NATIONAL INSTITUTE FOR PUBLIC POLICY

INFORMATION SERIES

Issue No. 591 July 2, 2024

Bolstering NC3 Emergency Backup Communications

Laurin Groover
Laurin Groover spent over a decade on Capitol Hill as senior staff to House Armed Services Committee leaders. With nearly 30 years at the nexus of government, politics, and industry, she is a business development and government relations consultant specializing in cyber solutions for the warfighter.

Col. Donald Fielden, USAF (Ret.)
Col. Donald J. Fielden recently retired from the U.S. Air Force after serving over 33 years as a command and control, cyber operations, and cybersecurity leader for the Department of Defense. He currently consults for the DoD and industry on cyber operations, cybersecurity, and information technology issues and serves as the Chief Information Officer for the Aerospace Center for Excellence.

Introduction

House Permanent Select Committee on Intelligence (HPSI) Chairman Mike Turner recently warned fellow lawmakers of an "urgent matter with respect to a destabilizing military capability"[1] purportedly under development by the Russian government. The "threat relates to a space-deployed Russian anti-satellite weapon. Such a weapon could pose a major danger to U.S. satellites that transmit billions of bytes of data each hour."[2] While the capability reportedly is not yet operational, the discovery was of sufficient concern that the "House Intelligence Committee voted 23 to 1 to make this information available to Members of Congress. White House officials confirmed that, in their view, the matter was 'serious.'"[3]

Satellite communications (SATCOM)—those billions of bytes of data transmitted each hour—are a major component of the Nuclear Command, Control, and Communications (NC3) enterprise, which is itself the backbone of the U.S. Government's nuclear deterrence strategy.

This threat underscores the urgent need for rapid development and deployment of an emergency backup "smart communications" capability that would provide continuity of operations given the very real possibility of SATCOM disruption.

The NC3 Enterprise

The NC3 enterprise is a complex and interconnected system designed to ensure effective global command, control, and communications capabilities for the nation's nuclear forces. According to the Department of Defense (DoD) *2022 Nuclear Posture Review* (NPR), which lays out Administration policy and strategy on nuclear forces as part of the *National Security Strategy*, "[o]ur NC3 system must provide command and control of U.S. nuclear forces at all times and under all circumstances, including during and following a nuclear or non-nuclear attack by any adversary. Resilient NC3 capabilities are a critical enabler of mission assurance for nuclear operations."[4]

Key to resilience and mission assurance is the communications piece of the NC3 architecture, the mechanism by which commanders issue orders and provide data to the warfighter. To address threats to communications, the NC3 enterprise incorporates redundant communications capabilities to promote resilience and continuity of command and control (C2) functions. Redundancy is achieved through multiple communications systems, diverse transmission paths, and backup systems to mitigate the impact of any single point of failure.

The main communications pathways facilitating information exchange between the NC3 nodes are based primarily on SATCOM and terrestrial pathways, with SATCOM as the vital and essential high-speed communications pathway enabler. Reliance upon SATCOM without an adequate backup communications system poses risks, however, as adversaries have prioritized communications disruption and are targeting SATCOM specifically.

China and Russia, in particular, "have observed U.S. military operations for the past 30 years"[5] and are well aware "that disrupting C2 systems could be one cost-effective solution to mitigating U.S. military advantages."[6] They have, therefore, "developed systems and strategies to reduce the effectiveness of U.S. command and control systems."[7] Because disruptions to communications degrade C2, China has focused upon developing "the ability to reduce the effectiveness of adversary satellites and communications systems and thus prevent adversary forces from connecting weapons systems and sharing data and information."[8] Russian military doctrine has likewise emphasized "disrupting an adversary's command, control, and communications systems."[9] Whether conventional or nuclear forces, the communications element of C3 is the most vulnerable to attack.

Development of a new and more dangerous Russian anti-satellite weapon has the potential to obliterate SATCOM data transmissions to the warfighter and thereby significantly impede the C2 capabilities of U.S. nuclear forces at a time when they are needed the most. Yet even without deployment of a new Russian anti-satellite weapon, worrisome vulnerabilities already exist within the SATCOM architecture.

INFORMATION SERIES
Issue No. 591 | July 2, 2024

Vulnerabilities in the Current System

Three major existing weaknesses posing significant risks to the NC3 enterprise for the United States, Allies, and partners include vulnerabilities in the cyber domain, risk to physical infrastructure, and post-nuclear events.

NC3 systems, like any other computer-based infrastructure, are susceptible to cyber threats. Cyber threats to SATCOM are of particular concern, as cyber attacks are the most cost-effective and least directly confrontational method of obstruction.[10] Malicious actors may also attempt to infiltrate or manipulate the NC3 network, potentially compromising the integrity, confidentiality, and availability of critical information. Cybersecurity risks pose numerous threats to the NC3 enterprise that could disrupt:

- Satellite ground stations used for C2 satellite constellations, putting communications satellites at risk, with satellite cross links further compounding the risks;
- Satellite ground stations used to route user traffic from satellite down link sites; and
- Communications nodes that route traffic to desired destinations.

Russia demonstrated its capacity for infiltrating satellites when it hacked a commercial satellite company prior to its invasion of Ukraine.[11] U.S. Government officials—notably the Office of the Director of National Intelligence, the Federal Bureau of Investigation, the National Counterintelligence and Security Center, and the Air Force Office of Special Investigations—issued a threat warning after a government-sponsored hacking challenge revealed that "it was now possible to circumvent the cybersecurity protections of satellites in orbit."[12] The hacked satellite belonged to the U.S. Government.

It is important to note that "government" satellites rely heavily upon infrastructure and services provided by commercial companies. As noted in a previous National Institute for Public Policy *Information Series* paper,[13] so much of the DoD communications enterprise, of which NC3 is a subset, utilizes commercial communications capabilities provided by many companies around the world. The multitudinous locations of these capabilities and the interconnected nature of the system actually serve to create more potential attack surfaces. This is because "[a]ny exchange of information is a potential access point for an adversary. A system designed and built to exchange information with many other systems and subsystems has more potential vulnerabilities to address than a system that has few such connections."[14] These vulnerabilities threaten even the most "hardened" cyber defenses.

There is disagreement within the NC3 community regarding the extent of the cyber threat against the NC3 ecosystem. The complexity of the elements of the NC3 ecosystem, especially considering the age of some systems, the classification of select systems, and other variables lead some to believe the costs to attack the NC3 infrastructure are too high to warrant significant consideration.[15] However, the recent explosion of artificial intelligence (AI) capabilities leading to the nesting of exponentially more attack vectors suddenly places even previously "protected" elements of the NC3 enterprise at risk.

In addition to cyber risks, the NC3 enterprise is vulnerable to physical risks including natural disasters, physical attacks, accidents, or technical failures. These risks affect every aspect of the physical infrastructure that routes critical data in support of nuclear operations, ranging from supply chain infiltrations, jamming of radio transmissions, intentional/non-intentional severing of communications cables (especially transoceanic cables), and more.

Post-nuclear events would cause significant issues for the NC3 enterprise, including loss of radio communications, destroyed equipment caused by electromagnetic pulse effects, and disrupted data streams induced by the electromagnetic effects of nuclear blasts. The increasing use of low earth orbiting satellites introduces additional problems, as such satellites are more affected by post-nuclear events than geostationary satellites.

The Need for An Emergency Communications "Backup System"

An effective, secure, and robust communications capability requires contingency and emergency communications services ensuring continuity for C2 during the most challenging of environments. Wideband High Frequency (HF) digital communications capabilities would serve as a robust backup system. Modern Wideband HF is an effective and low-cost capability that would build upon existing legacy HF infrastructure and significantly enhance the resiliency and survivability of the NC3 enterprise.

Utilization of radio-related capabilities as backup communications is not new to the DoD. The DoD currently has a substantial HF footprint utilizing legacy technology but providing valuable capabilities and services. The Military Auxiliary Radio System (MARS), for example, is a DoD-sponsored network consisting of over 1,000 specially trained and licensed amateur radio operators who support the armed forces and U.S. government operations and are capable of providing global communications services during times of national emergency. With respect to NC3 specifically, STRATCOM is currently using HF - the High Frequency Global Communications System (HFGCS) is the C2 network focusing upon communications with airborne platforms.

Specific benefits of modern Wideband HF include the following:

- Increased Bandwidth: Modern Wideband HF systems provide higher data rates compared to traditional narrowband HF systems. This increased bandwidth allows for faster and more efficient transmission of critical NC3 information, including command orders, status updates, and coordination messages, especially in post-nuclear environments.
- Improved Reliability: Wideband HF technology incorporates advanced modulation techniques and error correction algorithms, which enhance the reliability of communication links. This is particularly important for NC3 systems, as they require robust and resilient communication channels to ensure uninterrupted command and control in high-stakes situations.

- Extended Range: HF signals can propagate over long distances, including over the horizon. Wideband HF systems can take advantage of this characteristic, enabling extended communication range for NC3 operations. This capability is valuable for maintaining connectivity across large geographic areas or when dealing with challenging terrains.
- Anti-Jamming Capabilities: Wideband HF systems often employ modern advanced anti-jamming techniques, such as frequency hopping and adaptive modulation, to counter intentional or unintentional interference. These features enhance the resilience of NC3 communications by mitigating the effects of jamming attempts or electromagnetic disturbances.
- Interoperability: Modern Wideband HF systems are designed to be compatible with existing HF equipment and networks, as well as other communication technologies. This interoperability allows for seamless integration with a variety of communication platforms, ensuring smooth coordination and information exchange within the NC3 infrastructure.

The capabilities described above can be integrated seamlessly within existing NC3 networks. When SATCOM is disabled, communications would "disconnect" from SATCOM systems and operate as stand-alone networks solely within the HF network. These standalone operations would ensure isolation from cyber attacks which gain access through terrestrial or satellite-based communications systems. Additionally, stand-alone operations would allow continued command and control in nuclear post-scintillation environments, during which most other communications (terrestrial and satellite) would be disabled or destroyed. It is important to note that *HF systems are one of the very few capabilities able to operate in nuclear post-scintillation environments, enabling continued C2 of U.S. nuclear forces when all other systems have failed.*

Given the extraordinary volume of information generated, processed, stored, and shared via high-speed communications pathways, technology is necessary to manage the data such that only critical information is transmitted through the slower wideband HF communications pathways. This technology must account for the highly dynamic user environments and automatically distribute critical data through the backup HF communications systems.

Further Enhancements to Modern HF Capabilities—the Role of AI and ML

Previous criticism of HF systems included the limited data throughput compared to satellite and terrestrial communications systems and networks, as well as link reliability induced by varying atmospheric conditions such as sunspots and weather-related issues. While modern Wideband HF provides substantial improvements in bandwidth, high-volume distributed C2-relevant data requires significant bandwidth such as that provided by 5G, SATCOM, and high-speed fiber. HF, even Wideband HF, is only able to handle a small fraction of such throughputs as the portion of the frequency spectrum associated with HF is only 3—30 MHz. Transmitting

large Air Tasking Orders, complete with video and imagery, for example, is not possible with Wideband HF because bandwidth is limited to approximately 256 Kbps with current technologies.

Extremely data heavy C2 transmissions would congest the HF spectrum, essentially clogging the frequency so that data could not flow to the intended user. Developments in Artificial Intelligence (AI) and Machine Learning (ML) hold the key to filtering out unnecessary data to free up space in the spectrum so that urgent information would flow to the intended user without interruption. This "smart filtering" capability would have an "understanding" of the immediate user operation environment and filter the data stream to ensure that, while SATCOM is disrupted and Wideband HF systems are serving as the backup NC3 system, only the most critical data required for mission assurance is transmitted to the given user.

This automatic dynamic data prioritization would not only ensure that the most critical data is transmitted at any given time, it would also provide seamless and automated cutover from main C2 systems to the emergency HF systems. This would allow operators to maneuver without interruption on the battlefield and receive and execute orders without unnecessary delay.

With respect to the issue of link reliability, AI-based controllers would improve upon modern Wideband HF advances in modulation by actively monitoring atmospheric conditions and automatically, instantaneously optimizing the HF broadcast by adjusting transmission frequencies and modulation techniques to allow maximum data throughput at all times. This is the principle behind Automatic Link Establishment (ALE), which is in use today with HF radio communications.

It is important to note that AI and ML capabilities are not machines run amuck, despite popular public misconceptions. They are based upon mathematical algorithms developed by experts to achieve particular goals. Thus, the "smart filter" would reflect a human-originated policy on data priority.[16] And it would enable Wideband HF to serve as a critical emergency backup "smart communications" capability for U.S. nuclear forces' command and control during periods of SATCOM disruption, thereby ensuring the resiliency and survivability of the NC3 enterprise.

Recommendations for Congress

In its deliberations on the Fiscal Year (FY) 2024 National Defense Authorization Act (NDAA), the Senate Armed Services Committee (SASC) called for a DoD briefing on cyber risks and the resiliency of space assets.[17] The Conference Report further required that DoD establish a cross-functional team tasked with devising greater cyber defenses for the networks supporting the NC3 enterprise.[18] Bolstering the cyber defenses of NC3-related assets is vitally important and Congress should be commended for this initiative. However, as stated previously, even the most hardened of cyber defenses are not 100 percent resistant to attack and manipulation. This effort also does not address the communications-related threats to physical infrastructure and post-nuclear events.

While cyber defenses are of paramount importance and every effort must be made to defend networks to the maximum extent possible, resiliency—the ability to bounce back into operation in the event of a breach, or as discussed here, the ability to utilize emergency backup "smart communications" via AI and ML-enabled Wideband HF in the event of SATCOM disruption—is arguably of greater importance because it allows C2 directives to be issued and received without interruption or delay.

In its own consideration of the FY 2024 NDAA, the House Armed Services Committee acknowledged DoD efforts to incorporate AI into the NC3 enterprise and requested a DoD briefing on the issue. No language related to AI and ML-enabled HF was included in the Conference Report and the Department of Defense Appropriations Act for FY 2024 did not address the issue.

As Congress begins consideration of the FY 2025 NDAA and Defense Appropriations legislation, it is imperative that the defense committees provide DoD the necessary emphasis, authorization, and funding to accelerate development and fielding of Wideband HF capabilities that provide a robust "smart" emergency communications backup system in the event of SATCOM disruption, as well as for further development and integration of AI and ML technologies that would optimize operational effectiveness.

U.S. adversaries are targeting SATCOM to disrupt the communications which enable effective C2. As stated previously, if Russia is successful in deploying new and more sophisticated anti-satellite weaponry, SATCOM and the data it transmits are at substantial risk. Elimination of the communications upon which the NC3 enterprise relies would render U.S. nuclear deterrence strategy moot. Therefore, the U.S. must accelerate development and deployment of a resilient emergency backup "smart communications" capability utilizing AI and ML-enabled modern Wideband HF—a capability that would achieve the resilience prescribed by the NPR and ensure continuity of operations and C2 of U.S. nuclear forces at all times.

[1] Ellen Knickmeyer, Matthew Lee, Kevin Freking, and Zeke Miller, "Russian Efforts to Create Anti-Satellite Weapons are Cause for U.S. Concern," *AP News,* February 15, 2024, available at https://apnews.com/article/congress-national-security-6a4497fc2d74ebbe2ab3483ba43e09b3.

[2] Ibid.

[3] House Permanent Select Committee on Intelligence Press Release, February 15, 2024, available at https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=1361.

[4] Department of Defense, *2022 Nuclear Posture Review,* p. 22, available at https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[5] John R. Hoehn, Caitlin Campbell, and Andrew S. Bowen, "Defense Primer: What is Command and Control," Congressional Research Service, November 14, 2022, p. 1, available at https://crsreports.congress.gov/product/pdf/if/if11805.

[6] Ibid.

[7] Ibid.

[8] Ibid, pp. 1-2.

[9] Ibid, p. 2.

[10] See, for example, Maggie Miller, "Officials Plan for New Age of Cyber Threats to Satellites," *Politico*, March 25, 2024, available at https://www.politico.com/news/2024/03/25/satellite-cyber-threat-00148672.

[11] Patrick Howell O'Neill, "Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion," *MIT Technology Review,* May 10, 2022, available at https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

[12] John Breeden II, "US Issues Threat Warning After Hackers Break into a Satellite," *Defense One,* August 23, 2023, available at https://www.defenseone.com/threats/2023/08/national-intelligence-office-issues-cyber-warning-government-and-commercial-satellites/389671/.

[13] Laurin Groover and Col. Donald J. Fielden, USAF (ret.), *Cybersecurity Considerations for the New Congress, Information Series* No. 551 (Fairfax, VA: National Institute Press, April 1, 2023), available at https://nipp.org/information_series/laurin-groover-and-col-donald-j-fielden-usaf-ret-cybersecurity-considerations-for-the-new-congress-no-551-april-1-2023/.

[14] Government Accountability Office Report to Congress," Weapons Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors," March 2021, pp. 10-11, available at https://www.gao.gov/products/gao-21-179.

[15] Yasmin Afina, Calum Inverarity, and Beyza Unal, "Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems," ChathamHouse.org, July 2020, available at https://www.chathamhouse.org/sites/default/files/2020-07-17-cyber-resilience-nato-command-control-communication-afina-inverarity-unal_0.pdf.

[16] June 29, 2023, Interview with Jacob Bauer, Ph.D., Senior Data Scientist, Striveworks.

[17] Senate Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2024*, S. Rept. 118-58, July 12, 2023, p. 294, available at https://www.congress.gov/118/crpt/srpt58/CRPT-118srpt58.pdf.

[18] House Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2024*, H. Rept. 118-301, December 6, 2023, p. 410, available at https://www.congress.gov/118/crpt/hrpt301/CRPT-118hrpt301.pdf.

The National Institute for Public Policy's *Information Series* is a periodic publication focusing on contemporary strategic issues affecting U.S. foreign and defense policy. It is a forum for promoting critical thinking on the evolving international security environment and how the dynamic geostrategic landscape affects U.S. national security. Contributors are recognized experts in the field of national security. National Institute for Public Policy would like to thank the Sarah Scaife Foundation for the generous support that made this *Information Series* possible.