Nuclear Crisis Management in the Information Age

Stephen J. Cimbala@

The relationship between nuclear weapons and information technology will make at least marginal, if not fundamental, changes in the attributes of nuclear deterrence. These changes will affect not only prevailing theories about deterrence, but also the practice of nuclear deterrence and other military suasion by governments. Governments and their armed forces will have to adapt their bureaucratic hierarchies to the demands for faster and more flexible decision making and force application. In so doing, they will become progressively more cyber-implicated, cyber-dependent, and cyber-vulnerable. In addition, although cyberspace operations differ in important ways from kinetic operations, the various elements of information warfare "should now increasingly be considered elements of a larger whole rather than separate specialties that individually support kinetic military operations".[1]

[1] Martin C. Libicki, "The Convergence of Information Warfare," Strategic Studies Quarterly, no. 1 (Spring 2017), pp. 49-65, citation p. 50. In this study I use the terms information warfare and cyber war generically, although some cyber grammarians might insist that "cyber" war be restricted to digital attacks on information systems and networks per se, and information warfare to broader kinds of influence operations, possibly including digital and-or other methods. A sensible approach to this matter is used in P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know (New York: Oxford University Press, 2014), pp. 67-72 and passim., and in John Arquilla, Worst Enemy: The Reluctant Transformation of the

If the ultimate weapons of mass destruction--nuclear weapons--and the supreme weapons of soft power--information warfare—are commingled during a crisis, the product of the two may be an entirely unforeseen and unwelcome hybrid. Crises by definition are exceptional events. No Cold War crisis took place between states armed both with advanced information weapons and with nuclear weapons. But given the durability of the two trends, interest in infowar and in nuclear weapons, the potential for overlap and its implications for nuclear crisis management deserve further study and policy consideration.

The outcome of a nuclear crisis management scenario influenced by information operations may not be a favorable one. Despite the best efforts of crisis participants, the dispute may degenerate into a nuclear first use or first strike by one side and retaliation by the other. In that situation, information operations by either, or both, sides might make it more difficult to limit the war and bring it to a conclusion before catastrophic destruction and loss of life had taken place. Although there are no such things as "small" nuclear wars, compared to conventional wars, there can be different kinds of "nuclear" wars, in terms of their proximate causes and consequences.[2] Possibilities include: a nuclear attack from an unknown source; an ambiguous case of possible, but not proved, nuclear first use; a nuclear "test" detonation intended to

American Military (Chicago, Ill.: Ivan R. Dee, 2008), Ch. 6-7, in addition to sources in later notes.

[2] For pertinent scenarios, see George H. Quester, Nuclear First Strike: Consequences of a Broken Taboo (Baltimore, Md.: Johns Hopkins University Press, 2006), pp. 24-52.

intimidate but with no immediate destruction; or, a conventional strike mistaken at least initially for a nuclear one.

One illustration of the problem of managing escalation control and conflict termination along with information operations, is provided by the possibility of a joint NATO-Russian theater missile defense (possibly including air defenses) system. The idea has expert and highly visible political proponents on both sides of the Atlantic, and official Russian commentators have not closed the door to the possibility of some cooperation on ballistic missile defenses (BMD). Here NATO and Russia are facing in two political directions: wariness, but also openness, toward one another; and, second, concern about possible future Iranian or other Middle Eastern nuclear weapons in the hands of leaders beyond deterrence based on the credible threat of nuclear (or other) retaliation.

However, the problems of obtaining missile defense cooperation as between NATO and Russia are not only political. Even with the best of intentions among U.S., NATO and Russian negotiators, the military-technical problems of coordinating BMD command-control and communications systems are considerable. Indeed, they are not strictly "military-technical" but also heavily embedded with issues of political sovereignty, classified intelligence, and trust, among governments and militaries. Even the militaries among NATO members differ as to their national traditions, military service identities, experiences in nuclear arms control, and willingness to share on-line information in real times with temporary partners who may be future enemies. For example, if a European theater-wide system of intelligence and missile attack warning is established, how many capitals will host relevant servers and receive timely output? Who will decide that a missile warning is now a threat requiring activation of the European BMD system –can a single nation do so if a missile is headed its way, or must NATO (including the U.S.) and Russia agree before taking responsive action?

If a political crisis as between NATO and Russia erupts after a cooperative BMD system has been established, will Russian or American cyberwarriors attempt to spoof or otherwise negate the other's missile defense component? Would it be better to reassure Russia as to the surety of its individually based, or shared-with-NATO, missile defenses, as against the possibility of a conventional or nuclear preemption? Neither Russia nor the United States will want to relinquish sovereign control over its part of any cooperative missile defenses. However, would it be prudent to announce a withdrawal from the cooperative aspect of the regional BMD system during a crisis, or to maintain the fiction of cooperation while attacking the other side's cyber systems with Trojan horses, logic bombs and trap doors – just in case? Perhaps, in future nuclear or other crises, the U.S. and Russian cyber commands should have their own direct "hot line" –or, in this case, encrypted digital link.

The objective of infowar in conventional warfare is to deny enemy forces battlespace awareness and to obtain dominant awareness for oneself, as the United States largely was able to do in the Gulf War of 1991.[3] In a crisis with nuclear weapons

[3] As David Alberts notes, "Information dominance would be of only academic interest, if we could not turn this information dominance into battlefield dominance." See Alberts, "The Future of Command and Control with DBK," in Dominant Battlespace Knowledge, ed. Stuart E.

available to the side against which infowar is used, crippling the foe's intelligence and command and control systems is an objective possibly at variance with controlling conflict and prevailing at an acceptable cost. And under some conditions of nuclear crisis management, crippling the C4ISR of the foe may be self-defeating. Deterrence, whether it is based on the credible threat of denial or retaliation, must be successfully communicated to – and believed by – the other side.[4]

The preceding discussion raises larger and long term issues for research agendas over the next decade or so. Contemporary dependence of U.S. and other militaries on the new information environment, together with the possibility that adversaries will seek to exploit that environment for vulnerabilities, calls into question established notions of deterrence, compellence, assurance and other aspects of military persuasion. A number of these fundamental concepts that became established anchors for discussions during the Cold War and the First Nuclear Age may now be challenged by info-driven concepts, events, and controversies. Future agendas for research and policy studies must include nonlinear and even chaotically-based models that are open to contrarian assumptions.

Johnson and Martin C. Libicki (Washington: National Defense Univ., 1996), pp. 77-102, citation p. 80.

[4] As Colin S. Gray has noted, "Because deterrence flows from a relationship, it cannot reside in unilateral capabilities, behavior or intentions. Anyone who refers to the deterrent policy plainly does not understand the subject." Gray, Explorations in Strategy (Westport, Conn.: Greenwood Press, 1996), p. 33.

References

Allison, Graham T. Essence of Decision: Explaining the Cuban Missile Crisis. Boston: Little, Brown, 1971.

Andrew, Christopher and Oleg Gordievsky. KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev. New York: Harper Perennial, 1990.

Arquilla, John. Worst Enemy: The Reluctant Transformation of the American Military. Chicago, Ill.: Ivan R. Dee, 2008.

Blair, Bruce G. The Logic of Accidental Nuclear War (Washington: Brookings Institution, 1993), p. 237.

Davis, Paul K., “Deterrence, Influence, Cyber Attack, and Cyberwar,” International Law and Politics, v. 47 (2015), pp. 327-355.

Davis, Paul K., Peter Wilson, Jeongeun Kim, and Junho Park, “Deterrence and Stability for the Korean Peninsula,” The Korean Journal of Defense Analysis, no. 1 (March 2016), pp. 1-23.

Forsyth Jr., B. Chance Saltzman, and Gary Schaub Jr., “Remembrance of Things Past: The Enduring Value of Nuclear Weapons,” Strategic Studies Quarterly, no. 1 (Spring, 2010), pp. 74-90.

Futter, Andrew, “The double-edged sword: US nuclear command and control modernization,” Bulletin of the Atomic Scientists, June 29, 2016, http://thebulletin.org/double-edged-sword-us-nuclear-command-and-control-modernization.html.

Futter, Andrew, “War Games Redux? Cyberthreats, U.S.-Russian strategic stability, and new challenges for nuclear security and arms control,” European Security (December 2015), published online, DOI:10.1080/09662839.2015.1112276.

Futter, Andrew. Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy. London: Royal United Service Institute for Defence and Security Studies, RUSI Occasional Paper, July 2016), www.rusi.org.

Gartzke, Erik and Jon R. Lindsay, "Thermonuclear cyberwar," Journal of Cybersecurity (2017), pp. 1-12, <doi:10.1093/cybsec/tyw017>

Gates, Robert M. From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War. New York: Simon and Schuster, 1996.

George, Alexander L., "A Provisional Theory of Crisis Management," in George, ed., Avoiding War: Problems of Crisis Management (Boulder, Colo.: Westview Press, 1991), pp. 22-27.

George, Alexander L., "The Cuban Missile Crisis: Peaceful Resolution Through Coercive Diplomacy," in George and William E. Simons, eds., The Limits of Coercive Diplomacy (2d ed.; Boulder, Colo.: Westview Press, 1994), pp. 111-132.

George, Alexander L., "The Tension Between "Military Logic" and Requirements of Diplomacy in Crisis Management," in George, ed., Avoiding War: Problems of Crisis Management, pp. 13-21.

Gray, Colin S. Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling. Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, April 2013.

Holsti, Ole R., "Crisis Decision Making," in Behavior, Society and Nuclear War, Philip E. Tetlock, et al., eds., (New York: Oxford Univ. Press, l989), I, 8-84.

Howard, Michael. Studies in War and Peace. New York: Viking Press, 1971.

Itar-Tass, "Putin calls to strengthen protection against cyber attacks," Itar-Tass, July 5, 2013, in Johnson's Russia List 2013 - #122, July 5, 2013, davidjohnson@starpower.net

Jabbour, Kamaal T. and E. Paul Ratazzi, “Does the United States Need a New Model for Cyber Deterrence?,” Ch. 3 in Adam B. Lowther, ed., Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century (New York: Palgrave-Macmillan, 2012), pp. 33-45.

Jablonsky, David. Strategic Rationality Is Not Enough: Hitler and the Concept of Crazy States (Carlisle Barracks, Pa.: USAWC, Strategic Studies Institute, 8 August 1991), esp. pp. 5-8 and pp. 31-37.

Jervis, Robert. The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon. Ithaca, N.Y.: Cornell Univ. Press, 1989.

Koshkin, Pavel, “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, http://russia-direct.org, August 1, 2013, in Johnson’s Russia List 2013 - #143, August 6, 2013, davidjohnson@starpower.net.

Kristensen, Hans M. U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning. Washington, D.C.: Natural Resources Defense Council, February 2005.

Lebow, Richard Ned and Janice Gross Stein. We All Lost the Cold War. Princeton, N.J.: Princeton Univ. Press, 1994.

Lebow, Richard Ned. Between Peace and War: The Nature of International Crisis. Baltimore: Johns Hopkins Univ. Press, 1981.

Libicki, Martin C. “The Convergence of Information Warfare,” Strategic Studies Quarterly, no. 1 (Spring 2017), pp. 49-65.

Libicki, Martin C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge: Cambridge University Press, 2007.

Libicki, Martin C. Crisis and Escalation in Cyberspace. Santa Monica, Calif.: RAND Corporation, 2012.

Libicki, Martin C. Cyberdeterrence and Cyberwar. Santa Monica, Calif.: RAND, 2009.

Lieven, D.C.B. Russia and the Origins of the First World War. New York: St. Martin's Press, 1983.

Magee, Maj. Clifford S., USMC, "Awaiting Cyber 9/11," Joint Force Quarterly, Issue 70, 3rd quarter 2013, pp. 76-82.

March, James G. and Herbert A. Simon. Organizations. New York: John Wiley and Sons, 1958.

Morgan, Patrick M. Deterrence: A Conceptual Analysis. Beverly Hills, Calif.: Sage Publications, 1983.

Payne, Keith B. Deterrence in the Second Nuclear Age. Lexington: Univ. Press of Kentucky, 1996.

Payne, Keith B., 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.

President's Foreign Intelligence Advisory Board, The Soviet "War Scare," February 15, 1990, http://nsarchive.gwu.edu/nukevault/ebb533-The-Able-Archer-War-Scare-Declassified-PFIAB-Report-Released/2012-0238-MR.pdf.

Quester, George H. Nuclear First Strike: Consequences of a Broken Taboo. Baltimore, Md.: Johns Hopkins University Press, 2006.

Ritter, Gerhard. The Schlieffen Plan: Critique of a Myth. London: Oswald Wolff, 1958.

Sagan, Scott D. Moving Targets: Nuclear Strategy and National Security. Princeton, N.J.: Princeton Univ. Press, 1989.

Sanger, David E. and William J. Broad, “Trump Inherits a Secret Cyberwar Against North Korean Missiles,” New York Times, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=0

Sanger, David. E., “N.S.A. Leaks Make Plan for Cyberdefense Unlikely,” New York Times, August 12, 2013, http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html, downloaded August 13, 2013.

Singer, P.W. and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, 2014.

Thomas, Timothy L. Cyber Silhouettes: Shadows Over Information Operations. Ft. Leavenworth, Kansas: Foreign Military Studies Office, 2005.

Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (Washington, D.C.: U.S. Department of State, April 8, 2010), http://www.state.gov/documents/organization/140035.pdf.

Williams, Phil. Crisis Management. New York: John Wiley and Sons, l976.