JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 3(1), 2017, 37–48
doi: 10.1093/cybsec/tyw017
Advance Access Publication Date: 14 February 2017
Research paper

Research paper

Thermonuclear cyberwar

Erik Gartzke[1] and Jon R. Lindsay[2,*]

[1]Department of Political Science, University of California, San Diego 9500 Gilman Dr. La Jolla, CA 92093, USA and [2]Munk School of Global Affairs, University of Toronto 15 Bloor Street West, Toronto, Ontario, M5S 0A7 Canada

*Corresponding author. E-mail: jon.lindsay@utoronto.ca.

Received 23 December 2016; accepted 23 December 2016

Abstract

Nuclear command and control increasingly relies on computing networks that might be vulnerable to cyber attack. Yet nuclear deterrence and cyber operations have quite different political properties. For the most part, nuclear actors can openly advertise their weapons to signal the costs of aggression to potential adversaries, thereby reducing the danger of misperception and war. Cyber actors, in contrast, must typically hide their capabilities, as revelation allows adversaries to patch, reconfigure, or otherwise neutralize the threat. Offensive cyber operations are better used than threatened, while the opposite, fortunately, is true for nuclear weapons. When combined, the warfighting advantages of cyber operations become dangerous liabilities for nuclear deterrence. Increased uncertainty about the nuclear/cyber balance of power raises the risk of miscalculation during a brinksmanship crisis. We should expect strategic stability in nuclear dyads to be, in part, a function of relative offensive and defensive cyber capacity. To reduce the risk of crisis miscalculation, states should improve rather than degrade mutual understanding of their nuclear deterrents.

Key words: cyber warfare; networks; cyber actors

Introduction

In the 1983 movie *WarGames*, a teenager hacks into the North American Air Defense Command (NORAD) and almost triggers World War III. After a screening of the film, President Ronald Reagan allegedly asked his staff, "Could something like this really happen?" The Chairman of the Joint Chiefs of Staff replied, "Mr. President, the problem is much worse than you think." The National Security Agency (NSA) had been hacking Russian and Chinese communications for years, but the burgeoning personal computer revolution was creating serious vulnerabilities for the United States too. Reagan directed a series of reviews that culminated in a classified national security decision directive (NSDD-145) entitled "National Policy on Telecommunications and Automated Information Systems Security." More alarmist studies, and potential remedies, emerged in recent decades as technicians and policymakers came to appreciate the evolving threat [1–3].

Cyber warfare is routinely overhyped as a new weapon of mass destruction, but when used in conjunction with actual weapons of mass destruction, severe, and underappreciated, dangers emerge. One side of a stylized debate about cybersecurity in international relations argues that offensive advantages in cyberspace empower weaker nations, terrorist cells, or even lone rogue operators to paralyze vital infrastructure [4–8]. The other side argues that operational difficulties and effective deterrence restrains the severity of cyber attack, while governments and cybersecurity firms have a pecuniary interest in exaggerating the threat [9–13]. Although we have contributed to the skeptical side of this debate [14–16], the same strategic logic that leads us to view cyberwar as a limited political instrument in most situations also leads us to view it as incredibly destabilizing in rare situations. In a recent Israeli wargame of a regional scenario involving the United States and Russia, one participant remarked on "how quickly localized cyber events can turn dangerously kinetic when leaders are ill-prepared to deal in the cyber domain" [17]. Importantly, this sort of catalytic instability arises not from the cyber domain itself but through its interaction with forces and characteristics in other domains (land, sea, air, etc.). Further, it arises only in situations where actors possess, and are willing to use, robust traditional military forces to defend their interests.

Classical deterrence theory developed to explain nuclear deterrence with nuclear weapons, but different types of weapons or combinations of operations in different domains can have differential

effects on deterrence and defense [18, 19]. Nuclear weapons and cyber operations are particularly complementary (i.e. nearly complete opposites) with respect to their strategic characteristics. Theorists and practitioners have stressed the unprecedented destructiveness of nuclear weapons in explaining how nuclear deterrence works, but it is equally, if not more, important for deterrence that capabilities and intentions are clearly communicated. As quickly became apparent, public displays of their nuclear arsenals improved deterrence. At the same time, disclosing details of a nation's nuclear capabilities did not much degrade the ability to strike or retaliate, given that defense against nuclear attack remains extremely difficult. Knowledge of nuclear capabilities is necessary to achieve a deterrent effect [20]. Cyber operations, in contrast, rely on undisclosed vulnerabilities, social engineering, and creative guile to generate indirect effects in the information systems that coordinate military, economic, and social behavior. Revelation enables crippling countermeasures, while the imperative to conceal capabilities constrains both the scope of cyber operations and their utility for coercive signaling [21, 22]. The diversity of cyber operations and confusion about their effects also contrast with the obvious destructiveness of nuclear weapons.

The problem is that transparency and deception do not mix well. An attacker who hacks an adversary's nuclear command and control apparatus, or the weapons themselves, will gain an advantage in warfighting that the attacker cannot reveal, while the adversary will continue to believe it wields a deterrent that may no longer exist. Most analyses of inadvertent escalation from cyber or conventional to nuclear war focus on "use it or lose it" pressures and fog of war created by attacks that become visible to the target [23, 24]. In a US–China conflict scenario, for example, conventional military strikes in conjunction with cyber attacks that blind sensors and confuse decision making could generate incentives for both sides to rush to preempt or escalate [25–27]. These are plausible concerns, but the revelation of information about a newly unfavorable balance of power might also cause hesitation and lead to compromise. Cyber blinding could potentially make traditional offensive operations more difficult, shifting the advantage to defenders and making conflict less likely.

Clandestine attacks that remain invisible to the target potentially present a more insidious threat to crisis stability. There are empirical and theoretical reasons for taking seriously the effects of offensive cyber operations on nuclear deterrence, and we should expect the dangers to vary with the relative cyber capabilities of the actors in a crisis interaction.

Nuclear command and control vulnerability

General Robert Kehler, commander of US Strategic Command (STRATCOM) in 2013, stated in testimony before the Senate Armed Services Committee, "we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves" [28]. Nuclear command, control, and communications (NC3) form the nervous system of the nuclear enterprise spanning intelligence and early warning sensors located in orbit and on Earth, fixed and mobile command and control centers through which national leadership can order a launch, operational nuclear forces including strategic bombers, land-based intercontinental missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and the communication and transportation networks that tie the whole apparatus together [29, 30]. NC3 should ideally ensure that nuclear forces will always be available if authorized by the National Command Authority (to enhance deterrence) and never used without authorization (to enhance safety and reassurance). Friendly errors or enemy interference in NC3 can undermine the "always-never" criterion, weakening deterrence [31, 32].

NC3 has long been recognized as the weakest link in the US nuclear enterprise. According to a declassified official history, a Strategic Air Command (SAC) task group in 1979 "reported that tactical warning and communications systems … were 'fragile' and susceptible to electronic countermeasures, electromagnetic pulse, and sabotage, which could deny necessary warning and assessment to the National Command Authorities" [33]. Two years later, the Principal Deputy Under Secretary of Defense for Research and Engineering released a broad-based, multiservice report that doubled down on SAC's findings: "the United States could not assure survivability, endurability, or connectivity of the national command authority function" due to:

> major command, control, and communications deficiencies: in tactical warning and attack assessment where existing systems were vulnerable to disruption and destruction from electromagnetic pulse, other high altitude nuclear effects, electronic warfare, sabotage, or physical attack; in decision making where there was inability to assure national command authority survival and connection with the nuclear forces, especially under surprise conditions; and in communications systems, which were susceptible to the same threats above and which could not guarantee availability of even minimum-essential capability during a protracted war. [33]

The nuclear weapons safety literature likewise provides a number of troubling examples of NC3 glitches that illustrate some of the vulnerabilities attackers could, in principle, exploit [34–36]. The SAC history noted that NORAD has received numerous false launch indications from faulty computer components, loose circuits, and even a nuclear war training tape loaded by mistake into a live system that produced erroneous Soviet launch indications [33]. In a 1991 briefing to the STRATCOM commander, a Defense Intelligence Agency targeteer confessed, "Sir, I apologize, but we have found a problem with this target. There is a mistake in the computer code …. Sir, the error has been there for at least the life of this eighteen-month planning cycle. The nature of the error is such that the target would not have been struck" [37]. It would be a difficult operation to intentionally plant undetected errors like this, but the presence of bugs does reveal that such a hack is possible.

Following many near-misses and self-audits during and after the Cold War, American NC3 improved with the addition of new safeguards and redundancies. As General Kehler pointed out in 2013, "the nuclear deterrent force was designed to operate through the most extreme circumstances we could possibly imagine" [28]. Yet vulnerabilities remain. In 2010, the US Air Force lost contact with 50 Minuteman III ICBMs for an hour because of a faulty hardware circuit at a launch control center [38]. If the accident had occurred during a crisis, or the component had been sabotaged, the USAF would have been unable to launch and unable to detect and cancel unauthorized launch attempts. As Bruce Blair, a former Minuteman missileer, points out, during a control center blackout the antennas at unmanned silos and the cables between them provide potential surreptitious access vectors [39].

The unclassified summary of a 2015 audit of US NC3 stated that "known capability gaps or deficiencies remain" [40]. Perhaps more worrisome are the unknown deficiencies. A 2013 Defense Science Board report on military cyber vulnerabilities found that while the:

> nuclear deterrent is regularly evaluated for reliability and readiness …, most of the systems have not been assessed (end-to-end) against a [sophisticated state] cyber attack to understand possible

> weak spots. A 2007 Air Force study addressed portions of this issue for the ICBM leg of the U.S. triad but was still not a complete assessment against a high-tier threat. [41]

If NC3 vulnerabilities are unknown, it is also unknown whether an advanced cyber actor would be able to exploit them. As Kehler notes, "We don't know what we don't know" [28].

Even if NC3 of nuclear forces narrowly conceived is a hard target, cyber attacks on other critical infrastructure in preparation to or during a nuclear crisis could complicate or confuse government decision making. General Keith Alexander, Director of the NSA in the same Senate hearing with General Kehler, testified that:

> our infrastructure that we ride on, the power and the communications grid, are one of the things that is a source of concern . . . we can go to backup generators and we can have independent routes, but . . . our ability to communicate would be significantly reduced and it would complicate our governance . . . . I think what General Kehler has would be intact . . . [but] the cascading effect . . . in that kind of environment . . . concerns us. [28]

Kehler further emphasized that "there's a continuing need to make sure that we are protected against electromagnetic pulse and any kind of electromagnetic interference" [28].

Many NC3 components are antiquated and hard to upgrade, which is a mixed blessing. Kehler points out, "Much of the nuclear command and control system today is the legacy system that we've had. In some ways that helps us in terms of the cyber threat. In some cases it's point to point, hard-wired, which makes it very difficult for an external cyber threat to emerge" [28]. The Government Accountability Office notes that the "Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation's nuclear forces" [42]. While this may limit some forms of remote access, it is also indicative of reliance on an earlier generation of software when security engineering standards were less mature. Upgrades to the digital Strategic Automated Command and Control System planned for 2017 have the potential to correct some problems, but these changes may also introduce new access vectors and vulnerabilities [43]. Admiral Cecil Haney, Kehler's successor at STRATCOM, highlighted the challenges of NC3 modernization in 2015:

> Assured and reliable NC3 is fundamental to the credibility of our nuclear deterrent. The aging NC3 systems continue to meet their intended purpose, but risk to mission success is increasing as key elements of the system age. The unpredictable challenges posed by today's complex security environment make it increasingly important to optimize our NC3 architecture while leveraging new technologies so that NC3 systems operate together as a core set of survivable and endurable capabilities that underpin a broader, national command and control system. [44]

In no small irony, the internet itself owes its intellectual origin, in part, to the threat to NC3 from large-scale physical attack. A 1962 RAND report by Paul Baran considered "the problem of building digital communication networks using links with less than perfect reliability" to enable "stations surviving a physical attack and remaining in electrical connection . . . to operate together as a coherent entity after attack" [45]. Baran advocated as a solution decentralized packet switching protocols, not unlike those realized in the ARPANET program. The emergence of the internet was the result of many other factors that had nothing to do with managing nuclear operations, notably the meritocratic ideals of 1960s counterculture that contributed to the neglect of security in the internet's founding architecture [46, 47]. Fears of NC3 vulnerability helped to create the internet, which then helped to create the present-day cybersecurity epidemic, which has come full circle to create new fears about NC3 vulnerability.

NC3 vulnerability is not unique to the United States. The NC3 of other nuclear powers may even be easier to compromise, especially in the case of new entrants to the nuclear club like North Korea. Moreover, the United States has already demonstrated both the ability and willingness to infiltrate sensitive foreign nuclear infrastructure through operations such as Olympic Games (Stuxnet), albeit targeting Iran's nuclear fuel cycle rather than NC3. It would be surprising to learn that the United States has failed to upgrade its Cold War NC3 attack plans to include offensive cyber operations against a wide variety of national targets.

Hacking the deterrent

The United States included NC3 attacks in its Cold War counterforce and damage limitation war plans, even as contemporary critics perceived these options to be destabilizing for deterrence [48]. The best known example of these activities and capabilities is a Special Access Program named Canopy Wing. East German intelligence obtained the highly classified plans from a US Army spy in Berlin, and the details began to emerge publicly after the Cold War. An East German intelligence officer, Markus Wolf, writes in his memoir that Canopy Wing "listed the types of electronic warfare that would be used to neutralize the Soviet Union and Warsaw Pact's command centers in case of all-out war. It detailed the precise method of depriving the Soviet High Command of its high-frequency communications used to give orders to its armed forces" [49].

It is easy to see why NC3 is such an attractive target in the unlikely event of a nuclear war. If for whatever reason deterrence fails and the enemy decides to push the nuclear button, it would obviously be better to disable or destroy missiles before they launch than to rely on possibly futile efforts to shoot them down, or to accept the loss of millions of lives. American plans to disable Soviet NC3 with electronic warfare, furthermore, would have been intended to complement plans for decapitating strikes against Soviet nuclear forces. Temporary disabling of information networks in isolation would have failed to achieve any important strategic objective. A blinded adversary would eventually see again and would scramble to reconstitute its ability to launch its weapons, expecting that preemption was inevitable in any case. Reconstitution, moreover, would invalidate much of the intelligence and some of the tradecraft on which the blinding attack relied. Capabilities fielded through Canopy Wing were presumably intended to facilitate a preemptive military strike on Soviet NC3 to disable the ability to retaliate and limit the damage of any retaliatory force that survived, given credible indications that war was imminent. Canopy Wing included [50]:

- "Measures for short-circuiting . . . communications and weapons systems using, among other things, microscopic carbon-fiber particles and chemical weapons."
- "Electronic blocking of communications immediately prior to an attack, thereby rendering a counterattack impossible."
- "Deployment of various weapons systems for instantaneous destruction of command centers, including pin-point targeting with precision-guided weapons to destroy 'hardened bunkers'."
- "Use of deception measures, including the use of computer-simulated voices to override and substitute false commands from ground-control stations to aircraft and from regional command centers to the Soviet submarine fleet."

- "Us[e of] the technical installations of 'Radio Free Europe/Radio Liberty' and 'Voice of America,' as well as the radio communications installations of the U.S. Armed Forces for creating interference and other electronic effects."

Wolf also ran a spy in the US Air Force who disclosed that

> the Americans had managed to penetrate the [Soviet air base at Eberswalde]'s ground-air communications and were working on a method of blocking orders before they reached the Russian pilots and substituting their own from West Berlin. Had this succeeded, the MiG pilots would have received commands from their American enemy. It sounded like science fiction, but, our experts concluded, it was in no way impossible that they could have pulled off such a trick, given the enormous spending and technical power of U.S. military air research. [49]

One East German source claimed that Canopy Wing had a $14.5 billion budget for research and operational costs and a staff of 1570 people, while another claimed that it would take over 4 years and $65 million to develop "a prototype of a sophisticated electronic system for paralyzing Soviet radio traffic in the high-frequency range" [50]. Canopy Wing was not cheap, and even so, it was only a research and prototyping program. Operationalization of its capabilities and integration into NATO war plans would have been even more expensive. This is suggestive of the level of effort required to craft effective offensive cyber operations against NC3.

Preparation comes to naught when a sensitive program is compromised. Canopy Wing was caught in what we describe below as the cyber commitment problem, the inability to disclose a warfighting capability for the sake of deterrence without losing it in the process. According to *New York Times* reporting on the counterintelligence investigation of the East German spy in the Army, Warrant Officer James Hall, "officials said that one program rendered useless cost hundreds of millions of dollars and was designed to exploit a Soviet communications vulnerability uncovered in the late 1970's" [51]. This program was probably Canopy Wing. Wolf writes, "Once we passed [Hall's documents about Canopy Wing] on to the Soviets, they were able to install scrambling devices and other countermeasures" [49]. It is tempting to speculate that the Soviet deployment of a new NC3 system known as Signal-A to replace Signal-M (which was most likely the one targeted by Canopy Wing) was motivated in part by Hall's betrayal [50].

Canopy Wing underscores the potential and limitations of NC3 subversion. Modern cyber methods can potentially perform many of the missions Canopy Wing addressed with electronic warfare and other means, but with even greater stealth and precision. Cyber operations might, in principle, compromise any part of the NC3 system (early warning, command centers, data transport, operational forces, etc.) by blinding sensors, injecting bogus commands or suppressing legitimate ones, monitoring or corrupting data transmissions, or interfering with the reliable launch and guidance of missiles. In practice, the operational feasibility of cyber attack against NC3 or any other target depends on the software and hardware configuration and organizational processes of the target, the intelligence and planning capacity of the attacker, and the ability and willingness to take advantage of the effects created by cyber attack [52, 53]. Cyber compromise of NC3 is technically plausible though operationally difficult, a point to which we return in a later section.

To understand which threats are not only technically possible but also probable under some circumstance, we further need a political logic of cost and benefit [14]. In particular, how is it possible for a crisis to escalate to levels of destruction more costly than any conceivable political reward? Canopy Wing highlights some of the strategic dangers of NC3 exploitation. Warsaw Pact observers appear to have been deeply concerned that the program reflected an American willingness to undertake a surprise decapitation attack: they said that it "sent ice-cold shivers down our spines" [50]. The Soviets designed a system called Perimeter that, not unlike the Doomsday Device in *Dr. Strangelove*, was designed to detect a nuclear attack and retaliate automatically, even if cut off from Soviet high command, through an elaborate system of sensors, underground computers, and command missiles to transmit launch codes [54]. Both Canopy Wing and Perimeter show that the United States and the Soviet Union took nuclear warfighting seriously and were willing to develop secret advantages for such an event. By the same token, they were not able to reveal such capabilities to improve deterrence to avoid having to fight a nuclear war in the first place.

Nuclear deterrence and credible communication

Nuclear weapons have some salient political properties. They are singularly and obviously destructive. They kill in more, and more ghastly, ways than conventional munitions through electromagnetic radiation, blast, firestorms, radioactive fallout, and health effects that linger for years. Bombers, ICBMs, and SLBMs can project warheads globally without significantly mitigating their lethality, steeply attenuating the conventional loss-of-strength gradient [55]. Defense against nuclear attack is very difficult, even with modern ballistic missile defenses, given the speed of incoming warheads and use of decoys; multiple warheads and missile volleys further reduce the probability of perfect interception. If one cannot preemptively destroy all of an enemy's missiles, then there is a nontrivial chance of getting hit by some of them. When one missed missile can incinerate millions of people, the notion of winning a nuclear war starts to seem meaningless for many politicians.

As defense seemed increasingly impractical, early Cold War strategists championed the threat of assured retaliation as the chief mechanism for avoiding war [56–59]. Political actors have issued threats for millennia, but the advent of nuclear weapons brought deterrence as a strategy to center stage. The Cold War was an intense learning experience for both practitioners and students of international security, rewriting well-worn realities more than once [60–62]. A key conundrum was the practice of brinkmanship. Adversaries who could not compete by "winning" a nuclear war could still compete by manipulating the "risk" of nuclear annihilation, gambling that an opponent would have the good judgment to back down at some point short of the nuclear brink. Brinkmanship crises—conceptualized as games of Chicken where one cannot heighten tensions without increasing the hazard of the mutually undesired outcome—require that decision makers behave irrationally, or possibly that they act randomly, which is difficult to conceptualize in practical terms [63]. The chief concern in historical episodes of chicken, such as the Berlin Crisis and Cuban Missile Crisis, was not whether a certain level of harm was possible, but whether an adversary was resolved enough, possibly, to risk nuclear suicide. The logical inconsistency of the need for illogic to win led almost from the beginning of the nuclear era to elaborate deductive contortions [64–66].

Both mutually assured destruction (MAD) and successful brinksmanship depend on a less appreciated, but no less fundamental, feature of nuclear weapons: political transparency. Most elements of military power are weakened by disclosure [67]. Military plans are considerably less effective if shared with an enemy. Conventional weapons become less lethal as adversaries learn what different

systems can and cannot do, where they are located, how they are operated, and how to devise countermeasures and array defenses to blunt or disarm an attack. In contrast, relatively little reduction in destruction follows from enemy knowledge of nuclear capabilities. For most of the nuclear era, no effective defense existed against a nuclear attack. Even today, with evolving ABM systems, one ICBM still might get through and annihilate the capital city. Nuclear forces are more robust to revelation than other weapons, enabling nuclear nations better to advertise the harm they can inflict.

The need for transparency to achieve an effective deterrent is driven home by the satirical Cold War film, *Dr. Strangelove*: "the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn't you tell the world, eh?" During the real Cold War, fortunately, Soviet leaders paraded their nuclear weapons through Red Square for the benefit of foreign military attaches and the international press corps. Satellites photographed missile, bomber, and submarine bases. While other aspects of military affairs on both sides of the Iron Curtain remained closely guarded secrets, the United States and the Soviet Union permitted observers to evaluate their nuclear capabilities. This is especially remarkable given the secrecy that pervaded Soviet society. The relative transparency of nuclear arsenals ensured that the superpowers could calculate risks and consequences within a first-order approximation, which led to a reduction in severe conflict and instability even as political competition in other arenas was fierce [61, 68].

Recent insights about the causes of war suggest that divergent expectations about the costs and consequences of war are necessary for contests to occur [69–73]. These insights are associated with rationalist theories, such as deterrence theory itself. Empirical studies and psychological critiques of the rationality assumption have helped to refine models and bring some circumspection into their application, but the formulation of sound strategy (if not the execution) still requires the articulation of some rational linkage between cause and effect [19, 62, 74]. Many supposedly nonrational factors, moreover, simply manifest as uncertainty in strategic interaction. Our focus here is on the effect of uncertainty and ignorance on the ability of states and other actors to bargain in lieu of fighting. Many wars are a product of what adversaries do not know or what they misperceive, whether as a result of bluffing, secrecy, or intrinsic uncertainty [75, 76]. If knowledge of capabilities or resolve is a prerequisite for deterrence, then one reason for deterrence failure is the inability or unwillingness to credibly communicate details of the genuine balance of power, threat, or interests. Fighting, conversely, can be understood as a costly process of discovery that informs adversaries of their actual relative strength and resolve. From this perspective, successful deterrence involves instilling in an adversary perceptions like those that result from fighting, but before fighting actually begins. Agreement about the balance of power can enable states to bargain (tacit or overt) effectively without needing to fight, forging compromises that each prefers to military confrontation or even to the bulk of possible risky brinkmanship crises.

Despite other deficits, nuclear weapons have long been considered to be stabilizing with respect to rational incentives for war (the risk of nuclear accidents is another matter) [77]. If each side has a secure second strike—or even a minimal deterrent with some nonzero chance of launching a few missiles—then each side can expect to gain little and lose much by fighting a nuclear war. Whereas the costs of conventional war can be more mysterious because each side might decide to hold something back and meter out its punishment due to some internal constraint or a theory of graduated escalation, even a modest initial nuclear exchange is recognized to be extremely costly. As long as both sides understand this and understand (or believe) that the adversary understands this as well, then the relationship is stable. Countries engage nuclear powers with considerable deference, especially over issues of fundamental national or international importance. At the same time, nuclear weapons appear to be of limited value in prosecuting aggressive action, especially over issues of secondary or tertiary importance, or in response to aggression from others at lower levels of dispute intensity. Nuclear weapons are best used for signaling a willingness to run serious risks to protect or extort some issue that is considered of vital national interest.

As mentioned previously, both superpowers in the Cold War considered the warfighting advantages of nuclear weapons quite apart from any deterrent effect, and the United States and Russia still do. High-altitude bursts for air defense, electromagnetic pulse for frying electronics, underwater detonations for anti-submarine warfare, hardened target penetration, area denial, and so on, have some battlefield utility. Transparency *per se* is less important than weapon effects for warfighting uses, and can even be deleterious for tactics that depend on stealth and mobility. Even a single tactical nuke, however, would inevitably be a political event. Survivability of the second strike deterrent can also militate against transparency, as in the case of the Soviet Perimeter system, as mobility, concealment, and deception can make it harder for an observer to track and count respective forces from space. Counterforce strategies, platform diversity and mobility, ballistic missile defense systems, and force employment doctrine can all make it more difficult for one or both sides in a crisis to know whether an attack is likely to succeed or fail. The resulting uncertainty affects not only estimates of relative capabilities but also the degree of confidence in retaliation. At the same time, there is reason to believe that platform diversity lowers the risk of nuclear or conventional contests, because increasing the number of types of delivery platforms heightens second strike survivability without increasing the lethality of an initial strike [78]. While transparency is not itself a requirement for nuclear use, stable deterrence benefits to the degree to which retaliation can be anticipated, as well as the likelihood that the consequences of a first strike are more costly than any benefit. Cyber operations, in contrast, are neither robust to revelation nor as obviously destructive.

The cyber commitment problem

Deterrence (and compellence) uses force or threats of force to "warn" an adversary about consequences if it takes or fails to take an action. In contrast, defense (and conquest) uses force to "win" a contest of strength and change the material distribution of power. Sometimes militaries can change the distribution of information and power at the same time. Military mobilization in a crisis signifies resolve and displays a credible warning, but it also makes it easier to attack or defend if the warning fails. Persistence in a battle of attrition not only bleeds an adversary but also reveals a willingness to pay a higher price for victory. More often, however, the informational requirements of winning and warning are in tension. Combat performance often hinges on well-kept secrets, feints, and diversions. Many military plans and capabilities degrade when revealed. National security involves trade-offs between the goals of preventing war, by advertising capabilities or interests, and improving fighting power should war break out, by concealing capabilities and surprising the enemy.

The need to conceal details of the true balance of power to preserve battlefield effectiveness gives rise to the military commitment problem [79, 80]. Japan could not coerce the United States by revealing its plan to attack Pearl Harbor because the United States

could not credibly promise to refrain from reorienting defenses and dispersing the Pacific Fleet. War resulted not just because of what opponents did not know but because of what they could not tell each other without paying a severe price in military advantage. The military benefits of surprise (winning) trumped the diplomatic benefits of coercion (warning).

Cyber operations, whether for disruption and intelligence, are extremely constrained by the military commitment problem. Revelation of a cyber threat in advance that is specific enough to convince a target of the validity of the threat also provides enough information potentially to neutralize it. Stuxnet took years and hundreds of millions of dollars to develop but was patched within weeks of its discovery. The Snowden leaks negated a whole swath of tradecraft that the NSA took years to develop. States may use other forms of covert action, such as publicly disavowed lethal aid or aerial bombing (e.g. Nixon's Cambodia campaign), to discretely signal their interests, but such cases can only work to the extent that revelation of operational details fails to disarm rebels or prevent airstrikes [81].

Cyber operations, especially against NC3, must be conducted in extreme secrecy as a condition of the efficacy of the attack. Cyber tradecraft relies on stealth, stratagem, and deception [21]. Operations tailored to compromise complex remote targets require extensive intelligence, planning and preparation, and testing to be effective. Actions that alert a target of an exploit allow the target to patch, reconfigure, or adopt countermeasures that invalidate the plan. As the Defense Science Board points out, competent network defenders:

> can also be expected to employ highly-trained system and network administrators, and this operational staff will be equipped with continuously improving network defensive tools and techniques (the same tools we advocate to improve our defenses). Should an adversary discover an implant, it is usually relatively simple to remove or disable. For this reason, offensive cyber will always be a fragile capability. [41]

The world's most advanced cyber powers, the United States, Russia, Israel, China, France, and the United Kingdom, are also nuclear states, while India, Pakistan, and North Korea also have cyber warfare programs. NC3 is likely to be an especially well defended part of their cyber infrastructures. NC3 is a hard target for offensive operations, which thus requires careful planning, detailed intelligence, and long lead-times to avoid compromise.

Cyberspace is further ill-suited for signaling because cyber operations are complex, esoteric, and hard for commanders and policymakers to understand. Most targeted cyber operations have to be tailored for each unique target (a complex organization not simply a machine), quite unlike a general purpose munition tested on a range. Malware can fail in many ways and produce unintended side effects, as when the Stuxnet code was accidentally released to the public. The category of "cyber" includes tremendous diversity: irritant scams, hacktivist and propaganda operations, intelligence collection, critical infrastructure disruption, etc. Few intrusions create consequences that rise to the level of attacks such as Stuxnet or BlackEnergy, and even they pale beside the harm imposed by a small war.

Vague threats are less credible because they are indistinguishable from casual bluffing. Ambiguity can be useful for concealing a lack of capability or resolve, allowing an actor to pool with more capable or resolved states and acquiring some deterrence success by association. But this works by discounting the costliness of the threat. Nuclear threats, for example, are usually somewhat veiled because one cannot credibly threaten nuclear suicide. The consistently ambiguous phrasing of US cyber declaratory policy (e.g. "we will respond to cyber-attacks in a manner and at a time and place of our choosing using appropriate instruments of U.S. power" [82]) seeks to operate across domains to mobilize credibility in one area to compensate for a lack of credibility elsewhere, specifically by leveraging the greater robustness to revelation of military capabilities other than cyber.

This does not mean that cyberspace is categorically useless for signaling, just as nuclear weapons are not categorically useless for warfighting. Ransomware attacks work when the money extorted to unlock the compromised host is priced below the cost of an investigation or replacing the system. The United States probably gained some benefits in general deterrence (i.e. discouraging the emergence of challenges as opposed to immediate deterrence in response to a challenge) through the disclosure of Stuxnet and the Snowden leaks. Both revelations compromised tradecraft, but they also advertised that the NSA probably had more exploits and tradecraft where they came from. Some cyber operations may actually be hard to mitigate within tactically meaningful timelines (e.g. hardware implants installed in hard-to-reach locations). Such operations might be revealed to coerce concessions within the tactical window created by a given operation, if the attacker can coordinate the window with the application of coercion in other domains. As a general rule, however, the cyber domain on its own is better suited for winning than warning [83]. Cyber and nuclear weapons fall on extreme opposite sides of this spectrum.

Dangerous complements

Nuclear weapons have been used in anger twice—against the Japanese cities Hiroshima and Nagasaki—but cyberspace is abused daily. Considered separately, the nuclear domain is stable and the cyber domain is unstable. In combination, the results are ambiguous.

The nuclear domain can bound the intensity of destruction that a cyber attacker is willing to inflict on an adversary. US declaratory policy states that unacceptable cyber attacks may prompt a military response; while nuclear weapons are not explicitly threatened, neither are they withheld. Nuclear threats have no credibility at the low end, where the bulk of cyber attacks occur. This produces a cross-domain version of the stability–instability paradox, where deterrence works at the high end but is not credible, and thus encourages provocation, at low intensities. Nuclear weapons, and military power generally, create an upper bound on cyber aggression to the degree that retaliation is anticipated and feared [22, 83, 84].

In the other direction, the unstable cyber domain can undermine the stability of nuclear deterrence. Most analysts who argue that the cyber–nuclear combination is a recipe for danger focus on the fog of crisis decision making [85–87]. Stephen Cimbala points out that today's relatively smaller nuclear arsenals may perversely magnify the attractiveness of NC3 exploitation in a crisis: "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 concurrence of cyber and nuclear attack capabilities more alarming" [88]. Cimbala focuses mainly on the risks of misperception and miscalculation that emerge when a cyber attack muddies the transparent communication required for opponents to understand one another's interests, redlines, and willingness to use force, and to ensure reliable control over subordinate commanders. Thus a

nuclear actor "faced with a sudden burst of holes in its vital warning and response systems might, for example, press the preemption button instead of waiting to ride out the attack and then retaliate" [85].

The outcome of fog of decision scenarios such as these depend on how humans react to risk and uncertainty, which in turn depends on bounded rationality and organizational frameworks that might confuse rational decision making [89, 90]. These factors exacerbate a hard problem. Yet within a rationalist framework, cyber attacks that have already created their effects need not trigger an escalatory spiral. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target's awareness that its NC3 has been compromised in some way would help to convey new information that the balance of power is not as favorable as previously thought. This in turn could encourage the target to accommodate, rather than escalate. While defects in rational decision making are a serious concern in any cyber–nuclear scenario, the situation becomes even more hazardous when there are rational incentives to escalate. Although "known unknowns" can create confusion, to paraphrase Donald Rumsfeld, the "unknown unknowns" are perhaps more dangerous.

A successful clandestine penetration of NC3 can defeat the informational symmetry that stabilizes nuclear relationships. Nuclear weapons are useful for deterrence because they impose a degree of consensus about the distribution of power; each side knows the other can inflict prohibitive levels of damage, even if they may disagree about the precise extent of this damage. Cyber operations are attractive precisely because they can secretly revise the distribution of power. NC3 neutralization may be an expensive and rarified capability in the reach of only a few states with mature signals intelligence agencies, but it is much cheaper than nuclear attack. Yet the very usefulness of cyber operations for nuclear warfighting ensure that deterrence failure during brinksmanship crises is more likely.

Nuclear states may initiate crises of risk and resolve to see who will back down first, which is not always clear in advance. Chicken appears viable, ironically, because each player understands that a nuclear war would be a disaster for all, and thus all can agree that someone can be expected swerve. Nuclear deterrence should ultimately make dealing with an adversary diplomatically more attractive than fighting, provided that fighting is costly—as would seem evident for the prospect of nuclear war—and assuming that bargains are available to states willing to accept compromise rather than annihilation. If, however, one side knows, but the other does not, that the attacker has disabled the target's ability to perceive an impending military attack, or to react to one when it is underway, then they will not have a shared understanding of the probable outcome of war, even in broad terms.

Consider a brinksmanship crisis between two nuclear states where only one has realized a successful penetration of the rival's NC3. The cyber attacker knows that it has a military advantage, but it cannot reveal the advantage to the target, lest the advantage be lost. The target does not know that it is at a disadvantage, and it cannot be told by the attacker for the same reason. The attacker perceives an imbalance of power while the target perceives a balance. A dangerous competition in risk taking ensues. The first side knows that it does not need to back down. The second side feels confident that it can stand fast and raise the stakes far beyond what it would be willing to if it understood the true balance of power. Each side is willing to escalate to create more risk for the other side, making it more likely that one or the other will conclude that deterrence has failed and move into warfighting mode to attempt to limit the damage the other can inflict.

The targeted nature and uncertain effects of offensive cyber operations put additional pressure on decision makers. An intrusion will probably disable only part of the enemy's NC3 architecture, not all of it (which is not only operationally formidable to achieve but also more likely to be noticed by the target). Thus the target may retain control over some nuclear forces, or conventional forces. The target may be tempted to use some of them piecemeal to signal a willingness to escalate further, even though it cannot actually escalate because of the cyber operation. The cyber attacker knows that it has escalation dominance, but when even a minor demonstration by the target can cause great damage, it is tempting to preempt this move or others like it. This situation would be especially unstable if only second strike but not primary strike NC3 was incapacitated. Uncertainty in the efficacy of the clandestine penetration would discount the attacker's confidence in its escalation dominance, with a range of possible outcomes. Enough uncertainty would discount the cyber attack to nothing, which would have a stabilizing effect by returning the crisis to the pure nuclear domain. A little bit of uncertainty about cyber effectiveness would heighten risk acceptance while also raising the incentives to preempt as an insurance measure.

Adding allies into the mix introduces additional instability. An ally emboldened by its nuclear umbrella might run provocative risks that it would be much more reluctant to embrace if it was aware that the umbrella was actually full of holes. Conversely, if the clandestine advantage is held by the state extending the umbrella, allies could become unnerved by the willingness of their defender to run what appear to be outsize risks, oblivious of the reasons for the defender's confidence, creating discord in the alliance and incentives for self-protective action, leading to greater uncertainty about alliance solidarity.

The direction of influence between the cyber and nuclear realms depends to large degree on which domain is the main arena of action. Planning and conducting cyber operations will be bounded by the ability of aggressors to convince themselves that attacks will remain secret, and by the confidence of nuclear nations in their invulnerability. Fears of cross-domain escalation will tend to keep instability in cyberspace bounded. However, if a crisis has risen to the point where nuclear threats are being seriously considered or made, then NC3 exploitation will be destabilizing. Brinksmanship crises seem to have receded in frequency since the Cuban Missile Crisis but may be more likely than is generally believed. President Vladimir Putin of Russia has insinuated more than once in recent years that his government is willing to use tactical nuclear weapons if necessary to support his policies.

Cyber power and nuclear stability

Not all crises are the same. Indeed, their very idiosyncrasies create the uncertainties that make bargaining failure more likely [75]. So far our analysis would be at home in the Cold War, with the technological novelty of cyber operations. Yet not every state has the same cyber capabilities or vulnerabilities. Variation in cyber power relations across dyads should be expected to affect the strategic stability of nuclear states.

The so-called second nuclear age differs from superpower rivalry in important ways [91]. There are fewer absolute numbers of warheads in the world, down from a peak of over 70 000 in the 1980s to about 15 000 today (less than 5000 deployed), but they are distributed very unevenly [92]. The United States and Russia have comparably sized arsenals, each with a fully diversified triad of delivery platforms, while North Korea only has a dozen or so bombs and no meaningful delivery system (for now). China, India, Pakistan,

Britain, France, and Israel have modest arsenals in the range of several dozen to a couple hundred weapons, but they have very different doctrines, conventional force complements, domestic political institutions, and alliance relationships. The recent nuclear powers lack the hard-won experience and shared norms of the Cold War to guide them through crises, and even the United States and Russia have much to relearn.

Cyber warfare capacity also varies considerably across contemporary nuclear nations. The United States, Russia, Israel, and Britain are in the top tier, able to run sophisticated, persistent, clandestine penetrations. China is a uniquely active cyber power with ambitious cyber warfare doctrine, but its operational focus is on economic espionage and political censorship, resulting in less refined tradecraft and more porous defenses for military purposes [16]. France, India, and Pakistan also have active cyber warfare programs, while North Korea is the least developed cyber nation, depending on China for its expertise [93].

It is beyond the scope of this article to assess crisis dyads in detail, and data on nuclear and cyber power for these countries are shrouded in secrecy. Here, as a way of summing up the arguments above, we offer a few conjectures about how stylized aspects of cyber power affect crisis stability through incentives and key aspects of decision making. We do not stress relative nuclear weapon capabilities on the admittedly strong (and contestable) assumption that nuclear transparency in the absence of cyber operations would render nuclear asymmetry irrelevant for crisis bargaining because both sides would agree about the terrible consequences of conflict [94]. We also omit domestic or psychological variables that affect relative power assessments, although these are obviously important. Even if neither India nor Pakistan have viable cyber–nuclear capabilities, brinksmanship between them is dangerous for many other reasons, notably compressed decision timelines, Pakistan's willingness to shoot first, and domestic regime instability. Our focus is on the impact of offensive and defensive cyber power on nuclear deterrence above and beyond the other factors that certainly play a role in real-world outcomes.

First, does the cyber attacker have the organizational capacity, technical expertise, and intelligence support to "compromise" the target's NC3? Can hackers access critical networks, exploit technical vulnerabilities, and confidently execute a payload to disrupt or exploit strategic sensing, command, forces, or transport capacity? The result would be some tangible advantage for warfighting, such as tactical warning or control paralysis, but one that cannot be exercised in bargaining.

Second, is the target able to "detect" the compromise of its NC3? The more complicated and sensitive the target, the more likely cyber attackers are to make a mistake that undermines the intrusion. Attribution is not likely to be difficult given the constricted pool of potential attackers, but at the same time the consequences of misattributing "false flag" operations could be severe [95]. At a minimum, detection is assumed to provide information to the target that the balance of power is perhaps not as favorable as imagined previously. We assume that detection without an actual compromise is possible because of false positives or deceptive information operations designed to create pessimism or paranoia.

Third, is the target able to "mitigate" the compromise it detects? Revelation can prompt patching or network reconfiguration to block an attack, but this assumption is not always realistic. The attacker may have multiple pathways open or may have implanted malware that is difficult to remove in tactically meaningful timelines. In such cases the cyber commitment problem is not absolute, since the discovery of the power to hurt does not automatically disarm it. Successful mitigation here is assumed to restore mutual assessments of the balance of power to what they would be absent the cyber attack.

Table 1 shows how these factors combine to produce different deterrence outcomes in a brinksmanship (chicken) crisis. If there is no cyber compromise and the target detects nothing (no false positives) then we have the optimistic ideal case where nuclear transparency affords stable "deterrence." Transparency about the nuclear balance, including the viability of secure second strike forces, provides strategic stability. We also expect this box to describe situations where the target has excellent network defense capabilities and thus the prospect of defense, denial or deception successfully deters any attempts to penetrate NC3. This may resemble the Cold War situation (with electronic warfare in lieu of cyber), or even the present day US–Russia dyad, where the odds of either side pulling off a successful compromise against a highly capable defender are not favorable. Alternately the attack may be deemed risky enough to encourage serious circumspection. However, the existence of Canopy Wing does not encourage optimism in this regard.

Conversely, if there is a compromise that goes undetected, then there is a heightened risk of "war" because of the cyber commitment problem. This box may be particularly relevant for asymmetric dyads such as the United States and North Korea, where one side has real cyber power but the other side is willing to go to the brink where it believes, falsely, that it has the capability to compel its counterpart to back down. Cyber disruption of NC3 is attractive for damage limitation should deterrence fail, given that the weaker state's diminutive arsenal makes damage limitation by the stronger state more likely to succeed. The dilemma for the stronger state is that the clandestine counterforce hedge, which makes warfighting success more likely, is precisely what makes deterrence more likely to fail.

The United States would face similar counterforce dilemmas with other dyads like China or even Russia, although even a strong cyber power should be more circumspect when confronted with an adversary with a larger/more capable nuclear and conventional arsenal. More complex and cyber savvy targets, moreover, are more likely to detect a breach in NC3, leading to more ambiguous outcomes depending on how actors cope with risk and uncertainty. Paradoxically, confidence in cyber security may be a major contributor to failure; believing one is safe from attack increases the chance that an attack is successful.

If the successful compromise is detected but not mitigated, then the target learns that the balance of power is not as favorable as thought. This possibility suggests fleeting opportunities for "coercion" by revealing the cyber coup to the target in the midst of a crisis while the cyber attacker maintains or develops a favorable military advantage before the target has the opportunity to reverse or compensate the NC3 disruption. Recognizing the newly transparent costs of war, a risk neutral or risk averse target should prefer compromise. The coercive advantages (deterrence or compellence) of a detected but unmitigated NC3 compromise will likely be fleeting. This suggests a logical possibility for creating a window of opportunity for using particular cyber operations that are more robust to

Table 1. Cyber operations and crisis stability

	Not compromised	*Compromised*
Not detected	Deterrence	War
Detected but not mitigated	Bluff (or use-lose)	Coercion (or use-lose)
Detected and mitigated	Spiral	Spiral

revelation as a credible signal of superior capability in the midst of a crisis. It would be important to exploit this fleeting advantage via other credible military threats (e.g. forces mobilized on visible alert or deployed into the crisis area) before the window closes.

One side may be able gain an unearned advantage, an opportunity for coercion via a "bluff," by the same window-of-opportunity logic. A target concerned about NC3 compromise will probably have some network monitoring system and other protections in place. Defensive systems can produce false positives as a result of internal errors or a deception operation by the attacker to encourage paranoia. It is logically possible that some false positives would appear to the target to be difficult to mitigate. In this situation, the target could believe it is at a disadvantage, even though this is not in fact the case. This gambit would be operationally very difficult to pull off with any reliability in a real nuclear crisis.

Cyber–nuclear coercion and bluffing strategies are fraught with danger. Detection without mitigation might put a risk-acceptant or loss-averse target into a "use-lose" situation, creating pressures to preempt or escalate. The muddling of decision-making heightens the risk of accidents or irrational choices in a crisis scenario. Worry about preemption or accident then heightens the likelihood that the initiator will exercise counterforce options while they remain available. These pressures can be expected to be particularly intense if the target's detection is only partial or has not revealed the true extent of damage to its NC3 (i.e. the target does not realize it has already lost some or all of what it hopes to use). These types of scenarios are most usually invoked in analyses of inadvertent escalation [23–27]. The essential distinction between "use-lose" risks and "war" in this typology is the target's knowledge of some degree of NC3 compromise. Use-lose and other cognitive pressures can certainly result in nuclear war, since the breakdown of deterrence leads to the release of nuclear weapons, but we distinguish these outcomes to highlight the different decision making processes or rational incentives at work.

A "spiral" of mistrust may emerge if one side attempts a compromise but the defender detects and mitigates it. Both sides again have common mutual estimates of the relative balance of power, which superficially resembles the "deterrence" case because the NC3 compromise is negated. Unfortunately, the detection of the compromise will provide the target with information about the hostile intentions of the cyber attacker. This in turn is likely to exacerbate other political or psychological factors in the crisis itself or in the crisis-proneness of the broader relationship. The strange logical case where there is no compromise but one is detected and mitigated could result from a false positive misperception (including a third-party false flag operation) that could conflict spiraling [96, 97]. The bluff and coercion outcomes are also likely to encourage spiraling behavior once the fleeting bargaining advantage dissipates or is dispelled (provided anyone survives the interaction).

The risk of crisis instability is not the same for all dyads. It is harder to compromise the NC3 of strong states because of the redundancy and active defenses in their arsenal. Likewise, strong states are better able to compromise the NC3 of any states but especially of weaker states, because of strong states' greater organizational capacity and expertise in cyber operations. Stable deterrence or MAD is most likely to hold in mutually strong dyads (e.g. the United States and the Soviet Union in the Cold War or Russia today to a lesser extent). Deterrence is slightly less likely in other equally matched dyads (India–Pakistan) where defensive vulnerabilities create temptations but offensive capabilities may not be sufficient to exploit them. Most states can be expected to refrain from targeting American NC3 given a US reputation for cyber power (a general deterrence benefit enhanced by Stuxnet and Snowden). The situation is less stable if the United States is the attacker. The most dangerous dyad is a stronger and a weaker state (United States and North Korea or Israel and Iran). Dyads involving strong and middle powers are also dangerous (United States and China). The stronger side is tempted to disrupt NC3 as a warfighting hedge in case deterrence breaks down, while the weaker but still formidable side has a reasonable chance at detection. The marginally weaker may also be tempted to subvert NC3, particularly for reconnaissance; the stronger side is more likely to detect and correct the intrusion but will be alarmed by the ambiguity in distinguishing intelligence collection from attack planning [98]. In a brinksmanship crisis between them, windows for coercion may be available yet fleeting, with real risks of spiral and war.

Policy implications

Skeptics are right to challenge the hype about cyberwar. The term is confusing, and hacking rarely amounts to anything approaching a weapon of mass destruction. Cyberspace is most usefully exploited on the lower end of the conflict spectrum for intelligence and subversion, i.e., not as a substitute for military or economic power but a complement to it. Yet the logic of complementarity has at least one exception regarding conflict severity, and it is a big one.

Offensive cyber operations against NC3 raise the risk of nuclear war. They do so because cyber operations and nuclear weapons are extreme complements regarding their informational properties. Cyber operations rely on deception. Nuclear deterrence relies on clear communication. In a brinksmanship crisis, the former undermines the latter. Nuclear crises were rare events in Cold War history, thankfully. Today, the proliferation and modernization of nuclear weapons may raise the risk slightly. Subversion of NC3 raises the danger of nuclear war slightly more. Cyberwar is not war per se, but in rare circumstances it may make escalation to thermonuclear war more likely.

NC3 is a particularly attractive counterforce target because disruption can render the enemy's arsenal less effective without having to destroy individual platforms. US nuclear strategy in practice has long relied on counterforce capabilities (including Canopy Wing) [48, 99]. Deterrence theorists expect this to undermine the credibility of the adversary's deterrent and create pressures to move first in a conflict [100, 101]. If for some reason deterrence fails, however, countervalue strikes on civilian population centers would be militarily useless and morally odious. Counterforce strikes, in contrast, aim at preemptive disarmament or damage limitation by attacking the enemy's nuclear enterprise. Counterforce capabilities are designed for "winning" a nuclear war once over the brink, but their strategic purpose may still include warning if they can somehow be made robust to revelation. During the Cold War, the United States found ways to inform the Soviet Union of its counterforce ability to sink SSBNs, hit mobile ICBMs, and show off some electronic warfare capabilities without giving away precise details [102]. This improved mutual recognition of US advantages and thus clearer assessment of the consequences of conflict, but the military commitment problem was real nonetheless. The problem is particularly pronounced for cyber disruption of NC3. As one side builds more sophisticated NC3 to improve the credibility of its nuclear "warning," the other side engages in cyber operations to improve its capacity for nuclear "winning," thereby undermining the warning.

The prohibitive cost of nuclear war and the relative transparency of the nuclear balance has contributed to seven decades of nuclear peace. If this is to continue, it will be necessary to find ways to

maintain transparency. If knowledge of a shift in relative power is concealed, then the deterrent effect of nuclear capabilities is undermined. This will tend to occur in periods where concern over nuclear attack is heightened, such as in the midst of a militarized crises. Yet there is no reason to believe that states will wait for a crisis before seeking to establish advantageous positions in cyberspace. Indeed, given the intricate intelligence and planning required, offensive cyber preparations must precede overt aggression by months or even years. It is this erosion of the bulwark of deterrence that is most troubling.

What can be done? Arms control agreements to ban cyber attacks on NC3 might seem attractive, but the cyber commitment problem also undermines institutional monitoring and enforcement. Even where the United States would benefit from such an agreement by keeping this asymmetric capability out of the hands of other states, it would still have strong incentives to prepare its own damage limitation options should deterrence fail. Nevertheless, diplomatic initiatives to discuss the dangers of cyber–nuclear interactions with potential opponents should be pursued. Even if cyber–nuclear dangers cannot be eliminated, states should be encouraged to review their NC3 and ensure strict lines of control over any offensive cyber operations at that level.

Classified studies of the details of NC3, not just the technical infrastructure but also their human organizations, together with wargames of the scenarios above, may help nuclear war planners to think carefully about subverting NC3. Unfortunately, the same reconnaissance operations used to better understand the opponent's NC3 can be misinterpreted as attempts to compromise it [98]. More insidiously, private knowledge can become a source of instability insofar as knowing something about an adversary that improves one's prospects in war increases the incentive to act through force or to exploit windows of opportunity in a crisis that could inadvertently escalate.

Anything that can be done to protect NC3 against cyber intrusion will make the most dangerous possibility of successful but undetected compromises less likely. The Defense Science Board in 2013 recommended "immediate action to assess and assure national leadership that the current U.S. nuclear deterrent is also survivable against the full-spectrum cyber … threat" [41]. Defense in depth should include redundant communications pathways, error correction channels, isolation of the most critical systems, component heterogeneity rather than a vulnerable software monoculture, and network security monitoring with active defenses (i.e. a counterintelligence mindset). Older technologies, ironically, may provide some protection by foiling access of modern cyber techniques (Russia reportedly still uses punch-cards for parts of its NC3 [103]); yet vulnerabilities from an earlier era of inadequate safeguards are also a problem. For defense in depth to translate into deterrence by denial requires the additional step of somehow advertising NC3 redundancy and resilience even in a cyber degraded environment.

Cyber disruption of NC3 is a cross-domain deterrence problem. CDD might also be part of the solution. As noted above, CDD can help to bound the severity of instability in the cyber domain by threatening, implicitly or explicitly, the prospect of military, economic, law-enforcement, or diplomatic consequences. Cyber attacks flourish below some credible threshold of deterrence and rapidly tail off above it. CDD may also help in nuclear crises. CDD provides policymakers with options other than nuclear weapons, and perhaps options when NC3 is compromised. A diversity of options provides a variation on Schelling's classic "threat that leaves something to chance." In some dyads, particularly with highly asymmetric nuclear arsenals and technical capabilities, CDD may provide options for "war" and "coercion" outcomes (in the language of our typology) short of actual nuclear war. CDD does not necessarily improve deterrence and in many ways is predicated on the failure of deterrence, but the broadening of options may lessen the consequences of that failure (i.e. if a machine asks, "Do you want to play a game?" it would be helpful to have options available other than "global thermonuclear war"). The implications of choice among an expanded palette of coercive options in an open-ended bargaining scenario is a topic for future research.

Finally, every effort should be made to ensure that senior leaders—the President and the Secretary of Defense in the United States, the Central Military Commission in China, etc.—understand and authorize any cyber operations against any country's NC3 for any reason. Even intrusions focused only on intelligence collection should be reviewed and approved at the highest level. Education is easier said than done given the esoteric technical details involved. Ignorance at the senior level of the implications of compromised NC3 is a major risk factor in a crisis contributing to false optimism or other bad decisions. New technologies of information are, ironically, undermining clear communication.

Acknowledgements

We thank Scott Sagan, William J. Perry, the participants of the Stanford Cyber Policy Program (SCPP) Workshop on Strategic Dimensions of Offensive Cyber Operations, and the anonymous reviewers for their comments. This research was supported by SCPP and the Department of Defense Minerva Initiative through an Office of Naval Research Grant [N00014-14-1-0071].

References

1. Kaplan F. 'WarGames' and cybersecurity's debt to a hollywood hack. *The New York Times*. February 19, 2016.
2. Schulte SR. 'The WarGames Scenario': regulating teenagers and teenaged technology (1980-1984). *Television & New Media* August 19, 2008.
3. Warner M. Cybersecurity: a pre-history. *Intell Natl Security* 2012;**27**:781–99.
4. Borg S. Economically complex cyberattacks. *IEEE Security and Privacy Magazine* 2005;**3**:64–67.
5. Clarke RA, Knake RK. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2010.
6. Brenner J. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.
7. Kello L. The meaning of the cyber revolution: perils to theory and statecraft. *Int Security* 2013;**38**:7–40.
8. Peterson D. Offensive cyber weapons: construction, development, and employment. *J Strat Stud* 2013;**36**:120–24.
9. Dunn Cavelty M. Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *J Informat Technol & Polit* 2008;**4**:19–36.
10. Rid T. Cyber war will not take place. *J Strat Stud* 2012;**35**:5–32.
11. Lawson S. Beyond cyber-doom: assessing the limits of hypothetical scenarios in the framing of cyber-threats. *J Informat Technol & Polit* 2013;**10**:86–103.
12. Benson DC. Why the internet is not increasing terrorism. *Security Stud* 2014;**23**:293–328.
13. Valeriano B, Maness RC. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press, 2015.
14. Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to earth. *Int Security* 2013;**38**:41–73.
15. Lindsay JR. Stuxnet and the limits of cyber warfare. *Security Stud* 2013;**22**:365–404.

16. Lindsay JR. The impact of China on cybersecurity: fiction and friction. *Int Security* 2014;**39**:7–47.
17. Opall-Rome B. Israeli cyber game drags US, Russia to brink of Mideast war. *Defense News*, November 14, 2013. http://www.defensenews.com/article/20131115/C4ISRNET07/311150020/Israeli-Cyber- Game-Drags-US-Russia-Brink-Mideast-War.
18. Lindsay JR, Gartzke E. Cross-Domain Deterrence as a Practical Problem and a Theoretical Concept. *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Gartzke E and Lindsay JR (eds.), La Jolla, CA: Manuscript, 2016.
19. Carcelli S, Gartzke E. *Blast from the Past: Revitalizing and Diversifying Deterrence Theory*. Working Paper. La Jolla, CA, 2016.
20. Powell R. *Nuclear Deterrence Theory: The Search for Credibility*. New York: Cambridge University Press, 1990.
21. Gartzke E, Lindsay JR. Weaving tangled webs: offense, defense, and deception in cyberspace. *Security Stud* 2015;**24**:316–48.
22. Lindsay JR. Tipping the scales: the attribution problem and the feasibility of deterrence against cyber attack. *J Cybersecurity* 2015;**1**:53–67.
23. Posen BR. *Inadvertent Escalation: Conventional War and Nuclear Risks*. Ithaca, NY: Cornell University Press, 1991.
24. Cimbala SJ. Nuclear crisis management and 'Cyberwar': phishing for trouble? *Strat Stud Quart* 2011:117–131.
25. Goldstein A. First things first: the pressing danger of crisis instability in U.S.-China relations. *Int Security* 2013;**37**:49–89.
26. Gompert DC, Libicki M. Cyber warfare and Sino-American crisis instability. *Survival* 2014;**56**:7–22.
27. Talmadge C. Assessing the risk of chinese nuclear escalation in a conventional war with the United States. *Int Security* (Forthcoming).
28. *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program*, 2013.
29. Carter AD, Steinbruner JB, Zracket CA. *Managing Nuclear Operations*. Washington, DC: Brookings Institution Press, 1987.
30. Office of the Deputy Assistant Secretary of Defense for Nuclear Matters. "Nuclear Command and Control System." In *Nuclear Matters Handbook 2015*. Washington, DC: Government Printing Office, 2015, 73–81.
31. Bracken PJ. *The Command and Control of Nuclear Forces*. New Haven, CT: Yale University Press, 1985.
32. Blair B. *Strategic Command and Control*. Washington, DC: Brookings Institution Press, 1985.
33. U.S. Joint Chiefs of Staff. *A Historical Study of Strategic Connectivity, 1950-1981*. Special Historical Study Washington, DC: Joint Chiefs of Staff, Joint Secretariat, Historical Division, July 1982.
34. Gregory S. *The Hidden Cost of Deterrence: Nuclear Weapons Accidents*. London: Brassey's, 1990.
35. Sagan SD. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, NJ: Princeton University Press, 1995.
36. Eric S. *Command and Control: Nuclear Weapons, the Demascus Accident, and the Illusion of Safety*. New York: Penguin, 2014.
37. George Lee B. *Uncommon Cause: A Life at Odds with Convention, Volume II: The Transformative Years*. Denver, CO: Outskirts Press, 2016.
38. Ambinder M. Failure shuts down squadron of nuclear missiles. *The Atlantic* 2010.
39. Blair B. Could terrorists launch America's nuclear missiles? *Time* 2010.
40. Government Accountability Organization. *Nuclear Command, Control, and Communications: Update on DOD's Modernization.* GAO-15-584R. Washington, DC, June 15, 2015. http://www.gao.gov/products/GAO-15-584R.
41. *Resilient military systems and the advanced cyber threat*. Washington, DC: Defense Science Board, 2013.
42. *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*. Washington, DC: Government Accountability Office, 2016.
43. Futter A. The double-edged sword: US nuclear command and control modernization. *Bull Atomic Scientists* June 29, 2016. http://thebulletin.org/double-edged-sword-us-nuclear-command-and-control-modernization9593.
44. Haney C. Department of defense press briefing by Adm. Haney in the pentagon briefing room. U.S. Department of Defense, March 24, 2015. http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/607027
45. Baran P. *On Distributed Communications Networks*. Santa Monica, CA: RAND Corporation, 1962.
46. Clark DD. A cloudy crystal ball: visions of the future. Plenary presentation presented at the 24th meeting of the Internet Engineering Task Force, Cambridge, MA, July 17, 1992.
47. Abbate J. *Inventing the Internet*. Cambridge, MA: MIT Press, 1999.
48. Long A, Green BR. Stalking the secure second strike: intelligence, counterforce, and nuclear strategy. *J Strat Stud* 2014;**38**:38–73.
49. Wolf M, McElvoy A. *Man Without a Face: The Autobiography of Communism's Greatest Spymaster*. New York: Public Affairs, 1997.
50. Fischer BB. CANOPY WING: The U.S. war plan that gave the East Germans goose bumps. *Int J Intell CounterIntell* 2014;**27**:431–64.
51. Engelberg S, Wines M. U.S. says soldier crippled spy post set up in berlin. *The New York Times* 1989.
52. Owens WA, Dam KM, Lin HS. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009.
53. Herrick D, Herr T. Combating complexity: offensive cyber capabilities and integrated warfghting. Atlanta, 2016.
54. Hoffman D. *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*. New York: Random House, 2009.
55. Boulding KE. *Conflict and Defense: A General Theory*. New York: Harper & Row, 1962.
56. Brodie B, Dunn FS, Wolfers A *et al*. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co., 1946.
57. Wohlstetter A. The delicate balance of terror. *Foreign Affairs* 1959;**37**:211–34.
58. Kahn H. *On Thermonuclear War*. Princeton University Press, 1960.
59. Snyder GH. *Deterrence and Defense: Toward a Theory of National Security*. Princeton, NJ: Princeton University Press, 1961.
60. Trachtenberg M. *History and Strategy*. Princeton University Press, 1991.
61. Gavin FJ. *Nuclear Statecraft: History and Strategy in America's Atomic Age*. Ithaca: Cornell University Press, 2012.
62. Gartzke E, Kroenig M. Nukes with numbers: empirical research on the consequences of nuclear weapons for international conflict. *Ann Rev Polit Sci* 2016;**19**:397–412.
63. Powell R. Nuclear brinkmanship with two-sided incomplete information. *Am Polit Sci Rev* 1988;**82**:155–78.
64. Schelling TC. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.
65. Zagare F. Rationality and deterrence. *World Polit* 1990;**42**:238–60.
66. Schelling TC. *Arms and Influence: With a New Preface and Afterword*. New Haven, CT: Yale University Press, 2008.
67. Slantchev BL. Feigning weakness. *Int Organ* 2010;**64**:357–88.
68. Powell R. Nuclear brinkmanship, limited war, and military power. *Int Organ* 2015;**69**:589–626.
69. Blainey G. *Causes of War*, 3rd edn. New York: Simon and Schuster, 1988.
70. Fearon JD. Rationalist explanations for war. *Int Organ* 1995;**49**:379–414.
71. Powell R. *In the Shadow of Power: States and Strategies in International Politics*. Princeton, NJ: Princeton University Press, 1999.
72. Reiter D. Exploring the bargaining model of war. *Perspect Polit* 2003;**1**:27–43.
73. Wagner RH. *War and the State: The Theory of International Politics*. University of Michigan Press, 2010.
74. Betts RK. Is strategy an illusion? *Int Security* 2000;**25**:5–50.
75. Gartzke E. War is in the error term. *Int Organ* 1999;**53**:567–87.
76. Kaplow JM, Gartzke E. Knowing unknowns: the effect of uncertainty in interstate conflict. New Orleans, 2015.
77. Sagan SD, Waltz KN. *The Spread of Nuclear Weapons: An Enduring Debate*. 3rd ed, New York, NY: W. W. Norton & Company, 2012.

78. Gartzke E, Kaplow JM, Mehta RN. Offense, defense and the structure of nuclear forces: the role of nuclear platform diversification in securing second strike. Working Paper, 2015.
79. Gartzke E. War bargaining and the military commitment problem. New Haven, CT: Yale University, 2001.
80. Powell R. War as a commitment problem. *Int Organ* 2006;**60**:169–203.
81. Carson A, Yarhi-Milo K. Covert communication: the intelligibility and credibility of signaling in secret. *Security Stud* Forthcoming.
82. Ash C. *Remarks by Secretary Carter at the Drell Lecture Cemex Auditorium*. Stanford, CA: Stanford Graduate School of Business, 2015.
83. Lindsay JR, Gartzke E. Coercion through Cyberspace: The Stability-Instability Paradox Revisited. In *The Power to Hurt: Coercion in Theory and in Practice*, Greenhill KM and Krause PJP (eds.). New York: Oxford University Press, Forthcoming.
84. Colby E. Cyberwar and the nuclear option. *The National Interest*. June 24, 2013.
85. Cimbala SJ. *Nuclear Weapons in the Information Age*. Continuum International Publishing, 2012.
86. Fritz J. *Hacking Nuclear Command and Control*. International Commission on Nuclear Non-proliferation and Disarmament, 2009.
87. Futter A. Hacking the bomb: nuclear weapons in the cyber age. New Orleans, 2015.
88. Cimbala SJ. Nuclear deterrence and cyber: the quest for concept. *Air Space Power J* 2014;87–107.
89. Jervis R, Lebow RN, Stein JG. *Psychology and Deterrence*. Baltimore, MD: Johns Hopkins University Press, 1985.
90. Goldgeier JM, Tetlock PE. Psychology and international relations theory. *Ann Rev Polit Sci* 2001;**4**:67–92.
91. Yoshihara T and Holmes JR, eds. *Strategy in the Second Nuclear Age: Power, Ambition, and the Ultimate Weapon*. Washington, DC: Georgetown University Press, 2012.
92. Kristensen HM, Norris RS. Status of world nuclear forces. *Federation of American Scientists* 2016. http://fas.org/issues/nuclear-weapons/status-world-nuclear-forces (5 June 2016, date last accessed)
93. HP Security Research. *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*. HP Security Briefing. Hewlett-Packard Development Company, August 2014. http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.
94. Jervis R. *The Meaning Of The Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell University Press, 1989.
95. Rid T, Buchanan B. Attributing cyber attacks. *J Strat Stud* 2015;**38**:4–37.
96. Jervis R. *Perception and Misperception in International Politics*. Princeton University Press, 1976.
97. Tang S. The security dilemma: a conceptual analysis. *Security Stud* 2009;**18**:587–623.
98. Buchanan B. *The Cybersecurity Dilemma*. London: Hurst, 2016.
99. Long A. *Deterrence-From Cold War to Long War: Lessons from Six Decades of RAND Research*. Santa Monica, CA: RAND Corporation, 2008.
100. Jervis R. *The Illogic of American Nuclear Strategy*. Ithaca, NY: Cornell University Press, 1984.
101. Van Evera S. *Causes of War: Power and the Roots of Conflict*. Ithaca: Cornell University Press, 1999.
102. Green BR, Long AG. Signaling with Secrets–Evidence on Soviet Perceptions and Counterforce Developments in the Late Cold War. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Gartzke E and Lindsay JR (eds.), La Jolla, CA: Manuscript, 2016.
103. Peterson S. Old weapons, new terror worries. *Christian Science Monitor*, April 15, 2004. http://www.csmonitor.com/2004/0415/p06s02-woeu.html.