# Nuclear Crisis Management and Deterrence: Stalked by Cyberwar?

Stephen J. Cimbala

Cyberwar, preceding or during nuclear crises, can marginally or even fatally strain the requirements of nuclear deterrence stability and is capable of disrupting the communications between governments in times of crisis or confusing their assessments of ongoing events. This discussion considers the requirements for successful nuclear crisis management, the possible vulnerabilities induced by cyberwar, and the scenarios in which opportunistic failure is possible.

**Keywords**: Cyberwar, information warfare, deterrence, crisis stability, nuclear war, management, command-control, networks, communications, escalation control

## Introduction

The information age and its military-technical applications obviously will cause some changes in the character and attributes of nuclear deterrence. Exactly how cyberwar and nuclear deterrence might coexist or compete as paradigms for policy consideration is less apparent. Although cyber operations differ from kinetic operations, the various components of information warfare "should now increasingly be considered elements of a larger whole rather than

Stephen J. Cimbala is Distinguished Professor of Political Science at Penn State Brandywine. The author gratefully acknowledges Paul Davis, Andrew Futter, Lawrence Korb, and Timothy Thomas for insights into the topic of this study. They bear no responsibility for its content.

separate specialties that individually support kinetic military operations."[1] For example, Pavel K. Baev suggests that a new blend of corruption, intelligence operations, cyberattacks, and propaganda offensives is now the "trademark" of Russian foreign policy and requires a new kind of Western deterrence.[2]

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 unwelcomed hybrid. Crises by definition are exceptional events. No cold war crisis between states armed with both twenty-first century information weapons and nuclear weapons has yet occurred. In addition, the nuclear-cyber relationship has special significance for the United States and Russia: The two powers hold more than 90 percent of the world's nuclear weapons, and both have advanced offensive and defensive cyberwar capabilities.[3] The

1 Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* no. 1 (Spring 2017), p. 50 and see also pp. 49–65. In this study I use the terms "information warfare" and "cyberwar" interchangeably and generically, although some cyber grammarians might insist that "cyberwar" 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 American Military* (Chicago: Ivan R. Dee, 2008), ch. 6–7, in addition to sources in later notes.

2 Pavel K. Baev, "Corruption Spoils Every Attempt to Cooperate With Russia," *Eurasia Daily Monitor*, July 17, 2017, https://jamestown.org/analyst/pavel-k-baev, accessed August 7, 2017.

3 For a discussion of Russian cyber capabilities and doctrines, see Timothy L. Thomas, *Russia: Military Strategy—Impacting 21st Century Reform and Geopolitics* (Ft. Leavenworth, Kansas: Foreign Military Studies Office, 2015), pp. 253–299; for pertinent insights on the topic of cyber war and nuclear war, see Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar*, Journal of Cybersecurity* (2017), pp. 1–12, https://doi:10.1093/cybsec/tyw017; Andrew Futter, "The Double-Edged Word: 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; Andrew Futter, "Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy," *RUSI Occasional Paper* (July 2016), https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf; and Andrew Futter, "War Games Redux? Cyberthreats, U.S.-Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control," *European Security* (December 2015): 163–180.

discussion below proceeds toward that end in several steps. We consider concepts and definitions of crisis management; attributes and requirements for successful crisis management; challenges posed by information operations and cyberwar for nuclear crisis stability; and, finally, some possibly dangerous scenarios in which cyber-spiked nuclear crisis management might be especially problematic.

## Crisis Management

### *Concepts and Definitions*

Crisis management, including nuclear crisis management, is both a competitive and cooperative endeavor between military adversaries. By definition, a crisis is a time of great tension and uncertainty.[4] Threats are in the air and the time pressure on policymakers seems intense. Each side has objectives that it wants to attain and values or interests that it deems important to protect. During a crisis state, behaviors are especially interactive and interdependent with those of another state. It would not be too farfetched 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 compose 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

4 For the political and operational requirements of crisis management, see Alexander L. George, "A Provisional Theory of Crisis Management," in *Avoiding War: Problems of Crisis Management*, ed. Alexander L. George (Boulder: Westview Press, 1991), pp. 22–27; for descriptions of offensive and defensive crisis management strategies, see Alexander L. George, "Strategies for Crisis Management," in *Avoiding War*, ed. Alexander L. George, pp. 377–394. 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), 1:8–84; and Phil Williams, *Crisis Management* (New York: John Wiley and Sons, 1976). See also Alexander L. George, "The Cuban Missile Crisis: Peaceful Resolution Through Coercive Diplomacy," in *The Limits of Coercive Diplomacy,* ed. Alexander L. George and William E. Simons, 2nd ed.(Boulder: Westview Press, 1994), pp. 111–132.

compellent threats. Patrick Morgan's concept of "immediate" deterrence failure is useful in defining the onset of a crisis: One state identifies specific sources of hostile intent from another, they exchange threats, and they must now determine responses.[5] 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 (rapid escalatory momentum, with the meaningful and imminent risk of reaching more intensive hostilities; yet neither party has elected full hostilities and both parties still prioritize a de-escalation), limited time for decision, and a "fog of crisis" reminiscent of Clausewitz's "fog of war" that confuses crisis participants about what is happening. Before modern scholars had even invented the discipline of crisis management, historians had captured the rush-to-judgment character of much crisis decision making among the great powers.[6] 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 could take place should crisis management fail and is therefore often a de-escalatory factor. Short of that catastrophe, scholars are greatly interested in how the presence of nuclear weapons might affect the decision-making process during a crisis. The problem is conceptually elusive as many potentially important causal factors are relevant to a decision about war or peace. History is full of dependent variables in search of competing explanations.

## Crisis Management: The Requirements

First, successful crisis management requires communications transparency, although this generalization acknowledges that vague or oblique communication

5 See Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills: Sage Publications, 1983) and Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton: Princeton University Press, 1994), pp. 351–355.

6 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), pp. 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).

is useful in specific cases, such as the way Iran behaved in the crisis over its nuclear project. Transparency includes clear signaling and undistorted communications. Signaling refers to the requirement that each side must send the other its estimate of the situation. Although it is not necessary for the two sides to have identical or even initially complementary interests, a sufficient number of correctly sent and received signals is prerequisite to effectively transmit goals and objectives from one side to the other. If signals are poorly sent or misunderstood, steps taken by the sender or receiver may cause unintended consequences, including miscalculated escalation. The gravity of the situation may require complete transparency, although there are many examples in which only partial communication sufficed. Moreover, communication is not necessarily verbal; rather, it can be kinetic as in the assembly of forces or military preparations and signals of resolve.

Communications transparency also includes high-fidelity and technically dependable communication between adversaries and within the decision-making structures of each side. Everything that might interfere physically, mechanically, or behaviorally with accurate transmission can distort high-fidelity communication in a crisis. 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 between states can confound deterrence as practiced according to one side's theory. As Keith B. Payne notes about 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."[7]

Second, successful crisis management requires that the pressure of time exerted upon policymakers and commanders be minimized so that they do not take unintended, provocative steps toward escalation because they have misperceived that "time is up." Time pressure is one thing, but unintended

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

steps are another. Policymakers and military planners are capable of inventing fictive worlds of perception and evaluation in which the "H hour" becomes more than a useful benchmark for decision closure. In the decision pathologies possible in crisis conditions, deadlines may be confused with policy objectives themselves: Ends become means, and means become 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 they avoid decisive losses in war. The policymakers found that the structure of the mobilization timetables was not flexible enough for slowing down the momentum of late July and early August toward an irrevocable decision in favor of war.

One result of compressing 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 states' forces and may misinterpret nonroutine behavior. Unexpected surges in alert levels or uncharacteristic deployment patterns could trigger tactical operators to misread the indicators. As Bruce G. 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."[8]

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 expectations. In some cases, a graceful or cost-beneficial exit may not be available to either side; it will then become a competition in minimizing risk. The search for options should not back either 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

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

missiles previously deployed among the United States' NATO allies.[9] After some days of deliberation and having a clearer focus of the Soviet view of events, Kennedy and his inner circle recognized that publicly humiliating Khrushchev would cause the United States to lose and not gain, which in turn could diminish Khrushchev's interest in achieving any mutual agreement to resolving the crisis.

A fourth characteristic of successful crisis management is that each side maintains an accurate perception of the other side's intentions and military capabilities, including the opponent's susceptibilities and vulnerabilities. For example, posturing as if one is willing to escalate to war can sometimes terminate a crisis on favorable terms. Estimating opponents' intentions and capabilities becomes difficult during a crisis, however, because intentions and capabilities can change in the heat of a partly competitive relationship and a threat-intensive environment. Robert Jervis warned that beliefs in the inevitability of war during the Cold War might have created a self-fulfilling prophecy, writing that, "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."[10]

Intentions can shift during a crisis if policymakers become more optimistic about gains or more pessimistic about potential losses. The management of military alerts and the deployment or other movement of military forces can change capabilities. 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 nonthreatening steadiness of purpose in the face of enemy passivity. This mixed message is hard to relay under the best of crisis management conditions, since a state's behaviors and communications may seem inconsistent as observed by its opponent. Under the stress of time pressures and military threats, different wings of complex security organizations may make decisions from the perspective of their narrowly defined, bureaucratic interests. These decisions and actions may

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

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

not reflect the policymakers' intent or may not be done in coordination with the decisions and actions of other parts of government. As Alexander L. 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.[11]

As policymakers may be challenged to control numerous and diverse standard operating procedures, political leaders may also be insensitive 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 often come into play once higher levels of alert have been authorized.[12] In other cases, however, control is fairly tight. Crisis managers soon learn on the job an important lesson about the distinction between a crisis and an actual outbreak of war: The jump from one to another is less of a dichotomy than it is a continuum, and the end stage of crisis is not obvious until the fateful steps into war have been irrevocably taken. For example, heads of state in Europe in 1914 were at first overconfident in their ability to manage a crisis short of war, but as events gradually eluded them, they became more fatalistic in a self-defeating manner.

## Potential Disrupters

Information or cyber warfare has the potential to attack or to disrupt successful crisis management on each of the preceding attributes.[13] First, cyber warfare

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

12 George, "Tension Between Military Logic and Requirements of Diplomacy."

13 For useful definitions of cyberattack and cyberwar, see Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *International Law and Politics* 47 (2015): 327–355.

can muddy the signals being sent from one side to the other during a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other's communications networks.[14] 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, meet unexpected resistance, and cause a much more dangerous situation to develop. There is also the possibility of cyber-enabled preemption to disable enemy nuclear missiles before they reach the launch pad or during the launch itself. The United States apparently has used such "left-of-launch" techniques against North Korea.[15] During a nuclear crisis, would such a move be accepted by the attacked party as one of intimidation and deterrence? Or on the contrary, would offensive cyberwar against missile launches prompt a nuclear first use or first strike by the defender out of fear of losing its retaliatory capability?

Cyberwar can also destroy or disrupt communication channels necessary for successful crisis management. It can disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. This disruption might not be altogether intentional but could result from having earlier implanted malware that activated either unexpectedly or without the full control of its creators. From the standpoint of civil-military relations, two kinds of unanticipated problems are possible under these conditions. First, political leaders may have pre-delegated limited authority for nuclear release or launch under restrictive conditions:

14 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.

15 David E. Sanger 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. See also, Jesse T. Wasson and Christopher E. Bluesteen, "Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems," (Paper presented at the Annual Conference of International Studies Association, Baltimore, MD, 2017).

Only when these few conditions are met, according to the protocols of pre-delegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Clogged, destroyed, or disrupted communications could prevent the leaders from knowing that military commanders have perceived a situation far more desperate than it really is, and thus permissive of nuclear initiative. For example, during the Cold War, disrupted communications between the US National Command Authority and ballistic missile submarines, once the latter came under attack, could have led submarine officers and crew to jointly decide to launch in the absence of contrary instructions.

Critical reviewers of an earlier draft of this article pointed out correctly that it seemed paradoxical to assume that leaders would authorize cyberwar during a crisis that they would otherwise prefer to terminate before it resulted in war. It would make more sense, at least in principle, to conduct cyberwar in conjunction with a first strike but not before it. I concede the logic, but it has another side. First, cyberattacks during a crisis might not only be a means of creating technical glitches in the enemy's information systems and decision-making process but could also be a form of strategic bargaining for a more advantageous conflict termination or—if it came to that—a more favorable war outcome. For example, "left-of-launch" techniques for disrupting the networks that support missile launch systems could support one side's antimissile defense capabilities and increase the other side's self-doubts about favorable performance of its ballistic missile attacks.

Second, information warfare during a crisis will almost certainly increase the time pressure in which political leaders operate. It may do this literally or it may affect the perceived time frame during which the policymakers can make their 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 the United States' strategic nuclear war plan (SIOP) during the Cold War, for example, disruption of even portions of the strategic command, control, and communications system could have prevented competent execution of parts of the SIOP. 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 caused 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 it may reduce the search for available alternatives among the few and desperate. Policymakers searching for escapes from crisis denouements need flexible options and creative problem solving. Victims of cyber warfare may have a diminished ability to routinely solve problems, 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. As Blair states, "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."[16]

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions within nonmilitary bureaucratic organizations.[17] 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 great. During the Cuban missile crisis, for example, members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire thirteen 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 rise to the surface, the air strike and invasion might well have been the chosen alternative.[18] As Paul K. Davis has

16 Blair, *The Logic of Accidental Nuclear War*, p. 252.

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

18 Lebow and Stein, *We All Lost the Cold War*, pp. 335–336.

noted, "Usual discussions of crisis stability assume that leaders are in control of their nuclear capabilities. Again, history is sobering. President Kennedy became worried in 1961 about possible unilateral actions by military leaders to prepare a preemptive strike against the Soviet Union. He instigated efforts to tighten the President's personal control. Soviet leadership worried about survivability of its forces and developed capability for launch on warning and automated response. Such systems could be the source of accidental war."[19]

Finally, cyberwar can cause each side to convey flawed images of its intentions and capabilities, with potentially disastrous results. Another example from the Cuban missile crisis demonstrates the possible side effects of simple misunderstanding and noncommunication in 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.[20] Fortunately, Moscow chose to give the United States the benefit of the doubt in this instance and permitted 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.

The assessment below of expert analyst Martin Libicki on the relationship between cyberwar and crisis management underscores the preceding discussion and examples:

> 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

19 Paul K. Davis, Peter Wilson, Jeongeun Kim, and Junho Park, "Deterrence and Stability for the Korean Peninsula," *Korean Journal of Defense Analysis* no. 1 (March 2016): 14.

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

> 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.[21]

## Scenarios and Risks

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, cyber operations by either or both sides might make it more difficult to limit the war and end it before catastrophic destruction and loss of life has taken place. As in the prior discussion, the specifics of each case matter. In psychological warfare, attackers and the recipients of their attacks may intentionally misrepresent successes as failures or vice-versa if such misrepresentation contributes to a preferred outcome of de-escalation. Although "small" nuclear wars do not exist, there is an opposite view as well; during the Cold War, the notion of limited nuclear warfare, tactical nuclear warfare, or limited exchanges was developed, and similar ideas also floated around India-Pakistan. Compared to conventional wars, there can be different kinds of "nuclear" wars, in terms of their proximate causes and consequences.[22] Possibilities include a nuclear attack from an unknown source; an ambiguous case of possible but not proven nuclear first use; a nuclear "test" detonation intended to intimidate but with no immediate destruction; or, a conventional strike mistaken at least initially for a nuclear one. As George H. 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."[23]

---

21 Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012), p. 145.

22 For pertinent scenarios, see George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore: Johns Hopkins University Press, 2006), pp. 24–52.

23 Quester, *Nuclear First Strike*, p. 27.

The dominant scenario of a general nuclear war between the United States and the Soviet Union preoccupied Cold War policy makers, and as a result, 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.[24] 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 non-nuclear weapons states, stretches the ingenuity of military planners and fiction writers.

In addition to the world's worst characters engaged in nuclear threat or first use, backsliding is also possible, depending on the political conditions between the United States and Russia, or Russia and China, or China and India (among current nuclear weapons states). The nuclear "establishment" or P-5 thus includes cases of current debellicism or pacification that depend upon the continuation of favorable political auguries in regional or global politics. 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 along regional fault lines between blocs or major powers could expand into worse conflicts, as was the case also

24 Assessments of deterrence before and after the Cold War appear in Colin S. Gray, *The Future of Strategy* (Cambridge: Polity Press, 2015), pp. 98–106; Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt—Times Books, 2012); Adam B. Lowther, ed., *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century* (New York: Palgrave Macmillan, 2012); Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010), pp. 351–383; Michael Krepon, *Better Safe than Sorry: The Ironies of Living with the Bomb* (Stanford: Stanford University Press, 2009); Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004); Lawrence Freedman, *The Evolution of Nuclear Strategy,* 3rd ed. (New York: Palgrave Macmillan, 2003); Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: University Press of Kentucky, 2001); Colin S. Gray, *The Second Nuclear Age* (Boulder: Lynne Rienner, 1999); Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996); and Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989).

in the Balkan wars in the 1990s. In these cases, Russia's one-sided military advantage relative to Georgia in 2008 and NATO's military power vis-à-vis that of Bosnians of all stripes in 1995 and Serbia in 1999 contributed to terminating war without further international escalation.

Escalation of a conventional war into nuclear first use remains possible where operational or tactical nuclear weapons have been deployed with national or coalition armed forces. In allied NATO territory, the United States deploys several hundred sub-strategic, air delivered nuclear weapons among bases in Belgium, Germany, Italy, the Netherlands, and Turkey.[25] Russia likely retains several thousands of operational or tactical nuclear weapons, including significant numbers deployed in western Russia.[26] The New START agreement, once ratified, establishes a notional parity between the United States and Russia in nuclear systems of intercontinental range.[27] But the superiority of the United States and the allied NATO in advanced technology, information-based conventional military power leaves Russia heavily reliant on tactical nukes as compensation for its comparative weakness in non-nuclear forces. NATO's capitals breathed a sigh of relief when Russia's officially-approved Military Doctrine of 2010 did not seem to lower the bar for nuclear first use, compared to previous editions.[28]

---

25 For background on US tactical nuclear weapons deployed in Europe, see Hans M. Kristensen, *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning* (Washington, DC: Natural Resources Defense Council, February 2005).

26 See Pavel Podvig, "What to do about tactical nuclear weapons," *Bulletin of the Atomic Scientists*, February 25, 2010, https://thebulletin.org/2010/02/what-to-do-about-tactical-nuclear-weapons/ and Jacob W. Kipp, "Russia's Tactical Nuclear Weapons and Eurasian Security," *Eurasia Defense Monitor*, March 5, 2010, https://jamestown.org/program/russias-tactical-nuclear-weapons-and-eurasian-security/.

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

28 "The Military Doctrine of the Russian Federation," February 5, 2010, in *Johnson's Russia List* 2010, #35, February 19, 2010. See also Nikolai Sokov, "The New, 2010 Russian Military Doctrine: The Nuclear Angle," *Center for Nonproliferation Studies, Monterey Institute of International Studies*, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm.

Russia's military doctrine indicates a willingness to engage in nuclear first use in situations of extreme urgency, as defined by its political leadership.[29] And, despite evident superiority in conventional forces relative to those of Russia, neither the United States nor NATO is necessarily eager to get rid of their remaining sub-strategic nukes deployed among American NATO allies. An expert panel convened by NATO to set the stage for its 2010 review of its military doctrine was carefully ambivalent about NATO's forward deployed nuclear weapons. The issue of negotiating away these weapons in return for parallel concessions by Russia was left open for further discussion. On the other hand, the NATO expert report underscored the present sentiment of the majority of governments that these weapons provided a necessary link in the chain of alliance deterrence options.[30]

Imagine now the unfolding of a nuclear crisis or the making a decision for nuclear first use, under the conditions of both NATO and Russian campaigns employing strategic disinformation and information operations intended to disrupt enemy command-control, communications, and warning systems. Disruptive cyber operations against enemy systems on the threshold of nuclear first use, or shortly thereafter, could increase the already substantial difficulty of halting the fighting before a European-wide theater conflict or a strategic nuclear war occurs. The above cited difficulties in crisis management, under the shadow of nuclear deterrence and pending a decision for first use, would place the cohesion of allied governments under unprecedented stress and danger, undoubtedly aided by a confused situation on the battlefield.

NATO would be subjected to three new kinds of friction. First, the decision to use nuclear weapons falls solely within the US (or UK/French) chain of command. NATO has insufficiently considered the challenge of managing a decision-making process on the brink of war among the twenty-nine member states in the alliance, compared to the sixteen members during the Cold War years. The number of member states is not only larger but the diversity of their foreign policy and national security priorities—as well as their variable military-political doctrines—represents a formidable obstacle

29 See the analysis by Keir Giles, *The Military Doctrine of the Russian Federation 2010*, *NATO Research Review* (Rome: NATO Defense College, Research Division, February 2010), esp. pp. 1–2 and 5–6.

30 NATO, *NATO 2020: Assured Security; Dynamic Engagement, Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO* (Brussels: North Atlantic Treaty Organization, May 17, 2010), pp. 43–44.

in making decisions under duress, especially for nuclear first use. Second, reliable intelligence about Russian intentions following Russian or NATO first use would be essential but challenging to nail down. Third, the first use of a nuclear weapon in anger since Nagasaki would establish a new psychological, political, and moral universe in which negotiators seeking de-escalation and termination of war would somehow have to maintain their sangfroid, convince their militaries to agree to stand down, and return nuclear-capable launchers and weapons to secured but transparent locations. All of this would take place within the panic spread by the 24/7 news networks and the internet.

## Conclusion

The possible combination of information warfare with continuing nuclear deterrence after the Cold War could have unintended by-products, and these may be dangerous for stability. One possible objective of cyberwar in conventional warfare could be 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.[31] In a crisis in which nuclear weapons are available to the side under cyberattack, 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 (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) of the opponent 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.[32]

31 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. Johnson and Martin C. Libicki (Washington: National Defense University, 1996), p. 80, and also pp. 77–102.

32 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: Greenwood Press, 1996), p. 33.