Thermonuclear Cyberwar

Erik Gartzke† & **Jon Lindsay**‡.

Abstract: Cyberwar is routinely over-hyped as a substitute weapon of mass destruction. More typically, cyber operations work as complements to power in other domains, generally limiting the aggressive potential of cyberspace on its own. However, there are situations where complementarity can undermine the stability of other domains in the most dramatic fashion. We examine the unusual contingency of a nuclear brinksmanship crisis in which offensive cyber operations (OCO) against nuclear weapons and/or their command, control, and communications (NC3) undermine deterrence and make war more likely. Nuclear nations have traditionally been free to display their nuclear capabilities openly—often in contrast to other forms of military power—given the lack of effective countermeasures to nuclear attack and its obvious destructiveness. Nuclear transparency in turn makes it easier to judge the balance of power, reducing the danger of misperception and war. Military advantages achieved in cyberspace typically cannot be disclosed without compromising their military effectiveness. Because of this commitment problem, OCO are best used rather than threatened. Unfortunately, the same warfighting advantages of NC3 OCO become dangerous liabilities for deterrence. Variation in operational capacity to conduct, detect, and mitigate NC3 OCO can be expected to make brinksmanship crises more or less unstable, should they occur. Increased uncertainty about the true balance of power will tend to undermine both nuclear and conventional stability. Policy measures must look to improve rather than degrade nuclear transparency.

Note: This paper was prepared for a workshop on the strategic use of offensive cyber operations held in March 2016 and organized by the Stanford Cyber Policy Program. On August 18, 2016, this paper was submitted to the Journal of Cybersecurity for entry into its review process and perhaps for publication.

We thank Scott Sagan, William J. Perry, and the participants of the Stanford Cyber Policy Program (SCPP) Workshop on Strategic Dimensions of Offensive Cyber Operations 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].

†The University of California, San Diego. email: egartzke@ucsd.edu.
‡The University of Toronto. email: jon.lindsay@utoronto.ca

Introduction

The 1983 movie *WarGames* popularized the problem of computer security with a fictional plot about a teenager who 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." Many increasingly alarmist documents emerged in the following decades as policymakers came to appreciate the evolving threat.[1–3]

The steady drumbeat of cyber threat rhetoric, combined with an historical absence of cyber catastrophes, has encouraged a stylized debate in the security studies literature between revolutionaries and skeptics. The former argue that societal dependence on cyberspace for everything including electrical power, food production, industrial manufacturing, and military communications empowers weak states or non-state actors (terrorists) to wreak mass destruction.[4–8] The latter argue that those who have the ability to surmount the non-trivial barriers to weaponization see little benefit in doing so, while government agencies and the cybersecurity industry have a pecuniary interest in hyping cyberwar.[9–16] At the risk of oversimplification, the revolutionary argument is that cyberwar is a *substitute* for traditional military power or even a new kind of weapon of mass destruction; the skeptical argument is that cyber operations are a *complement* for power, augmenting traditional political-military strengths through espionage, fraud, covert sabotage and subversion, and symbolic protest or hacktivism. The 2010 Stuxnet attack on Iranian nuclear enrichment and 2015 BlackEnergy attack on Ukrainian electrical power distribution systems demonstrate that revolutionary concerns are plausible, but in both cases stronger states conducted cautious probing for years against weaker victims, exercising notable restraint during the disruptive. Cyber operations

appear to make strong governments somewhat stronger and possibly enable weaker actors to harass their more capable adversaries on the margins where they are not resolved to respond.

Although we find the skeptical side of this debate generally persuasive, complacency is not warranted. The same strategic logic that leads us to view cyberwar as a complement rather than a substitute, and therefore a limited political instrument by itself in most situations, also leads us to view cyberwar as incredibly destabilizing in some other, thankfully rare, situations. Cyberwar, for example, which is more helpfully described as offensive cyber operations (OCO), could be used in conjunction with conventional military strikes in a U.S.-China conflict scenario to blind sensors and confuse decision making, and this possibility could create incentives for both sides to rush to preempt or escalate.[17,18] It is also possible, however, that "blinding" through OCO will simply make more traditional offensive operations more difficult, shifting the advantage to defenders and making conflict less likely.

There are also issues of scale in cyber conflict. In a recent Israeli wargame of a regional scenario, the United States and Russia nearly clashed, suggesting to one participant "how quickly localized cyber events can turn dangerously kinetic when leaders are ill-prepared to deal in the cyber domain."[19] Importantly, this catalytic instability arises not from the cyber domain on its own but through its interaction with forces in other domains (land, sea, air, etc.), and it arises only in situations where actors possess and are willing to use traditional military forces to defend their interests. This *cross-domain* problem becomes particularly acute if nuclear weapons are involved.[20] OCO targeting nuclear command, control, and communications systems (NC3), or the functionality, precision or operational effectiveness of the weapons themselves presents policymakers with a serious problem. It also provides us a unique opportunity to understand how cross-domain deterrence works. Cyberwar is not itself a weapon of mass destruction, but when used in conjunction with weapons of mass destruction, the extreme differences between these domains creates underappreciated dangers for all sides of the deterrence relationship.

The military and political characteristics of various types of weapons can have differential effects on deterrence and defense, but this fact has received little attention in classical deterrence theory.[21] Nuclear weapons and OCO are particularly complementary (i.e., nearly complete opposites) with respect to their informational 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 transparent, as well as lethal. Deterrence requires the holders of nuclear weapons to publicly display details of their nuclear arsenals. Fortunately, nuclear nations can do so with relatively little concern that disclosure of this information will reduce their ability to strike or retaliate; credible communication about nuclear capabilities does not degrade, but rather enhances, the deterrent effect of these incredibly destructive weapons.[22] OCO, by contrast, relies on undisclosed vulnerabilities, social engineering, and creative guile to generate indirect effects in the information systems that control behavior beyond the cyber domain. Revelation tends to expose OCO to crippling countermeasures, while the imperative to conceal constrains both the scope of OCO and its utility for coercive signaling.[23,24]

The obvious problem is that transparency and deception do not mix well. An attacker who conducts NC3 OCO will gain an advantage over a nuclear adversary that the attacker cannot reveal, while the nuclear target may continue to attempt to wield a deterrent that it does not realize is degraded or may even no longer exist. Most analyses of inadvertent escalation have focused on the 'use it or lose it' pressures created by NC3 attacks that become visible to the target.[17,25,26] This is plausible, but the revelation of information about a newly unfavorable balance of power might also encourage compromise. We suggest that clandestine attacks present a much more insidious threat to crisis stability.

We develop this argument in six parts. First we sketch the vulnerabilities of NC3, gleaned from open sources and declassified documents. Second we point out that transparency about nuclear capabilities is a critical component of credible deterrence. Third we argue that the secrecy requirements of OCO create a commitment problem that makes OCO better for *winning* than *warning*, the extreme inverse of nuclear weapons. Fourth we analyze the implications for deterrence of combining these complementary domains.

Fifth we briefly discuss how relative abilities to conduct, detect, and mitigate NC3 OCO might affect crisis stability. The conclusion returns to the motivating policy problem with a discussion of what can be done to lessen some of the hazards as we outline them here.

Hacking NC3

NC3 systems span four major segments of the nuclear enterprise including intelligence and early warning sensors located in orbit and on Earth, command and control hubs where national leadership can order a launch, operational nuclear forces including bombers, land-based missiles, and ballistic missile submarines, and the communication and transport networks that tie the whole apparatus together.[27] OCO might conceivably compromise any of these 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. The objectives of NC3 OCO could thereby range from gaining a clandestine intelligence and warning advantage over the target to active interference in the target's ability to conduct nuclear operations. The actual feasibility of any given OCO will depend on the material configuration of software and hardware together with organizational practices in play at the time of an attack.

NC3 vulnerabilities emerge from a combination of antiquated infrastructure and sophisticated computer exploitation techniques that are increasing in number, diversity and availability. Admiral Cecil Haney, the commander of U.S. Strategic Command (STRATCOM) in charge of U.S. nuclear forces, testified to Congress 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."[28] The NC3 challenges faced by the United States are not unique; they can be expected to be similar or worse for other nuclear powers.

NC3 has long been recognized as the weakest link in the U.S. 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."[29] Two years later the Principal Deputy Under Secretary of Defense (Research and Engineering) released a broad-based, multi-service 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."[29]

Although these reports focused on survivability during a nuclear exchange, the fragility of NC3 to other means of attack also became apparent. Following many near-misses and self-audits during and after the Cold War, U.S. NC3 has improved due to new safeguards and redundancies, but the unclassified summary of a 2015 audit of U.S. NC3 stated that "known capability gaps or deficiencies remain."[30]

The same declassified history noted that NORAD has received numerous false launch indications from faulty computer components, loose circuits, and even a nuclear war training tape loaded into a live system by mistake.[29] Industrial accidents are often used to provide examples of how hacking might disrupt critical infrastructure, and the nuclear weapons safety literature likewise provides a number of troubling examples of NC3 glitches.[31–33] If it could happen by mistake, one must assume that it is at least technically possible for it to happen intentionally. Of course, any real attacker must solve formidable challenges of intelligence, planning, control, and strategic interaction, to include

counterintelligence detection, to convert a mere technical possibility into a usable cyber weapon.[34] NORAD discovered and recovered from its mistakes, after all. Yet even if U.S. NC3 presents a hard target, other countries' NC3 may be easier to compromise, especially new entrants to the nuclear club like North Korea. The United States has already demonstrated, moreover, a willingness and ability to penetrate sensitive foreign nuclear infrastructure through Operation Olympic Games (Stuxnet), albeit targeting Iran's nuclear fuel cycle rather than NC3 for tactical advantage, our focus here.

The willingness of the United States to pursue NC3 OCO can be further inferred from analogous initiatives during the Cold War. An East German intelligence officer obtained classified documents, allegedly from a NATO source, on a U.S. special access program named CANOPY WING, which included features such as:[35]

> • "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."

The purported details of CANOPY WING precisely illustrate the potential and limitations of NC3 OCO. CANOPY WING relied on electronic warfare and kinetic attacks to degrade NC3, but OCO could perform many of the same missions today, with

even greater stealth and precision. It is unlikely that there would have been any serious plans to disable NC3 without a complementary strike to destroy Soviet nuclear forces, as the 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 an 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. The United States would thus understand that it had just one opportunity for preemption, thus heavily encouraging a "use or lose" mentality, with an exercise of capabilities through a massive attack, rather than through threats backed up by evidence of capabilities. CANOPY WING thus appears to have been intended to facilitate a preemptive NATO strike on Soviet NC3 to disable the Soviet ability to retaliate, and to limit the damage of any retaliatory force that survived. Although the details of CANOPY WING remain sketchy, they are consistent with other aggressive U.S. counterforce initiatives fielded during the Cold War.[36] It is reasonable to assume that OCO has since been added to this quiver.

Although modern OCO and NC3 are both highly classified realms, it is widely believed, or feared, that together they are a recipe for instability.[37–39] Stephen Cimbala points out that today's relatively smaller nuclear arsenals may perversely magnify the attractiveness of NC3 OCO 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."[40] Cimbala focuses mainly on the risks of misperception and miscalculation that emerge when OCO 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."[37] This of course depends on how humans react to risk and uncertainty. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target's awareness of

compromises to its NC3 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 compromise rather than escalate. Although 'known unknowns' can create confusion, to paraphrase Donald Rumsfeld, the 'unknown unknowns' would seem far more dangerous.

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 had 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."[41] 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.[42,43] To sum up, 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.

Nuclear Transparency and Deterrence

NC3 OCO is a plausible concern and has been for some time, as far as can be gleaned from open sources. This judgment stops where the majority of discussions about cyber insecurity stop, however, with a demonstration of the technological possibility of cyber catastrophe. Yet there are many possible disasters that never come to pass because no one expects to benefit from setting them into motion. A further logic of political or economic cost and consequence is needed to understand which threats are not only possible but that are also probable under some circumstance.[11] An analysis of the incentives grounded in rational deterrence theory can help to determine whether dismal predictions are justified or not (irrational decisions defy prediction by definition). It turns out that NC3 OCO provides the rare case in the cyber debate where reality might be worse than the rhetoric.

Nuclear weapons are unusual in several ways. 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. The loss-of-strength ratio (a description of the attenuation of capabilities caused by geographic distance[44]) for nuclear weapons appears especially attenuated. The loss-of-strength ratio is. Aerial bombers, intercontinental ballistic missiles (ICBMs) and submarine launched ballistic missiles (SLBMs) can project nuclear warheads considerable distances without significantly mitigating their lethality. It is all but impossible to intercept every munition, even with modern ballistic missile defenses. When one missed missile can incinerate millions of people, the idea of winning a nuclear war appears almost meaningless for most policymakers.

The advent of nuclear weapons thus brought deterrence as a strategy from obscurity to center stage, even as the nuclear nightmare dramatically increased the potential consequences of getting deterrence wrong. The nuclear era has been an extraordinarily intense learning experience for both practitioners and students of international security, rewriting well-worn realities more than once.[45–47] As defense became impractical and war unthinkable, early Cold War strategists championed the threat of nuclear retaliation as the chief mechanism for avoiding war.[48–51]

It is tempting to claim that 'the delicate balance of terror' was the major driver behind the circumspection of nuclear adversaries during the Cold War; however, one of the key conundrums in this perspective is the presence and practice of brinkmanship. Adversaries 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. If Cold War adversaries were indeed too terrified to risk nuclear war, then they could not credibly threaten that which was precisely what they feared. 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.[52] Winning at nuclear diplomacy thus means inducing temporary periods of instability (crises) that paradoxically makes deterrence less successful by intentionally raising the risk of accidental nuclear war. This logical inconsistency led almost from the beginning of the nuclear era to elaborate deductive contortions.[53–56]

Incredibly destructive and impossible to thwart, nuclear weapons form a uniquely effective deterrent. Put another way, it was not only that the nuclear era made deterrence necessary, but that it also made reliable deterrence possible. If the Cold War was fundamentally stable because of mutually assured destruction (MAD), then the chief strategy practiced by its protagonists was to attempt to undermine that stability, at least incrementally, and if only for brief intervals. The chief concern in historical episodes of chicken, such as the Berlin Crisis and Cuban Missile Crisis, was consistently *not* whether a certain level of harm was possible, but whether an adversary was resolved enough, possibly, to risk nuclear suicide. Rather than bottling up aggressions, nuclear adversaries sought ways to liberate them through nuclear threats, enunciated however obliquely, even irrationally. Yet both MAD and successful brinksmanship further depended on a less appreciated, but no less fundamental, feature of nuclear weapons: ready transparency.

Most elements of military power are weakened by disclosure.[57] Military plans are considerably less effective if shared with an enemy. Conventional weapons become less lethal as opponents learn what systems can and cannot do, where they are located, how they are operated, and so on. Information about capabilities and plans generally allows opponents to devise countermeasures and array defenses to blunt or even disarm the attack. In contrast, relatively little reduction in destruction follows from enemy knowledge of nuclear capabilities. One ICBM still might get through and annihilate the capital city. As always, there is a price to be paid for allowing an enemy to learn about one's secrets, but in the case of nuclear capabilities this price is relatively modest. Precisely because of the futility of defense and their obvious destructive potential, nuclear forces are more robust to the disclosure of information than other weapons, which enables a state to advertise to adversaries the harm which it is capable of inflicting.

Secret capabilities cannot deter. In the satirical masterpiece *Dr. Strangelove*, the 'Doomsday Machine' is an underground super bomb programmed to incinerate the Earth's atmosphere should the Soviet Union ever be attacked. Deterrence fails spectacularly in the film when a rogue American commander orders an unauthorized U.S. nuclear strike. The need for transparency in effecting deterrence is driven home by the President's eponymous science advisor in excited conversation with the Russian

ambassador, “the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn’t you tell the world, eh?” Devastating weapons kept secret because “the premier likes surprises” or any other reason are a recipe for tragedy.

During the real Cold War, fortunately, Soviet leaders paraded their nuclear deterrent through Red Square for the benefit of foreign military attaches and the international press corps. They also allowed their missile and submarine bases to be spied on by orbiting satellites. While other aspects of military affairs in both societies were 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. Orthodox strategic history emphasizes the role of fear and insecurity, but cooperative transparency also contributed to superpower peace.

Rationalist bargaining models of war imply that costly conflict can result when nations have different expectations about what outcome war will produce.[58–62] It follows that wars themselves, or at least some wars, are a product of what adversaries do not know, or what they misperceive.[63,64] If knowledge of capabilities or resolve is a prerequisite for deterrence, then one reason for deterrence failure is the failure to credibly communicate the status of relative capabilities or resolve. Put a different way, war itself is a product of different expectations about the balance of power (capabilities, costs, interests), as well as incentives to conceal this information and bluff in order to retain diplomatic leverage.[59] Discrepant expectations can be produced in many ways, including cultural misperception, domestic politicization, and strategic dissembling, but it is important to note that they could also be resolved where an interest exists in sharing information—as was the case in the Cold War nuclear stalemate—or if information itself is difficult to conceal. Successful bluffing can produce better circumstances or even explicit bargains as opponents make concessions or agree to compromises that they would not otherwise accept. But ecologically, the presence of bluffing means that claims are not always believed, leading to challenges that are only probabilistically correct. In every contest, at least one side is mistaken about the eventual disposition of disputed issues, influence or territory after the contest. Fighting thus informs adversaries of the true state of the balance of power.

From this perspective, successful deterrence involves instilling in an adversary perceptions like those that result from fighting, but before the fighting begins. Deterrence thus requires transparency to impart information to an adversary that causes the adversary to act with greater discretion. The relative transparency of nuclear arsenals during the Cold War helped the superpowers to calculate risks and consequences within a first order approximation, and they were certainly terrible. The transparency that made deterrence possible also made it easier for states to bargain more effectively, forging compromises that each preferred to military confrontation or even to the bulk of possible risky brinkmanship crises. Because of their transparency, nuclear weapons minimize uncertainty about the balance of power, leading to a reduction in conflict and instability.[65]

The transparency of nuclear weapons is not absolute, of course. Platform mobility can make it harder for an observer to track and count respective forces from space. Counterforce strategies (including attacks on NC3), platform diversity, ballistic missile defense systems, and force employment doctrine can make it more difficult for one or both sides in a crisis to know whether an attack will likely succeed or fail, affecting not only estimates of the balance of power but also the degree of confidence in retaliation. (There is reason to believe that platform diversity in particular lowers the risk of nuclear or conventional contests, because increasing the number of types of delivery platforms heightens second strike survival without increasing the lethality of an initial strike.[66]) By the same token, both superpowers considered the warfighting advantages of nuclear weapons, quite apart from their utility as a deterrent. These include high-altitude airbursts for air defense, electromagnetic pulse effects for frying electronics, underwater detonations for anti-submarine warfare, and so on. Transparency *per se* is less important than weapon effects for these situations, and might even be deleterious for the tactical operation insofar as tactics depend on stealth and mobility. Yet the use of nuclear weapons for any reason is costly for the employing state, first in the risk of retaliation in kind and secondarily in the political opprobrium of mass killing.

The third nuclear weapon used in anger will be a major event in world history. Yet for the same reason, nuclear weapons are ideal for coercion. Compared to any other weapon ever

invented, the primary, and paradoxical, purpose of nuclear weapons is to prevent the use of nuclear weapons.

Nuclear weapons appear to have been a source of surprising stability in international affairs. 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. The deterrent effect of nuclear weapons is aided in particular by their robustness to revelation. The relative transparency of nuclear weapons is what makes credible deterrence possible. Cyber operations, by contrast, have exactly the opposite characteristics.

The Cyber Commitment Problem

OCO depends on deception. Attackers subverts the openness of public and corporate networks to infiltrate and exfiltrate data, masquerading as legitimate applications among hosts and users who cannot distinguish safe code from malware. OCO may use technical features or flaws in ways that engineers and network administrators do not intend, and would have blocked had they the insight or foresight to do so, or social engineering techniques that con gullible users into disclosing credentials or installing malware. Defensive cyber operations can also use deception to ensnare attackers in honeypots or 'hack back' against the attacker. Compromise of these offensive or defensive gambits is relatively easily achieved through disclosure; revelation of OCO can often enable the target to adapt and defeat them.[23,67]

All military capabilities are designed to serve two very different functions: conquest (defense) and compellence (deterrence). Force can be used to *win* a contest of strength by destroying, outmaneuvering the adversary, and changing the distribution of power. Force can also be used, or merely displayed, to *warn* an adversary of unpleasant consequences if it takes or fails to take an action. Traditional warfare often does a little of both. A

mobilization of military forces in a crisis signifies resolve and displays a credible warning, but it also makes those forces more potent since a higher condition of readiness makes it easier to attack or defend. Persistence in a battle of attrition not only bleeds an adversary but also reveals a willingness to pay a price for victory higher than the adversary may have thought possible. However, the informational requirements of winning and warning are often in tension. While deterrence requires transparency, combat performance often hinges on well-kept secrets, feints, and diversions. A visible castle on the frontier may deter attack, but stones and mortar are less effective if the enemy has infiltrated the garrison or tunneled under the castle walls. These stratagems are most successful, moreover, when defenders are unaware that their defenses have been compromised. Sharing information about the balance of power can be operationally harmful to the extent that military plans and capabilities degrade when revealed. National security thus turns on the tradeoffs between the objectives of preventing war by advertising capabilities or interests and whatever improvements in fighting power are likely to stem from concealing capabilities and effecting surprise, should war break out.

The *military commitment problem* involves this need to conceal information about the true balance of power in order to preserve battlefield effectiveness.[68,69] Competitors may choose to conceal details relevant to the likelihood of victory or cost of fighting if by doing so they ensure that an adversary is less likely to prevail. Japan failed to warn the United States about its intentions/ability to attack Pearl Harbor in large part because the United States could not credibly promise not to use this information to weaken the effectiveness of the Japanese attack by adopting a war posture, dispersing the Pacific Fleet, etc. 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 terms of military advantage. In *Dr. Strangelove* President Merkin Muffley is willing to pay this price when he invites the Soviet Ambassador into the war room over General Buck Turgidson's objection that "he'll see the big board!" Muffley tries to demonstrate his benign intentions to the Soviet Ambassador by revealing valuable information that undermines U.S. military capabilities, even helping the Soviets to shoot down American bombers.

OCO suffers from an extreme version of the military commitment problem. The notion of 'winning' here must be understood to cover not only military action on the battlefield but also successful intelligence collection or covert action. All depend on deceptive tools and techniques (intelligence tradecraft) that work through guile and trickery, not kinetic force. OCO requires considerable creativity, testing, and expense to use effectively. Revelation of OCO is likely to invalidate months or years of careful preparation. Stuxnet took years and hundreds of millions of dollars to develop but was patched within weeks of its discovery. So-called zero day vulnerabilities sell for hundreds of thousands of dollars on the gray market but are worth almost nothing once disclosed to the public. The Edward Snowden leaks negated a whole swath of signals intelligence tradecraft that the NSA took years to develop. Cyber operations, therefore, like most intelligence collection operations, are conducted in extreme secrecy because secrecy is a condition for their efficacy.

Cyber weapons are literally just information but, ironically, they are not very informative. Presidents can use other forms of covert action such as publicly disavowed lethal aid or aerial bombing (e.g., Nixon's Cambodia campaign) to 'privately' signal their interests, but such cases work because the revelation itself doesn't disarm the rebels or prevent the airstrikes.[70] By contrast, disclosure of a cyber threat tends to undermine the threat. If the communication of a cyber threat is detailed enough to convince a target of the credibility of significant harm to network operations or the compromise of data, then the information supplied is specific enough to defeat the threat by patching or reconfiguring defenses.

Vague threats are not credible because they are indistinguishable from casual bluffing. This point is regularly misconstrued. Ambiguity does not deter. However, ambiguity can be used to conceal a lack of capability or resolve, allowing an actor to pool with more capable or resolved states and acquiring some deterrence success by association. Nuclear threats have to be ambiguous because nuclear nations cannot credibly threaten nuclear suicide. The consistently ambiguous phrasing of U.S. cyber declaratory policy—"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"[71]—seeks to operate across domains to use 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 OCO.

This does not mean that OCO is categorically useless for signaling, just as nuclear weapons are not categorically useless for warfighting. A reputation for OCO skill may increase general deterrence by discouraging serious cyber challenges (contrasted with immediate deterrence in a specific crisis[72]) or encouraging a degree of paranoia in potential adversaries. The United States has probably gained some such benefits through the disclosure of Stuxnet and the Snowden leaks, but the very fact that these revelations were absolutely unintended and emphatically repudiated by many U.S. officials because they compromised tradecraft highlights the salience of the cyber commitment problem. Ransomware attacks can work when the money extorted to unlock the compromised host is priced below the effort of initiating an investigation or reinstalling the system. Some OCO may actually be hard to mitigate within tactically meaningful timelines (e.g., perhaps the attacker has installed wirelessly activated implants in hard-to-reach hardware components). If so, then some offensive cyber operations could be revealed to coerce concessions within the tactical window created by a given operation. In general, however, compared to other types of capabilities, OCO are far better suited for winning than warning. Cyber and nuclear weapons fall on extreme opposite sides of this spectrum.

Ambiguous Complements

Differences between OCO and nuclear weapons have contrasting implications for stability within each domain. OCO relies on deceptive or secretive tradecraft that is easy to counter once revealed. Defense against nuclear weapons is all but futile, which makes it possible to reveal capabilities and effects. Considered separately, the nuclear domain is stable and the cyber domain is unstable. In combination, the results are ambiguous.

Nuclear weapons have long been considered to be stabilizing with respect to rational incentives for war (the risk of nuclear accidents is another matter).[73] If each side has a secure second strike—or even a minimal deterrent with some non-zero chance of launching even 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 theory of graduated escalation, in even a modest initial

nuclear exchange the costs will be extremely high, even if the impact on military power in the short term will often be minimal. As long as both sides understand this and understand (or believe) that the adversary understands this as well, then the relationship is stable. Nuclear weapons have been used only twice, but cyberspace is abused daily.

OCO directly creates none of the horrific lethal effects created by nuclear or other more "kinetic" military capabilities. OCO effects work indirectly, for example by triggering a series of events in some sociotechnical system, such as causing an electrical power failure by over-tasking transmission lines, de-activating breakers, and concealing these activities from operators and safety systems. Few intrusions create disruptive physical consequences that rise to the level of attacks such as Stuxnet or BlackEnergy, but even these efforts pale beside the harm imposed by even a small war. Not many actors are technically capable of the most sophisticated penetrations, but those who are tend to be engaged in a wide portfolio of exploitation for intelligence and politico-military operations. To the extent that sophisticated cyber-physical operations evince restraint, whether because of concerns about retaliation or wariness about the prospect of compromised capability or collateral damage, then stability does obtain for a narrow class of OCO, even as the same actors indulge in many other types of OCO. Where actors feel they can maintain their deceptive cover and the plausible deniability of an operation in pursuit of marginal revision of the distribution of power, stability goes out the window.

Criminal exploitation, hacktivist harassment, intelligence operations, state surveillance, and information control activities unfold continuously, with new modulations ever emerging. Most OCO focuses on exploitation for intelligence collection of valuable data to gain a competitive advantage in other military, diplomatic, or economic arenas. Other OCO conducts information operations to influence opinions online and, indirectly, the social behavior of the target group (e.g., to curtail violent extremist radicalization). More exotic OCO provides a wartime reserve capability prepared well in advance to create havoc in enemy command and control systems in time of war (e.g., disabling radar coverage to support an airstrike) or to effect some subtle sabotage in peacetime. In every case OCO works indirectly to influence activities in other domains, to borrow a slogan of U.S. Army Special Forces, 'by, with, and through' the networks of others. The cyber

domain is fundamentally cross-domain: it is useful not for its own sake but rather because it affords political, economic, or military control in other areas.

The strategic implications of combinations across the cyber and nuclear domains are ambiguous. On one hand, the stability of the nuclear domain can help to stabilize the inherently unstable cyber domain by bounding the intensity of destruction an attacker would be willing to inflict on an adversary. The U.S. has attempted to signal through its declaratory policy that massive cyber attacks on vital critical infrastructure could prompt a military response, and while nuclear is not explicitly threatened neither is it withheld. All options are 'on the table' to respond to the deliberate crippling of critical infrastructure. Such threats have no credibility at the low end, where the bulk of attacks occur and where most penetrations continue unabated. But threats of this type do create a potential upper bound on cyber aggression, posing as a deterrent to the degree that retaliation is anticipated and feared.[74,24]

At the other end of the conflict spectrum, the instability of the cyber domain can also undermine the stability afforded by nuclear MAD. Nuclear stability has often been attributed to "the balance of terror," but that term is misleading. First, the balance of nuclear consequences have very little to do with deterrence, as noted above. Second, while terror may be critical in motivating risk aversion, it is clarity about the nuclear capabilities and their consequences that is critical. States may initiate crises of risk and resolve to see who will back down first, which is not always clear, but each understands that a nuclear war would be a disaster for all. If uncertainty is a major cause of war, and if nuclear weapons remove this uncertainty because of their ready transparency and signaling characteristics, then nuclear weapons strongly stabilize. It is not simply that both sides are afraid, but rather that both sides see the contest similarly. NC3 OCO undermines precisely this understanding.

If OCO effects a successful clandestine penetration of NC3 networks, then it can potentially defeat the informational symmetry that stabilizes nuclear relationships. Nuclear stability is founded upon a mutual recognition that each side will be able to inflict prohibitive levels of damage—an agreement on the distribution of power. 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 this consensus is compromised. One side knows that it has advantage, but cannot reveal the advantage to their adversary, lest it be lost. We described this as the cyber commitment problem. The other side does not know that it has a perilous deterrence liability, and cannot be told by the other side, for the same reason.

Nuclear weapons are useful for deterrence because they enable agreement about the distribution of power. This should make dealing with an adversary diplomatically much 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 seeking compromise rather than annihilation. OCO, by contrast, is attractive precisely because it can secretly revise the distribution of power. If the penetration is conducted thoroughly, expertly, and clandestinely, then it is possible that this revision can undermine the ability of nuclear adversaries to find a compromise. OCO, furthermore, will tend to be irresistible to states that believe that they can keep offensive cyber operations hidden, especially given the enormous benefits involved in reducing the risk of nuclear attack. OCO 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 war. Yet the very success of OCO makes deterrence failure during brinksmanship crises more likely.

NC3 OCO threatens to create a dangerous competition in risk taking during a nuclear crisis. 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 do if it understood how disadvantageous the balance of power really was. 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 possibly producing incentives for self-protective action.

The potential for instability can be taken one step further, to the ecological level. Nuclear nations must gradually become aware of the risk that the national strategic deterrent *may* be undermined. The fact that it is technically possible to carry out NC3 OCO, combined with the incentives attackers have to keep their efforts clandestine, mean that nuclear powers must imagine that they may have been compromised, whether they have or not. In terms of the risk of war, it is not necessarily a problem if nations fear that their deterrent is incomplete. This may even encourage greater circumspection in world affairs. However, those states that are affected will nevertheless typically underestimate their vulnerability, continuing to rely on a deterrent that is incomplete or wholly absent.

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 somewhat confined. However, if a crisis has risen to the point where nuclear threats are being seriously considered or made, then NC3 OCO will be destabilizing. This may occur more frequently than is generally believed. President Vladimir Putin of Russia has insinuated more than once in recent years of a willingness to use tactical nuclear weapons if necessary to support his policies.

Operational Capacity and Crisis Stability

Not all crises are the same. Indeed, their very idiosyncrasies create the uncertainties that make bargaining failure more likely.[63] So far our analysis would be at home in the Cold War with the technological novelty of OCO added in, but not every state has the same ability to conduct NC3 OCO, or the same vulnerability. The so-called second nuclear age differs from superpower rivalry in important ways.[75] There are fewer absolute numbers of warheads in the world, down from a peak of over seventy thousand in the 1980s to about fifteen thousand today (less than five thousand deployed), but they are distributed very unevenly.[76] 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 more recent nuclear powers lack the hard-won experience and shared norms of the Cold War to guide them through a crisis. Cyber warfare capacity also varies considerably across these states. 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.[15] France, India, and Pakistan also have active cyber warfare programs, while North Korea is the least developed cyber nation and depends heavily on China for its expertise.[77]

It is reasonable to expect the uneven distribution of capabilities and expertise to influence the impact of NC3 OCO on crisis stability. It is beyond the scope of this article to assess empirical crisis dyads in detail, and data on NC3 and OCO for these countries are shrouded in secrecy in any case. In this section we sketch out the implications of three stylized factors that describe the *operational* success or failure of NC3 OCO. We do not stress relative nuclear weapon capabilities on the admittedly strong assumption that nuclear transparency in the absence of OCO would render nuclear asymmetry irrelevant for crisis bargaining because both sides would agree about the balance of power. 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 NC3 OCO capabilities, brinksmanship between them is dangerous for many other reasons, notably compressed decision timelines, Pakistan's willingness to shoot first, and domestic regime instability. We are interested here in the impact of NC3 OCO on nuclear transparency above and beyond these other factors that clearly also play a role in real world outcomes.

First, does the OCO attacker have the organizational capacity, technical expertise, and intelligence support to *compromise* the target's NC3? This includes gaining access to critical networks, exploiting technical vulnerabilities, and executing a payload to disrupt or exploit any NC3 segment including strategic sensing, command, forces, or transport

capacity. The result of compromise is some tangible but tangible advantage—but one that cannot be exercised in bargaining—such as tactical warning or control paralysis.

Second, is the target able to *detect* the compromise of its NC3? The more complicated and sensitive the target, the more likely OCO operators are to make a mistake and leave clues that compromise the existence if not the extent and intent of the operation. Intent is especially difficult to discern for OCO given that disruptive attacks use many of the same methods as reconnaissance missions for navigation and targeting. Attribution in such a case is not likely to be difficult as the context of the crisis will have radically constricted the pool of potential suspects, but at the same time the consequences of misattributing 'false flag' operations could be severe.[78] At a minimum detection is assumed to provide some information to the target that the balance of power is perhaps not as favorable as thought previously. We assume that detection without an actual compromise is possible because of false positives or deceptive information operations to create paranoia but with no actual shift in the balance of power.

Third, is the target able to *mitigate* the compromise it has detected? An ideal-type OCO such as we have been describing in this article is disarmed upon discovery. Revelation thus results in patching or network reconfiguration that blocks the attack. This assumption is not always realistic. The attacker may have multiple pathways still 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 signal of potential harm 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 NC3 OCO. We assume that mitigation is predicated on detection.

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

Table 1 shows how the three variables combine to produce different deterrence outcomes in a brinksmanship (chicken) crisis. If there is no NC3 compromise and the target detects nothing (no false positives) then we have the optimistic ideal case described above where nuclear transparency affords stable *deterrence*. We expect this box to describe situations where the target has excellent network defense capabilities and thus the prospect of defensive, denial or deception successfully deters the adversary's attempts at NC3 OCO. This may resemble the Cold War situation, or even the present day U.S.-Russia dyad, where the odds of either side pulling off a successful compromise against a highly capable network defender are not favorable or at least they are risky enough to encourage restraint. The historical existence of CANOPY WING, however, does not make us terribly optimistic on this score.

If there is a compromise that goes undetected—that is, NC3 OCO succeeds substantially or completely—then there is heightened risk of *war* because of the discrepant assessment of the balance of power resulting from the cyber commitment problem. This is the pessimistic ideal case described in the previous section. This box may be a good description of circumstances in asymmetric dyads, such as the United States and North Korea, where one side has the ability to pull off decisive NC3 OCO but the other side is willing to go to the brink where it believes, falsely, that it has sufficient capability to compel its counterpart to back down (an advantage in resolve). NC3 OCO is terrifically attractive for damage limitation should deterrence fail, given that the weaker state's diminutive arsenal makes damage limitation by the stronger power all the more likely to succeed. This poses a terrible dilemma for the stronger state, however, because the clandestine counterforce hedge is precisely what makes deterrence more likely to fail.

The United States would face similar counterforce dilemmas with other dyads like China or perhaps Russia, but states should be more circumspect when confronted with an adversary with a larger/more capable arsenal. More complex and cyber savvy targets, moreover, are more likely to detect a breach in NC3 systems, leading to coercion, use-lose, or spiral outcomes as described below. The remaining outcomes in our typology are more ambiguous and depend on how actors deal with risk and uncertainty.

If the successful compromise is detected but not mitigated, then the target will have learned that the balance of power is not as favorable as it had previously thought. This possibility suggests fleeting opportunities for *coercion* by revealing the cyber coup to the target in the midst of a crisis while the OCO attacker maintains or develops a favorable military advantage before the target has the opportunity to reverse or compensate for the NC3 disruption. Recognizing the newly transparent costs of war, the target is better equipped to negotiate and accept a compromise, allowing the cyber attacker to leverage deterrence (compellence) to maintain (revise) the status quo. It should be emphasized that coercive advantages of a detected but unmitigated NC3 compromise will typically be fleeting. This suggests two things. First, temporary advantages gleaned from OCO create their own commitment problem, since diplomatic bargains achieved with this kind of leverage can simply be repudiated once the advantage subsides. Second, there exists the possibility of creating a window of opportunity for forms of OCO that are more robust to 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 to the crisis area) before the window closes.

A target concerned about NC3 OCO will probably have some counterintelligence or intrusion detection system in place. This system can produce false positives as a result of internal error or a deception operation by the adversary to encourage paranoia in the target. It is again a logical possibility that some false positives would appear to the target to be difficult to mitigate. In this situation, the target believes it is at a disadvantage, even though this is not in fact the case. The adversary can thus gain an unearned advantage, an opportunity for coercion via a *bluff*, by the window-of-opportunity logic outlined above.

Either of these moves—coercion and bluffing—are fraught with danger, however. Detection without mitigation might put the 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 of NC3 OCO is only partial or has not

revealed the true extent of the compromise (i.e., the target doesn't realize that it has already lost some or all of what it hopes to use). These are the types of scenarios analyzed by Cimbala and others who focus on the hazard of inadvertent escalation.[18,25,26] The essential distinction between these heightened risks and what we label here as "war" is the target's knowledge of some degree of NC3 compromise. Use-lose in this instance is equivalently war, since the breakdown of deterrence leads to the release of nuclear weapons, but we distinguish these outcomes to highlight the ideational factors at work.

If the detected compromise is mitigated, however, then both sides will have restored their common mutual estimates of the relative balance of power. This superficially resembles the first deterrence case because the NC3 compromise is negated. This would seem to promote stability. Unfortunately, the detection of the compromise will provide the target with information about the hostile intentions of the OCO attacker. This in turn is likely to exacerbate other factors that may contribute to a negative *spiral* in the crisis itself or the crisis-proneness of the broader relationship. In unusual instances, there may be no cyber compromise but one could be detected *and* (believed to be) mitigated. This circumstance constitutes a misperception that also feeds the potential for conflict spirals.[79,80] Note that the bluff and coercion outcomes are also likely to encourage the spiraling of conflict once the fleeting bargaining advantage dissipates or is dispelled.

The risk of crisis instability is therefore not the same for all dyads. It is harder to compromise the NC3 of capable countries because of the redundancy and active defenses in their arsenals. 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 OCO. 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 much 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 U.S. NC3 with OCO given a U.S. reputation for cyber prowess.

This asymmetry favoring the United States becomes, ironically, destabilizing in a brinksmanship crisis. NC3 OCO compromise is much more likely if the United States is the attacker. The most dangerous dyad is a stronger and a weaker state (e.g., 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 will almost certainly conduct NC3 OCO as a warfighting hedge in case deterrence breaks down, while the weaker but still formidable side has a reasonable chance at detection. The weaker may also be tempted conduct NC3 OCO, particularly for reconnaissance. The stronger side is more likely to detect and correct the intrusion but will be alarmed by the intelligence-disruption ambiguity inherent in OCO.[81] In a brinksmanship crisis between nuclear states, windows for coercion may be available yet fleeting, and war and spirals are real risks.

Conclusion

Skeptics are right to challenge the hype about cyberwar. The term is confusing, and computer hacking rarely amounts to anything even approaching weapons of mass destruction. Cyberspace is most usefully exploited at the lower end of the conflict spectrum, as a complement for capabilities and activities in other domains. Yet the logic of complementarity has at least one exception regarding conflict intensity, and it is a big exception.

Offensive cyber operations against nuclear command and control systems can raise the risks of nuclear war. They do this precisely because cyber operations and nuclear weapons are extreme complements regarding their informational properties. OCO relies on secrecy. Nuclear deterrence relies on transparency. In a brinksmanship crisis, the former undermines the latter. Nuclear crises were rare events in Cold War history, thankfully. Today, the proliferation of nuclear powers and the modernization of nuclear weapons may raise the risk slightly. NC3 OCO raises a still miniscule risk slightly more. The enormity of nuclear use, and the attendant dangers of increased conventional conflict (even if nuclear weapons are not used), make even a slight heightening of risk notable.

Nuclear weapons are unique in that they cause competitors to think in terms of cost or risk rather than the probability of victory. The high cost of nuclear contests and the

distinctive transparency of the nuclear balance ensured that nuclear weapons have not been used for seven decades. If this nuclear stability is to continue, however, it will be necessary to find ways to maintain transparency. New technologies of communication are ironically undermining this transparency, as OCO offers a means to defeat an adversary's deterrent capabilities covertly. If knowledge of a shift in relative power is concealed, then the deterrent effect of nuclear capabilities will be at least partially undermined. This will tend to occur in periods where concern over nuclear attack is heightened, such as in the midst of militarized crises. However, there is no reason to believe that states will wait for a crisis before seeking to establish advantageous positions in cyberspace. OCO will and must often precede overt demands or aggression by months or even years. It is this erosion of the bulwark of deterrence that is most troubling. Today, as we face new or near nuclear powers, the question of nuclear stability cannot be ignored. Maintaining limited levels of aggression at limited conflict intensities requires more, not less, transparency.

U.S. nuclear strategy has long emphasized counterforce capabilities in practice.[36,82] Many theorists find them to be destabilizing because they undermine the credibility of the adversary's deterrent and create pressures to move first in the event of a crisis.[83,84] If deterrence fails, however, countervalue strikes on civilian population centers appear to be militarily useless and morally odious. Counterforce strikes by contrast aim at preemptive disarmament or damage limitation by attacking the enemy's nuclear enterprise. ("I'm not saying we wouldn't get our hair mussed," as General Turgidson says to President Muffley, "But I do say no more than ten to twenty million killed, tops.") Counterforce capabilities are designed for 'winning' a nuclear war once a crisis has slipped over the brink. But their strategic purpose may still include warning if they can 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 mission-critical and vulnerable details. This improved mutual recognition of U.S. advantages and thus clearer assessment of the balance of power, but the military commitment problem was real nonetheless.

NC3 has been and will remain a particularly attractive counterforce target because disruption can render the enemy's arsenal less effective without having to destroy

individual platforms. The problem with NC3 OCO, however, is that it is both exquisitely tempting for counterforce but also extremely sensitive to revelation. As one side builds more sophisticated NC3 to improve the credibility of its nuclear 'warning,' the other side engages in OCO to improve its capacity for nuclear 'winning,' thereby undermining the warning element central to successful deterrence.

What can be done? Arms control agreements to ban NC3 OCO might seem attractive, but a technology that depends on deception creates serious obstacles for monitoring and enforcement. Even where the U.S. 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 limiting counterforce options in the form of NC3 OCO should deterrence fail.

Better appreciation of the risks of NC3 OCO, founded on classified studies of the details of NC3 including their human organizations, might help nuclear war planners to exercise some restraint in NC3 OCO. Unfortunately the same reconnaissance operations used to better understand the opponent's NC3 can be misinterpreted as attempts to compromise it.[81] More insidiously, private knowledge is a source of warfare, in that knowing something about an adversary that improves one's prospects of victory in a conflict increases the incentive to act through force, or to exploit coercive windows of opportunity in a crisis that could inadvertently escalate to open violence. At the very least, every effort should be made to ensure that senior leaders—the President and the Secretary of Defense—understand and authorize any NC3 OCO for any reason. Education is easier said than done given the esoteric technical details involved.

Anything that can be done to make NC3 OCO harder to employ will make the most dangerous possibility of successful but undetected compromises less likely. Defense in depth, including redundant communications pathways, error correction channels, and the isolation of the most critical systems, is essential for NC3 reliability in general. Older technologies, ironically, may provide some protection by foiling access of modern digital OCO techniques (Russia reportedly still uses punch-cards for some NC3[85]), but older technologies may also have inadequate safeguards against modern techniques. The

broader principle is the importance of component heterogeneity for robust defense, rather than cultivating a vulnerable software monoculture. For defense in depth to translate into deterrence by denial requires the additional step of somehow advertising redundancy and the ability to continue to function in a cyber degraded environment.

NC3 OCO 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. With additional options, the 'spiral' outcomes that follow from detected and mitigated compromises are more likely, which may encourage restraint in creating crises. 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 short of 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. The implications of choice among an expanded palette of coercive options in an open-ended bargaining scenario is a topic for future research. Yet if a machine asks, "Do you want to play a game?" it would be helpful to have options available other than "global thermonuclear war."

Sources

1. Kaplan, F. 'WarGames' and Cybersecurity's Debt to a Hollywood Hack. *The New York Times* (2016).
2. Schulte, S. R. 'The WarGames Scenario': Regulating Teenagers and Teenaged Technology (1980-1984). *Telev. New Media* (2008). doi:10.1177/1527476408323345
3. Warner, M. Cybersecurity: A Pre-history. *Intell. Natl. Secur.* **27,** 781–799 (2012).
4. Borg, S. Economically Complex Cyberattacks. *IEEE Secur. Priv. Mag.* **3,** 64–67 (2005).
5. Clarke, R. A. & Knake, R. K. *Cyber war: the next threat to national security and what to do about it*. (Ecco, 2010).
6. Brenner, J. *America the vulnerable: inside the new threat matrix of digital espionage, crime, and warfare*. (Penguin Press, 2011).
7. Kello, L. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *Int. Secur.* **38,** 7–40 (2013).
8. Peterson, D. Offensive Cyber Weapons: Construction, Development, and Employment. *J. Strateg. Stud.* **36,** 120–124 (2013).
9. Dunn Cavelty, M. Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *J. Inf. Technol. Polit.* **4,** 19–36 (2008).
10. Rid, T. Cyber war will not take place. *J. Strateg. Stud.* **35,** 5–32 (2012).
11. Gartzke, E. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *Int. Secur.* **38,** 41–73 (2013).
12. Lindsay, J. R. Stuxnet and the Limits of Cyber Warfare. *Secur. Stud.* **22,** 365–404 (2013).
13. Lawson, S. Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *J. Inf. Technol. Polit.* **10,** 86–103 (2013).
14. Benson, D. C. Why the Internet Is Not Increasing Terrorism. *Secur. Stud.* **23,** 293–328 (2014).
15. Lindsay, J. R. The Impact of China on Cybersecurity: Fiction and Friction. *Int. Secur.* **39,** 7–47 (2014).
16. Valeriano, B. & Maness, R. C. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. (Oxford University Press, 2015).
17. Gompert, D. C. & Libicki, M. Cyber Warfare and Sino-American Crisis Instability. *Survival* **56,** 7–22 (2014).
18. Goldstein, A. First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations. *Int. Secur.* **37,** 49–89 (2013).
19. Opall-Rome, B. Israeli cyber game drags US, Russia to brink of Mideast war. *Defense News* (2013).
20. Lindsay, J. R. & Gartzke, E. in *Cross-Domain Deterrence: Strategy in an Era of Complexity* (eds. Gartzke, E. & Lindsay, J. R.) (Manuscript, 2016).
21. Shannon Carcelli. *Blast from the Past: Updating and Diversifying Deterrence Theory*. (2016).
22. Powell, R. *Nuclear Deterrence Theory: The Search for Credibility*. (Cambridge University Press, 1990).
23. Gartzke, E. & Lindsay, J. R. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Secur. Stud.* **24,** 316–348 (2015).
24. Lindsay, J. R. Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack. *J. Cybersecurity* **1,** 53–67 (2015).
25. Posen, B. R. *Inadvertent Escalation: Conventional War and Nuclear Risks*. (Cornell University Press, 1991).
26. Cimbala, S. J. Nuclear Crisis Management and 'Cyberwar': Phishing for Trouble? *Strateg. Stud. Q.* (2011).
27. Office of the Deputy Assistant Secretary of Defense for Nuclear Matters. in *Nuclear Matters Handbook 2015* 73–81 (Government Printing Office, 2015).
28. Haney, C. Department of Defense Press Briefing by Adm. Haney in the Pentagon Briefing Room. (2015).
29. U.S. Joint Chiefs of Staff. *A Historical Study of Strategic Connectivity, 1950-1981*. (Joint Chiefs of Staff, Joint Secretariat, Historical Division, 1982).

30. Government Accountability Organization. *Nuclear Command, Control, and Communications: Update on DOD's Modernization*. (2015).
31. Gregory, S. *The Hidden Cost of Deterrence: Nuclear Weapons Accidents*. (Brassey's, 1990).
32. Sagan, S. D. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. (Princeton University Press, 1995).
33. Eric Schlosser. *Command and Control: Nuclear Weapons, the Demascus Accident, and the Illusion of Safety*. (Penguin, 2014).
34. Herrick, D. & Herr, T. Combating Complexity: Offensive Cyber Capabilities and Integrated Warfghting. in (2016).
35. Fischer, B. B. CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps. *Int. J. Intell. CounterIntelligence* **27,** 431–464 (2014).
36. Long, A. & Green, B. R. Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy. *J. Strateg. Stud.* **38,** 38–73 (2014).
37. Cimbala, S. J. *Nuclear Weapons in the Information Age*. (Continuum International Publishing, 2012).
38. Fritz, J. *Hacking Nuclear Command and Control*. (International Commission on Nuclear Non-proliferation and Disarmament, 2009).
39. Futter, A. Hacking the Bomb: Nuclear Weapons in the Cyber Age. in (2015).
40. Cimbala, S. J. Nuclear Deterrence and Cyber: The Quest for Concept. *Air Space Power J.* 87–107 (2014).
41. Baran, P. *On Distributed Communications Networks.* (RAND Corporation, 1962).
42. Clark, D. D. A Cloudy Crystal Ball: Visions of the Future. (1992).
43. Abbate, J. *Inventing the Internet*. (MIT Press, 1999).
44. Boulding, K. E. *Conflict and Defense: A General Theory*. (Harper & Row, 1962).
45. Trachtenberg, M. *History and Strategy*. (Princeton University Press, 1991).
46. Gavin, F. J. *Nuclear Statecraft: History and Strategy in America's Atomic Age*. (Cornell University Press, 2012).
47. Gartzke, E. & Kroenig, M. Nukes with Numbers: Empirical Research on the Consequences of Nuclear Weapons for International Conflict. *Annu. Rev. Polit. Sci.* **19,** 397–412 (2016).
48. Brodie, B., Dunn, F. S., Wolfers, A., Corbett, P. E. & Fox, W. T. R. *The absolute weapon: atomic power and world order*. (Harcourt, Brace and Co., 1946).
49. Wohlstetter, A. The Delicate Balance of Terror. *Foreign Aff.* **37,** 211–234 (1959).
50. Kahn, H. *On Thermonuclear War*. (Princeton University Press, 1960).
51. Snyder, G. H. *Deterrence and defense: toward a theory of national security*. (Princeton University Press, 1961).
52. Powell, R. Nuclear Brinkmanship with Two-Sided Incomplete Information. *Am. Polit. Sci. Rev.* **82,** 155–178 (1988).
53. Schelling, T. C. *The Strategy of Conflict*. (Harvard University Press, 1960).
54. Schelling, T. C. *Arms and Influence: With a New Preface and Afterword*. (Yale University Press, 2008).
55. Freedman, L. in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (ed. Paret, P.) 735–778 (Oxford, 1986).
56. Zagare, F. Rationality and Deterrence. *World Polit.* **42,** 238–260 (1990).
57. Slantchev, B. L. Feigning Weakness. *Int. Organ.* **64,** 357–388 (2010).
58. Blainey, G. *Causes of War, 3rd Ed.* (Simon and Schuster, 1988).
59. Fearon, J. D. Rationalist Explanations for War. *Int. Organ.* **49,** 379–414 (1995).
60. Powell, R. *In the Shadow of Power: States and Strategies in International Politics*. (Princeton University Press, 1999).
61. Reiter, D. Exploring the Bargaining Model of War. *Perspect. Polit.* **1,** 27–43 (2003).
62. Wagner, R. H. *War and the State: The Theory of International Politics*. (University of Michigan Press, 2010).
63. Gartzke, E. War Is in the Error Term. *Int. Organ.* **53,** 567–587 (1999).
64. Kaplow, J. M. & Gartzke, E. Knowing Unknowns: The Effect of Uncertainty in Interstate Conflict. in (2015).
65. Powell, R. *Nuclear Deterrence Theory: The Search for Credibility*. (Cambridge University Press, 1990).

66. Gartzke, E., Kaplow, J. M. & Mehta, R. N. Offense, defense and the structure of nuclear forces: The role of nuclear platform diversification in securing second strike. (2015).
67. Bodmer, S., Kilger, M., Carpenter, G. & Jones, J. *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. (McGraw-Hill, 2012).
68. Gartzke, E. War, Bargaining, and the Military Commitment Problem. in (2001).
69. Powell, R. War as a Commitment Problem. *Int. Organ.* **60,** 169–203 (2006).
70. Carson, A. & Yarhi-Milo, K. Covert Communication: The Intelligibility and Credibility of Signaling in Secret. *Secur. Stud.* (Forthcoming).
71. Ash Carter. Remarks by Secretary Carter at the Drell Lecture Cemex Auditorium, Stanford Graduate School of Business, Stanford, California. (2015).
72. Morgan, P. M. *Deterrence Now*. (Cambridge University Press, 2003).
73. Sagan, S. D. & Waltz, K. N. *The Spread of Nuclear Weapons: An Enduring Debate*. (W. W. Norton & Company, 2012).
74. Colby, E. Cyberwar and the Nuclear Option. *The National Interest* (2013).
75. *Strategy in the second nuclear age: power, ambition, and the ultimate weapon*. (Georgetown University Press, 2012).
76. Kristensen, H. M. & Norris, R. S. Status of World Nuclear Forces. *Federation of American Scientists* (2016). Available at: http://fas.org/issues/nuclear-weapons/status-world-nuclear-forces. (Accessed: 5th June 2016)
77. HP Security Research. *Profiling an enigma: The mystery of North Korea's cyber threat landscape*. (Hewlett-Packard Development Company, L.P.).
78. Rid, T. & Buchanan, B. Attributing Cyber Attacks. *J. Strateg. Stud.* **38,** 4–37 (2015).
79. Jervis, R. *Perception and Misperception in International Politics*. (Princeton University Press, 1976).
80. Tang, S. The Security Dilemma: A Conceptual Analysis. *Secur. Stud.* **18,** 587–623 (2009).
81. Buchanan, B. *The Cybersecurity Dilemma*. (Hurst, 2016).
82. Long, A. *Deterrence-From Cold War to Long War: Lessons from Six Decades of RAND Research*. (RAND Corporation, 2008).
83. Jervis, R. *The Illogic Of American Nuclear Strategy*. (Cornell University Press, 1984).
84. Van Evera, S. *Causes of war: power and the roots of conflict*. (Cornell University Press, 1999).
85. Peterson, S. Old weapons, new terror worries. *Christian Science Monitor* (2004).