COMMUNICATION DISRUPTION ATTACKS ON NC3

Recommended Citation

Paul Bracken, "COMMUNICATION DISRUPTION ATTACKS ON NC3", NAPSNet Special Reports, May 28, 2020, https://nautilus.org/napsnet/napsnet-special-reports/communication-disrupt-on-attacks-on-nc3/

PAUL BRACKEN

MAY 28, 2020

I. INTRODUCTION

In this essay, Paul Bracken argues "*in a nuclear world we should be careful about attacking enemy communications* because doing so leads to greater risks of uncontrolled escalation. The worst possible situation is the one the United States is now in, that is, to not be clear in our own minds about what we are doing when it comes to disrupting communications."

Paul Bracken is professor of management and political science at Yale University.

The paper was prepared for the Antidotes For Emerging NC3 Technical Vulnerabilities, A Scenarios-Based Workshop held October 21–22, 2019 and convened by The Nautilus Institute for Security and Sustainability, Technology for Global Security, The Stanley Center for Peace and Security, and hosted by The Center for International Security and Cooperation (CISAC)—Stanford University.

A podcast with Paul Bracken, Philip Reiner and Peter Hayes is found **here**

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

Acknowledgments: The workshop was funded by the John D. and Catherine T. MacArthur Foundation. Maureen Jerrett provided copy editing services.

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 PAUL BRACKEN

COMMUNICATION DISRUPTION ATTACKS ON NC3

MAY 28, 2020

This paper analyzes the importance of *communications* for nuclear deterrence, crises, and wars. It recommends that the United States ought to distinguish between attacks *designed* to maximize disruption of communications and attacks which happen to disrupt communications as a collateral side effect. The idea behind this argument is that in a nuclear world we should evaluate disruption to enemy communications similar to the way we analyze collateral damage to civilians. Namely, that high levels of civilian casualties may be acceptable only when there are other important objectives, as recognized in the Laws of Armed Conflict*. But broadly speaking, in a nuclear world we should be careful about attacking enemy communications* because doing so leads to greater risks of uncontrolled escalation. The worst possible situation is the one the United States is now in, that is, to not be clear in our own minds about what we are doing when it comes to disrupting communications.

Some military attacks are intended to disrupt the enemy's communications. Other kinds of attack are aimed at weapons, but they spill over into disrupting communications. Why is it important to

distinguish between these two kinds of attack? The answer is straightforward. It's that communications is one of the three building blocks of a deterrent strategy. These are capability, communications, and credibility, the three C's of deterrence. Two of these, capability and credibility, receive a large amount of attention and resources. Today, virtually all nuclear weapon states are putting resources into increasing nuclear *capability*. This includes the United States, China, Russia, and India. It also includes Pakistan, North Korea, and Israel. They are either building more weapons or are developing new ones.

There is also a consideration of nuclear *credibility*, which has been much debated in academic and think tank circles. Tailored deterrence, conventional counterforce, low yield "mini-nukes," and cyber have been offered to make deterrence more credible. Each one of these, it has been argued, creates more options and, therefore, moves strategy away from big nuclear salvoes. The suggested options are controversial for this reason. I do not wish to enter this debate, but the options underscore my point that credibility receives considerable attention in force planning and strategy.

Communications is an outlier in this respect. It is both a darling and a stepchild of deterrence. It is a darling because there's wide agreement that a country needs to communicate red lines that might trigger nuclear use. Yet it is a stepchild because most analyses overlook what is clear to the military—the biggest military vulnerability is often communications. This condition is found in conventional and nuclear postures. This vulnerability makes it a prime target, but one which at a strategic level no-one admits to. I believe that no one admits to it is because of thoughtlessness in the sense that conventional and nuclear operations are seen to be different categories of operations. Academics and think tank studies as well as the military that deal with these weapons also compartmentalize NC3 from force vulnerability considerations. It comes from history as it defined the fundamental dividing line of the Cold War.

There are additional reasons for not focusing on attack of communications. It is thought to undermine deterrence by signaling restraint of targets that would not be struck. This is seen as conveying weakness. And more, seriously analyzing the consequences of communications attacks would necessarily take us into thinking about the unthinkable, that is to say, nuclear war. No one in the U.S. wishes to do that.

I could go on about why this is not examined more seriously, but the key point is that we are in a situation where the military fully expects to attack enemy communications and develops plans accordingly. Yet these plans do not account for the consequences of escalation that follow from this approach.

Some Examples

There are many examples that illustrate *direct* attacks on communication, and of what I am calling *collateral* communication damage attacks. Some cases are planned, and some are hypothetical. In the Cold War, for example, attacks on U.S. communications were an example of what was an expected attack. There was serious worry in the Air Force about a nuclear attack against Washington, DC, the "Ma Bell" telephone network,[1] the electric power grid, and command and control centers. Nuclear electromagnetic pulse (EMP) attack, anti-satellite weapons (ASAT), and electronic warfare, as well as nuclear strikes were in these plans.

The idea of attacking communications, along with missiles, bombers, and nuclear submarines in port was to make the U.S. strike back with a damaged force that would be less than the full weight of an undamaged force. Such an attack on U.S. communications would have led to a ragged U.S. response that was less devastating than one with an undamaged force. Many war games and Strategic Air Command studies began with an opening Soviet nuclear salvo against Washington and with high

altitude EMP bursts over Nebraska to knock out the U.S. power and telephone networks.

In the 1980s it became clear that the U.S. communications system—not the weapons themselves—was the weak link in the nuclear posture.[2] Buying more weapons served little purpose for bolstering deterrence if communications vulnerabilities could paralyze the retaliatory blow. A great deal of money was spent to "harden" the U.S. system and clarify procedural responses in a chaotic environment. These procedural responses were especially important because they more clearly defined authority over nuclear retaliation. They included predelegation of launch authority, line of succession in the command system, and, importantly, the timing and procedures for determining who was alive and capable of taking charge of the military in cataclysmic circumstances.

Let's consider the other end of the spectrum. Some attacks led to disruption as a collateral, unanticipated, or unknown consequence of an attack aimed at military or other targets. On 9/11 the attack on the World Trade Center and the Pentagon illustrated how the U.S. communication system broke down. These attacks were intended to destroy visible symbols of American power—the World Trade Center and the Pentagon. They were not designed to disrupt U.S. communications. Yet they had this effect. It is worth reiterating: relative to nuclear war, a very small, non-nuclear attack on the United States caused a significant breakdown in communications that delayed timely action, distorted the military's understanding of what was taking place and endangered national leaders.

Some examples show this in detail.[3] One of the most serious was the initial Air Threat Conference Call initiated by the National Military Command Center (NMCC) in the Pentagon after the attack on the World Trade Center Towers, but before the attack on the Pentagon. NORAD (the North American Aerospace Defense Command in Colorado Springs) asked three times for inclusion of an FAA representative (Federal Aviation Administration) in the conference call with the NMCC. NORAD's first request for this was at 10:03 am Colorado time on 9/11. It was only at 10:17 am that an FAA representative did join the call. But this individual knew nothing about emergency response procedures, either of the FAA or the NMCC. He also had no access or communications to other FAA officials who might have such knowledge.[4]

In the context of the crisis on 9/11 these fourteen minutes had little bearing on the outcome of that dreadful day. But fourteen minutes, or longer if we recognize that the individual joining the call on behalf of the FAA had virtually no useful knowledge or authority, is a long time. In a nuclear world of hypersonic and ballistic missiles it is an enormously long time, long enough to destroy an enemy force on the ground.

A second communications breakdown during 9/11 was the continuity of a government plan for protecting U.S. leadership and ensuring that it had communication links to the military. This plan utterly failed to be implemented because the officials involved either didn't know what it was or declined to follow their assignments in the chaos of the situation. In yet another example that truth is stranger than fiction, the protection plan for senior leaders on 9/11 collided with an unrelated, long planned nuclear war game exercise. This game called for uploading live warheads onto B-52 bombers at Barksdale Air Force Base, Louisiana, among others.

This was the base chosen to refuel Air Force One, however, after its emergency evacuation of the president from Florida. As a response to 9/11 the Pentagon wanted to raise the U.S. alert level. But to do this they needed to secure the live bombs used in the exercise, and this created a lot of problems. One obvious difficulty was that this would require presidential approval at a time when the president was airborne, not in communication with the Pentagon, and set to land on an airfield full of dispersed hydrogen bombs. It is worth thinking about this for a moment because it shows a set of coincidences that were incredibly unlikely—and yet they happened. A review of Cold War

nuclear-related accidents shows the same thing, the tendency for the real world to come up with scenarios that were far more creative and dangerous than any planner could think up in peacetime. If the scenario that did occur on 9/11 was offered as a Hollywood script it would be rejected out of hand as implausible. Yet it happened.

I do not know whether Russian intelligence picked up the coincidental and unrelated activities of the nuclear war game. But this seems likely knowing how these things work. The Russians have long used spotters at major U.S. bases to look for changes in operating levels. They would not know, of course, that events at Barksdale on that day were driven by two parallel developments, the war game and the 9/11 attack. Astoundingly, we now know that Putin sought reassurance about the increased alert level, but the White House could not reach the U.S. President to respond.[5]

In sum, the President was not in touch with U.S. forces because he couldn't communicate with them. More fundamentally however, no one could have anticipated the contingency that developed, one with the military out of position on many fronts and what turned out to be a "small" attack by the standards of nuclear war. Everyone was in the dark, reaching out for information that wasn't coming in because the bureaucracies involved weren't designed for this kind of contingency.

Discussion of the Examples

The lesson I take from these examples is that no complex system can perform well under conditions it doesn't anticipate happening. It's all well and good to talk about flexibility and agility. But there are serious limits to what can be accomplished with these. It takes repeatable experience, learning, and practice to achieve high levels of performance under conditions of real-world stress. No one can possibly anticipate all the developments that one discovers in actual operations. Think of the U.S. Army in World War II. In the assault on North Africa it saw one setback after another. It greatly improved its performance during the invasion of Italy. And in France it was one of the most impressive fighting organizations in history. There was a tremendous amount of learning that went on over a two-year span, and it came from real world operations.

The lesson I take from these examples is that software improvements, stress testing, fault trees, blockchain, system hardening, etc., are less important for performance than drill, experience, and learning from realistic practice of operations. I think 9/11 showed this clearly. A small, unanticipated attack paralyzed elements of the command system. The attack wasn't even intended to do this, yet it did.

The heart of the problem is that there is nothing like actual experience to work out the bugs in a system. And with nuclear forces you can't really get experience of what a war would be like in peacetime. So what are the options?

The answers, I would suggest, are either to "change worlds," or to do the best we can in the world we are given. By "changing worlds" I refer to things like nuclear abolition and global zero, that is, to eliminate nuclear weapons altogether. Or drive them into the deep background so that they are irrelevant except in certain unimaginable circumstances, like an all-out Russian surprise nuclear attack on the United States.

The other alternative is to do the best we can in the world we are in. Here, there are grounds for optimism. That is, we can do better. And one way to do better is to make the distinction in plans on whether enemy communications is a high priority target, or whether it may merely receive collateral damage from attacks on other targets.

Are We on a New Learning Curve?

A question that really needs to be asked follows from this discussion. It's a different question than the one usually posed about command and control. The standard question is "How can we field a modern, reliable, effective nuclear command and control system?" The range of answers to this question involve various kinds of redundancy, double checking (for example, via blockchain type systems), better software, etc.

But I think there's a different question that also needs to be considered. As nuclear weapons spread, and as advanced technologies (cyber, AI, drones, hypersonics) spill into the nuclear competition, are we about to climb a new learning curve in a new nuclear environment? What I am really questioning is what the learning curve of a second nuclear age will look like.

In the Cold War a learning curve developed, one with different technologies and political background. In the 1950s the United States and the Soviet Union began to climb a 20-year learning curve of nuclear interactions. This learning curve was punctuated by several crises: Taiwan, Berlin, Cuba, Lebanon, U-2s over Russia. These crises exposed big gaps, similar to the ones discovered on 9/11. In the 1962 Cuban crisis, for example, it was extremely difficult to communicate with Moscow in a timely way. And it was impossible to reach allies in Latin America because the telephone system simply couldn't handle it.

Yet over a twenty-year period the two sides developed a complicated "system dynamics" of interactions.[6] I've long thought that this nuclear learning was one of the greatest arms control successes in history.

Today there are multiple possibilities for nuclear threats, not just one. I think we need to consider the interactions of countries even if the United States is not directly involved. India and Pakistan come to mind. And the technologies are very different now as well. Cyber, drones, ASAT, etc., change the nature of the interactions in ways that are as yet poorly understood. One of the conclusions of the January 2019 NC3 conference was that there's an increasing overlap between the command and control for conventional forces with that of the nuclear forces.[7] This arises, for example, from growing dependence on sensor data, satellites, cyber, and AI in the military enterprise.[8]

The learning curve question, then, may be stated as follows. *Are we on a new learning curve for nuclear interactions, and might this trajectory offer opportunities to gain experience about communications during peacetime and crises?* Shifting from obsolete, simple generalizations about NC3 from the Cold War to what Nye termed "complex integrated understandings grounded in realistic attention to detail"[9] in modern conditions is analogous to the learning process that evolved in the 1950s and 1960s.

This question requires a deliberative response. Jumping to an answer is the wrong way to approach it. So, what does an answer to the question look like? Let's put together a list of possible answers. I will do this in a reverse order of antagonism. That is, the options listed at the top of the list pertain to situations that have a low order of conflict, risk, and strain, whereas those below have a high order.

1. We must not view the question of a new learning curve as posed here as the important one. Rather, we should do everything possible to climb an altogether different learning curve to move us toward disarmament, arms reduction, and making nuclear weapons irrelevant in international affairs. At least we should confine nuclear weapons to highly unlikely and largely unimaginable contingencies. This preclusion would include an all-out Russian or Chinese surprise attack on U.S. cities, intercontinental ballistic missiles, and bombers.

2. As long as the U.S. possesses the capacity to strike back with a large counter blow after absorbing a worst-case attack, there really is no learning curve. Another way of putting this is to say that the new (and old) learning curve is a step function. You either have a second-strike capability or you don't. If you do, that's all you need and no further assessment or systems are needed.
3. Double down on drills and practice under the new conditions of cyber attack on nuclear forces, missile threats from second tier countries like North Korea and Iran, and their attacks on supporting systems like communications, space assets, and electric power. I would argue that the U.S. has moved in this direction in the last four years. This response recognizes there are new conditions in a second nuclear age, that the environment has changed, and the military plans and exercises must take account of the change. The new conditions are technological and political. So far, most U.S. action in this regard has been to deal with the technological changes, not the political ones. That is, there is more recognition of cyber threats to U.S. nuclear forces, ASAT, etc. However, there is not much realistic political play in this space. The political action is "wooden" and highly scripted. A scenario of the president being out of touch with the forces, live weapons dispersed around airfields, and confusion—what happened on 9/11—couldn't be examined in today's planning studies because it would be too controversial.
4. A nuclear context will shape future crises between the U.S. and other countries. By this I mean not just the recognition that nuclear weapons exist, but that nuclear weapons will come to the foreground as a crisis develops between nuclear armed states. In peacetime this nuclear context is dismissed. Because of the vast destruction inherent in these weapons the middle and upper rungs of the escalation ladder are effectively blocked off as political options. Thus, the focus will shift to lower rungs of escalation. This includes moving nuclear weapons around, going on alert, preparing forces to fire— but not actually firing. The purpose of these moves is what I have called "nuclear head games." It's political signaling but with a broader unspecific message, "This crisis could get out of control because neither one of us understands our forces. For this reason, you'd better be reasonable and back down."

Again, let me emphasize that I am not advocating any one of the above possible responses. Different actors in the debate will advocate different options. But it does appear there are obvious and immediate consequences that can be drawn from my list. If the purpose of improved, efficient, modernized command and control is to ensure the U.S can deliver a retaliatory blow then the challenge is greatly simplified. We can do this with high probability of success.

Yet "getting off the retaliatory blow" may not match the real-world imperatives we face. The last two responses come closer to this world. And if we prepare for a world where *only* getting off the retaliatory blow is what matters, then we may invite nuclear threats at lower levels of crises and provocations.

A Policy Recommendation

My opening recommendation follows from this discussion. The United States—indeed, all nuclear-armed states--should distinguish between attacks whose intent is to destroy enemy communications outright and those which do so incidentally to attacks *undertaken for other purposes*.

The reason for the recommendation is because current trends in technology and plans are mixing up conventional and nuclear forces. They both use the same systems. For example, missile warning systems are used in both. In addition, communications is so clearly the weak link in the three C's framework of deterrence (capability, communications, credibility) that it stands out as a prime target.

Someone might say that there is always going to be damage to enemy communications in war, and that this cannot be precluded, and, therefore, my recommendation is impractical. But such thinking is exactly why we need the distinction. My concern, really, is that we're using advanced technology (cyber, hypersonic missiles, etc.) to disrupt enemy communications without thinking it through. Moreover, it is not clear to me that civilian leaders understand that this nuclear and conventional targeting of nuclear communications is taking place. They might, for example, approve "conventional" attacks, which are not really conventional in their consequences.

I am not proposing a "no attack" policy on enemy communications. Fifty years ago, arguments were made that there is always going to be large-scale collateral damage to civilians in war. No one in the U.S. says this any longer in light of changing sensitivities to unnecessary civilian damage. This doesn't mean that civilians are no longer killed. But rather that collateral damage levels are now a category in plans and in the planning process. There is always an annex in a plan or a briefing to senior leadership about expected collateral damage levels.

In the multipolar nuclear world that is now emerging it is unacceptable and dangerous to leave collateral damage to communications to muddled treatment. The potential for escalation arising from conventional attacks which employ advanced technologies like cyber, stealth, anti-satellite attacks, and AI induced deception are considerable. But, in addition there are nuclear weapons. The conventional-nuclear divide that defined the escalation universe of the Cold War, at least conceptually, is now considerably more complicated. We do not understand this divide. It is not a good strategy to discover the contours of this divide in a real crisis or war. For this reason, the bias should be on attacking enemy communications only after a much more sober assessment of its consequences. This paper argues that a good way to begin this assessment is to make key distinctions in how we frame the analysis. Simply making the distinction between direct purposive attack on enemy communications, and indirect collateral attack as a result of other operations is an example of a key distinction.[10] Moreover, more realistic war games and models need to factor in communications. These distinctions, models, and games are a good start to addressing some of the big challenges of the world we are entering.

III. ENDNOTES

[1] The "Ma Bell" network refers to the national AT&T telephone system before it was broken up for anti-trust reasons in the early 1980s. This network was critical to delivering the firing order from civilian leadership to the nuclear forces.

[2] Here, the work of Desmond Ball, John Steinbruner, Bruce Blair, and the author can be mentioned.

[3] The author would like to thank Peter Hayes for bringing these examples to my attention, in the form of a reading package of communications breakdowns during the 9/11 attacks.

[4] This description draws on *9/11 Commission Report*, Staff Statement No. 17.

[5] According to William Arkin and Robert Windrem: "Because of inadequate communications equipment and procedures, top U.S. officials couldn't talk to each other or to anyone else." Russian President Vladimir Putin wanted to speak to Bush to know why the U.S. was preparing to go to DEFCON 3—but the White House couldn't put him through to Air Force One. Bush had no way to receive phone calls." In "Secrets of 9/11: New Details of Chaos, Nukes Emerge," September 11, 2016, at:

https://www.nbcnews.com/storyline/9-11-anniversary/secrets-9-11-new-details-chaos-nuk-

s-emerge-n645711

[6] Joseph Nye delineates this learning in his “Nuclear Learning and U.S.-Soviet Security Regimes,” *International Organizations* 41:3 Summer 1987, pp. 371–402. My own work on *The Second Nuclear Age* is written on this theme as well.

[7] See https://nautilus.org/napsnet/napsnet-special-reports/synthesis-report-nc3-systes-and-strategic-stability-a-global-overview/

[8] James Acton, "FOR BETTER OR FOR WORSE: THE FUTURE OF C3I ENTANGLEMENT", NAPSNet Special Reports, November 21, 2019, https://nautilus.org/napsnet/napsnet-special-reports/for-better-or-for-worse-the-future-of-c3i-entanglement/

[9] Nye, *ibid,* p. 378.

[10] Another example of a basic distinction in a nuclear context is between the types of communications failures. Some failures come from a breakdown in communications, that is, a message is sent but it never gets through. Other failures can arise from messages that get through but contain incorrect, or mistaken content, for example, a “don’t fire” message is sent and received, when the *intended* message was “fire.” This is called the Byzantine Generals Problem in computer science. It is treated in a forthcoming paper by the author.

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/communication-disruption-attacks-on-nc3/

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