NC3 AND CRISIS INSTABILITY–GROWING DANGERS IN THE 21ST CENTURY



Recommended Citation

Daryl K. Press, "NC3 AND CRISIS INSTABILITY–GROWING DANGERS IN THE 21ST CENTURY", NAPSNet Special Reports, October 17, 2019, https://nautilus.org/napsnet/napsnet-specia--reports/nc3-and-crisis-instability-growing-dangers-in-the-21st-century/

DARYL G. PRESS

OCTOBER 17 2019

I. INTRODUCTION

In this essay Daryl Press focuses on the growing threats to nuclear command and control and communication (NC3) systems around the world and the links between vulnerable NC3 and strategic instability due to the risky steps that nuclear weapons states may adopt to protect their arsenals during crises or wars.

Daryl Press is Associate Professor of Government at Dartmouth College, author of *Calculating Credibility: How Leaders Assess Military Threats* (2007) and co-founder of the annual Strategic Forces Analysis Bootcamp

A podcast with Daryl Press, Peter Hayes, and Philip Reiner on NC3 and crisis instability is found **here**.

Acknowledgments: This essay is based on collaborative work with Keir Lieber. The workshop at which the paper was presented was funded by the John D. and Catherine T. MacArthur Foundation.

This report is published simultaneously here by Nautilus Institute and here by Technology for Global Security and is published under a 4.0 International Creative Commons License the terms of which are found here.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

Banner image is by Lauren Hostetter of Heyhoss Design

II. NAPSNET SPECIAL REPORT BY DARYL G. PRESS

NC3 AND CRISIS INSTABILITY--GROWING DANGERS IN THE 21ST CENTURY

OCTOBER 17 2019

Summary

For decades nuclear deterrence analysts have recognized the dangers of strategic instability and its more virulent cousin crisis instability. Strategic instability exists when one or more countries perceive that their nuclear arsenal may be vulnerable to attack. Faced with that danger, the vulnerable country may feel compelled to protect its arsenal, but its efforts to do so could trigger an arms race or even accidental or unauthorized nuclear war. These dangers are most acute during crises. The topic of strategic / crisis instability attracted substantial analysis during the Cold War, but that attention faded when the superpower standoff ended.

The problems of strategic instability may be returning in a particularly dangerous form. This paper focuses on the growing threats to nuclear command and control and communication (NC3) systems around the world and the links between vulnerable NC3 and strategic instability. Although elements of the U.S. NC3 system require modernization, this paper focuses on a greater source of danger: the

growing vulnerability of other countries' NC3 systems, and the risky steps that those countries may adopt to protect their arsenals during crises or wars. I focus on three sources of danger to NC3 systems: (1) changes in technology that make it easier to locate and target nuclear forces – including NC3; (2) changes in conventional war, which put NC3 in the cross-hairs during conflicts; and (3) changes in several countries' nuclear employment plans – which require them to ask more of their own NC3, and hence increase their sensitivity to degradation of their NC3 capabilities.

In the pages that follow, I briefly describe the concept of strategic instability and its connection to NC3. Then I discuss each of the worrisome trends in turn.

The Link between NC3 and Crisis Instability

The term "strategic stability" refers to the situation in which two countries in a deterrent relationship are both confident that (a) they can absorb a nuclear disarming strike and subsequently execute essential nuclear operations; and (b) their nuclear adversaries recognize this fact.[1] Strategic *instability* occurs when one or both countries fear that their nuclear arsenals are vulnerable to destruction. Deterrence analysts worry that countries whose forces are at risk may adopt a range of policies to mitigate their vulnerability, which have the side effect of increasing nuclear dangers.

For example, countries with vulnerable arsenals may: engage in arms buildups, which could trigger multilateral arms races; adopt elevated alert levels, which could raise the risks of accidental nuclear war;[2] and disperse nuclear forces and decentralize launch authority, which could raise the danger of unauthorized nuclear use.[3] In the midst of a military crisis or a conventional war, a heightened version of strategic instability ("crisis instability") could occur, in which a nuclear armed state took measures to rapidly reduce its vulnerability (e.g., force dispersal, or activation of wartime emergency communication systems), inadvertently sending its adversaries indications of imminent nuclear escalation. Those steps, though adopted to enhance deterrence, may have the opposite effect: triggering preemptive strikes.

There is an inherent link between strategic stability concerns and NC3. Because some level of NC3 functionality is required for any nuclear operation, political, military, and technological changes that threaten NC3 systems undermine strategic stability.

It is essential to note that an attack on NC3 does not need to completely paralyze the victim's nuclear forces to be highly effective. Strikes that merely delay critical NC3 functions – e.g., reduce warning, delay decision making, or hinder communication to deployed forces – may be an essential component of a disarming strike (i.e., using some weapons to delay NC3 functions, buying time for other weapons destroy delivery systems). As a result, attacks that merely degrade NC3 functions may appear to be precursors of a disarming strike, and hence trigger destabilizing responses by the victim.

In short, developments that threaten NC3 systems undermine strategic stability. The remainder of this paper explores three trends that do exactly that.

Growing Threats to NC3

Three trends are exacerbating the vulnerability of NC3 systems around the world and increasing the risks of crisis instability. First, technology is evolving in directions that make NC3 more vulnerable than before – i.e., easier to locate and easier to attack. Second, changes in the U.S. style of conventional war increases the likelihood that the United States will attack adversary NC3 during a conventional conflict even if Washington seeks to prevent escalation. Third, several nuclear-armed

states appear to have adopted nuclear doctrines that demand more of their NC3, reducing the threshold of damage that their NC3 can suffer before they are pushed to escalate. Each of these trends is discussed below.

Technological Change, and the Growing Threats to NC3

Over the past few decades, a series of technological changes has reduced the survivability of nuclear arsenals around the world – and especially NC3 systems. Leaps in the accuracy of delivery systems have largely negated one of the principal strategies that states employ to protect their nuclear forces from destruction: hardening. The revolution in remote sensing is eroding the other foundation of survivability: concealment / mobility. The consequences of pinpoint accuracy and new sensing technologies are numerous and synergistic. Taken together, they create major challenges for force planners tasked with keeping their arsenals secure and new opportunities for those devising novel counterforce strategies.[4]

The implications of pinpoint accuracy are broader than initially appears. The direct consequence of improved accuracy is straightforward: targets, if located, can be destroyed with much higher probability than in the past. But the accuracy revolution has deeper implications for nuclear force vulnerability. For example, the creation of highly-accurate delivery systems has multiplied the size of the counterforce arsenals available to the major nuclear powers. Submarine-launched ballistic missiles, which were once too inaccurate to target hardened sites, became lethal counterforce weapons at the end of the Cold War, greatly expanding the inventory of weapons that could be used in disarming strikes.[5] In the past few years, new leaps in ballistic missile accuracy – stemming from upgrades to the fuses on ballistic missiles – have again multiplied the number of available counterforce weapons.[6] Perhaps the most consequential effect of the accuracy revolution is still emerging: the widespread deployment of very accurate, long-range conventional weapons with the capability of destroying hardened targets. The deployment of those weapons in large numbers, which appears inevitable, will greatly increase the vulnerability of nuclear delivery systems and NC3 sites in fixed, hardened locations.[7]

While advances in accuracy are negating the value of hardening, leaps in remote sensing are eroding the other main approach to protecting one's nuclear deterrent: concealment. At least six trends are eroding the security that mobility once provided. (1) Sensor platforms have become more diverse – e.g., Cold War mainstays like satellites and aircraft are now supplemented by remotely piloted vehicles (RPVs) in the air and at sea; land- and sea-based autonomous sensors; and cyber platforms for sensing. (2) Sensors are collecting a wider array of signals from across the electromagnetic spectrum and employing new analytic techniques (e.g., high resolution spectroscopy, interferometry, and inverse SAR). (3) Remote sensing platforms are providing persistent observation – the snapshots provided by satellites in low earth orbits are now supplemented by the streams of data gathered by loitering RPVs and unattended ground sensors. (4) Sensor resolution is increasing, and (5) data communication and processing is accelerating. (6) Artificial intelligence is helping sift through streams of data and assist with target identification. To be clear finding concealed forces, particularly mobile ones, remains a major challenge. But in the competition between "hiders" and "seekers," waged by ballistic missile submarines, road-mobile missiles, mobile NC3 assets, and the forces that seek to track them, the hider's job is growing more difficult.[8]

The consequences of these technological innovations for NC3 vulnerability have not been adequately highlighted in the unclassified deterrence literature.[9] For at least two important reasons, NC3 may be more vulnerable than delivery systems. First, the number of NC3 targets is far smaller than the number of delivery systems. Even the United States, with a dispersed and redundant NC3 architecture, likely has only a few dozen critical NC3 nodes – compared with the hundreds of targets

that are directly associated with delivery systems.[10] Second, although the mobile NC3 systems of the most sophisticated nuclear powers can be very secure, most nuclear-armed states have fewer resources to spend on those systems.[11] The history of the Cold War demonstrates that even a superpower (i.e., the Soviet Union) can have difficulty preserving the survivability of its mobile nuclear delivery systems (i.e., its submarines).[12] The small, mobile NC3 assets of poorer nuclear states may be even more vulnerable.

Trends in technology are making every nuclear-armed country's NC3 system more vulnerable, but not equally so. Those countries with vast resources, large defense budgets, access to cutting edge technology, and substantial experience operating nuclear forces will have an easier time keeping their arsenals secure. Those with few resources, smaller arsenals, bare-bones NC3, and minimal experience face a more difficult challenge – especially if their arsenals are being hunted by the leading military powers. During a crisis the threats to nuclear forces, and especially to NC3, may trigger significant crisis instability.

U.S. Conventional Operations and Adversary NC3 Vulnerability

The second trend that is enhancing threats to NC3, and which may cause crisis instability, is rooted in the evolving nature of conventional war – especially as practiced by leading conventional military powers such as the United States. Over the past twenty-five years, the United States has developed a style of conventional war that seeks to dismantle enemy military power by destroying or degrading adversary command and control. Almost every major U.S. military operation since 1991 has begun with an intense air- and missile-campaign designed to deny adversary situational awareness and impede adversary operations. Those strikes have focused on air defense radars, military communications, and leadership. This approach to war has been highly effective, contributing substantially to the one-sided battlefield victories enjoyed by the United States and its allies. But if conducted against a nuclear-armed adversary, this style of operations poses major threats to NC3.

The modern style of conventional war threatens NC3 for at least three reasons. First, many nuclear-armed countries – including potential U.S. adversaries – entangle their conventional and nuclear command and control systems. Ordinary conventional strikes, intended merely to degrade an adversary's conventional military capabilities, may seriously degrade its NC3 capabilities.[13] Second, even if NC3 and conventional command and control are separate, intelligence may misidentify the purpose of some facilities; furthermore, attacks on conventional command and control networks may have unintended downstream effects on NC3. Finally, attacks on senior military and political leadership are a common element of U.S. conventional operations, and senior personnel may have critical roles in nuclear decision making. Striking leadership targets – a major element of U.S. conventional war plans – may be *de facto* nuclear decapitation operations, whether intended or not.

During the Cold War, the United States and its allies understandably worried about how NATO's command and control and intelligence systems would function during an intense, fast-moving war in Europe. Today, a war on the Korean Peninsula, or around the Baltic states, or in the Western Pacific would likely be less intense than the feared massive battle between Warsaw Pact and NATO forces. But the command and control capabilities of U.S. adversaries are, in many cases, not robust. As adversary air defense radars are destroyed; as their communications are jammed; as military leadership bunkers are destroyed; and as leaders lose confidence that they know what is occurring in / over / around their territory, it is likely their confidence in their own control over their nuclear arsenal will waver.

Increased Adversary Reliance on Nuclear Weapons

A third, critical link between NC3 vulnerability and crisis instability stems from the missions that several nuclear armed states now ask of their nuclear forces. Several nuclear-armed countries (e.g., Pakistan, North Korea, Russia) rely upon nuclear weapons to deter or thwart their adversaries' superior conventional forces. The problem is that this mission – controlled, coercive wartime escalation – places great demands on NC3. As a result, even modest degradation of one of those country's NC3 during a conventional war may jeopardize its ability to execute its critical functions, triggering the dangerous behaviors (e.g., alerts, dispersals, predelegation, employment) that scholars of crisis instability fear.

If a country's only mission for its nuclear weapons was to deter nuclear attacks by threatening punitive retaliation, its NC3 requirements would be relatively limited. An NC3 system would merely need to retain sufficient bandwidth to communicate orders for a simple retaliatory spasm against a set of pre-selected targets. In reality, even that mission is not simple. For example, developing command arrangements that are both immune from unauthorized use and secure from decapitation attacks is a perennial dilemma. And a retaliatory strike from a small, heavily attrited nuclear arsenal might need to be coordinated to penetrate alerted air and missile defenses. But those challenges are modest compared to the NC3 challenges that a country faces if it has a more ambitious set of purposes for its nuclear arsenal.

If a country wishes to employ nuclear weapons during a conventional conflict to coerce an end to conventional operations (i.e., NATO's strategy during much of the Cold War), its NC3 must retain substantial capability even as it absorbs conventional strikes, and even after the nuclear threshold has been crossed. For Pakistan, North Korea, or Russia to employ nuclear weapons during a war as they claim they would, their command and control would need to (a) retain situational awareness of the battlefield even after days or weeks of conventional operations (to determine whether conventional "red lines" that warrant escalation have been crossed, and to identify the location of potential nuclear targets); (b) monitor its own nuclear forces, to know which have been destroyed through conventional operations; (c) devise plans for the limited employment of its remaining nuclear weapons and communicate them to surviving delivery systems; (d) evaluate the effectiveness of any ordered nuclear operation; and (e) retain the ability to negotiate after a limited nuclear exchange. In the Cold War context, NATO analysts understandably worried whether this level of NC3 was feasible during an intense conventional war. These are now the demands that Pakistan, North Korea, and Russia are placing on their own NC3.

The problem for the United States, its allies, and India is that even mild degradation of these countries' NC3 – e.g, through the "normal" style of conventional operations described in the previous section – may undermine the ability of their adversaries' nuclear forces to carry out their vital functions. That is precisely the condition, according to strategic stability theory, in which countries may feel compelled to take dangerous, escalatory steps. To say this differently, the strategic stability literature focuses on the danger that results when nuclear-armed states doubt their ability to retaliate, and hence take risky steps to ensure their retaliatory capabilities. But for countries whose nuclear missions are broader than simply "retaliation," the threshold for taking those risky protective steps may be much lower.

Conclusions

Concerns about strategic stability are not new. But attention to these issues declined at the end of the Cold War just as the problem grew worse. For all the dangers of the Cold War standoff, both superpowers recognized that a major conventional war in Europe would raise very high risks of nuclear escalation – a recognition that helped prevent that conflict from occurring.

Today many foreign policy analysts recognize that there is *some* risk that a war between nuclear

armed powers might escalate, but those dangers are often binned with other "low likelihood / terrible outcome" concerns. In fact, the growing threats to the NC3 of weaker nuclear powers, and the nature of modern conventional war, may be making the dangers of escalation far greater than is commonly recognized. In the conflict with the highest escalation risks – on the Korean Peninsula – it would be surprising if a major conventional war did *not* go nuclear. Escalatory risks in a Baltic conflict are less serious – but still very worrisome – and those in a U.S.-China war in the Western Pacific are still worthy of serious study.[14]

III. ENDNOTES

[1] For an excellent guide to the literature on these concepts, see Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations*, Strategic Studies Institute, U.S. Army War College, 2013. In his essay for that volume, Colby defines strategic stability with reference to a country's ability to absorb a nuclear strike and subsequently *retaliate*. I broaden that concept slightly because even if a country can retaliate in some fashion after absorbing an attack, if it fears it cannot execute essential nuclear operations after an attack it may feel vulnerable and take dangerous steps to reduce its vulnerability. Colby, "Defining Strategic Stability: Reconciling Stability and Deterrence," pp. 47-84.

[2] If an increased alert level permits a country to respond quickly to signs of an incoming nuclear attack, it may also increase the risk that erroneous indications of attack may trigger accidental nuclear war.

[3] For a dispersal to reduce a country's vulnerability to a disarming strike, the capability to launch must be decentralized beyond the senior political / military leaders. Otherwise, the dispersed force would be vulnerable to a disarming counter-leadership attack. But dispersing the capability to launch increases the possibility of unauthorized nuclear employment.

[4] Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* Vol. 41, No. 4 (Spring 2017).

[5] The deployment of the Trident II missile beginning in the 1990s made, for the first time, the thousands of warheads deployed on U.S. SSBNs potent counterforce systems – greatly expanding the number of U.S. counterforce-capable warheads. See discussion and implications in Lieber and Press, "The New Era of Counterforce," pp. 6-14.

[6] The recent deployment of burst-height compensated fuses on U.S. SLBMs has multiplied the size of the U.S. counterforce arsenal again, by providing sufficient accuracy to make the smaller-yield and more numerous W76 warhead a very effective option against hardened targets. See Theodore Postol, "Monte Carlo Simulations of Burst-Height Fuse Kill Probabilities," unpublished presentation, July 28, 2015; Hans M. Kristensen, Matthew McKinzie, Theodore Postol, "How U.S. nuclear force modernization is undermining strategic stability: The burst-height compensating super-fuze," *Bulleting of Atomic Scientists*, March 1, 2017.

[7] The implications of the accuracy revolution for nuclear targeting go beyond what is summarized in this paragraph. For example, accuracy improvements have largely negated the problem of nuclear fratricide, which was a principal impediment to counterforce strikes during the Cold War. Improvements in accuracy have also opened the door to low-fallout nuclear targeting by employing air bursts against hardened targets. For a more detailed discussion, see Lieber and Press, "The New Era of Counterforce," pp. 9, 18-32.

[8] Lieber and Press, "The New Era of Counterforce," pp. 17-18

[9] For example, in previous work a co-author and I modeled the effects of the revolutions in accuracy and sensing against Russian target sets comprised of nuclear delivery systems, not NC3 targets. See Keir A. Lieber and Daryl G. Press, "The End of MAD? The Nuclear Dimension of U.S. Primacy," *International Security* Vol. 30, No. 4 (Spring 2006); and Lieber and Press, "The New Era of Counterforce." Real war plans likely focus heavily on NC3 – to delay an adversary's characterization of an incoming attack, disrupt his decision making, and slow his communication and execution of responses (while additional weapons arrive to destroy delivery systems). By focusing solely on the effects of attacks on delivery systems, which is the standard in the field, our models built an additional level of conservatism into our analysis – but did so at the cost of distracting attention from the potentially greater vulnerability of NC3.

[10] A disarming strike focused on U.S. nuclear delivery systems would need to strike approximately 500 targets: roughly 450 individual silos, a few dozen missile launch control centers, at least three airfields, two SSBN bases, and several warhead storage sites. For a description of contemporary U.S. nuclear force structure, see Hans M. Kristensen, "United States nuclear forces, 2018," *Bulletin of the Atomic Scientists*, Vol. 74, No. 2 (Spring 2018).

[11] Some U.S. analysts worry that the NC3 mission is not a high enough priority within the U.S. nuclear community – bombers, missiles, and submarine get more support from the military and its political backers than the NC3 architecture that knits those weapon systems together. The same dynamics likely occur in smaller, poorer nuclear armed states, especially because the resource tradeoffs are sharper.

[12] Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy", *Journal of Strategic Studies* Vol. 38, Nos 1-2 (December 2014): pp. 38-73.

[13] On the threat that high-intensity conventional operations pose to nuclear systems, see Keir A. Lieber and Daryl G. Press, "The Nukes We Need: Preserving the American Deterrent," *Foreign Affairs* (November / December 2009); and Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* Vol. 41, No. 4 (Spring 2017).

[14] On the highly escalatory nature of war on the Korean Peninsula, see Keir A. Lieber and Daryl G. Press, "The Next Korean War," *Foreign Affairs*, April 1, 2013; and Lieber and Press, "Coercive Nuclear Campaigns in the 21st Century: Understanding Adversary Incentives and Options for Nuclear Escalation," Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction, Naval Postgraduate School, March 2013. For analyses of the escalatory risks of a maritime war in the Pacific, see Joshua Rovner, "AirSea Battle and Escalation Risks," SITC-NWC 2012 Policy Briefs, 2012 (policy brief 12); and Caitlin Talmadge, "Why a U.S.-Chinese War Could Spiral Out of Control," *Foreign Affairs* (November / December 2018).

IV. NAUTILUS INVITES YOUR RESPONSE

The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/nc3-and-crisis-instability-growing-dangers-in-the-21st-century/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org