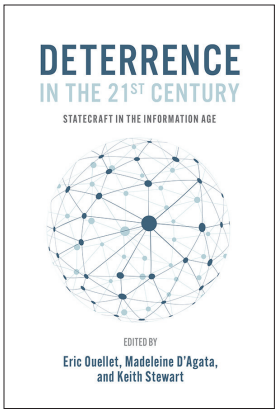
UNIVERSITY OF CALGARY
Press



DETERRENCE IN THE 21ST CENTURY: STATECRAFT IN THE INFORMATION AGE

Edited by Eric Ouellet, Madeleine D'Agata, and Keith Stewart

ISBN 978-1-77385-404-5

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

2

Nuclear Crisis Management for the Information Age

Stephen J. Cimbala and Adam B. Lowther

The growing importance of the cyber domain to warfare requires a major rethinking of information's use during conflict. Technologies that increase the sensor-to-shooter speed in which a war fighter can find, fix, and kill a target enhance battlespace awareness, but can also pose a risk to effective target assessment and reduce understanding of an action's consequences. One case in point is the relationship between digital decision tools and the management of crises, especially crises with the inherent risk of escalation to nuclear first use or first strike. Nuclear deterrence is, at its core, an information operation that employs information, disinformation, and misinformation in order to shape the risk-reward calculation of an adversary. If the ultimate goal of deterrence is to create a perception of risk that makes changing the status quo too risky, then it should come as no surprise that this volume includes a chapter on deterrence and nuclear crisis management. The following discussion considers how the goals of nuclear crisis management might be circumscribed or even overcome by the interaction of new information technologies with command-and-control stability, communication between adversaries, and other aspects of crisis decision making. This all occurs as part of information operations where opposing sides are attempting to shape an adversary's perception of risk through information manipulation.

It is worth noting that the Cold War did not see a crisis in which states were armed with advanced cyber weapons and nuclear weapons. Employment of mis- and disinformation was a much slower process than it is today. Analog systems were state of the art for much of the Cold War, and certainly for much of the technology used in nuclear delivery systems. They were reliable and,

at least for the United States, the periodic modernization effort that was due in the 1990s never took place because of the Soviet Union's collapse in 1991. Thus, the implications of cyber-based information warfare and cross-domain deterrence—using capabilities in one domain to deter action in a different domain—were far less complex than they are now. Recent advances in the cyber and space domains are changing the fundamental dynamics of deterrence and making Cold War "general deterrence" obsolete. It is worth noting that any nuclear crisis, and possible war, will likely begin with an effort to manipulate an adversary's situational awareness and create a false perception.

Today, the nuclear-cyber relationship has special significance for the United States and Russia and makes deterrence a much more complex task—particularly as the United States undertakes a digital transformation of its nuclear command, control, and communication (NC3) system (Lowther, 2020). If cyber-security experts are correct about the "D5" of cyber security, then it should come as no surprise that the United States can expect Russian and Chinese cyber warriors to focus on ways to deceive, degrade, deny, disrupt, and destroy a new digital NC3 architecture in an effort to prevent the United States from understanding what they may be doing and from commanding and controlling their nuclear forces (Reed, 2013). In such an information operation, disinformation plays a critical role because it is deception, not destruction, that is the apex of cyber conflict. Too few appreciate fully the role information and information operations play in deterrence because it is too easy to focus on the destructive capacity of nuclear weapons. Thus, in the pages that follow, it is important to keep in mind the role information operations play in crisis and escalation management. With Russia and the United States possessing approximately 90 per cent of the world's nuclear weapons and employing the most advanced offensive and defensive cyber capabilities, the real threat of employing disinformation through the cyber domain is growing (Thomas, 2015). This chapter explores the implications of this development in two steps (Futter, 2016a, 2016b; Gartzke, 2017). First, it considers the larger question of nuclear-cyber relationships in the present and near term. Second, it turns to specific issues related to nuclear crisis management.

Understanding the Nuclear-Cyber Nexus

What are the implications of potential overlap between concepts or practices for cyber war and nuclear deterrence (Arquilla, 2008; Libicki, 2009, 2017; Singer & Friedman, 2014)? Although cyber war and nuclear conflict may seem

to take place at opposite ends of the conflict spectrum, they are distinctly interrelated. Cyber weapons should appeal to those who prefer a non-nuclear military-technical arc of development, but they are also the thread that ties nuclear decision making to nuclear weapons employment. War in the cyber domain offers a possible means of crippling enemy assets without the need for kinetic attack—potentially minimizing physical destruction (Koshkin, 2013; Thomas, 2005). Nuclear weapons, on the other hand, are the very epitome of "mass" destruction. Their use for deterrence—the avoidance of war by the manipulation of risk—is preferred to their actual use in conflict. Unfortunately, neither nuclear deterrence nor cyber war exist in distinct policy universes, something that was possible in the Cold War and the early post–Cold War period.

Nuclear weapons, whether held back for deterrence or fired in anger, require effective command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). These weapons and their C4ISR systems must be protected from physical and cyber-attack (Lowther, 2020). Decision makers managing nuclear forces should ideally have the best possible information about the status of their own forces, adversary forces, and the probable intentions and risk acceptance of an adversary. In short, the task of managing nuclear-deterrence operations demands clear thinking and good information. Where there was a clearly defined boundary between peace and war during the Cold War, both China and Russia now employ doctrine that sees war as a constant and something that begins in the information environment (Bowen, 2020; Goode, 2008). Cyber weapons are designed to impede clear assessment of the strategic environment by achieving one or more of the "D5" effects (degrade, deny, disrupt, destroy, deceive), with a focus on deception, in the C4ISR networks of the United States (Libicki, 2007; Reed, 2013). The temptation to use cyber-attacks early against NC3 networks, for example, might make a nuclear crisis less stable rather than pre-empt a conflict altogether. In short, attempts to introduce disinformation during a nuclear crisis can lead to greater instability.

Ironically, the downsizing of American and Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and non-proliferation, makes cyber and nuclear attack capabilities more alarming as the incentive moves toward use of both to pre-empt an adversary. The supersized deployments of missiles and bombers and expansive numbers of weapons kept by the Cold War Americans

and Soviets had at least one virtue. Those arsenals provided so much redundancy against first-strike vulnerability that relatively linear systems for nuclear attack warning, command and control, and responsive launch under or after attack, sufficed. At the same time, Cold War cyber weapons were primitive compared to those available now, and it was almost impossible to penetrate command-and-control networks for the purpose of introducing disinformation. In addition, countries and their armed forces were less dependent on the fidelity of their information systems for national security. Thus, the reduction of American and Russian 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 (Forsyth, 2010; Payne, 2013). Although the mathematics of minimum deterrence would shrink the size of attackers' as well as defenders' arsenals, defenders with smaller forces might have greater fears of absolute compared to relative losses—and, therefore, be more prone to pre-emption-dependent strategies than defenders with larger forces. In other words, deception carries a much greater cost.

Offensive cyber operations are very much on the minds of American military leaders (Kaplan, 2016; Sanger, 2013). Russia is explicit about its cyber concerns. President Vladimir Putin urged the Russian Security Council in early July 2013 to improve state security against cyber-attacks, and it remains concerned about cyber-attacks on NC3 networks ("Putin calls," 2013). The war in Ukraine has only heightened this concern. Russian security expert Vladimir Batyuk, commenting favourably on a June 2013 Russo-American agreement for protection, control, and accounting of nuclear materials (a successor to the recently expired Nunn-Lugar agreement on nuclear risk reduction) warned that pledges by Presidents Putin and Obama for co-operation on cyber security were even more important: "Nuclear weapons are a legacy of the 20th century. The challenge of the 21st century is cyber security" (Earle, 2013).

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 negotiators seeking cyber arms control can certify that hackers within their own states are sufficiently under control for cyber verification and transparency. Both Russia and China reportedly use ad hoc and unofficial hackers to conduct operations to which governments would prefer to remain officially unconnected. For example, Russia's hacking into the email account of the Democratic National Committee in 2016 was attributed by some sources to

Table 2.1. Comparative Attributes of Cyber War and Nuclear Deterrence

Cyber war	Nuclear deterrence
The source of attack may be ambiguous—third-party intrusions masquerading as other actors are possible.	The source of attack is almost certain to be identified if the attacker is a state. Even terrorist attackers with nuclear materials are traceable.
Damage is primarily focused on data, although physical effects are possible.	Damage, even in the case of a limited nuclear war, can be large-scale destruction of property and life.
Denial of an attacker's objectives is feasible if defences are sufficiently robust and/or penetrations can be repaired in good time.	Deterrence by denial is less credible than the threat of punishment by assured retaliation.
The objective of cyber-attacks is typically disruption or confusion rather than destruction.	Nuclear deterrence rests on the credible threat of massive and prompt destruction of assets and populations.
Cyber-attacks can continue over an extended period without detection and sometimes without doing obvious or significant damage.	The first use of a nuclear weapon since 1945 by a state or non-state actor for a hostile purpose would be a game-changing event.
The price of entry for cyber war is comparatively low.	Building and operating a nuclear deterrent requires that a state spend significant time, talent, and treasure.

Sources: Gartzke, 2017; Libicki, 2017; Thomas, 2012.

"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 FSB—the official Russian security agency—with involvement by Russian military intelligence (Lourie, 2017; Roberts, 2016; Thomas, 2012). In this case, email was exfiltrated and exposed to cause political chaos. How much worse could the consequences be of a disinformation campaign within American nuclear command-and-control networks?

On the one hand, cyber cuts across the land, sea, air, and space domains. Cyber, compared to the other domains, suffers from a lack of historical perspective. The cyber domain "has been created in a short time and has not had the same level of scrutiny as other battle domains," as one author has argued (Magee, 2013). What this might mean for the cyber-nuclear intersection is far from obvious. Table 2.1 above summarizes some of the major attributes that distinguish nuclear deterrence from cyber war according to experts, but the differences between nuclear and cyber listed here do not contradict the prior observation that cyber and nuclear operations inevitably interact in practice.

Crisis Management: Definitions and Parameters

One of the most important areas where the development of the cyber domain is reshaping nuclear deterrence is the realm of crisis management. Where Cold War nuclear crises were largely an issue of accurately judging the will of the adversary, cyber warfare, particularly attacks against NC3 systems, are certain to reshape deployed systems, the trustworthiness of information, and how data is used. Crisis management, including nuclear crisis management, is both a competitive and co-operative endeavour between adversaries. A crisis is, by definition, a time of great tension and uncertainty (George, 1991; George & Simons, 1994; Tetlock, 1990; Williams, 1976).

All crises are characterized to some extent by a high degree of threat, limited decision-making windows, and a "fog of crisis" reminiscent of Clausewitz's "fog of war" that leaves crisis participants confused as to what is happening—a particular problem in a digital-dependent world. The influence of nuclear weapons on crisis decision making is not easy to measure or document because the avoidance of war is ascribed to many causes. The presence of nuclear forces obviously influences the degree of destruction that can be done should crisis management fail. As in the past, information about an adversary's capability and will are critical elements in a decision maker's selection of a course of action. If, for example, the presidents of Russia or of the United States fear they are the victims of disinformation and do not trust the information they receive or their ability to command and control nuclear forces, they may find themselves unwilling to show the strategic patience displayed during the nuclear crises of the Cold War (Burr, 2021).

Crisis Management: The Requirements

The first requirement for successful crisis management is the ability to trust one's intelligence and effective communications that include clear signalling and undistorted messaging. *Signalling* 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 accurate and correctly sent and received signals are a prerequisite to effective transfer of enemy goals and objectives from one side to the other. If signals are poorly sent or misunderstood, steps taken by the sender or receiver may lead to unintended consequences, including miscalculated escalation.

Messaging 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 behaviourally with accurate transmission. As Keith B. Payne notes,

With regard to the potential for deterrence failure in the post–Cold War period:

> unfortunately, our expectations of opponents' behavior frequently are unmet, not because our opponents necessarily are irrational but because we do not understand them—their individual values, goals, determination, and commitments—in the context of the engagement, and therefore we are surprised when their "unreasonable" behavior differs from our expectations. (Payne, 1996, p. 57)

This challenge is made harder when adversaries are actively engaged in a disinformation campaign against the very systems that allow decision makers to evaluate data. Such an added challenge was not present during the Cold War and is still poorly understood by modern scholars.

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 resolution. In decision pathologies possible under 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 self-fulfilling prophecy shared among leaders in Berlin, St. Petersburg, and Vienna that only by prompt mobilization and attack could decisive losses be avoided in war (Tuchman, 2004). This view resulted from the inability of ruling monarchs to have accurate information concerning the capability and will of a rival. Today, a similar challenge exists in nuclear conflict, where nuclear armed adversaries possess cyber capabilities that generate a similar effect—compressing the time to decide.

One result of attack time compression, which is the shortening of response time that results from weapons reaching targets more quickly and the possible disabling of integrated tactical warning and attack assessment (ITW/AA) in a cyber-attack (introduction of disinformation), is that the likelihood of undetected attacks and falsely detected attack errors increases—a real fear in an era when an adversary may have the ability to penetrate one's NC3 system and either introduce false positives or hide inbound weapons (Erwin, 2021). During the Cold War, there was little concern that a cyber-attack would make it impossible for the United States to trust its own ITW/AA. Tactical warning and intelligence networks grow accustomed to the routine behaviour of other states' forces. However, the real possibility that an adversary can penetrate NC3 systems and deceive those networks creates greater instability and a preference for striking before NC3 systems—and trusted data—are lost to cyber-attack. Thus, stability during a crisis is certain to depend on modernized NC3 networks that assure the nuclear mission in the face of cyber-attack—no easy task.

A third attribute of successful crisis management is that each side should be able to offer the other a safety valve or a face-saving exit from a predicament that has escalated beyond its original expectations. The search for options should back neither crisis participant into a corner from which there is no graceful retreat. For example, during the Cuban Missile Crisis of 1962, President John F. Kennedy was able to offer Soviet premier Nikita Khrushchev a face-saving exit from his overextended missile deployments. Kennedy publicly committed the United States to refraining from future military aggression against Cuba and privately agreed to remove and dismantle Jupiter medium-range ballistic missiles deployed within NATO nations (Lebow & Stein, 1995). Kennedy and his inner circle recognized, after some days of deliberation and clearer focus on the Soviet view of events, that the United States would lose, not gain, by a public humiliation of Khrushchev that might, in turn, diminish Khrushchev's interest in any mutually agreed solution to the crisis. A debilitating cyber-attack, making it impossible to have situational awareness, early in a crisis/conflict could make an action untenable. Given the often unknown consequences and second- or third-order effects of a cyber-attack, reversing course may prove challenging.

A fourth attribute of successful crisis management is that each side maintains an accurate perception of the other's intentions and military capabilities—the antithesis of what disinformation seeks to achieve. 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. Maintaining the confidence to wait is an important aspect of managing a crisis. This is largely dependent on each adversary's certainty that the information upon which they rely to make decisions is trustworthy. Thus, it should come as no surprise that the most dangerous of the D5 effects is deceive, not destroy. When decision makers cannot trust information, which may support holding firm over acting, Robert Jervis's admonition becomes increasingly relevant. Jervis warned that Cold War beliefs in the inevitability of war might have created a self-fulfilling prophecy:

> The superpowers' beliefs about whether or not war between them is inevitable create reality as much as they reflect it. Because pre-emption 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. (Jervis, 1989, p. 183)

Intentions can change during a crisis if policy-makers become more optimistic about gains or more pessimistic about potential losses. Capabilities can change due to the management of military alerts and the deployment or other movement of military forces. Heightened states of military readiness on each side are intended to send a two-sided signal of readiness for the worst if the other side attacks and of a non-threatening steadiness of purpose in the face of enemy passivity. This mixed message is hard to send under the best of crisis-management conditions, since each state's behaviours and communications, as observed by its opponent, may not seem consistent. It is even harder when the very information used to make decisions is under attack.

Under the stress of time pressures and military threats, different parts of complex security organizations make decisions consistent with bureaucratic interests. These decisions may not coincide with a national leader's intent, or with the decisions and actions of other parts of the government. As Alexander L. George explains,

> 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. (George, 1991, p. 18)

This challenge is unimaginably harder when the very NC3 system that allows a president or prime minister to communicate with forces is itself the target of an adversary.

UNCERTAINTY

Cyber warfare is certain to disrupt successful crisis management on each of the preceding attributes (Davis, 2015). For a decision maker, it is imperative that intelligence and NC3 information is trustworthy. The possibility of cyber-enabled pre-emption—to disable enemy nuclear missiles before they reach the launch pad or during the launch itself—is a real possibility that military leaders in China, Russia, and the United States all fear. Such "left-of-launch" techniques were used by the United States against North Korea (Sanger, 2017). 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? The answer to this question is unknown.

Cyber warfare can also destroy or disrupt communication channels necessary for successful crisis management. One way cyber warfare can do this is to disrupt communication links between policy-makers and military commanders during a period of high threat and severe time pressure. Two kinds of unanticipated problems, from the standpoint of civil-military relations, are possible under these conditions. First, political leaders may have pre-delegated limited authority for nuclear release or launch under restrictive conditions: only when these few conditions are present, according to the protocols of pre-delegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Disrupted communications could prevent top leaders from understanding the perceptions of military commanders, who may see circumstances as far more desperate, and thus permissive of nuclear initiative, than the reality of the situation would warrant. 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 resulted in a decision by submarine officers to launch in the absence of contrary instructions.

Second, cyber-attacks during a crisis will almost certainly increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived timelines within which the policy-making process results in decisions. Once either side sees parts of its nuclear command, control, and communications system being degraded, disrupted, denied, destroyed, or deceived, its sense of panic at the possible loss of military options becomes enormous. We cannot underscore enough the serious implication of disinformation efforts in nuclear crisis management. In the case of US Cold War nuclear war plans, for example, disruption of even portions of the strategic command, control, and communications system could have prevented competent execution of parts of the single integrated operational plan (SIOP). The Cold War SIOP depended upon finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets. Mis- or disinformation in the NC3 system was likely to lead 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 options, the potential slide toward pre-emption, based on mistaken or exaggerated fears of command-and-control vulnerability, casts a shadow over deterrence stability. As Bruce Blair 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. (Blair, 1993, p. 118)

A third potentially disruptive effect of cyber-attacks on nuclear crisis management is that such attacks may reduce the search for available alternatives to the few and desperate. Policy-makers searching for an escape from crisis denouements need flexible options and creative problem solving. Victims of information warfare may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be poorly posed,

and responses (if available at all) will be driven toward the least common denominator of previously programmed standard operating procedures. Retaliatory systems that depend on launch on warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives:

> A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality. (Blair, 1993, p. 252)

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions in non-military bureaucratic organizations (March & Simon, 1958). 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—a particular challenge when an adversary is targeting the information that allows you to command and control forces. This challenge did not exist during the Cold War because the technical capacity to wage cyber war did not exist.

Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban Missile Crisis, for example, several members of the presidential advisory group continued to propound air strikes and invasion of Cuba during the entire thirteen days of deliberation (Allison & Zelikow, 1999). Had less time been available for debate, and had President Kennedy not deliberately structured the discussion in a way that forced alternatives to the surface, the air strike and invasion might well have been the chosen alternative (Lebow & Stein, 1995). As Paul K. Davis notes,

> 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 pre-emptive 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. (Davis, 2015, p. 14)

If the challenge for effective decision making and the fear of a mistake was this high during an era when an adversary could not achieve D5 effects against NC3 systems, it is easy to imagine how much more complex today's challenge is for a president or prime minister who faces a cyber challenge they do not fully understand.

Fourth, cyber-attacks can cause flawed images of each side's intentions and capabilities to be conveyed to the other, with potentially disastrous results. Another example from the Cuban Missile Crisis demonstrates the possible side effects of simple misunderstanding and non-communication on American crisis management. At the tensest period of the crisis, a U-2 reconnaissance aircraft strayed into Soviet airspace. American and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defences might have interpreted the U-2 flight as either a pre-strike reconnaissance mission or a bomber, calling for a compensatory response by Moscow (Allison & Zelikow, 1999; Lebow & Stein, 1995; Sagan, 1989). Fortunately, Moscow chose to give the United States the benefit of the doubt in this instance and to permit American 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. This Cold War example of uncertainty generated by a lack of information is similar to the psychological affect generated by a cyber-attack, although, in this incident, neither side's ability to command, control, and communicate with nuclear forces was threatened, which gave both sides, particularly the Soviets, more breathing room to withhold action.

The preceding discussion is underscored by the assessment of Martin Libicki, who writes,

> 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. (Libicki, 2012)

SCENARIOS AND RISKS

The outcome of a nuclear crisis influenced by cyber-attacks may not be favourable. 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-attacks 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 takes place. Although there is no such thing as a "small" nuclear war, compared to conventional war, there can be different kinds of nuclear wars, in terms of their proximate causes and consequences (Questor, 2006). 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 low- or very-low-yield nuclear detonation.

The prospect of a general nuclear war between the United States and the Soviet Union preoccupied Cold War policy-makers. 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, offered a more complicated menu of nuclear possibilities and responses and led to the creation of tailored deterrence, which suggested it was imperative to understand an adversary's history, culture, and other characteristics to design a tailored deterrence approach for that specific country (Questor, 2006). General deterrence was no longer enough. 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, stretched the ingenuity of military planners and fiction writers alike.

In addition to the world's worst characters engaged in nuclear threat or first use, there was also the possibility of backsliding in political conditions as between the United States and Russia, or Russia and China, or China and India (among current nuclear weapons states). The nuclear "establishment" or P-5 thus includes cases of current de-bellicization or pacification that

depend upon the continuation of favourable political auguries in regional or global politics. A common susceptibility to cyber intrusion and the injection of disinformation across all critical command, control, and communication networks also creates mutual vulnerability that helps deter any nuclear power acting too aggressively. Politically unthinkable conflicts of one decade have a way of evolving into the politically unavoidable wars of another—the First World War 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. 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 are deployed with national or coalition armed forces. In NATO territory, the United States deploys several hundred air-delivered nuclear weapons among bases in Belgium, Germany, Italy, the Netherlands, and Turkey (Kristensen, 2005). Russia retains at least several thousand non-strategic nuclear weapons, including significant numbers deployed in western Russia (Kipp, 2010; Podvig, 2010). The New START agreement establishes notional parity between the United States and Russia in nuclear systems of intercontinental range (Cimbala, 2020; Payne, 2020). But American superiority in advanced technology and information-based conventional military power leaves Russia heavily reliant on tactical nuclear weapons as compensation for 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 (Pietkiewicz, 2018; Sokov, 2010). Vladimir Putin's nuclear threats in the wake of Russia's invasion of Ukraine changed that (Arnold, 2022). With Putin incorporating disinformation into his larger information operation against NATO, it is even harder to make sense of his nuclear threats.

Outside of the current conflict, Russia's military doctrine indicates a willingness to engage in nuclear first use in situations of extreme urgency for Russia, as defined by its political leadership (Giles, 2010). 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

tactical nuclear weapons, deployed among NATO allies. An expert panel convened by NATO 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 issue 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 majority sentiment of governments that these weapons provided a necessary link in the chain of alliance deterrence options (NATO, 2010). As the authors were told in a 2016 visit to NATO headquarters, "NATO is a nuclear alliance" (Delegation, 2016). This last statement is even more important in the wake of Russian aggression and threats.

Imagine now the unfolding of a nuclear crisis or the taking 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 opposed command, control, and communications. Disruptive cyber-attacks 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 European-wide conflict or a strategic nuclear war. All of 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 is crossed.

Three new kinds of frictions are posed for NATO. The cohesion of allied governments is tested under conditions of unprecedented stress and danger, doubtless aided by a confused situation on the battlefield. Second, reliable intelligence about Russian intentions following first use is essential. Third, the first use of a nuclear weapon in anger since Nagasaki establishes a new psychological, political, and moral universe within which negotiators for de-escalation and war termination somehow have to maintain their sang-froid, obtain agreed stand-downs, and return nuclear-capable launchers and weapons to secured, but transparent, locations. All of this would be taking place within the panic-spreading capabilities of 24/7 news networks, disinformation-filled social media, and the larger Internet.

Theoretically, one might finesse the issue by eliminating cyber operations that potentially conflict with de-escalation. But the political desire to do so is in conflict with the military necessity for timely information gathering, assessment, and penetration of enemy networks—in order to accomplish two necessary, but somewhat opposed, missions. First, each side wants to

correctly anticipate the timing and character of the other's decision for nuclear first use—and, if possible, to throw logic bombs, Trojan Horses, electronic warfare, or other impediments in the way (or, if finesse is not at hand, bombing the relevant installations is always an option, although an obviously provocative one). Second, and somewhat opposed, is the need to communicate reliably with the other side as regards their preferences for de-escalation, a willingness to do so if reciprocity can be obtained, and an awareness of the possibility that the situation will shortly get out of hand. Consider the Russian president and general staff filtering messages while forces were fighting in Georgia, Ukraine (having been taken into NATO membership the previous year, over Russia's objections), or elsewhere.

The problem of nuanced messages and the management of de-escalation, even short of war, is illustrated by NATO's command post exercise Able Archer, conducted 7–11 November 1983. An annual exercise, Able Archer was intended to practise nuclear release procedures. Soviet intelligence routinely monitored these exercises. However, the 1983 version took place against a backdrop of rising Soviet-American 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. Russian sensitivities to the possibility of US or NATO nuclear first strike were high because NATO began deploying Pershing II ballistic missiles and ground-launched cruise missiles, 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 US intentions (N. Jones, 2018; Kastner, 2018). The case illustrates how mistaken interpretations of "normal" events can overvalue pessimistic assessment at just the wrong time (Andrew & Gordievsky, 1990; Gates, 1996;). 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. (N. Jones, 2018)

Similar problems in coordinating the management of de-escalation and conflict termination with the conduct of cyber conflict may appear in two other situations. First, already alluded to, is the use of a bunker-busting or other advanced technology conventional weapons that the other side, during the fog of crisis or war, confused 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. New START counting rules will regard conventionally armed ballistic missiles as also nuclear-capable launchers and, therefore, subject to overall restrictions on the numbers of deployed launchers and weapons. American plans for prompt global strike (PGS) systems, including missiles or future space planes, were first approved during the George W. Bush administration, and carried forward under the Obama administration.

A second illustration, apart from escalation in Europe, of the problem of managing escalation control and conflict termination along with information operations is provided by the possibility of a joint NATO-Russian theatre missile defence (possibly including air defences) system. The idea has expert and highly visible political proponents on both sides of the Atlantic, and official Russian commentators do not close the door to co-operation on ballistic missile defences (BMD). NATO and Russia are facing in two political directions: (1) wariness, but also openness, toward one another; and (2) concern about possible future Iranian or other Middle Eastern nuclear weapons in the hands of leaders beyond deterrence based on the credible threat of nuclear (or other) retaliation.

However, the problems of obtaining missile defence co-operation as between NATO and Russia are not only political. Even with the best of intentions among American, European, and Russian negotiators, the military-technical problems of coordinating BMD command, control, and communications systems are considerable—even before Russia's invasion of Ukraine. Indeed, they are not strictly "military-technical" but also heavily embedded with issues of political sovereignty, classified intelligence, and trust among governments and militaries that are currently waging low-level cyber war against one another. Even NATO militaries differ in their views. For example, if a

European theatre-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 and Russia agree before responding? Perhaps most importantly, can NATO members trust that Russia will not engage in cyber-attacks against such a system?

If a political crisis between NATO and Russia erupts—and the war in Ukraine arguably is such a crisis—and both sides already deploy missile defences, will Russian or American cyber warriors attack the other's missile defences? Would it be better to reassure Russia as to the surety of its independent capabilities or share capabilities with NATO? Neither Russia nor the United States want to relinquish sovereign control over missile defences. However, it may be prudent to co-operate to establish trust and de-escalate the growing cyber conflict that is causing increasing instability in the nuclear deterrence relationship between the two countries. Although, missile defences may appear tangential to the larger issue of nuclear deterrence and cyber-attack, it is an opportunity for two countries that are clearly at war in cyberspace to co-operate in a needed and useful manner (S. Jones, 2018).

Conclusion

The United States and Russia learned to manage nuclear crises and peacetime deterrence during the Cold War and prior to the rise of the cyber domain. Advanced cyber-attacks against nuclear production facilities (e.g., Stuxnet) are well-known. Convincing American, Chinese, or Russian leaders that NC3 systems are also likely targets takes very little effort. The implications for such attacks on crisis stability are unknown in that such an event has yet to take place, leaving us to speculate about the impact of cyber-attacks and efforts to inject technical disinformation into systems responsible for nuclear crisis management. What we do know is that the decades ahead are unlikely to look like the Cold War (Ellsberg, 2017; Fursenko & Naftali, 1997; Khrushchev, 1990). As the discussion above suggests, the future is likely filled with increased risk and the possibility of imminent attack and a bias for pre-emptive action, where striking first is 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 successfully communicated to, and believed by, the other side. Deterrence is fundamentally an information operation that, because of

technological developments, is increasingly susceptible to the injection of disinformation into nuclear command, command, and control systems (Sechser & Fuhrmann, 2017; Gray, 1996). Contrary to popular belief, deterrence and disinformation are intrinsically linked.

REFERENCES

Allison, G., & Zelikow, P. (1999). Essence of decision: Explaining the Cuban Missile Crisis. Pearson.

Andrew, C., & Gordievsky, O. (1990). KGB: The inside story of its foreign operations from Lenin to Gorbachev. Harper.

Arnold, L. (2022, 9 November). Why Russia's nuclear threats are difficult to dismiss: QuickTake. Washington Post. https://www.washingtonpost.com/business/why-russias-nuclear-threats-are-difficult-to-dismiss-quicktake/2022/11/09/2934f1b0-603d-11ed-a131-e900e4a6336b_story.html

Arquilla, J. (2008). Worst enemy: The reluctant transformation of the American military. Ivan R. Dee.

Blair, B. (1993). The logic of accidental nuclear war. Brookings Institution Press.

Bowen, A. (2020, 20 August). Russia armed forces: Military doctrine and strategy. In Focus. Congressional Research Service. https://sgp.fas.org/crs/row/IF11625.pdf

Burr, W. (2021, 26 May). Alerts, crises, and DEFCONS. National Security Archives. https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2021-03-17/alerts-crises-defcons

Cimbala, S. J. (2020). The United States, Russia, and nuclear peace. Palgrave Macmillan.

Davis, P. K. (2015). Deterrence, influence, cyber-attack, and cyber War. International Law and Politics, 47(4), 327–57.

Davis, P. K., Wilson, P., Kim, J., & Park, J. (2016). Deterrence and stability for the Korean Peninsula. Korean Journal of Defense Analysis, 28(1), 1–23.

Delegation, UN. (2016, 17 May). Discussion of nuclear strategy [Interview]. Brussels.

Earle, J. (2013, 18 June). US and Russia sign new anti-proliferation deal. Moscow Times. https://www.themoscowtimes.com/2013/06/18/us-and-russia-sign-new-anti-proliferation-deal-a25070

Ellsberg, D. (2017). The doomsday machine: Confessions of a nuclear war planner. Bloombury Publishing.

Erwin, S. (2021, 2 May). Sen. Angus King: Cybersecurity a major concern in US nuclear command-and-control system. Space News. https://spacenews.com/sen-angus-king-cybersecurity-a-major-concern-in-u-s-nuclear-command-and-control-system/

Forsyth, J. W. (2010). Remembrance of things past: The enduring value of nuclear weapons. Strategic Studies Quarterly, 4(1), 74–89. https://www.jstor.org/stable/26269780

Fursenko, A., & Naftali, T. (1997). "One hell of a gamble": Khrushchev, Castro, and Kennedy, 1958–1964. W. W. Norton.

Futter, A. (2016a, 15 July). Cyber threats and nuclear weapons: New questions for command and control, security and strategy. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/occasional-papers/cyber-threats-and-nuclear-weapons-new-questions-command-and-control-security-and-strategy/

Futter, A. (2016b, 29 June). The double-edged sword: US nuclear command and control modernization. Bulletin of the Atomic Scientists. https://thebulletin.org/2016/06/the-double-edged-sword-us-nuclear-command-and-control-modernization/#:~:text=In%20the%20realm%20of%20nuclear%20command%20and%20control%2C,vulnerable%20to%20those%20seeking%20to%20interfere%20with%20them

Gartzke, E. (2017). Thermonuclear cyberwar. Journal of Cybersecurity, 3(1), 37–48. https://doi.org/10.1093/cybsec/tyw017

Gates, R. (1996). From the shadows: The ultimate insider's story of five presidents and how they won the Cold War. Simon and Schuster.

George, A. (1991). Avoiding war: Problems of crisis management. Westview Press.

Giles, K. (2010). The military doctrine of the Russian Federation 2010. Research Review. Research Division—NATO Defense College. Retrieved 20 June 2023 from https://www.academia.edu/343489/The_Military_Doctrine_of_the_Russian_Federation_2010

George, A. L., & Simons, A. G. (1994). The limits of coercive diplomacy. Westview Press.

Goode, M. (2008). Chinese national strategy of total war [Graduate research paper]. Air Force Institute of Technology. https://apps.dtic.mil/dtic/tr/fulltext/u2/a487635.pdf

Gray, C. (1996). Explorations in strategy. Greenwood Press.

Jablonsky, D. (1991). Strategic rationality is not enough: Hitler and the concept of crazy states. Progressive Management.

Jervis, R. (1989). The meaning of the nuclear revolution: Statecraft and the prospect of armageddon. Cornell University Press.

Jones, N. (2018, 5 November). The Soviet side of the 1983 war scare. National Security Archives. https://nsarchive.gwu.edu/briefing-book/aa83/2018-11-05/soviet-side-1983-war-scare

Jones, S. (2018, 1 October). Going on the offesive: A US strategy to confront US information warfare. Centre for Strategic and International Studies. https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare

Kaplan, F. (2016). Dark territory: The secret history of cyber war. Simon and Schuster.

Kastner, J. (2018, 31 May). Standing on the brink: The secret war scare of 1983. The Nation. https://www.thenation.com/article/archive/standing-on-the-brink-the-secret-war-scare-of-1983/#:~:text=Standing%20on%20the%20Brink%3A%20The%20

Secret%20War%20Scare,November%203%2C1983%2C%20press%20briefing%20at%20the%20White%20House

Khrushchev, N. S. (1990). Khrushchev remembers: The Glasnost tapes. Little and Brown.

Kipp, J. (2010). Russia's tactical nuclear weapons and Eurasian security. Eurasia Daily Monitor, 7(44). https://jamestown.org/program/russias-tactical-nuclear-weapons-and-eurasian-security/

Koshkin, P. (2013). Are cyber wars between great powers possible? A group of Russian security experts debate the likelihood of a cyber war involving the US, Russia, or China. Russia Direct. https://russia-direct.org/debates/are-cyberwars-between-major-powers-possible

Kristensen, H. (2005). A Review of post–Cold War policy, force levels, and war planning. Natural Resources Defense Council. https://www.nuclearinfo.org/wp-content/uploads/2021/09/NRDC_Kristensen_US_Nuclear_Weapons_in_Europe_A_Review_of_post_cold_War_Policy_Force_Levels_and_war_planning_February_2005_volume_1_of_1..pdf

Lebow, R. N., & Stein, J. G. (1995). We all lost the Cold War. Princeton University Press.

Libicki, M. C. (2007). Conquest in cyberspace: National security and information warfare. Cambridge University Press.

Libicki, M. C. (2009). Cyberdeterrence and cyber war. RAND Coprporation.

Libicki, M. C. (2012). Crisis and escalation in cyberspace. RAND Coprporation.

Libicki, M. C. (2017). The convergence of information warfare. Strategic Studies Quarterly, 11(1), 49–65. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf

Lourie, R. (2017). Putin: His downfall and Russia's coming crash. St. Martins Press.

Lowther, A. (Ed.). (2020). Guide to nuclear deterrence in the age of great power competition. Louisiana Tech Research Institute.

Magee, C. (2013). Awaiting cyber 9/11. Joint Forces Quarterly, 70(3), 76–82. https://www.thefreelibrary.com/Awaiting+cyber+9/11.-a0338119401

March, J. M., & Simon, H. A. (1958). Organizations. John Wiley and Sons.

NATO. (2010, 17 May). NATO 2020: Assured security; dynamic engagement. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natolive/official_texts_63654.htm

Payne, K. (1996). Deterrence in the second nuclear age. University of Kentucky Press.

Payne, K. (2013). Minimum deterrence: Examining the evidence. Routledge.

Payne, K. (2020). Shadows on the wall: Deterrence and disarmament. National Institute of Public Policy.

Pietkiewicz, M. (2018). The military doctrine of the Russian Federation. Polish Political Science Yearbook, 47(3), 505–20.

Podvig, P. (2010, 25 February). What to do about tactical nuclear weapons. Bulletin of the Atomic Scientists. https://thebulletin.org/2010/02/what-to-do-about-tactical-nuclear-weapons/

"Putin calls to strengthen protection against cyber-attacks." (2013, 5 July). Itar-Tass. https://tass.com/russia/696603

Questor, G. (2006). Nuclear first strike: Consequences of a broken taboo. Princeton University Press.

Reed, J. (2013, 12 April). The five deadly Ds of the air force's cyber arsenal. Foreign Policy. https://foreignpolicy.com/2013/04/12/the-five-deadly-ds-of-the-air-forces-cyber-arsenal/

Roberts, B. (2016). The case for US nuclear weapons in the 21st century. Stanford University Press.

Sagan, S. (1989). Moving targets: Nuclear strategy and national security. Little and Brown.

Sanger, D. (2013, 13 August). NSA leaks make plan for cyberdefense unlikely. New York Times. https://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html#:~:text=But%20administration%20officials%20say%20the%20plan%2C%20championed%20by,over%20the%20recent%20disclosures%20about%20its%20surveillance%20programs

Sanger, D. (2017, 4 March). Trump inherits a secret cyberwar against North Korean missiles. New York Times. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html

Sechser, T.S., & Fuhrmann, T. (2017). Nuclear weapons and coercive diplomacy. Cambridge University Press.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Sokov, N. (2010, 5 February). The new, 2010 Russian military doctrine: The nuclear angle. James Martin Center for Nonproliferation Studies. https://nonproliferation.org/new-2010-russian-military-doctrine/

Tetlock, P. E. (1990). Introduction. In P. E. Tetlock, J. L. Husbands, R. Jervis, P. C. Stern, & C. Tilly, (Eds.), Behavior, society, and nuclear war (pp. 8–84). Oxford University Press.

Thomas, T. L. (2005). Cyber silhouettes: Shadows over information operations. Foreign Military Studies Office.

Thomas, T. L. (2012). Three faces of the cyber dragon: Cyber peace activist, spook, attacker. Foreign Military Studies Office.

Thomas, T. L. (2015). Russia: Military strategy—impacting 21st century reform and geopolitics. Foreign Military Studies Office.

Tuchman, B. (2004). The guns of August. Presidio Press.

Williams, P. (1976). Crisis management. John Wiley and Sons.