Naval War College Review

Volume 75
Number 1 *Winter 2022*

Article 5

Nuclear-Crisis Management and Cyber War—A Dangerous Crossroads

Stephen J. Cimbala
Penn State Brandywine

Follow this and additional works at: https://digital-commons.usnwc.edu/nwc-review

Recommended Citation
Cimbala, Stephen J. () "Nuclear-Crisis Management and Cyber War—A Dangerous Crossroads," *Naval War College Review*: Vol. 75: No. 1, Article 5.
Available at: https://digital-commons.usnwc.edu/nwc-review/vol75/iss1/5

This Article is brought to you for free and open access by the Journals at U.S. Naval War College Digital Commons. It has been accepted for inclusion in Naval War College Review by an authorized editor of U.S. Naval War College Digital Commons. For more information, please contact repository.inquiries@usnwc.edu.

NUCLEAR-CRISIS MANAGEMENT AND CYBER WAR

A Dangerous Crossroads

Stephen J. Cimbala

The full implications of combining the worst weapons of mass destruction with advanced weapons for cyber war are still obscure. The nuclear revolution that dominated the Cold War took place in an environment of relative information scarcity and primitive information technology (IT), compared with those of the present and the foreseeable future, given current trends. One aspect of the nuclear-cyber conjunction lies in its potential impact on nuclear-crisis management. For the United States and Russia, the nuclear-cyber relationship has special significance: the two powers hold more than 90 percent of the world's nuclear weapons; both have advanced offensive and defensive cyberwar capabilities; and both Washington and Moscow have experienced the stress of nuclear-crisis management under Cold War and later conditions.[1]

The implications of the nuclear-cyber nexus are explored below in four steps.[2] The first considers important conceptual issues emerging from the overlap of nuclear and cyber. The second discusses definitions, parameters, and requirements for crisis management. The third examines potential disrupters of or threats to successful crisis management. The fourth discusses scenarios and risks. The conclusion summarizes the findings and offers policy recommendations.

Stephen J. Cimbala is Distinguished Professor of Political Science at Penn State Brandywine. Dr. Cimbala coedited and coauthored Defending the Arsenal: Why America's Nuclear Modernization Still Matters *(2017).*

Naval War College Review, *Winter 2022, Vol. 75, No. 1*

CONCEPTUAL ISSUES

What are the implications of the potential overlap between the concepts and practices applicable to cyber war and those for nuclear deterrence?[3] Cyber war and nuclear weapons seem worlds apart.

Naval War College Review, Vol. 75 [], No. 1, Art. 5

Cyber weapons should appeal to those who prefer a nonnuclear, or even a post-nuclear, military-technical arc of development. War in the digital domain offers, at least in theory, a possible means of crippling or disabling enemy assets without the need for kinetic attack, or at least while minimizing physical destruction.[4] Nuclear weapons, on the other hand, are the very epitome of "mass" destruction, such that their use for *deterrence*—the avoidance of war by the manipulation of risk—is preferred to the actual firing of same. Unfortunately, neither nuclear deterrence nor cyber war will be able to live in a distinct policy universe for the near or distant future.

Nuclear weapons, whether held back for deterrence or fired in anger, are incorporated into systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The weapons and their C4ISR systems must be protected from attacks both kinetic and digital in nature. In addition, the decision makers who must manage nuclear forces during a crisis ideally should have the best possible information about the status of their own nuclear and cyber forces and command systems, about the forces and C4ISR of possible attackers, and about the probable intentions and risk acceptance of possible opponents. In short, the task of managing a nuclear crisis demands good information and clear thinking. But the employment of cyber weapons in the early stages of a crisis could impede clear assessments by creating confusion in networks and the action channels that depend on those networks.[5] The temptation to take preemptive cyber action—for example, intrusive cyber reconnaissance of command-and-control (C2) systems—might "succeed" to the point at which nuclear-crisis management becomes weaker instead of stronger. Related to this, one challenge of the second nuclear age is that conventional war is more likely to take place within a nuclear context. Paul Bracken has noted the following:

> Cyber's effect on conventional operations has barely been considered in the current nuclear debate. Cyber could cripple U.S. command and control. Space war is also overlooked. Disruptions, from cyber, ASAT [antisatellite], and hacks to our reconnaissance system[,] make good sense from the enemy point of view, to blind our reconnaissance targeting. This would turn our precision strike force into blunt carpet bombing, and likely [result in] a vast increase in collateral damage. Obviously this has political implications. It could lead to a U.S. reluctance to act. This may well be the real intent of such a move on the part of the enemy, to create a kind of nuclear digital brinkmanship that forces the United States to back off in a crisis.[6]

IT systems provide invaluable intelligence during a crisis, using databases, big data, visualization, geographic-information-systems mapping, artificial intelligence (AI), image recognition, and other means. If the confidentiality, integrity, or availability of these systems is doubtful, leaders will feel that they have lost control and are left groping for options.

Ironically, the downsizing of U.S. and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the confluence of cyber- and nuclear-attack capabilities more alarming. The overkill deployments of missiles and bombers and expansive numbers of weapons that the Cold War Americans and Soviets deployed had at least one virtue; those arsenals provided so much redundancy against first-strike vulnerability that relatively linear systems for nuclear-attack warning, C2, and responsive launch, under or after attack, sufficed. At the same time, Cold War tools for military cyber action were primitive compared with those available now. In addition, countries and their armed forces were less dependent on the fidelity of their information systems for national security. Thus, the reduction of U.S., Russian, and possibly other forces to the size of "minimum deterrents" might compromise nuclear flexibility and resilience in the face of kinetic attacks preceded or accompanied by cyber war.[7] In addition, although the mathematics of minimum deterrence would shrink the size of attackers' as well as defenders' arsenals, defenders with smaller-size forces might have greater fears of absolute, compared with relative, losses, and therefore might be more prone to preemption-dependent strategies than defenders with larger forces would be. One of the reasons for Cold War force redundancy was that superpowers lacked confidence in the reliability or availability of some of their nuclear systems.

[N]either nuclear deterrence nor cyber war will be able to live in a distinct policy universe for the near or distant future.

Offensive and defensive information warfare (infowar), as well as other cyber-related activities, is obviously very much on the minds of U.S. military leaders and others in the American and allied national-security establishments.[8] Russia also has been explicit about its cyber-related concerns. In early July 2013, President Vladimir V. Putin urged the Russian Security Council to improve state security against cyber attacks.[9] Russian security expert Vladimir I. Batyuk, commenting favorably on a June 2013 U.S.-Russian agreement for the protection, control, and accounting of nuclear materials (a successor to the then recently expired Nunn-Lugar agreement on nuclear risk reduction), warned that pledges by Presidents Putin and Barack H. Obama of cooperation on cybersecurity were even more important: "Nuclear weapons are a legacy of the 20th century. The challenge of the 21st century is cybersecurity."[10]

On the other hand, arms control for cyber is apt to run into daunting security and technical issues, even assuming a successful navigation of political trust for matters as sensitive as these. Of special significance is whether cyber arms-control negotiators can certify that hackers operating within their own states

Naval War College Review, Vol. 75 [], No. 1, Art. 5

are sufficiently under control for cyber verification and transparency. There is extensive evidence that Russia, China, and other states use civilian hackers to support national goals. For example, some sources attributed Russia's hacking into the e-mail account of the Democratic National Committee in 2016 to "Guccifer 2.0"—an homage to the original Romanian hacker using that name. Some forensic evidence supports the hypothesis that Guccifer 2.0 was run by the Russian FSB (the country's principal security agency), with some involvement by Russian military intelligence.[11] Another uncertainty is the potential role of hacktivists who routinely join in conflicts even without state sanction. If a country is in a state-versus-state crisis, then finds itself on the receiving end of an effective, widespread cyber attack that affects "the man on the street," pressure on the government for a kinetic (i.e., military) response may become overwhelming. Technically minded, determined individuals or small groups of hacktivists now have the potential to shake the world through cyber warfare.

The cyber domain cuts across the other geostrategic domains for warfare as well: land, sea, air, and space. On the other hand, the cyber domain, compared with the others, suffers from a lack of historical perspective; it "has been created in a short time and has not had the same level of scrutiny as other battle domains," as one author has argued.[12] What this might mean for the cyber-nuclear intersection is far from obvious.

CRISIS MANAGEMENT

Definitions and Parameters

Crisis management, including nuclear-crisis management, is both a competitive and a cooperative endeavor between military adversaries. A *crisis* is, by definition, a time of great tension and uncertainty.[13] Threats are in the air, and time pressure on policy makers seems intense. Each side has objectives that it wants to attain and values 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 referring to something completely separate from the state or individual behaviors that make it up. The system aspect implies reciprocal causation of the crisis behaviors of A by B and vice versa.

One aspect of crisis management is this 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. In defining

the onset of a crisis, Patrick M. Morgan offers the useful concept of *immediate deterrence failure:* specific sources of hostile intent have been identified by one state with reference to another, threats have been exchanged, and responses now must be decided on.[14] The passage into a crisis is equivalent to the shift from a Hobbesian world of omnipresent potential violence to the actual movement of troops and exchanges of diplomatic démarches.

All crises are characterized to some extent by a high degree of threat; a 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 modern scholars ever invented the discipline of crisis management, historians had captured the rush-to-judgment character of much crisis decision-making among great powers.[15] The influence of nuclear weapons on crisis decision-making is 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 inflicted 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 on war versus peace. History is full of dependent variables in search of competing explanations.

Crisis Management: The Requirements

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 is a prerequisite for the effective communication of goals and objectives from one side to the other. If signals are sent poorly 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 and 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 B. Payne notes with regard to the potential for deterrence failure in the post–Cold War period, "Unfortunately, our

Naval War College Review, Vol. 75 [], No. 1, Art. 5

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."[16]

A second requirement of successful crisis management is the reduction of time pressure on policy makers and commanders so that no unintended, provocative steps are taken toward escalation mainly or solely as a result of a misperception that "time is up." Policy makers 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 that emerge under crisis conditions, deadlines may be confused with policy objectives themselves; ends become means, and means, ends.[17] For example, the war plans of the great powers in July 1914 contributed to a shared, self-fulfilling prophecy among leaders in Berlin, Saint Petersburg, and Vienna: that only by prompt mobilization and attack could they avoid decisive losses in war. Plans predicated on the unchangeable structure of mobilization timetables proved insufficiently flexible for policy makers who wanted to slow down the momentum of late July and early August toward an irrevocable decision in favor of war.[18]

A . . . potentially disruptive effect of infowar on nuclear-crisis management is that it may reduce the search for available alternatives to the few and desperate.

One result of the compression of decision time in a crisis, compared with 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 may trigger tactical operators to misread indicators. Bruce G. Blair has argued that "[i]n 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."[19]

A third attribute of successful crisis management is that each side should be able to offer the other a safety valve or face-saving exit from a predicament that has escalated beyond 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 John F. Kennedy was able to offer Soviet premier Nikita S. 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 on the soil of America's NATO allies. Kennedy and his inner circle recognized—after some days of deliberation and a clearer focus on the Soviet view of events—that the United States would lose, not gain, by a public humiliation of Khrushchev that, in turn, might diminish Khrushchev's interest in any mutually agreed-upon solution to the crisis.[20]

A fourth attribute of successful crisis management is that each side maintains an accurate perception of the other side's intentions and military capabilities. This 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 in 1989 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."[21]

Intentions can change during a crisis if policy makers become more optimistic about gains or more pessimistic about potential losses. Capabilities can change owing 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 nonthreatening 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.

In addition, 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 policy makers' intent or with the decisions and actions of other parts of the government. Alexander L. George explains as follows:

> 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.[22]

Naval War College Review, Vol. 75 [], No. 1, Art. 5

As policy makers may be challenged to control numerous and diverse standard operating procedures (SOPs), political leaders also may 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.[23]

POTENTIAL DISRUPTERS

Information or cyber warfare has the potential to attack or to disrupt successful crisis management with regard to each of the preceding attributes.[24] First, infowar 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.[25] 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; however, destroyed or altered information also may mislead either side into thinking that its signal has been interpreted correctly 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 what it has received as a "yield" message, may decide to continue its aggression, but then meets unexpected resistance, causing 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 launchpad or during the launch itself. Apparently, the United States has used such "left-of-launch" techniques against North Korea.[26] During a nuclear crisis, would such a move be accepted by the attacked party as one of intimidation and deterrence or, to the contrary, would offensive cyber war against missile launches prompt a nuclear first use or first strike by the defender for fear of losing its retaliatory capability?

Infowar also can destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is by disrupting communication links between policy makers and military commanders during a period of high threat and severe time pressure. Unanticipated problems, from the standpoint of civil-military relations, may arise under these conditions. For example, political leaders may have predelegated limited authority for nuclear release or launch under restrictive conditions; only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their commands.[27] Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceive a situation to be far more desperate, and thus permissive of nuclear initiative, than it really is. For example, during the Cold War, disrupted communications between the U.S. national command authority

and ballistic-missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers and crew, in the absence of contrary instructions, to launch.

Second, infowar during a crisis almost certainly will increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived timelines within which the policy-making process yields 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 American 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 Single Integrated Operational Plan (SIOP), the nation's strategic nuclear war plan. The Cold War SIOP depended on finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets.[28] Partly 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. Even in the post–Cold War world of flexible nuclear-response plans, the potential slide toward preemption, on the basis of mistaken or exaggerated fears of C2 vulnerability, casts a shadow over deterrence stability. As Blair has warned, "There are no widely accepted methods for calculating command and control performance under wartime conditions, and empirical validation of such an assessment cannot be done. Compared with the tight and tidy standard calculations of force vulnerability, any objective assessment of command and control systems would raise more questions than it answered."[29]

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. Policy makers seeking escapes from crisis denouements need flexible options and creative problem-solving. Victims of infowar 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 posed poorly, and responses (if available at all) will be driven toward the least common denominator of previously programmed SOPs. Retaliatory systems that depend on launch-on-warning dynamics 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."[30]

Naval War College Review, Vol. 75 [], No. 1, Art. 5

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.[31] In civil-military C2 systems under the stress of nuclear-crisis decision-making, the first available alternative quite literally may be the last—or so policy makers and their military advisers may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, for example, a number of members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire 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 the surface, the air strike and invasion might well have been the chosen course of action.[32] Paul K. Davis and coauthors have noted the following:

The rule book for nuclear-crisis management in the age of cyber deterrence and cyber war remains to be written.

> 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 automatic response. Such systems could be the source of accidental war.[33]

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 missile crisis demonstrates the possible side effects on U.S. crisis management of simple misunderstanding and noncommunication. At the most tense period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. U.S. 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.[34] Fortunately, Moscow chose to give Washington the benefit of the doubt in this instance and to permit U.S. fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not aborted once the crisis began never has been revealed fully; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policy makers who failed to appreciate the risk of "normal" reconnaissance under these extraordinary conditions.

The significance of the preceding discussion and examples is underscored by the assessment of expert analyst Martin C. Libicki about the relationship between cyber war and crisis management.

> To generalize, a situation in which there is little pressure to respond quickly, in which a temporary disadvantage or loss is tolerable, and in which there are grounds for giving the other side some benefit of the doubt is one in which there is time for crisis management to work. Conversely, if the failure to respond quickly causes a state's position to erode, a temporary disadvantage or degree of loss is intolerable, and there are no grounds for disputing what happened, who did it, and why—then states may conclude that they must bring matters to a head quickly.[35]

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, information operations by either side or both might make it more difficult to limit the war and bring it to a conclusion before catastrophic destruction and loss of life has taken place. Although there are no such things as "small" nuclear wars compared with conventional wars, there can be different kinds of "nuclear" wars, in terms of their proximate causes and consequences.[36] 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; or a conventional strike mistaken, at least initially, for a nuclear one.

With regard to the last-mentioned case, George H. Quester has noted that 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."[37] In such an instance, the adversary may question why its command posts or strategic assets are being targeted and assume the actions are the prelude to an all-out strategic strike.

The dominant scenario of a general nuclear war between the United States and the Soviet Union preoccupied Cold War policy makers, so concerns about escalation control and war termination were swamped by apocalyptic visions of the end of days. The second nuclear age, coinciding roughly with the end of the Cold War and the demise of the Soviet Union, offers a more complicated menu of nuclear possibilities and responses.[38] Interest in the threat or use of nuclear weapons by rogue states, aspiring regional hegemons, or terrorists, abetted by

Naval War College Review, Vol. 75 [], No. 1, Art. 5

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 possibility of the world's worst characters engaging in nuclear threat or first use, there also may be backsliding in political conditions, such as between the United States and Russia, or Russia and China, or China and India (among current nuclear-weapons states). Arguments assuming the continuation of stable deterrence among major powers depend on the continuation of favorable political auguries in regional or global politics. Conflicts that are politically unthinkable in one decade have a way of evolving into wars that are politically unavoidable in 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. So, too, were the Balkan wars of Yugoslav succession in the 1990s. In these cases, Russia's one-sided military advantage relative to Georgia in 2008 and NATO's military power relative to that of Bosnians of all stripes in 1995 and Serbia in 1999 contributed to war termination 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 substrategic, air-delivered nuclear weapons among bases in Belgium, Germany, Italy, the Netherlands, and Turkey.[39] Russia probably retains several thousand operational or tactical nuclear weapons, including significant numbers deployed in western Russia.[40] The New Strategic Arms Reduction Talks (New START) agreement establishes a notional parity between the United States and Russia in nuclear systems of intercontinental range.[41] But U.S. and allied NATO superiority in advanced-technology, information-based conventional military power leaves Russia heavily reliant on tactical nukes as compensation for comparative weakness in nonnuclear forces. NATO's members 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 with previous editions.[42]

However, Russia's military doctrine does indicate a willingness to engage in nuclear first use in situations of extreme urgency for Russia, as defined by its political leadership.[43] And, despite NATO's evident superiority in conventional forces relative to those of Russia, neither the United States nor the rest of NATO is necessarily eager to get rid of its remaining substrategic nukes deployed among America's NATO allies. An expert panel that NATO convened to set the stage for its 2010 review of the alliance's military doctrine was carefully ambivalent on the issue of the alliance's forward-deployed nuclear weapons. The possibility of negotiating away these weapons in return for parallel concessions from Russia

was left open for further discussion. On the other hand, the NATO expert report underscored the present majority sentiment of governments that these weapons provided a necessary link in the chain of alliance deterrence options.[44]

Imagine now the unfolding of a nuclear crisis or the making of 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 C3 and warning systems. Disruptive information operations against enemy systems on the threshold of nuclear first use, or shortly thereafter, could increase the already substantial difficulty of bringing fighting to a halt before a Europe-wide theater conflict or a strategic nuclear war ensues. All the previously cited difficulties in crisis management under the shadow of nuclear deterrence pending a decision for first use would be compounded by additional uncertainty and friction after the nuclear threshold had been crossed.

In addition, three new kinds of frictions would be posed for NATO. First, the cohesion of allied governments would be tested under conditions of unprecedented stress and danger, doubtless aided by a confused situation on the field of battle. 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 within which negotiators for de-escalation and war termination would have to maintain somehow their sangfroid, obtain agreed stand-downs from their militaries, and return nuclear-capable launchers and weapons to secured but transparent locations. All this would be taking place within the panic-spreading capabilities of 24/7 news networks and the Internet.

Theoretically, one might finesse the issue by eliminating cyber operations that potentially conflict with de-escalation. But the political desire to do so conflicts with the military need 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, and other impediments in the way. (Or, if methods of finesse are not available, bombing the relevant installations is always an option, although obviously a provocative one.) The second, and somewhat opposed, mission is to communicate reliably to the other side one's preference for de-escalation, one's willingness to de-escalate if reciprocity can be obtained, and one's awareness of the possibility that the situation shortly will get out of hand. Consider the Russian General Staff and the president's office filtering this hydra-headed group of messages while their forces are grappling in Georgia or Ukraine, with the smaller country having been taken into NATO membership, say, a year earlier, over Russia's objections.

Naval War College Review, Vol. 75 [], No. 1, Art. 5

The problem of nuanced messages and the management of de-escalation, even short of war, is illustrated by the 1983 iteration of NATO's command-post exercise ABLE ARCHER, held 7–11 November that year. An annual exercise, ABLE ARCHER was intended to practice nuclear-release procedures. Soviet intelligence routinely monitored these exercises. However, the 1983 version took place against a background of rising U.S.-Soviet political tensions and heightened suspicions within the Soviet political leadership and military high command that the United States and NATO might be preparing for a nuclear first strike. One reason that Russian sensitivities to the possibility of U.S. or NATO nuclear first use or first strike were high at this time was NATO's decision to begin deploying Pershing II ballistic missiles and ground-launched cruise missiles of intermediate range in Europe, beginning in the fall of 1983. Soviet and Warsaw Pact reactions to ABLE ARCHER 83 included an unprecedented surge of Warsaw Pact technical collection, a significant increase in reconnaissance by Soviet strategic and naval aviation, and other unusual Soviet moves that indicated increased concern about NATO and U.S. intentions.[45] The case illustrates how mistaken interpretations of "normal" events can overvalue pessimistic assessment at just the wrong time.[46] As the President's Foreign Intelligence Advisory Board concluded in 1990, "We believe that the Soviets perceived that the correlation of forces had turned against the USSR, that the US was seeking military superiority, and that the chances of the US launching a nuclear first strike—perhaps under cover of a routine training exercise—were growing. We also believe that the US intelligence community did not at the time, and for several years afterwards, attach sufficient weight to the possibility that the war scare was real."[47]

States' actual experience in managing nuclear crises or peacetime deterrence situations occurred almost entirely prior to the information age as we know it today.

The possibility of nuclear war by inadvertent escalation did not disappear with the end of the Cold War. The Russian General Staff remained alert to the possibility of a U.S. nuclear attack even as political relations between the two early post–Cold War states were officially nonhostile. In one instance, a U.S.-Norwegian Black Brant research rocket was launched from an island off the coast of Norway on 25 January 1995 to study the northern lights. This triggered a reaction from Russia's missile-early-warning system, which alerted senior Russian defense officials, including then-President Boris Yeltsin, who for the first time activated his nuclear briefcase until confirmation was received that no attack was in progress.[48]

Avoiding mistaken nuclear preemption in a complex information environment is one kind of challenge; the problems in coordinating the management of de-escalation and conflict termination with the conduct of information

operations offer another. Two examples follow. The first, already alluded to, is the use of a bunker-busting or other advanced-technology conventional weapon that the other side, during the fog of crisis or war, confuses with a nuclear first use or first strike. Russia expressed this concern specifically during New START negotiations in 2010, with regard to American plans to deploy some conventionally armed ballistic missiles on nuclear-capable intercontinental or transoceanic launchers.[49] New START counting rules regard conventionally armed ballistic missiles as being nuclear-capable launchers, and therefore subject to overall restrictions on the numbers of deployed launchers and weapons. U.S. plans for Prompt Global Strike systems to include missiles or future space planes were approved first during the George W. Bush administration and carried forward under the Obama administration.

A second illustration of the problem of managing escalation control and conflict termination alongside information operations, one separate from the issue of escalation in Europe, is provided by the proposal for a joint NATO-Russian theater-missile-defense (possibly including air defenses) system. The idea had 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 (BMDs). Here, NATO and Russia are facing in two political directions: toward each other, displaying wariness but also openness; but regarding Iranian or other Middle Eastern leaders who may get their hands on nuclear weapons in the future, and who may be beyond deterrence based on the credible threat of nuclear (or other) retaliation, displaying concern.

However, the problems of achieving missile-defense cooperation between NATO and Russia are not only political. Even with the best of intentions among U.S., NATO, and Russian negotiators, the military-technical difficulties involved in coordinating BMD C3 systems are considerable. Indeed, they are not strictly "military-technical" but also heavily embedded with issues of political sovereignty; classified intelligence; and trust, among both governments and militaries. Even among NATO members, militaries differ in their national traditions, military-service identities, experiences in nuclear arms control, and willingness to share online information in real time 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 United States) and Russia agree before any action is taken in response?

If a political crisis between NATO and Russia erupts, and both sides already have deployed missile defenses, will Russian or American cyber warriors attempt

Naval War College Review, Vol. 75 [], No. 1, Art. 5

to spoof or otherwise negate the other's missile-defense component? Would it be better to reassure Russia regarding the surety of its own 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 more 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 trapdoors—just in case? Perhaps, in future nuclear or other crises, the U.S. and Russian cyber commands should have their own direct "hotline," or in this case an encrypted digital link.

The rule book for nuclear-crisis management in the age of cyber deterrence and cyber war remains to be written. States' actual experience in managing nuclear crises or peacetime deterrence situations occurred almost entirely prior to the information age as we know it today.

Military cyber war already has been used to attack nuclear-production facilities, to hijack computers and servers for hostile purposes, to infiltrate networks with lurking malware awaiting timely activation, and to divert or prevent rocket launches by hostile powers.[50] Advanced cyberwar capabilities also might interfere with future crisis management, either intentionally or otherwise, resulting in misperceptions, faulty communications, caricatures of the other side's intentions and capabilities, and hasty judgments based on stereotypical thinking pushed forward under duress.[51] Added to this list, in the case of nuclear crisis, is the possibility of imminent attack with historically unprecedented consequences, creating a bias for preemptive action—"striking first in the last resort." Finally, it is important to emphasize that deterrence, whether it is based on the credible threat of denial or retaliation, must be communicated successfully to, and believed by, the other side. The "deterree" has the decisive vote.[52]

Technology alone will not resolve the dilemmas of nuclear-cyber overlap; to the contrary, it may worsen the risks of accidental or inadvertent nuclear war. For example, the outsourcing to AI or other expert systems of nuclear warning, attack assessment, and response functions—on the assumption that they can work faster and more accurately than can fallible humans—creates temptations to resolve the human-machine interface by defaulting to technology. This is part of the wider debate about keeping the human in the loop and is important in many areas of AI, not only the military.[53]

One policy recommendation following from this analysis is that political and military leaders need to wargame continually these types of scenarios, in which cyber weapons might exert significant influence on crisis-management outcomes. These war games do not need to be excessively complicated, but they

should capture the environment of crisis decision-making under constrained conditions of limited information, insufficient time for full consideration of all options, and perception of the enemy "through a glass darkly." On the other hand, there are caveats in following this prescription; timing is everything. As soon as the wargame scenarios start to explore what happens if the adversary is under the same level of attack, the other states might speculate about the motives for such war games; they might suspect that such games are a prelude to someone developing a capability to attack their systems as preparation for war.

NOTES

The author gratefully acknowledges Paul Davis, Andrew Futter, Lawrence Korb, Adam Lowther, Gabi Siboni, and Timothy Thomas for insights into the topic of this article, along with the anonymous referees of this journal. None of these persons bears any responsibility for its content. This article includes some material from the author's previously published study "Nuclear Crisis Management and 'Cyberwar': Phishing for Trouble?," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011), pp. 117–31.

1. Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt / Times Books, 2012).
2. For insights on this topic, see Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (March 2017), pp. 37–48, doi.org/10.1093/cybsec/tyw017, and Andrew Futter, "The Double-Edged Sword: US Nuclear Command and Control Modernization," *Bulletin of the Atomic Scientists,* 29 June 2016, thebulletin.org/. See also Andrew Futter, *Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy,* RUSI Occasional Paper (London: Royal United Service Institute for Defence and Security Studies, July 2016), available at www.rusi.org/, and Andrew Futter, "*War Games* Redux? Cyberthreats, US-Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control," *European Security* 25, no. 2 (December 2015), available at doi.org/10.1080/09662839.2015.1112276.
3. This article uses 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 other methods. For sensible approaches to these issues, see Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* 11, no. 1 (Spring 2017), pp. 49–65; P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford Univ. Press, 2014), esp. pp. 67–72; John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago, IL: Ivan R. Dee, 2008), chaps. 6–7; and Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).
4. On the information-operations concepts of major powers, see Timothy L. Thomas, *Cyber Silhouettes: Shadows over Information Operations* (Fort Leavenworth, KS: Foreign Military Studies Office, 2006), esp. chaps. 5–6, 10, 14. See also Timothy L. Thomas, *Russia: Military Strategy; Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth, KS: Foreign Military Studies Office, 2015), pp. 253–99 for a discussion of Russian cyber capabilities and doctrines, and Pavel Koshkin, "Are Cyberwars between Major Powers Possible?," *Russia Direct,* 1 August 2013, russia-direct.org/.
5. Cyber weapons are not necessarily easy to use effectively as enabling instruments for operational-tactical or strategic effect. See Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, U.K.: Cambridge Univ. Press, 2007), esp. chaps. 4–5.

Naval War College Review, Vol. 75 [], No. 1, Art. 5

6. Paul Bracken, "Deter[r]ence in a Second Nuclear Age," *United States Senate Committee on Armed Services,* 28 April 2021, www.armed-services.senate.gov/.

7. An expert critique of proposals for minimum deterrence for U.S. nuclear forces appears in Keith B. Payne et al., *Minimum Deterrence: Examining the Evidence* (Fairfax, VA: National Institute Press, 2013). For a favorable expert assessment of the prospects for minimum deterrence, see James Wood 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.

8. Plans by U.S. Cyber Command and others for improving U.S. cyber defense against attacks on computer networks and other targets may have been delayed or diverted by political controversy over National Security Agency surveillance. See David E. Sanger, "N.S.A. Leaks Make Plan for Cyberdefense Unlikely," *New York Times,* 12 August 2013, www.nytimes.com/. See also Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), esp. pp. 176–81.

9. "Putin Calls to Strengthen Protection against Cyber Attacks," *TASS,* 5 July 2013, tass.com/.

10. Batyuk, cited in Jonathan Earle, "U.S. and Russia Sign New Anti-proliferation Deal," *Moscow Times,* 18 June 2013, themoscowtimes.com/.

11. Richard Lourie, *Putin: His Downfall and Russia's Coming Crash* (New York: St. Martin's, 2017), p. 205. On Chinese approaches to cyber conflict, see Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), esp. pp. 34–37, 39–66. The evolving U.S.-Chinese nuclear relationship is treated with expertise in Brad Roberts, *The Case for U.S. Nuclear Weapons in the 21st Century* (Stanford, CA: Stanford Univ. Press, 2015), pp. 141–75, esp. p. 165, as well as note 76.

12. Clifford S. Magee [Maj., USMC], "Awaiting Cyber 9/11," *Joint Force Quarterly,* no. 70 (3rd Quarter 2013), p. 76.

13. For important 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, 1991), pp. 22–27, for the political and operational requirements of crisis management; and Alexander L. George, "Strategies for Crisis Management," in George, *Avoiding War,* pp. 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 Univ. Press, 1989), vol. 1, pp. 8–84, and Phil Williams, *Crisis Management: Confrontation and Diplomacy in the Nuclear Age* (New York: Wiley, 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, CO: Westview, 1994), pp. 111–32.

14. See Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage, 1983), and Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton, NJ: Princeton Univ. Press, 1995), pp. 351–55.

15. For example, see Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore, MD: Johns Hopkins Univ. Press, 1981); Michael Howard, *Studies in War and Peace* (New York: Viking, 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, 1983).

16. Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: Univ. 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: Strategic Studies Institute, 1991), esp. pp. 5–8, 31–37.

17. Holsti, "Crisis Decision Making"; Williams, *Crisis Management*.

18. Stephen J. Cimbala, "Steering through Rapids: Russian Mobilization and World War I," *Journal of Slavic Military Studies* 9, no. 2 (1996), pp. 376–98, available at doi.org/10.1080/13518049608430238.

19. Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington, DC: Brookings Institution, 1993), p. 237. See also Peter

Douglas Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, NY: Cornell Univ. Press, 1992), on the typology of errors.

20. Lebow and Stein, *We All Lost the Cold War,* pp. 122–23.
21. Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell Univ. Press, 1989), p. 183.
22. Alexander L. George, "The Tension between 'Military Logic' and Requirements of Diplomacy in Crisis Management," in George, *Avoiding War,* p. 18.
23. Ibid.
24. For useful definitions of *cyber attack* and *cyber war,* see Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *International Law and Politics* 47 (2015), pp. 327–55.
25. For pertinent terminology, see Singer and Friedman, *Cybersecurity and Cyberwar*.
26. David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar against North Korean Missiles," *New York Times,* 4 March 2017, www.nytimes.com/. See also Jesse T. Wasson and Christopher E. Bluesteen, "Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems" (working paper presented at International Studies Association Annual Convention, Baltimore, MD, 25 February 2017).
27. Fred Kaplan, *The Bomb: Presidents, Generals, and the Secret History of Nuclear War* (New York: Simon & Schuster, 2020).
28. See ibid., and Bruce G. Blair, *Strategic Command and Control: Redefining the Nuclear Threat* (Washington, DC: Brookings Institution, 1985).
29. Blair, *The Logic of Accidental Nuclear War,* p. 118.
30. Ibid., p. 252.
31. James G. March and Herbert A. Simon, *Organizations* (New York: Wiley, 1958), pp. 140, 146.
32. Lebow and Stein, *We All Lost the Cold War,* pp. 335–36.
33. Paul K. Davis et al., "Deterrence and Stability for the Korean Peninsula," *Korean Journal of Defense Analysis* 28, no. 1 (March 2016), p. 14.
34. 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, NJ: Princeton Univ. Press, 1989), p. 147, and Lebow and Stein, *We All Lost the Cold War,* p. 342.
35. Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND, 2012), p. 145.
36. For pertinent scenarios, see George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore, MD: Johns Hopkins Univ. Press, 2006), pp. 24–52.
37. Ibid., p. 27.
38. Assessments of deterrence before and after the Cold War appear in Keith B. Payne, *Shadows on the Wall: Deterrence and Disarmament* (Fairfax, VA: National Institute Press, 2020); Stephen J. Cimbala, *The United States, Russia and Nuclear Peace* (New York: Palgrave Macmillan, 2020); Colin S. Gray, *The Future of Strategy* (Cambridge, U.K.: Polity, 2015), pp. 98–106; Bracken, *The Second Nuclear Age;* 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, U.K.: Cambridge Univ. Press, 2010), pp. 351–83; Michael Krepon, *Better Safe Than Sorry: The Ironies of Living with the Bomb* (Stanford, CA: Stanford Univ. Press, 2009); Lawrence Freedman, *Deterrence* (Cambridge, U.K.: Polity, 2004); Lawrence Freedman, *The Evolution of Nuclear Strategy,* 3rd ed. (New York: Palgrave Macmillan, 2003); Patrick M. Morgan, *Deterrence Now* (Cambridge, U.K.: Cambridge Univ. Press, 2003); Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: Univ. Press of Kentucky, 2001); Colin S. Gray, *The Second Nuclear Age* (Boulder, CO: Lynne Rienner, 1999); Payne, *Deterrence in the Second Nuclear Age;* and Jervis, *The Meaning of the Nuclear Revolution*.
39. For detailed information on U.S. tactical nuclear weapons deployed in Europe, see Hans M. Kristensen, *U.S. Nuclear Weapons in Europe: A Review of Post–Cold War Policy,*

Naval War College Review, Vol. 75 [], No. 1, Art. 5

Force Levels, and War Planning (Washington, DC: Natural Resources Defense Council, February 2005).

40. See Pavel Podvig, "What to Do about Tactical Nuclear Weapons," *Bulletin of the Atomic Scientists,* 25 February 2010, thebulletin.org/, and Jacob W. Kipp, "Russia's Tactical Nuclear Weapons and Eurasian Security," *Eurasia Defense Monitor* 7, no. 44 (5 March 2010), available at jamestown.org/, for pertinent insights and analysis.

41. Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, Russ.-U.S., 8 April 2010, available at www.state.gov/.

42. "The Military Doctrine of the Russian Federation," www.Kremlin.ru, 5 February 2010. See also Nikolai Sokov, "The New, 2010 Russian Military Doctrine: The Nuclear Angle," *Middlebury Institute of International Studies at Monterey—James Martin Center for Nonproliferation Studies,* 5 February 2010, nonproliferation.org/.

43. See the analysis by Keir Giles, "The Military Doctrine of the Russian Federation 2010," *NATO Research Review* (February 2010), esp. pp. 1–2, 5–6.

44. Madeleine K. Albright et al., *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, 17 May 2010), pp. 43–44.

45. President's Foreign Intelligence Advisory Board, *The Soviet "War Scare"* (15 February 1990), esp. pp. vii, 69–74, available at nsarchive.gwu.edu/. See also Jill Kastner, "Standing on the Brink: The Secret War Scare of 1983," *The Nation,* 31 May 2018, thenation.com/, in addition to sources cited below.

46. On Able Archer and its implications, see Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (New York: HarperCollins, 1990), pp. 599–601. Additional parts of the background relevant to political tensions at this time include U.S.-announced plans for the Strategic Defensive Initiative in the spring of 1983, the KAL 007 shootdown by a Soviet fighter in September 1983, and an ongoing KGB-GRU intelligence operation (RYaN) to detect telltale signs of any U.S. or NATO decision for a nuclear attack. Ibid., pp. 582–98. See also Robert M. Gates, *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War* (New York: Simon & Schuster, 1996), p. 273, also cited in Davis et al., "Deterrence and Stability for the Korean Peninsula," p. 21.

47. President's Foreign Intelligence Advisory Board, *The Soviet "War Scare,"* p. vii.

48. Peter Vincent Pry, *War Scare: Russia and America on the Nuclear Brink* (New York: ABC-CLIO, 1999).

49. For elaboration on New START, see Cimbala, *The United States, Russia and Nuclear Peace*.

50. David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018).

51. Some of these and other decision pathologies actually happened during the Cuban missile crisis of 1962, about which a large literature exists. See, for example, Aleksandr Fursenko and Timothy Naftali, *"One Hell of a Gamble": Khrushchev, Castro, and Kennedy, 1958–1964* (New York: W. W. Norton, 1997), and Allison, *Essence of Decision*. See also recent reflections and discussion by Daniel Ellsberg, *The Doomsday Machine: Confessions of a Nuclear War Planner* (New York: Bloomsbury, 2017), pp. 186–222. Khrushchev's perspective is provided in Jerrold L. Schecter and Vyacheslav V. Luchkov, *Khrushchev Remembers: The Glasnost Tapes* (Boston: Little, Brown, 1990), pp. 170–83. Lessons from nuclear-security crises are addressed by experts in Henry D. Sokolski and Bruno Tertrais, eds., *Nuclear Weapons Security Crises: What Does History Teach?* (Carlisle, PA: Strategic Studies Institute / U.S. Army War College Press, July 2013).

52. As 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" (emphasis in original). Colin S. Gray, *Explorations in Strategy* (Westport, CT: Greenwood, 1996), p. 33. As Sechser and Fuhrmann argue, nuclear coercion (or compellence) may be more problematical than deterrence for this reason. "Many of the problems that make coercive nuclear threats incredible are less acute in deterrence contexts. Most notably, nuclear

deterrent threats are often more credible because the stakes for nuclear defenders tend to be higher than they are for nuclear coercers." Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (Cambridge, U.K.: Cambridge Univ. Press, 2017), esp. p. 255.

53. Vincent Boulanin, "Regulating Military AI Will Be Difficult. Here's a Way Forward," *Bulletin of the Atomic Scientists,* 3 March 2021, thebulletin.org/; George Galdorisi and Sam Tangredi, "Algorithms of Armageddon: What Happens When We Insert AI into Our Military Weapons Systems?" (online presentation to the DoD Strategic Multilayer Assessment Program, 27 April 2021), available at nsiteam.com/.