Nuclear Deterrence in Cyber-ia

Challenges and Controversies©

Dr. Stephen J. Cimbala[*]

The information age has arrived, including in military affairs, but theory and policy related to nuclear deterrence are racing to keep up with a cyber-driven world. Future military conflicts, including those involving the exercise of nuclear deterrence and crisis management, will include a digital aspect. Information or "cyber" warfare is here although it is not the driver of every conflict. It exists in the foreground of any attacks against the enemy's brain and central nervous system of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).[1] On the other hand, far too often nuclear deterrence and cyber warfare issues are treated as separate and distinct challenges. This cyber-nuclear separatism is understandable as a matter of division of labor among experts, but it casts a shadow over the reality of nuclear deterrence or crisis management under cyber-intensive conditions.

This article first examines some of the broader theoretical implications of the nuclear-cyber nexus for students of national security policy and warfare. Second, it focuses specifically on American and Russian strategic nuclear deterrence and arms control as policy-related settings for nuclear and cyber relationships. Third, it analyzes how the combination of nuclear and cyber attacks might at least hypothetically affect the stability of nuclear deterrence. Finally, the article draws pertinent conclusions about the nuclear-cyber interface insofar as it might pertain to future arms control, nonproliferation, and deterrence.

How Far Apart?

What are the implications of potential overlap between concepts or practices for cyber war and for nuclear deterrence?[2] Cyber war and nuclear weapons seem worlds apart. Cyber weapons should appeal to those who prefer a nonnuclear military-technical arc of development. War in the digital domain offers, at least in theory, a possible means of crippling or disabling enemy assets without the need for kinetic attack or of minimizing physical destruction.[3] Nuclear weapons, though, are the very epitome of "mass" destruction—so much so that their use for deterrence or the

avoidance of war by the manipulation of risk is preferred to their actual firing. Unfortunately, neither nuclear deterrence nor cyber war will be able to live in distinct policy universes for the near or distant future.

Nuclear weapons, whether held back for deterrence or fired in anger, must be incorporated into systems for C4ISR. The weapons and their C4ISR systems must be protected from attacks both kinetic and digital in nature. In addition, decision makers who have to manage nuclear forces during a crisis should ideally have the best possible information about the status of their own nuclear and cyber forces and command systems, about the forces and C4ISR of possible attackers, and about the probable intentions and risk acceptance of possible opponents. In short, the task of managing a nuclear crisis demands clear thinking and good information. But the employment of cyber weapons in the early stages of a crisis could impede clear assessment by creating confusion in networks and the action channels that depend on those networks.[4] The temptation for early cyber preemption might "succeed" to the point at which nuclear crisis management becomes weaker instead of stronger. As Andrew Futter has noted,

> With US and Russian forces ready to be used within minutes and even seconds of receiving the order, the possibility that weapons might be used by accident (such as the belief that an attack was underway due to spoofed early warning or false launch commands), by miscalculation (by compromised communications, or through unintended escalation), or by people without proper authorization (such as a terrorist group, third party or a rogue commander) is growing. Consequently, in this new nuclear environment, it is becoming progressively important to secure nuclear forces and associated computer systems against cyber attack, guard against nefarious outside influence and "hacking," and perhaps most crucially, to increase the time it takes and the conditions that must be met before nuclear weapons can be launched.[5]

Ironically, the downsizing of US and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, although a positive development from the perspectives of nuclear arms control and nonproliferation, makes the concurrence of cyber and nuclear attack capabilities more alarming. The enormous and redundant deployments by the Cold War Americans and Soviets had at least one virtue. Those arsenals provided so much redundancy against first-strike vulnerability that relatively linear systems for nuclear attack warning, command and control (C2), and responsive launch under—or after—attack sufficed. At the same time, Cold War tools for military cyber mischief were primitive compared to those available now. In addition, countries and their armed forces were less dependent on the fidelity of their information systems for national security. Thus, the reduction of US, Russian, and possibly other forces to the size of "minimum deterrents" might compromise nuclear flexibility and resilience in the face of kinetic attacks preceded or accompanied by cyber war.[6] For example, Bruce Blair, nuclear policy expert and author of a number of studies on nuclear C2, has observed that

> the communications and computer networks used to control nuclear forces are supposed to be firewalled against the two dozen nations (including Russia, China and North Korea) with dedicated computer-attack programs and from the thousands of hostile intrusion attempts made every day against U.S. military computers. But investigations into these firewalls have revealed glaring weaknesses.[7]

The preceding discussion does acknowledge that "nuclear-" and "cyber-related" theories, as well as derivative policy prescriptions, have unique attributes and warning signs against facile analogies. Nevertheless, the cyber "domain" cuts across the other geostrategic domains for warfare: land, sea, air, and space. On the other hand, the cyber domain, compared to the others, suffers from the lack of a historical perspective: the cyber domain "has been created in a short time and has not had the same level of scrutiny as other battle domains," as Maj Clifford S. Magee, USMC, has argued.[8] Brian M. Mazanec also points out the "relative secrecy surrounding most cyber operations with no extensive record of customary practices of states."[9] James Wood Forsyth Jr. and Maj Billy E. Pope emphasize that cyberspace has enabled "a new form of war that no one can see, measure, or presumably fear."[10] However, experts also expect that since we are in the early stages of cyber conflict, we can anticipate that more numerous and more sophisticated cyber weapons will be developed and integrated into states' national military strategies and operational planning guidance. As Mazanec has argued,

> Thus, cyberwarfare capabilities will play an increasingly decisive role in military conflicts and are becoming deeply integrated into states' doctrine and military capabilities. Over 30 countries have taken steps to incorporate cyberwarfare capabilities into their military planning and organizations, and the use of cyberwarfare as a "brute force" weapon is likely to increase. Military planners are actively seeking to incorporate offensive cyber capabilities into existing war plans, which could lead to offensive cyber operations playing an increasingly decisive role in military operations at the tactical, operational, and strategic levels.[11]

Table 1 summarizes information about some of the more publicized computer network attacks (CNA) between 2007 and 2013.

Table 1. Selected computer network attacks

Attack Name	Date	Target	Effect	Suspected Perpetrator
Estonia	April–May 2007	Commercial and governmental web services (civilian target)	Major distributed denial of service (DDOS) attack	Russia
Syrian air defense system (part of Operation Orchard)	September 2007	Military air defense system (military target)	Degradation of air defense capabilities allowing kinetic strike	Israel
Georgia	July 2008	Commercial and governmental web services (civilian target)	Major DDOS attack	Russia
Stuxnet	Late 2009–10, possibly as early as 2007	Iranian centrifuges (military target)	Physical destruction of Iranian centrifuges	United States
Saudi Aramco	August 2012	State-owned commercial enterprise (civilian target)	Large-scale destruction of data and attempted physical disruption of oil production	Iran
Operation Ababil	September 2012–March 2013	Large US financial institutions (civilian target)	Major DDOS attack	Iran

Adapted from Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable," *Strategic Studies Quarterly* 9, no. 2 (Summer 2015): 81, http://www.au.af.mil/au/ssq/digital/pdf/summer_2015/SSQ_Summer_2015.pdf. CNAs include computer network exploitation.

Of course, CNAs are not the only cyber threat posed by potential US adversaries or other state or nonstate actors. According to Joel Brenner, former inspector general and former senior counsel at the National Security Agency,

> The U.S. Navy spent about $5 billion to develop a quiet electric drive for its submarines and ships so they'd be silent and hard to track. Chinese spies stole it. The navy spent billions more to develop new radar for their top-of-the-line Aegis Cruiser. Chinese spies stole that, too. The electronic intelligence services of the Chinese and the Russians are working us over—taking advantage of our porous networks and indifference to security to steal billions of dollars' worth of military and commercial secrets. Some of our allies, like the French and the Israelis, have tried it too.[12]

Brenner asserts that the United States' military-industrial complex "is the world's fattest espionage target" and that more than 100 foreign intelligence services target the United States.[13] As a reminder of this horse race between cyber attackers and defenders, the US government reported large attacks by Russian hackers against the Internal Revenue Service and by Chinese hackers against the majority of US federal agencies during the first week of June 2015.[14]

Notwithstanding the significance of cyber-related challenges to US national security, it does not necessarily follow that deterrence concepts or methods will be applicable to cyberspace. As Dorothy E. Denning notes, authors comparing nuclear deterrence to cyber deterrence "have generally found that the principles that have made nuclear deterrence effective for over half a century fall apart in cyberspace."[15] She cautions that "just as we do not sweep all physical weapons into a single strategy of deterrence, we should not try to sweep all cyber weapons into a single strategy. Rather, we need to narrow our treatment of deterrence as it relates to cyberspace."[16]

Denning suggests two possible approaches to the application of deterrence to cyberspace. The first involves focusing on specific types of cyber weapons for which deterrence might be feasible, such as nuclear electromagnetic pulse weapons. A second approach to deterrence in cyberspace, according to Denning, might be the application of existing deterrence regimes to some cyber activities, including international regimes governing states' behavior or domestic regimes dealing with criminal behavior.[17] Table 2 summarizes some of the major genetic markers that set unique identities for cyber war and nuclear deterrence, even as they are pushed closer together by technology creep, by the demands of policy and strategy, and by international rivalry.

Table 2. Comparative attributes of cyber war and nuclear deterrence

Cyber War	Nuclear Deterrence
The source of attack may be ambiguous—third-party intrusions masquerading as other actors are possible.	The source of attack is almost certain to be identified if the attacker is a state, and even terrorist attackers' nuclear materials may be traceable.
Damage is mostly to information systems, networks, and their messaging contents although these might have spillover effects to the operations of military combat systems, economy, and social infrastructure. (Stuxnet was an exceptional, purpose-built destroyer of targeted nuclear facilities.)	Failure of deterrence can lead to historically unprecedented and socially catastrophic damage even in the case of a "limited" nuclear war by Cold War standards.

Table 2 *(continued)*

Denial of the attacker's objectives is feasible if defenses are sufficiently robust and/or penetrations can be repaired in good time.	Deterrence by means of threat to deny the attacker its objectives is less credible than the threat of punishment by assured retaliation (although improved missile defenses seek to change this scenario).
The objective of cyber attacks is typically disruption or confusion rather than destruction per se.	Nuclear deterrence has rested for the most part on the credible threat of massive, prompt destruction of physical assets and populations.
Cyber war and information attacks can continue over an extended period of time without being detected and sometimes without doing obvious or significant damage—some are not even reported after having been detected.	The first use of a nuclear weapon since 1945 by a state or nonstate actor for a hostile purpose (other than a test) would be a game-changing event in world politics, regardless of the size of the explosion and the immediate consequences.
The price of entry to the games table for cyber war is comparatively low—actors from individual hackers to state entities can play.	Building and operating a second-strike nuclear deterrent requires a state-supported infrastructure, scientific and technical expertise on a large scale, and long-term financial commitments.

Sources: Author. See also Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly* 77 (2nd Quarter 2015): 8–15, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf; Edward Geist, "Deterrence Stability in the Cyber Age," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015): 44-61; Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Institute, 2012), 60–66; Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012); and Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009).

Cyber and Nuclear Crisis Management

Since nuclear weapons are deployed primarily for the purpose of avoiding war by means of deterrence, the relationship between evolving forms of cyber or information warfare and nuclear crisis management becomes an important agenda item for analysts and military planners. Either information or cyber warfare has the potential to attack or to disrupt successful crisis management on each of four important attributes.[18] First, information warfare can muddy the signals being sent from one side to the other in a crisis. This deception can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other's communications networks.[19] The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber victim to arrange a military attack. But destroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when in fact it has not. Thus, side A may intend to signal "resolve" instead of "yield" to its opponent on a particular issue. Side B, misperceiving a "yield" message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dangerous situation to develop.

Information warfare can also destroy or disrupt communication channels necessary for successful crisis management. It can do so by disrupting communication links between policy makers and military commanders during a period of high threat and severe time pressure. Two kinds of unanticipated problems, from the standpoint of civil-military relations, are possible under these conditions. First, political leaders may have predelegated limited authority for nuclear release or

launch under restrictive conditions: only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceived a situation to be far more desperate—and thus permissive of nuclear initiative—than it really was. For example, during the Cold War, disrupted communications between the US president and secretary of defense and ballistic missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers and crew to launch in the absence of contrary instructions.

Second, information warfare during a crisis will almost certainly increase the time pressure under which political leaders operate. It may do so literally, or it may affect the perceived time lines within which the policy-making process can make its decisions. Once either side sees parts of its command, control, and communications system being subverted by phony information or extraneous cyber noise, its sense of panic at the possible loss of military options will be enormous. In the case of US Cold War nuclear war plans, for example, disruption of even portions of the strategic command, control, and communications system could have prevented competent execution of parts of the Single Integrated Operational Plan (the strategic nuclear war plan). The plan depended upon finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets. Partially misinformed or disinformed networks and communications centers would have led to redundant attacks against the same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations.

A third potentially disruptive effect of information warfare on nuclear crisis management is that such warfare may reduce the search for available alternatives to the few and desperate. Policy makers searching for escapes from crisis denouements need flexible options and creative problem solving. Victims of information warfare may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be poorly posed, and responses (if available at all) will be driven toward the least common denominator of previously programmed standard operating procedures. Retaliatory systems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives.

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions in nonmilitary bureaucratic organizations.[20] In civil-military C2 systems under the stress of nuclear crisis decision making, the first available alternative may quite literally be the last—or so policy makers and their military advisers may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, for example, a number of members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire 13 days of crisis deliberation. Had less time been available for debate and had President Kennedy not deliberately structured the discussion in a way

that forced alternatives to the surface, the air strike and invasion might well have been the chosen alternative.

Fourth—and finally on the issue of crisis management—information warfare can cause flawed images of each side's intentions and capabilities to be conveyed to the other, with potentially disastrous results. Another example from the Cuban missile crisis demonstrates the possible side effects of simple misunderstanding and non-communication on US crisis management. At the tensest period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. US and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defenses might have interpreted the U-2 flight as a prestrike reconnaissance mission or as a bomber, calling for a compensatory response by Moscow.[21] Fortunately, the Soviet leadership chose to give the United States the benefit of the doubt in this instance and to permit US fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not scrubbed once the crisis began has never been fully revealed; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policy makers who failed to appreciate the risk of "normal" reconnaissance under these extraordinary conditions.

The preceding discussion and examples are underscored by the assessment of expert analyst Martin Libicki regarding the relationship between cyber war and crisis management:

> To generalize, a situation in which there is little pressure to respond quickly, in which a temporary disadvantage or loss is tolerable, and in which there are grounds for giving the other side some benefit of the doubt is one in which there is time for crisis management to work. Conversely, if the failure to respond quickly causes a state's position to erode, a temporary disadvantage or degree of loss is intolerable, and there are no grounds for disputing what happened, who did it, and why—then states may conclude that they must bring matters to a head quickly.[22]

This overview of the possible dysfunctions in nuclear crisis management when it overlaps with cyber war is not necessarily totally pessimistic. Human beings remain in charge, not computers and information networks. If those human beings bring to the table an awareness of human fallibility, an appreciation of historical precedent, and a clear sense of proportion about the use of technology in times of peace, crisis, and war, they have every chance for success. On the other hand, decision makers who are overconfident of their abilities, unaware of historical precedents, and besotted with technical hubris or military systems for their own sake can accomplish a considerable amount of mayhem in a very short time.

Conclusions

Cyber tools will not obviate the need for nuclear deterrence, and analytical models designed for the study of nuclear deterrence cannot be transferred directly into the realm of cyber conflict without creating paradigm pandemonium. Military planners and policy makers, however, will find points of intersection between nuclear and cyber problems. The issue of truly "strategic" cyber war apart from kinetic attacks poses a less imminent concern than does cyber as an enabler (or disabler) of suc-

cess in conventional war or nuclear deterrence. The future of digital technology as it applies to military affairs is a magical mystery tour of unknowns. But a safe wager is that future nuclear C2 and communications systems, however driven by digital improvements, will nevertheless have to satisfy the policy and strategy requirements for prompt response to authorized commands, for avoidance of false positives in early warning and reaction, and for maintenance of a spectrum of viable options for policy makers and commanders, even under the duress of war or of imminent threat of war.

The relationship between nuclear crisis management and the information age is a work in progress, but several potential ambushes for nuclear deterrence and crisis stability can be identified now. First, cyber war or software malfunctions might interfere with reliable communication. Second, cyber attacks might take place more rapidly than decision makers could interpret the results and/or resolve upon an appropriate response. Third, the identity of a cyber attacker might remain unclear for the duration of a crisis; indeed, a third party could "impersonate" an American or Russian communication or create an information embolism in either state's networks. In an extreme case, a state-directed hacker or individual malware malcontent might trigger an incorrect attack warning or trigger an inauthentic launch command. Furthermore, even if we assume that current and prospective US and Russian nuclear systems are proof against mistaken warnings or accidental launches, the vulnerability of other states' nuclear C2 and launch systems to cyber war is unknown. ✪

Notes

1. P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), esp. 126–38.

2. US defense strategy defines three primary Department of Defense (DOD) cyber missions: defense of DOD networks, systems, and information; defense of the US homeland and national interests against cyber attacks of significant consequence; and cyber support for military operations and contingency plans. See US Department of Defense, *The DOD Cyber Strategy* (Washington, DC: US Department of Defense, April 2015), esp. 4–6, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy /Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. See also Cheryl Pellerin, "DARPA's Plan X Gives Military Operators a Place to Wage Cyber Warfare," US Department of Defense, 12 May 2016, http:// www.defense.gov/News-Article-View/Article/758219/darpas-plan-x-gives-military-operators-a-place-to -wage-cyber-warfare; Edward Geist, "Deterrence Stability in the Cyber Age," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015): 44–61; Robert Spalding III and Adam Lowther, "The New MAD World: A Cold War Strategy for Cyberwar," *National Interest*, 22 June 2015, http://nationalinterest.org/feature/the -new-mad-world-cold-war-strategy-cyberwar-13154; Singer and Friedman, *Cybersecurity and Cyberwar*; Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle, PA: Strategic Studies Institute, US Army War College, April 2013); Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012); Kamaal T. Jabbour and E. Paul Ratazzi, "Does the United States Need a New Model for Cyber Deterrence?," chap. 3 in *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century*, ed. Adam B. Lowther (New York: Palgrave Macmillan, 2012), 33–45; and Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

3. The "Stuxnet" virus is a contrarian example since it was specifically designed and intended for the destruction of nuclear centrifuges in Iran. See Singer and Friedman, *Cybersecurity and Cyberwar*, esp. 114–20. On the information operations concepts of major powers, see Timothy L. Thomas, *Cyber Silhouettes: Shadows over Information Operations* (Fort Leavenworth, KS: Foreign Military Studies Office, 2005), chaps. 5–6, 10, 14, and passim. See also Pavel Koshkin, "Are Cyberwars between Major Powers

Possible? A Group of Russian Cybersecurity Experts Debate the Likelihood of a Cyberwar Involving the U.S., Russia or China," *Russia Direct*, 1 August 2013, http://russia-direct.org, in *Johnson's Russia List, 2013*, no. 143 (6 August 2013), davidjohnson@starpower.net.

4. Cyber weapons are not necessarily easy to use effectively as enabling instruments for operational/tactical or strategic effect. See Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), esp. chaps. 4–5.

5. Andrew Futter, "Cyber Threats and the Challenge of De-alerting US and Russian Nuclear Forces," NAPSNet Policy Forum, 15 June 2015, http://nautilus.org/napsnet-policy-forum/cyber-threats-and-the-challenge-of-de-alerting-us-and-russian-nuclear-forces/. See also Franz-Stefan Gady, "Could Cyber Attacks Lead to Nuclear War?," *Diplomat*, 4 May 2015, http://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/.

6. An expert critique of proposals for minimum deterrence for US nuclear forces appears in Dr. Keith B. Payne, study director, and Hon. James Schlesinger, chairman, Senior Review Group, *Minimum Deterrence: Examining the Evidence* (Fairfax, VA: National Institute for Public Policy, National Institute Press, 2013). For a favorable expert assessment of the prospects for minimum deterrence, see James Wood Forsyth Jr.; Col B. Chance Saltzman, USAF; and Gary Schaub Jr., "Remembrance of Things Past: The Enduring Value of Nuclear Weapons," *Strategic Studies Quarterly* 4, no. 1 (Spring 2010): 74–90.

7. Bruce Blair, "Could Terrorists Launch America's Nuclear Missiles?," *Time*, 11 November 2010, http://content.time.com/time/nation/article/0,8599,2030685,00.html. One reviewer for this article objected to Blair's argument as quoted, responding that his assessment was "patently false."

8. Maj Clifford S. Magee, USMC, "Awaiting Cyber 9/11," *Joint Force Quarterly* issue 70 (3rd Quarter 2013): 76, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_76-82_Magee.pdf.

9. Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable," *Strategic Studies Quarterly* 9, no. 2 (Summer 2015): 80, http://www.au.af.mil/au/ssq/digital/pdf/summer_2015/SSQ_Summer_2015.pdf.

10. James Wood Forsyth Jr. and Maj Billy E. Pope, USAF, "Structural Causes and Cyber Effects: Why International Order Is Inevitable in Cyberspace," *Strategic Studies Quarterly* 8, no. 4 (Winter 2014): 118, http://www.au.af.mil/au/ssq/digital/pdf/winter_14/forsyth.pdf. See also Mazanec, "International Order in Cyberspace," 96. The issue of whether cyber is a "domain" or something else is an epistemological debate not entered into here.

11. Mazanec, "International Order in Cyberspace," 83.

12. Joel Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (New York: Penguin Books, 2013), 3.

13. Ibid., 73.

14. David E. Sanger and Julie Hirschfield Davis, "Hacking Linked to China Exposes Millions of U.S. Workers," *New York Times*, 4 June 2015, http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html; and Chris Frates, "IRS Believes Massive Data Theft Originated in Russia," *CNN*, 4 June 2015, http://www.cnn.com/2015/05/27/politics/irs-cyber-breach-russia/.

15. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly* 77 (2nd Quarter 2015): 11, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf.

16. Ibid., 12.

17. Ibid., 13–15.

18. For useful definitions of *cyber attack* and *cyber war*, see Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *International Law and Politics* 47 (2015): 327–55, esp. 328.

19. A virus is a self-replicating program intended to destroy or alter the contents of other files stored on floppy disks or hard drives. Worms corrupt the integrity of software and information systems from the "inside out" in ways that create weaknesses exploitable by an enemy.

20. James G. March and Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958), 140, 146.

21. Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971), 141. See also Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton, NJ: Princeton University Press, 1989), 147.

22. Libicki, *Crisis and Escalation in Cyberspace*, 145.
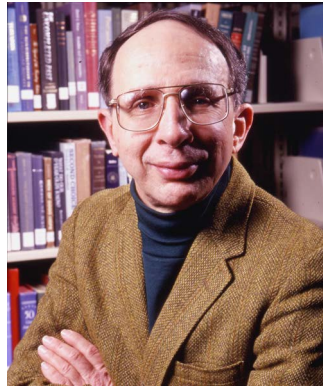
Dr. Stephen J. Cimbala

Dr. Cimbala (BA, Penn State; MA, PhD, University of Wisconsin–Madison) is Distinguished Professor of Political Science at Penn State–Brandywine. An award-winning Penn State teacher, he is the author of numerous works in the fields of nuclear arms control, deterrence, national security policy, and other topics. He recently authored *The New Nuclear Disorder: Challenges to Deterrence and Strategy* (Ashgate, 2015). Dr. Cimbala has served on the editorial boards of academic journals, has consulted for various US government agencies and contractors, and has contributed to US and foreign media discussions of US national security issues.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

http://www.airpower.au.af.mil.