

Nuclear Crisis Management and “Cyberwar” Phishing for Trouble?

Stephen J. Cimbala

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 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 discussion below proceeds toward that end, by looking at relevant concepts and examples including information warfare, crisis management, the link between cyberwar and nuclear crisis management, and its implications.

Information Warfare

Information warfare can be defined as activities by a state or nonstate actor to exploit the content or processing of information to its advantage in time of peace, crisis, or war and to deny potential or actual foes the ability to exploit the same means against itself.¹ This is an expansive, and permissive, definition, although it has an inescapable bias toward military- and security-related issues.² Information warfare can include both cyberwar and netwar. *Cyberwar*, according to John Arquilla and David Ronfeldt, is a comprehensive, information-based approach to battle, normally discussed in terms of high-intensity or mid-intensity conflict.³ *Netwar* is defined by the same authors as a comprehensive, information-based approach

Stephen J. Cimbala, PhD, is Distinguished Professor of Political Science at Penn State University–Brandywine. Dr. Cimbala is the author of numerous works in the fields of national security policy, nuclear arms control, and other topics. The award-winning Penn State teacher has also served as a consultant for various US government agencies and private contractors. His recent publications include *The George W. Bush Defense Program* (Potomac Publishers) and, with Peter Forster, *Multinational Military Intervention* (Ashgate).

to societal conflict. Cyberwar is more the province of states and conventional wars; netwar more characteristic of nonstate actors and unconventional wars.⁴

Cyberwar is distinct from the problem of deterrence, although there are obvious “real world” overlaps. The concept of “cyber deterrence” involves degrees of uncertainty and complexity, including a leap of analytic faith beyond what we know about conventional or nuclear deterrence. Cyber attacks generally obscure the identity of the attackers, can be initiated from outside of or within the defender’s state territory, are frequently transmitted through third parties without their complicity or knowledge, and can sometimes be repeated almost indefinitely by skilled attackers, even against agile defenders. In addition, the contrast between the principles of cyber deterrence and nuclear deterrence encourages modesty in the transfer of principles from the latter to the former.⁵

Added to this is the civil-military interaction that will take place between designated military cyber samurai and their civilian DoD (and other) superiors in the chain of command who may be cyber-challenged or even pre-cyber in their understanding of information technology and its impacts. The nexus among new information capabilities, their implications for decision making, and their potential vulnerabilities to attack may be comprehended by a select few, if at all. But politics will ultimately drive all strategy—including cyber strategy—for better or worse. At its apex, strategy is the bridge that connects political objectives with military operations, whether digital or kinetic.⁶

Crisis Management—Nuclear and Other

Crisis management, including nuclear crisis management, is both a competitive and cooperative endeavor between military adversaries. A *crisis* is, by definition, a time of great tension and uncertainty.⁷ Threats are imminent, and time pressure on policymakers seems intense. Each side has objectives it wants to attain and values it deems important to protect. During a crisis, state behaviors are especially interactive and interdependent with those of another state. It would not be far-fetched to refer to this interdependent stream of interstate crisis behaviors as a system, provided the term *system* is not understood as an entity completely separate from the state or individual behaviors that comprise it. The system aspect

implies reciprocal causation of the crisis behaviors of "A" by "B," and vice versa.

One aspect of crisis management is the deceptively simple question: What defines a crisis as such? When does the latent capacity of the international order for violence or hostile threat assessment cross over into the terrain of actual crisis behavior? A breakdown of general deterrence in the system raises threat perceptions among various actors, but it does not guarantee that any particular relationship will deteriorate into specific deterrent or compellent threats. Patrick Morgan's concept of "immediate" deterrence failure is useful in defining the onset of a crisis: specific sources of hostile intent have been identified by one state with reference to another, threats have been exchanged, and responses must now be decided upon.⁸ The passage into a crisis is equivalent to the shift from Hobbes' world of omnipresent potential for violence to the actual movement of troops and exchanges of diplomatic demarches.

All crises are characterized to some extent by a high degree of threat, short time for decision, and a "fog of crisis" reminiscent of Clausewitz's "fog of war" that confuses crisis participants about what is happening. Before the discipline of crisis management was ever invented by modern scholarship, historians had captured the rush-to-judgment character of much crisis decision making among great powers.⁹ The influence of nuclear weapons on crisis decision making is therefore not easy to measure or document, because the avoidance of war can be ascribed to many causes. The presence of nuclear forces obviously influences the degree of destruction that can be done should crisis management fail. Short of that catastrophe, the greater interest of scholars is in how the presence of nuclear weapons might affect the decision-making process itself in a crisis. The problem is conceptually elusive: there are so many potentially important causal factors relevant to a decision with regard to war or peace. History is full of dependent variables in search of competing explanations.

Another question involves the "level of analysis" problem for explanations of, and predictions about, crisis management. Who, for example, is likely to be affected by cyber attacks during a nuclear crisis? Disruption of communications or data flows to enemy senior policymakers and force commanders is a candidate stratagem for an attacker. But the head of the snake is not necessarily the most vulnerable part of a bureaucracy or political system. Advanced nuclear powers will have both political orders of succession and delegations of military command authority in place against

decapitation attacks. Cyber mischief might be more efficiently targeted on the opponent's civilian infrastructure, including that part of the civilian infrastructure that overlaps with military use. An example of this kind of attack would be efforts to disrupt information or communication flows in the electrical power grids or financial systems of another state by means of viruses, Trojan horses, botnets, distributed denial-of-service (DDOS) attacks, or other deceptive or destructive measures.

Cyber strikes could also be aimed directly at the opponent's nuclear infrastructure in time of peace or war. For example, the "Stuxnet" virus that attacked Iran's nuclear facilities in 2010 was assumed by some to have been created by Israel and/or the United States. According to a German computer expert who was among the first to analyze the Stuxnet code, the virus (or worm) may have set back Iran's nuclear program by two years. Describing the Stuxnet worm as the most "advanced and aggressive malware in history," the German expert added, "This was nearly as effective as a military strike, but even better since there are no fatalities and no full-blown war."¹⁰ This cyber attack took place in "peacetime" and reportedly will require considerable time and effort for Iran to remove the virus, replace affected computer equipment, and rebuild centrifuges at its uranium enrichment facility at Natanz.¹¹

Suppose an attack of this nature had been attempted by unknown parties after Iran had already become a nuclear weapons state and entered into a crisis with Israel. And the phrase "unknown parties" is not an idle one. Third parties could conceivably use cyber strikes to provoke catalytic wars between two rivals—say, for example, Serbians or Balts firing cyber bullets into a Russo-Georgian clash or Japanese or Chinese hackers cyber surfing during a war between North and South Korea. The sources of third-party disruption (either condoned by governments or based on freelancers with their own political agendas) against a colliding dyad of state actors could also be nonstate actors—including terrorists, criminals, or "super-empowered individuals"—piggybacking on crises for their own reasons.¹² Nor is it inconceivable that during a crisis two disputants or third parties might fire up their own equivalents of WikiLeaks and disclose potentially incriminating details about other states' policymaking or force planning, or about their leaders' personality flaws. Throw "NikiLeaks" into the Cuban missile crisis or "GorbyLeaks" into the August 1991 failed putsch in Moscow, and stir the historically counterfactual mix.

Attributes for Successful Crisis Management

The first requirement of successful crisis management is communications transparency. Transparency includes clear signaling and undistorted communications. Signaling refers to the requirement that each side must send its estimate of the situation to the other. It is not necessary for the two sides to have identical or even initially complementary interests. But a sufficient number of correctly sent and received signals are prerequisite to effective transfer of enemy goals and objectives from one side to the other. If signals are poorly sent or misunderstood, steps taken by the sender or receiver may lead to unintended consequences, including miscalculated escalation.

Communications transparency also includes high-fidelity communication between adversaries and within the respective decision-making structures of each side. High-fidelity communication in a crisis can be distorted by everything that might interfere physically, mechanically, or behaviorally with accurate transmission. Electromagnetic pulses that disrupt communication circuitry or physical destruction of communication networks are obvious examples of impediments to high-fidelity communication. Cultural differences that prevent accurate understanding of shared meanings between states can confound deterrence as practiced according to one side's theory. As Keith Payne notes, with regard to the potential for deterrence failure in the post-Cold War period:

Unfortunately, our expectations of opponents' behavior frequently are unmet, not because our opponents necessarily are irrational but because we do not understand them—their individual values, goals, determination, and commitments—in the context of the engagement, and therefore we are surprised when their "unreasonable" behavior differs from our expectations.¹³

A second requirement of successful crisis management is reducing time pressure on policymakers and commanders so no unintended, provocative steps are taken toward escalation mainly or solely as a result of a misperception that "time is up." Policymakers and military planners are capable of inventing fictive worlds of perception and evaluation in which "H-hour" becomes more than a useful benchmark for decision closure. In decision pathologies possible under crisis conditions, deadlines may be confused with policy objectives themselves: ends become means, and means, ends. For example: the war plans of the great powers in July 1914 contributed to a shared self-fulfilling prophecy among leaders in Berlin, St. Petersburg, and Vienna that only by prompt mobilization and attack could decisive

losses be avoided in war. Plans predicated on the determinism of mobilization timetables proved insufficiently adaptive for policymakers who wanted to slow down the momentum of late July and early August toward an irrevocable decision in favor of war.

One result of compressing the decision time in a crisis, compared to typical peacetime patterns, is that the likelihood of Type I (undetected attack) and Type II (falsely detected attack) errors increases. Tactical warning and intelligence networks grow accustomed to the routine behavior of other state forces and may misinterpret nonroutine behavior. Unexpected surges in alert levels or uncharacteristic deployment patterns could trigger misreadings of indicators by tactical operators. As Bruce Blair has argued:

In fact, one distinguishing feature of a crisis is its murkiness. By definition, the Type I and Type II error rates of the intelligence and warning systems rapidly degrade. A crisis not only ushers in the proverbial fog of crisis symptomatic of error-prone strategic warning but also ushers in a fog of battle arising from an analogous deterioration of tactical warning.¹⁴

A third attribute of successful crisis management is that each side should be able to offer the other a safety valve or a face-saving exit from a predicament that has escalated beyond its original expectations. The search for options should back neither crisis participant into a corner from which there is no graceful retreat. For example, during the Cuban missile crisis of 1962, President Kennedy was able to offer Soviet premier Khrushchev a face-saving exit from his overextended missile deployments. Kennedy publicly committed the United States to refrain from future military aggression against Cuba and privately agreed to remove and dismantle Jupiter medium-range ballistic missiles previously deployed among its NATO allies.¹⁵ Kennedy and his inner circle recognized, after some days of deliberation and clearer focus on the Soviet view of events, that the United States would lose, not gain, by a public humiliation of Khrushchev that might, in turn, diminish Khrushchev's interest in any mutually agreed solution to the crisis.

A fourth attribute of successful crisis management is that each side maintains an accurate perception of the other's intentions and military capabilities. Clarity of perception becomes difficult during a crisis because, in the heat of a partly competitive relationship and a threat-intensive environment, intentions and capabilities can change. Robert Jervis warned that Cold War beliefs in the inevitability of war might have created a self-fulfilling prophecy:

The superpowers' beliefs about whether or not war between them is inevitable create reality as much as they reflect it. Because preemption could be the only rational reason to launch an all-out war, beliefs about what the other side is about to do are of major importance and depend in large part on an estimate of the other's beliefs about what the first side will do.¹⁶

Intentions can change during a crisis if policymakers become more optimistic about gains or more pessimistic about potential losses during the crisis. Capabilities can change due to the management of military alerts and the deployment or other movement of military forces. Heightened states of military readiness on each side are intended to send a two-sided signal: of readiness for the worst if the other side attacks, and of a non-threatening steadiness of purpose in the face of enemy passivity. This mixed message is hard to send under the best of crisis management conditions, since each state's behaviors and communications, as observed by its opponent, may not seem consistent. Under the stress of time pressures and of military threats, different parts of complex security organizations may be making decisions from the perspective of their narrowly defined, bureaucratic interests. These bureaucratically chosen decisions and actions may not coincide with the policymakers' intent, nor with the decisions and actions of other parts of the government. As Alexander George has explained:

It is important to recognize that the ability of top-level political authorities to maintain control over the moves and actions of military forces is made difficult because of the exceedingly large number of often complex standing orders that come into effect at the onset of a crisis and as it intensifies. It is not easy for top-level political authorities to have full and timely knowledge of the multitude of existing standing orders. As a result, they may fail to coordinate some critically important standing orders with their overall crisis management strategy.¹⁷

As policymakers may be challenged to control numerous and diverse standard operating procedures, political leaders may also be insufficiently sensitive to the costs of sudden changes in standing orders or unaware of the rationale underlying those orders. For example, heads of state or government may not be aware that more permissive rules of engagement for military forces operating in harm's way come into play once higher levels of alert have been authorized.¹⁸

Cyberwar plus Nuclear Crisis Management

This section discusses how cyberwar might adversely affect nuclear crisis management. Readers are advised, however, that history is indeterminate. It might turn out that, in some fortuitous cases, the United States could use nuclear deterrence and cyberwar as joint multipliers toward a successful outcome in crisis or war. For example, in facing down an opponent with a comparatively small or no nuclear arsenal and inferior conventional strike capabilities, the United States or another power could employ information warfare aggressively “up front” while forgoing explicit mention of its available nuclear capability. Russia’s five-day war against Georgia in August 2008 involved obvious cyber attacks as well as land and air operations, but no explicit nuclear threats. On the other hand, had Georgia already been taken into membership by NATO prior to August 2008 or had Russo-Georgian fighting spread into NATO member-state territory, the visibility of Russia’s nuclear arsenal as a latent and potentially explicit threat would have been much greater.

Notwithstanding the preceding disclaimers, information warfare has the potential to attack or disrupt successful crisis management on each of four dimensions. First, it can muddy the signals being sent from one side to the other in a crisis. This 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 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.

Infowar can also destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is to disrupt communication links between policymakers 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 pre-delegated 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. During the Cold War, for example, disrupted communications between the US National Command Authority and ballistic missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers 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 this literally, or it may affect the perceived timelines within which the policymaking process can make its decisions. Once either side sees parts of its command, control, and communications (C³) 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 C³ system could have prevented competent execution of parts of the SIOP (the strategic nuclear war plan). The SIOP 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 infowar on nuclear crisis management is that it may reduce the search for available alternatives to the few and desperate. Policymakers 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:

A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of

launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.²⁰

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.²¹ In civil-military command and control systems under the stress of nuclear crisis decision making, the first available alternative may quite literally be the last; or so policymakers and their military advisors may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, 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.²²

Fourth and finally on the issue of crisis management, infowar 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 crisis demonstrates the possible side effects of simple misunderstanding and noncommunication on US crisis management. At the most tense 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.²³ Fortunately Moscow 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 policymakers who failed to appreciate the risk of "normal" reconnaissance under these extraordinary conditions.

Further Issues and Implications

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.²⁴ 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 intimidate but with no immediate destruction; and a conventional strike mistaken, at least initially, for a nuclear one. As George Quester has noted:

The United States and other powers have developed some very large and powerful conventional warheads, intended for destroying the hardened underground bunkers that may house an enemy command post or a hard-sheltered weapons system. Such "bunker-buster" bombs radiate a sound signal when they are used and an underground seismic signal that could be mistaken from a distance for the signature of a small nuclear warhead.²⁵


The dominant scenario of a general nuclear war between the United States and the Soviet Union preoccupied Cold War policymakers, and under that assumption concerns about escalation control and war termination were swamped by apocalyptic visions of the end of days. The second nuclear age, roughly coinciding with the end of the Cold War and the demise of the Soviet Union, offers a more complicated menu of nuclear possibilities and responses.²⁶ Interest in the threat or use of nuclear weapons by rogue states, by aspiring regional hegemons, or by terrorists abetted by the possible spread of nuclear weapons among currently nonnuclear weapons states stretches the ingenuity of military planners and fiction writers.

In addition to the world's worst characters engaged in nuclear threat of first use, there is also the possibility of backsliding in political conditions, as between the United States and Russia, or Russia and China, or China and India (among current nuclear weapons states). Politically unthinkable conflicts of one decade have a way of evolving into the politically unavoidable wars of another—World War I is instructive in this regard. The war between Russia and Georgia in August 2008 was a reminder that local

conflicts on regional fault lines between blocs or major powers have the potential to expand into worse.

If information operations might get in the way of de-escalation during a nuclear crisis, then why not just omit them? The political desire to do so conflicts with the military necessity for timely information gathering, assessment, and penetration of enemy networks to accomplish two necessary, but somewhat opposed, missions. First, each side would want to anticipate correctly the timing and character of the other's decision for nuclear first use—and, if possible, to throw logic bombs, Trojan horses, electronic warfare, or other impediments in the way (or if finesse is not preferred, bombing the relevant installations is always an option, although an obviously provocative one). The second, and somewhat opposed, mission is to communicate reliably with the other side one's preference for de-escalation, willingness to do so if reciprocity can be obtained, and awareness of the possibility that the situation will shortly get out of hand.

Conclusion

The objective of cyberwar in conventional conflicts 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 1991.²⁷ In a crisis with nuclear weapons 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. Whether nuclear or other deterrence can work in a particular cyber context is more dependent upon political, as opposed to military, variables. As Lawrence Freedman has noted, strategic studies have sometimes been too preoccupied with military capabilities and thus insufficiently sensitive to the point that “the balance of terror rests upon a particular arrangement of political relations as much as on the quantity and quality of the respective nuclear arsenals.”²⁸ 

Notes

1. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), argues that strategic cyberwar is unlikely to be decisive, although operational cyberwar has an important niche role. Libicki also warns that deterrence in the cyber realm is unlikely to behave as it does in

other domains, including conventional war and nuclear deterrence. See also Will Goodman, “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–35. Goodman argues that cyberspace poses unique challenges for deterrence but not necessarily impossible ones.

2. Concepts related to information warfare are discussed in David S. Alberts, John J. Garstka, Richard E. Hayes, and David T. Signori, *Understanding Information Age Warfare*, 3rd ed. (Washington: DoD, October 2004), esp. 53–94; and Alberts, Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 6th printing (Washington: DoD, April 2005), esp. 87–122. Col Thomas X. Hammes, USMC, retired, discusses the Pentagon’s Joint Publication 3-13, *Information Operations*, and the DoD understanding of information in modern warfare in Hammes, “Information Warfare,” chap. 4, in *Ideas as Weapons: Influence and Perception in Modern Warfare*, eds. G. J. David Jr. and T. R. McKeldin III (Washington: Potomac Books, 2009), 27–34. See also John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), esp. chaps. 6–7. For perspective on the role of information operations in Russian military policy, see Timothy L. Thomas, “Russian Information Warfare Theory: The Consequences of August 2008,” chap. 4, in *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, eds. Stephen J. Blank and Richard Weitz (Carlisle, PA: Strategic Studies Institute, US Army War College, July 2010); and Thomas, “Russia’s Asymmetrical Approach to Information Warfare,” chap. 5, in *The Russian Military into the Twenty-first Century*, ed. Stephen J. Cimbala (London: Frank Cass, 2001), 97–121.

3. Richard A. Clarke, former counterterrorism coordinator for the George W. Bush and Clinton administrations, and coauthor Robert K. Knake include both cyberwar and netwar activities, as defined by John Arquilla and David Ronfeldt in their concept of “cyber war.” See Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: HarperCollins, 2010). For an introduction to this topic, see John Arquilla and David Ronfeldt, “A New Epoch—and Spectrum—of Conflict,” in *In Athena’s Camp: Preparing for Conflict in the Information Age*, ed. Arquilla and Ronfeldt (Santa Monica: RAND, 1997), 1–22. See also, on definitions and concepts of information warfare, Martin C. Libicki, *What Is Information Warfare?* ACIS Paper 3 (Washington: National Defense University, August 1995); Libicki, *Defending Cyberspace and other Metaphors* (Washington: NDU, Directorate of Advanced Concepts, Technologies, and Information Strategies, February 1997); Arquilla and Ronfeldt, *Cyberwar Is Coming!* (Santa Monica: RAND, 1992); and David S. Alberts, *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative* (Washington: NDU, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, April 1996).

4. John Arquilla and David Ronfeldt, “The Advent of Netwar,” in *In Athena’s Camp*, 275–94. With regard to the tasks for US Cyber Command (established in 2009) and its implications for the national security decision-making process, see Wesley R. Andruess, “What U.S. Cyber Command Must Do,” *Joint Force Quarterly*, issue 59 (4th Quarter 2010): 115–20.

5. Libicki, *Cyberdeterrence and Cyberwar*, xvi.

6. This concept is elegantly explained in Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010), esp. 96–120.

7. For pertinent concepts, see Alexander L. George, “A Provisional Theory of Crisis Management,” in *Avoiding War: Problems of Crisis Management*, ed. Alexander L. George (Boulder, CO: Westview Press, 1991), 22–27, for the political and operational requirements of crisis management; and George, “Strategies for Crisis Management,” *ibid.*, 377–94, for descriptions of offensive and defensive crisis management strategies. See also Ole R. Holsti, “Crisis Decision Making,” in *Behavior, Society and Nuclear War*, ed. Philip E. Tetlock et al. (New York: Oxford University Press, 1989), I, 8–84; and Phil Williams, *Crisis Management* (New York: John Wiley

and Sons, 1976). See also George, "Coercive Diplomacy: Definition and Characteristics," in *The Limits of Coercive Diplomacy*, 2d ed., George and William E. Simons (Boulder, CO: Westview Press, 1994), esp. 8–9; and in the same volume, George, "The Cuban Missile Crisis: Peaceful Resolution through Coercive Diplomacy," 111–32.

8. See Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage Publications, 1983); and Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton, NJ: Princeton University Press, 1994), 51–55.

9. For example, see Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981); Michael Howard, *Studies in War and Peace* (New York: Viking Press, 1971), 99–109; Gerhard Ritter, *The Schlieffen Plan: Critique of a Myth* (London: Oswald Wolff, 1958); and D. C. B. Lieven, *Russia and the Origins of the First World War* (New York: St. Martin's Press, 1983).

10. Yaakov Katz, "Stuxnet virus set back Iran's nuclear program by 2 years," *Jerusalem Post*, 15 December 2010, <http://www.jpost.com/LandedPages/PrintArticle.aspx?id=199475>.

11. *Ibid.*

12. On the problem of attributing cyber attacks to their sources, see Libicki, *Cyberdeterrence and Cyberwar*, chap. 3, esp. 41–49 and *passim*.

13. Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996), 57. See also David Jablonsky, *Strategic Rationality Is Not Enough: Hitler and the Concept of Crazy States* (Carlisle, PA: Strategic Studies Institute, 8 August 1991), esp. 5–8, 31–37.

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

15. Lebow and Stein, *We All Lost the Cold War*, 122–23.

16. Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989), 183.

17. Alexander L. George, "The Tension Between 'Military Logic' and Requirements of Diplomacy in Crisis Management," in *Avoiding War: Problems of Crisis Management*, 13–21, citation 18.

18. *Ibid.*

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. Blair, *Logic of Accidental Nuclear War*, 252.

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

22. Lebow and Stein, *We All Lost the Cold War*, 335–36.

23. Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown and Co., 1971), 141. See also Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton, NJ: Princeton University Press, 1989), 147; and Lebow and Stein, *We All Lost the Cold War*, 342.

24. For pertinent scenarios, see George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore: Johns Hopkins University Press, 2006), 24–52. An escalation ladder with 44 rungs and seven major groups, from subcrisis maneuvering through civilian central wars with nuclear weapons, is defined in Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Frederick S. Praeger, 1965), esp. 37–51.

25. *Ibid.*, 27.

26. Assessments of deterrence before and after the Cold War appear in: Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); Colin S. Gray, *The Second Nuclear Age* (Boulder, CO: Lynne Rienner, 1999); Keith B. Payne, *Deterrence in the Second*

Nuclear Crisis Management and “Cyberwar”

Nuclear Age (Lexington: University Press of Kentucky, 1996); Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989); and Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St. Martin's Press, 1981, 1983). Michael Krepon emphasizes that deterrence in the first nuclear age “worked,” to the extent that it did so, only in conjunction with containment, diplomacy, military strength, and arms control. See Krepon, *Better Safe than Sorry: The Ironies of Living with the Bomb* (Stanford, CA: Stanford University Press, 2009), passim.

27. As David Alberts points out, “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*, eds. Stuart E. Johnson and Martin C. Libicki (Washington: National Defense University, 1996), 77–102, citation p. 80.

28. Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave Macmillan, 2003), 463.