

Several aspects of the proposed definition of cyberspace merit consideration by government decision makers:

- That cyberspace simultaneously influences three different functions: global strategic domains, dimensions of national power, and instruments of national power. These three functions complicate cyberspace activity considerably, because cyberspace has a variety of impacts, depending on the context in which it is used across these three functions. Decision makers need to consider specifically which of those functions involve cyberactivity, and which function should be used in responding to a threat, if warranted.
- Cyberspace is a system composed of hardware, digital data, and human beings. It is a man-made system, with inherent vulnerabilities stemming from its design and construction, especially its network structure that continues to evolve in a scale-free fashion that has little overall organization or function.
  - Decision makers should identify and prioritize cyberspace vulnerabilities (especially to critical infrastructures) according to the risks posed by a targeted attack on the continued well-being of U.S. national and economic security.
  - Methods or strategies to reduce or eliminate those prioritized structural vulnerabilities can then be identified (or become a research priority), to enhance the continued operation of functions performed to support national security.
- Cyberspace exists to facilitate human activity and is subject to human decision making with all of its foibles; people must be involved in cyberspace operations, creating or initiating even automated cyber activity that then operates without direct human intervention. Human decision making is not formulaic; it is based on different individuals' sometimes idiosyncratic assessments of costs and benefits, beliefs about fundamental issues of politics and strategy, skills in bargaining, and escalation dynamics. Cyberspace-based responses should be made by human decision makers, not predicated solely on an algorithmic response, given that these decision makers created the circumstances that require a response.

Recommendation Two: Government should apply the definition of "strategic domain" to managing these domains.

The relationship between cyber and the four other spheres, and the unique nature of cyberspace's strategic domain, involves both an independent space in which cyber activity takes place and the other four strategic domains. This makes national security decisions involving cyberspace extremely complex. An increase in knowledge about the cyber domain and its role and function in the strategic environment will allow decision makers to identify different strategic options and should lead to more sophisticated anticipation of threats as well as more nuanced and effective responses that account for costs and benefits of various choices.

Particular efforts should to be devoted to identify from which strategic domain the cyberactivity originated. Making decisions in the strategic context of cyberspace is as much about managing uncertainty across multiple domains that cyberspace activity affects as it is about achieving a specific, goal. Successful strategic decision making and management in cyberspace involves:

- Clear identification of goals
- A profound (or deep) understanding of the relevant strategic environment
- A clear assessment of the comparative advantages offered by one proposed solution over another, as it affects the entire environment
- A calculation of costs through an objective appraisal of an action's affect on national resource

Effective government cyber decision making will manage between the internal cyber domain environment and the external domain environments, with an understanding of goals and values, resources and capabilities, structure, and systems and the range of options that an understanding of cyberspace's domain would help decision makers to identify.

Questions to Consider in Applying Cyberspace Within a Strategic Domain

- At what point does the degradation of cyber and other critical infrastructure systems become so serious that it jeopardizes the nation's ability to act in response to threats?
- In what instances should government ignore problematic activity against cyberinfrastructure? The level of risk acceptance across critical infrastructure sectors should be identified and prioritized to determine what constitutes a national security risk as opposed to a "nuisance" (i.e., cyberactivity that is annoying or interferes with the operation of the national cyberinfrastructure but does not rise to the level of threatening its existence or operability). Identification and prioritization of risk relevant for a critical infrastructure could lead to the establishment of a typology of activity based on risk acceptance, which could assist decision makers in deciding how best to respond to the cyberactivity.
- When is an escalation of cyberactivity in response to a threat or a preemptive action warranted?
- What activity would prompt movement across strategic domains? What could those linkages be and how might they shape a cyber conflict? Should escalation into other domains be sequentially ordered? What are acceptable parameters for the following:
  - **Authority:** Who acts, where, and when?
  - **Response:** What actions to take? What are the rules of engagement (ROE)?
  - **Resources:** What are the scope and scale of the following actions:
    - Which dimension(s) of national power to use, and in what mix?
    - Which elements of national power to use, and in what mix?
    - Which domain(s) to act within?
  - **Impact:** What are the likely consequences of a response?
  - **Crisis:** When does cyberactivity become a crisis (e.g., given a unexpected occurrence, time constraints, widely unacceptable degree of risk, or high importance of a decision)? Crisis management and cyber-incident response can be challenging, especially when the perpetrator of a hostile act seeks to go undetected. What level of threat and other internal and external forces (e.g. type, severity, internal dynamics, range of outcomes) could impede adequate management of a cyber crisis?

Recommendation Three: Educate practitioners about the nature of cyberspace, to help government effectively manage across the range of cyber risks and response options. Training can provide important context to frame actions in the event of a cyber system degradation or shutdown, especially a cyber event that jeopardizes the nation's health and welfare.

Understanding the nature of potential impacts across cyberspace and related domains will improve the capacity of government to anticipate and act in the face of these threats. Anticipation, built through training, will diminish the risk of miscalculations and misunderstandings that could provoke an escalating spiral of actions harmful to security. Such training should include:

- A series of scenarios that could be developed to depict different cyber threat/risk situations in all of the spheres of interaction, along with calculations of threat and risk impact, so that decision makers and operators have the benefit of existing knowledge and practice to hone their ability to confront these risks. Such scenarios could address answers to the questions above and be framed to accommodate:
  - Results
  - Time
  - Attribution error
  - Precedent-setting activities
  - Type and extent of responses
- More sophisticated scenarios that could be generated to depict two- or multi-factor risk/threat situations, to assess possible actions proposed to introduce asymmetric risk (an investment involving uneven gains and losses). Such scenarios could be made more realistic through simulations that involve both nation-state decision makers and those who jeopardize nation states, by generating activity in both the cyber and physical spheres of interaction.
- Estimates of the probable effectiveness of responses to a given scenario that could be modeled, providing decision makers with a tool to understand the potential impacts of these types of decisions.
- Digitized training that could be developed that involves "gamifying" different situations, using video techniques to reflect cross-domain impacts.

RESEARCH ROUNDTABLE PARTICIPANTS

I am grateful to the individuals who contributed their time and guidance to make this project as useful as possible to strategic thinkers, the cyberspace community, and national security practitioners and decision makers. I appreciate their participation, thoughtful input, and sage advice on the substantive discussions of the nature and definition of cyberspace during both the roundtable meetings and in the assessment of the findings. Without these participants, this project would not have been possible nor would the findings they developed.

Cyberspace Roundtable Participants

Davis Bobrow, Graduate School of Public and International Affairs, University of Pittsburgh

David Chambers (Moderator), Department of Political Science, Indiana University of Pennsylvania

Michael Driscoll, Indiana University of Pennsylvania

Casey Dunlevy, BAE

Waleed Farag, Department of Computer Science, Indiana University of Pennsylvania

Dighton Fiddner, Department of Political Science, Indiana University of Pennsylvania

Michael Fowler, Roger Williams University/Naval War College

Steve Jackson, Department of Political Science, Indiana University of Pennsylvania

Benoit Morel, Engineering and Public Policy, and Physics, Carnegie Mellon University

Issac Porche, RAND Corporation

Phil Williams, Ridgway Center for International Security Studies, Graduate School of Public and International Affairs, University of Pittsburgh

Blank, Stephen. (in press.) Information warfare a la Russe. In D. Fiddner and P. Williams (Ed.) (Untitled). Strategic Studies Institute, U.S. Army War College, Carlisle, PA.

Broad, William J., Markoff, John and Sanger, David E. "Israel tests on worm called crucial in Iran nuclear delay." *New York Times*, 15 January 2011. Retrieved July 6, 2014, from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0

Clark, David. *Characterizing cyberspace: past, present and future*. MIT CSAIL Version 1.2 of March 12, 2010 Retrieved June 18, 2013, from http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf

David, Javier E. "Head of online currency exchange found dead in Singapore." CNBC.com, 5 March 2014. Retrieved July 6, 2014 from http://www.cnbc.com/id/101468694

Fiddner, Dighton. (August 2011) *National cyber security strategy against malevolent use of the global cyberspace*. Paper Presented World International Studies Committee (WISC) 3rd Global International Studies Conference, University of Porto, Porto, Portugal.

Frankfort-Nachmias, Chava, and David Nachmias (2008) *Research methods in the social sciences. 7th edition*. New York: Worth Publishers.

Helmer, Oalf. (March 1967) *Analysis of the future: The Delphi Method* (P3558), Santa Monica: The RAND Corporation.

Herrera-Flanigan, Jessica. (March 2001) *Cybersecurity ecosystem: The future?* Nextgov: Cybersecurity Report, Retrieved August 5, 2011, from http://www.nextgov.com/cybersecurity/cybersecurity-report/2011/03/cybersecurity-ecosystem-the-future/54390/

Holden, Dan. (January 2013) "Global espionage network hacks computers, smart phones." SV411. Retrieved July 4, 2014, from http://www.sv411.com/index.php/2013/01/global-espionage-network-hacks-computers-smart-phones

IRS Notice 2014-21. Retrieved July 4, 2014, from http://www.irs.gov/pub/irs-drop/n-14-21.pdf?utm_source=3.31.2014+Tax+Alert&utm_campaign=3.31.14+Tax+Alert&utm_medium=email

Jorgensen, Jane and Philippe Rossignol. *Information asssurance cyber ecology*. (January 2003). AFRL-IF-RS-TR-2003-1. Final Technical Report. Air Force Research Laboratory, Information Directorate, Rome Research Site. Rome, N.Y Retrieved August 5, 2011, from http://handle.dtic.mil/100.2/ADA411943

Libicki, Martin. (2009). *Cyberdeterrence and cyberwar*. Santa Monica: RAND.

Mandiant: A FireEyeTM Company .(February 2013) *APT1: Exposing one of China's cyber espionage units*, Mandiant. Retrieved July 6, 2013, from http://intelreport.mandiant.com/

Molineux, Matthew. C., Colonel, USAF. Director, Aerospace Studies, US Army War College and Director, Eisenhower Series College Program. Carlisle, PA..matthew.c.mollineux.mil@mail.mil, Subject: RE: Eisenhower Series College Program – US Army War College (UNCLASSIFIED), 08/21/13 11:46 AM).

Inskeep, Steve and Singer, Peter W. "Cybersecurity forces U.S. to examine technological changes," National Public Radio, 20 December 2013.

NATO. "The history of cyber attacks — a timeline." *NATO Review.* Retrieved July 6, 2104, from http://www.nato.int/docu/review/2013/Cyber/EN/index.htm

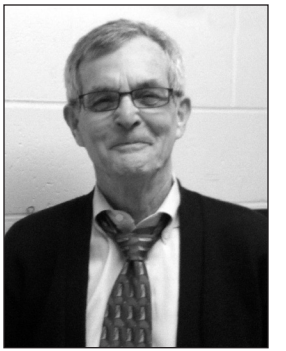
"Operation Red October: Cyber espionage campaign against many governments," *The Hacker News*, 24 January 2013, Retrieved July 4, 2014, from http://thehackernews.com/2013/01/operation-red-october-cyber-espionage.html

Thomas, Timothy. (in press) "China's reconnaissance and system sabotage activities: Supporting information deterrence." In D. Fiddner and P. Williams (Ed.) (Untitled). Strategic Studies Institute, U.S. Army War College, Carlisle, PA.

U.S. Chairman of the Joint Chiefs of Staff. (November 2012) *Information Operations.* Joint Publication 3-13. Washington, D.C. Retrieved July 4, 2013, from http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

U.S. Department of Defense (November 2010 as amended, May 2011) Joint Pub. 1–02: *DOD Dictionary of Military and Associated Terms*. Retrieved July 4, 2013, from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

U.S. Department of Homeland Security. (March 2011) *White Paper: Enabling distributed security in cyberspace: Building a healthy and resilient cyber ecosystem with automated collective action*. Washington, D.C. Retrieved May 13, 2012, from http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf



Dighton Fiddner, PhD is assistant professor in the Department of Political Science at Indiana University of Pennsylvania. He currently teaches international relations, American foreign policy, and public policy courses. His interests also include national and international security policy, complexity, and the information system as a national security risk.

In recent years, he has published numerous articles on cyberspace. He has hosted seven collaborative roundtables on cyberspace's role in national security. He has also presented his research on cybersecurity at four national and four international conferences.

Prior to his academic career, Fiddner served in the U.S. Army, retiring as a lieutenant colonel in September 1988. During his military career, he worked on various national security issues. His career included service in the Office of the Secretary of Defense.

Fiddner received his PhD in political science from the School of Public and International Affairs at University of Pittsburgh, an MA in Political Science from Kansas University, and a BS in psychology from Davidson College.

To contact the author:

Dr. Dighton Fiddner
Assistant Professor
Department of Political Science
103 Keith Hall
Indiana University of Pennsylvania
Indiana, PA 15705
(724) 357-2290

e-mail: fiddner@iup.edu

REPORTS from
The IBM Center for The Business of Government

Acquisition

Eight Actions to Improve Defense Acquisition by Jacques S. Gansler and William Lucyshyn

A Guide for Agency Leaders on Federal Acquisition: Major Challenges Facing Government by Trevor L. Brown

Controlling Federal Spending by Managing the Long Tail of Procurement by David C. Wyld

Collaborating Across Boundaries

Inter-Organizational Networks: A Review of the Literature to Inform Practice by Janice K. Popp, H. Brinton Milward, Gail MacKean, Ann Casebeer, Ronald Lindstrom

Adapting the Incident Command Model for Knowledge-Based Crises: The Case of the Centers for Disease Control and Prevention by Chris Ansell and Ann Keller

Engaging Citizens in Co-Creation in Public Services: Lessons Learned and Best Practices by Satish Nambisan and Priya Nambisan

Improving Performance

Four Actions to Integrate Performance Information with Budget Formulation by John Whitley

Incident Reporting Systems: Lessons from the Federal Aviation Administration's Air Traffic Organization by Russell W. Mills

Predictive Policing: Preventing Crime with Data and Analytics by Jennifer Bachner

Innovation

A Guide for Making Innovation Offices Work by Rachel Burstein and Alissa Black

The Persistence of Innovation in Government: A Guide for Innovative Public Servants by Sandford Borins

Leadership

Best Practices for Succession Planning in Federal Government STEMM Positions by Gina Scott Ligon, JoDee Friedly, and Victoria Kennel

Managing Finance

Managing Budgets During Fiscal Stress: Lessons For Local Government Officials by Jeremy M. Goldberg and Max Neiman

Using Technology

Participatory Budgeting: Ten Actions to Engage Citizens via Social Media by Victoria Gordon

A Manager's Guide to Assessing the Impact of Government Social Media Interactions by Ines Mergel

Cloudy with a Chance of Success: Contracting for the Cloud in Government by Shannon Howle Tufts and Meredith Leigh Weiss

Federal Ideation Programs: Challenges and Best Practices by Gwanhoo Lee

IBM Center for
The Business of Government

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit: ibm.com

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342
website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.