Resilient Communications for Command and Control of Nuclear Forces

A Technology Primer

BY OSCAR GUERRERO

TYPE	CHARACTERISTICS	RISK FACTORS
Platform Control and Information Support	Speed, Persistence, Resilience	Dual-use

DOMAIN	COUNTRY
Multidomain	United States, Russia

- The current United States Nuclear Command, Control, and Communications (NC3) enable the transport of situation monitoring from Intelligence, Surveillance, and Reconnaissance (ISR) data, nuclear force management, nuclear force direction in a communications system that uses multiple redundant, diverse, and resilient datalinks as part of the NCCS.
- The worldwide span of control of the nuclear triad imposes operational requirements for data links: they must operate in all domains (air, land, sea, and space) and through kinetic attacks, non-kinetic attacks, and the effects of nuclear weapons in the hostile environment of a nuclear exchange.
- The four types of links that are part of the current NCCS are (1) the Strategic Automated Command and Control System (SACCS), (2) Ultra High Frequency (UHF) Line of Sight links, (3) Extremely High Frequency (EHF) SATCOM links, and (4) a one way Very Low Frequency / Low Frequency (VLF/LF) low data rate link.
- These resilient data links are used for NC3 message transport, but they are also “dual-use” systems that are used in support of tactical users for day to day activities.
- Outside of the NC3 realm tactical commercial communications systems have been advancing the state of the technological innovation with the developments of Mobile Ad Hoc Network (MANET) capabilities, Spectrum Sensing Cognitive Radios, and data encryption schemes for a post-quantum world.
- These capabilities have the potential to augment the resiliency and flexibility of NC3; however, countries could find it difficult to signal that they are using them for NC3.
- These techniques are all dual use and will also be implemented by tactical forces using many of the same type of wired and wireless links used by NC3 communications systems.

Introduction

Communications for Command and Control (C2) of nuclear forces is the component of the U.S. Nuclear Command and Control System (NCCS) that provides the transport of leadership decisions to nuclear forces via a survivable communications system.[1] To support the credible deterrent against a nuclear attack, the NCCS Communications System of Systems must be resilient against a myriad of environmental conditions and hostile environments and function through the nuclear trans-attack and post-attack stressing scenarios.[2] The communications system must have a high availability to support operations of nuclear forces, be able to function through the effects of nuclear attack, have sufficient redundancy to transport data through the loss of several nodes from kinetic effects, and resist electronic countermeasures, all while ensuring the integrity and maintaining the confidentiality of the messages.[3]

The NCCS employs several methods to provide a highly available communications system. The NCCS uses path redundancy and path diversity by incorporating multiple parallel wired and wireless propagations modes to reduce the opportunity for any single points of failure or vulnerability. Wired communications links consist of terrestrial cabling infrastructure that is a hybrid network of twisted pair copper conductor wire bundles near the edge nodes with fiber optic cables at telecommunications aggregation points.[4] Wireless communications links use (1) direct wave line of sight (LOS) transmissions, (2) ground wav e transmissions, (3) sky wave transmissions, and (4) relay transmissions using aircraft or satellites in frequency bands ranging from very low frequency (VLF) up through extremely high frequency (EHF) as a mitigation against nuclear weapons effects to reach land based, airborne, and undersea nuclear forces[i] as shown below in figure 1.[5]

---

[1] Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, Nuclear Matters Handbook 2016, (Washington, D.C.: Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, 2016) 73-81. https://www.acq.osd.mil/ncbdp/nm/nmhb/docs/NMHB_2016-optimized.pdf.

[2] Systems of Systems are independently useful systems into a larger system that delivers unique capabilities. See: Office of the Deputy Under Secretary of Defense for Acquisition and Technology, *Systems and Software Engineering. Systems Engineering Guide for Systems of Systems,Version 1.0*, (Washington, DC: ODUSD(A&T)SSE, 2008) https://www.acq.osd.mil/se/docs/se-guide-for-sos.pdf; Trans-attack period is the "period from the initiation of the (nuclear) attack to its termination - the post-attack period extends from the termination of the physical attack until political authorities agree to terminate hostilities (that may still have post nuclear detonation effects)." See: U.S. Department of Defense, Office of the Secretary of Defense, *Deterrence, Nuclear Strategy and the Post-Attack Environment,* by Kostas J. Liopiros, June 22, 1981, declassified March 1, 2016, https://www.archives.gov/files/2011-016-doc01.pdf.

[3] Availability refers to the ability of users to use a system when it is needed without delays or service interruptions; A communications node is a relay, redistribution, or end point in a communications network; Integrity refers to assuring the accuracy and completeness of messages and data over a system; Confidentiality means assuring that the messages are only processed or read by the intended recipient(s).

[4] Cellular Service towers (ENodeB stations) use terrestrial backhaul networks to tie into telecommunications infrastructure; In areas lacking physical wiring infrastructure wireless microwave relays are used as terrestrial relays.

[5] Ashton Carter, "The Command and Control of Nuclear War", *Scientific American*, January 1985, https://www.belfercenter.org/sites/default/files/legacy/files/scientificamerican0185-32.pdf; Project Sanguine Extremely Low Frequency (ELF) Transmitters were shut down by the US Navy in 2004. See Joseph Stromberg, "Why the US Navy once wanted to turn Wisconsin into the world's largest antenna," *Vox*, April 10, 2015, https://www.vox.com/2015/4/10/8381983/project-sanguine.

To maintain the confidentiality and integrity of messages, communications systems use transmission security techniques such as frequency hopping spread spectrum and communications security techniques of data in transit encryption using strong cryptography. [6]

State of Play

The current United States Nuclear Command, Control, and Communications (NC3) enable the transport of situation monitoring from Intelligence, Surveillance, and Reconnaissance (ISR) data, nuclear force management, and nuclear force direction in a communications system that uses multiple redundant, diverse, and resilient datalinks as part of the NCCS. The Department of Defense (DoD) NC3 Architecture is split into two distinct layers. The first is the "thick-line" layer, a day-to-day and crisis management layer that provides "secure, reliable, immediate, and continuous access to the President and provides robust command and control over nuclear and supporting government operations."[7] The second layer is the "thin-line" layer that provides assured, unbroken, redundant, survivable, secure, and enduring connectivity to and among the president, the secretary of defense, the chairman of the Joint Chiefs of Staff, and the designated commanders through all threat environments to perform all necessary Nuclear Command and Control (NC2) functions.[8] The "thin-line" layer is the focus of this primer. The "thin-line" layer encompasses the resilient data links that transport real time ISR data from early warning and surveillance assets. These assets support nuclear armed forces and provide situational awareness to leadership as well as providing the means by which leadership commands are sent to nuclear delivery systems of the nuclear triad: land-based intercontinental ballistic missile, submarine-launched ballistic missiles, and nuclear armed strategic bombers—and own force status messages are sent back to National Command Authority.

The worldwide span of control of the nuclear triad imposes operational requirements for data links. These links must operate in all domains: air, land, sea, and space[9] and through kinetic attacks, non-kinetic attacks, and the effects of nuclear weapons in the hostile environment of a nuclear exchange.[10] [11]The resilient data links that provide the communications for NC3 are comprised of "terrestrial (e.g., land-based underground cables, overhead cables, and undersea cables), airborne relay (e.g., E-4B Nightwatch National Airborne Operations Center and the E-6B Mercury Airborne Command Post), and satellite datalinks to transmit and receive voice or data.[12] One key feature that the wireless links have in common is the ability to operate in a nuclear contested environment. Philip J. Dolan and Samuel Glasstone noted that during the various above ground nuclear

---

[6] Spreading the spectrum of signals reduces the effectiveness of narrowband interference from jammers while also reducing the probability of detection as the spreading of the signals may be interpreted as background electronic noise. Frequency hopping switches amongst available frequency channels in a pseudorandom sequence to mitigate jamming and eavesdropping.

[7] *Nuclear Matters Handbook 2016,* 81.

[8] Ibid.

[9] Col. Alfonso LaPuma, "Air Force Nuclear Weapons Center/Nuclear Command, Control and Communications (NC3) Integration Directorate New Horizons Briefing," https://docplayer.net/49760114-Afnwc-nc-new-horizons-briefing.html, 5.

[10] Non-kinetic attacks are electronic attack and/or cyberattack.

[11] *Nuclear Matters Handbook 2016,* 81.

[12] *Nuclear Matters Handbook 2016,* 76.

weapons tests, wireless transmissions in the extremely low frequency (ELF), VLF, and low frequency (LF) bands that used a ground wave propagation mode were unaffected by nuclear weapons effects. Other frequency bands, such as high frequency (HF), very high frequency (VHF), and ultra high frequency (UHF), experienced blackouts that had durations spanning between a few minutes to hours or days—especially for those links that used sky wave propagation modes for beyond line of sight (BLOS)[13] communications. Similarly, satellite transmissions in frequency bands up through SHF suffer from blackouts due to the scintillated atmosphere but can operate through a nuclear event using EHF RF transmissions with limited blackouts that last a few minutes after a nuclear detonation.[14]

The "thin line" NC3 Communications are reliable, assured, enduring, redundant, survivable, secure, timely, flexible, and accurate.[15] The four types of links that are part of the current NCCS are (1) the Strategic Automated Command and Control System (SACCS), (2) UHF LOS links, (3) EHF SATCOM links, and (4) a one way VLF/LF low data rate link. The satellite constellation provides near-worldwide, secure, survivable satellite communications to deliver data rates of between 75 bits per second (bps) and 19.2 kbps using signals in the EHF band. [16]Additionally, the EHF SATCOM link can use very narrow beam widths (spot beams) when operating to provide a low probability of detection/intercept (LPD/LPI) and anti-jam (AJ)[17] capabilities to network participants enabling covert communications that are difficult to detect by opponents. The VLF/LF network supports a much lower data rate but can reach across hundreds if not thousands of miles under ideal or stressing conditions without the need of a satellite constellation for relay through the use of ground wave signal propagation to provide an extremely reliable command link.[18] There is, however, a key limitation to VLF/LF in that the links are only "one way" from a command element, such as the "Take Charge and Move Out" (TACAMO E-6B Mercury) platform[19] to nuclear forces. The UHF link is a vestigial capability from the legacy Post Attack Command and Control System (PACCS) that is limited in range (line of sight) and availability (blacked out during trans attack) but highly available in the post-attack phase of a nuclear conflict. Lastly, there is the relatively simple wired terrestrial landlines that provide the network connectivity for SACCS/SACCS-R that is comparable to a commercial long-distance telecommunications provider. The survivability of a wired network

---

[13] *The Effects of Nuclear Weapons*, *3rd Edition*, ed Samuel Glasstone and Philip Dolan, (Washington, D.C.: U.S. Department of Defense and U.S, Department of Energy, 1977, https://www.dtra.mil/Portals/61/Documents/NTPR/4-Rad_Exp_Rpts/36_The_Effects_of_Nuclear_Weapons.pdf.

[14] U.S. Congress Office of technology, *MX Missile Basing*, (Washington, D.C: U.S Congress Office of Technology, 1981), http://govinfo.library.unt.edu/ota/Ota_5/DATA/1981/8116.PDF, 281.

[15] *Nuclear Matters Handbook 2016,* 80.

[16] Strategic links have requirements for 19.2 kbps in non-stressed conditions and 75 bps in stressed environments; "Advanced Extremely High Frequency System," *Air Force Space Command*, March 22, 2017, http://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249024/advanced-extremely-high-frequency-system/.

[17] MX Missile Basing, 281.

[18] Long-term actual TRIDENT connectivity of greater than 99.99 percent has been demonstrated, and no alert TRIDENT submarine has ever missed an exercise launch order or actual retargeting message. See: Adm Richard Miles, "The SSBN in National Security," http://www.public.navy.mil/subfor/underseawarfaremagazine/Issues/Archives/issue_05/ntlsecurity.html.

[19] *China's Nuclear Force Modernization*, ed. Lyle J. Goldstein, (Newport: Naval War College, 2005), https://apps.dtic.mil/dtic/tr/fulltext/u2/a430846.pdf, 7-22.

with static nodes is highly questionable as the non-kinetic effects of an EMP or kinetic attacks of fixed sites may neutralize the critical nodes within the SACCS network.[20]

As of 2018, there are multiple active development and acquisition programs within DoD focused on maintaining existing capabilities with incremental improvements through technology refresh efforts. In 2016, the U.S. Air Force Global Strike Command (GSC) created a new program executive office (PEO) to manage all the modernization efforts for NC3 to improve interoperability and realize improved efficiencies in acquisitions. The organization is still nascent and new efforts do not yet include any revolutionary approaches to communications in support of NC3.

While these resilient data links are used for NC3 message transport, they are also "dual-use" systems that are used in support of tactical users for day to day activities. The tremendous costs of assured, secure, and highly available datalinks—and in the case of MILSATCOM, the worldwide coverage and data rates[21]—have led to the use of AEHF SATCOM for tactical applications in addition to strategic uses with non-nuclear forces spawning several low cost, non-hardened, AEHF tactical SATCOM terminals.[22] Furthermore, wired military and commercial networks are indistinguishable from the NC3-dedicated SACCS wired network and have permeated across the entire United States, and to a lesser extent other nations, as the backhaul link for general telecommunications services. Similar to the United States, Russia and China have also deployed resilient data links for their early warning and nuclear forces. Both have military satellite communications that have dual use missions for strategic and tactical forces and both have terrestrial VLF transmitters to communicate with their nuclear submarines (Russia ZEVS at Murmansk and China at Changde and Datong).

Advancements to Traditional Communications Networks

Outside of the NC3 realm, tactical commercial communications systems have been advancing the state of the technological innovation with the developments of mobile ad hoc network (MANET) capabilities, spectrum sensing cognitive radios, and data encryption schemes for a post-quantum world. These advancements are all dual use in both connotations; the technologies can be used for both strategic and tactical operations as well as commercially for non-military uses.

Traditional networks

Traditional communications network infrastructures are created using a hub and spoke (star) topologies or ring topologies to connect multiple nodes in both wired and wireless networks. In the hub and spoke communications network topology, separate sites, also called nodes, are connected to a central hub site that manages all the message traffic occurring on the network to provide data transport between all connected nodes. A ring topology network has each node connected to two other peers to form a logical ring structure, such that all traffic is

---

[20] Fixed targets are easy to target as opposed to mobile assets that have some degree of location uncertainty in targeting.

[21] "Advanced Extremely High Frequency System."

[22] "Bringing Protected Satellite Communications to the Tactical User" *Northrop Grumman Newsroom*, August 23, 2017, https://news.northropgrumman.com/news/releases/bringing-protected-satellite-communications-to-the-tactical-user-industry-team-successfully-tests-low-cost-terminal-with-on-orbit-aehf-satellite.

relayed through peer nodes to reach the intended destination.[23] Unlike a hub and spoke topology, ring networks do not have a central node that manages traffic, as each peer node can relay messages to the next peer allowing for improved fault tolerance and damage. The resiliency of a ring topology is only a slight improvement over a hub and spoke in that any two logical links in the chain will segment the overall network and cut off nodes from each other. There are also additional drawbacks in the form of cost from the greater functionality needed at each node as well as performance in that each node is managing relay traffic intended for other nodes in addition to messages that are indented for the node itself.

MANETs

An alternative that has been gaining in use since it was first introduced in the 1970s are MANETS. MANETs are a collection of wireless terminals that are distributed, disaggregated, and operate without reliance on centralized resources or fixed infrastructure and are self-forming and self-healing.[24] In the commercial domain, the applications are used to support temporary spikes in demand from transient mobile users or to mitigate failures of fixed infrastructure. In military use cases, the needs are similar but are focused on the transient nature of evolving battle spaces and loss of nodes from enemy action or mishaps. All the radios in a MANET are preconfigured to connect and authenticate in a secure manner to participate in the highly dynamic network.[25] The configurations set operating parameters such as frequencies, waveforms, frequency hopping schemes, encryptions keys, and authentication on the network. MANETs offer an incredibly flexible communications network that can operate through the loss of multiple nodes and the exit or entry of nodes in a highly dynamic environment—a highly desirable characteristic for operations in a chaotic trans-attack and post-nuclear attack scenarios. MANETs have been developed using several different protocols ranging from 802.11 Wi-Fi, unlicensed spectrum radios, and military radios using joint tactical radio system waveforms such as the Wideband Networking Waveform and the Soldier Radio Waveform.

The drawback to MANETs is the routing overhead introduced from all the nodes in the network simultaneously acting as routers and the changes that have to propagate through the network as nodes join or exit the network that can dramatically decrease the available throughput for messages on the network. Recent DoD operational tests have concluded that the MANET waveforms have “several deficiencies, including poor range compared to legacy systems, excessive power consumption, and a high level of network and spectrum management that may not be operationally feasible.”[26] There are several academic, commercial, and DoD efforts that are focused on reducing the overhead resources of MANET implementations to reduce battery consumption for mobile users and increase the ratio or throughput to routing overhead for enhanced efficiencies.

---

[23] The nodes do not have to be located in a physical ring layout.

[24] “Mobile Ad Hoc Networking, *Cisco,* https://www.cisco.com/c/en/us/products/ios-nx-os-software/mobile-ad-hoc-networking/index.html.

[25] Non-secure MANETs (open networks) are possible but not a usual use case.

[26] M.S. Marwick, C.M. Kramer, and E.J. Laprade, *Analysis of Soldier Radio Waveform Performance in Operational Test*, (Alexandria: Institute for Defense Analyses, 2015).

Spectrum Sensing Cognitive Radios

Spectrum sensing cognitive radios are another emerging technological advancement currently still in development in the tactical and commercial spheres that have an application to strategic communications. In the early 2000s, the notion that the growth in the use of software defined radios (SDRs)[27] would provide a new capability to observe every parameter possible by the radio and dynamically adjust the operating parameters of the radio to maximize throughput while reducing power led to the concept of the fully cognitive (Mitola) radio.[28] In a case where radios are designed to operate openly and collaboratively to share the wireless spectrum, this would include information such as frequency channels in use, TDMA schemes, CDMA schemes, and SNR parameters. [29] In the commercial world, cognitive radios will greatly improve the utilization of the wireless spectrum by allowing opportunistic use of allocated wireless spectrum when the primary users (owners) are not using the spectrum in a fixed space and time. Cognitive radio technology will allow "secondary" users to opportunistically use the spectrum when the primary users are not actively broadcasting.

In the tactical and strategic battle space, the focus is on spectrum sensing cognitive radios that can sense the conditions of the electromagnetic environment. These conditions include wireless signal congestion, electronic attack (jamming), and electromagnetic environment (EME) effects from nuclear detonations that "black out" the spectrum. Both commercial and military efforts to develop spectrum sensing cognitive radios or fully cognitive (Mitola) radios are still in the research and development stages and have yet to work out critical issues, such as how two disconnected cognitive radios can negotiate spectrum utilization if each radio has different EME conditions at each location, or how security and covertness can be maintained when radios are broadcasting their presence through discovery signals to find other participants in the network.

Post-Quantum Cryptology

Lastly are the future advancements in communications security that will be provided by post-quantum cryptography. Most commercial and military cryptography in use today was developed to secure data in motion against brute force attacks from classical computers that would require years of computation to determine the encryption keys. Quantum computers currently in development will reduce the time required to break encryption keys and will compromise the confidentiality and integrity of communications.[30] Several entities ranging from non-governmental organizations such as the Internet Engineering Task Force (IETF)[31] to government

---

[27] Software Defined Radios are a type of reconfigurable radio in which some or all of the physical layers of functionality are implemented in software and/or firmware. See "Software Defined Radios," *NASA*, November 4, 2012, https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_sdr.html.

[28] Joseph Mitola, "Cognitive Radio for Flexible Mobile Multimedia Communications," (paper presented at the IEEE International Workshop on Mobile Multimedia Communications, San Diego, California, November 15-17, 1999).

[29] Code Division Multiple Access is a sharing of a wireless spectrum to allow use by multiple participants within the same time and space through coding of the signal; Signal to Noise is a measurement of the energy of the intended signal over the electromagnetic noise in the environment expressed as a ratio; Time Division Multiple Access is a time sharing of a wireless spectrum to allow use by multiple participants in the same space separated in time.

[30] An attacker could also use a large array of processors but that would dramatically increase the cost 9in resources) to an adversary; Machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. See Lily Chen et alia, *Report on Post Quantum Cryptography*, (Washington, D.C.: U.S. Department of Commerce, 2016) https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[31] P. Hoffman, "The Transition from Classical to Post-Quantum Cryptography," *Internet Engineering Task Force,* August 14, 2017, https://tools.ietf.org/html/draft-hoffman-c2pq-02.

organizations such as the National Institute of Standards and Technology (NIST) and the National Security Agency are actively working to mitigate the threats to encryption posed by quantum computing.[32] As of June 2018, NIST has outlined a schedule to have post-quantum cryptography algorithms and standards within the 2022/2024 time frame but has not addressed an implementation schedule. China has taken an alternative approach and has developed and demonstrated a satellite with quantum cryptography service demonstrating a secure video conference between Europe and China.[33] China's Micius satellite uses a one-time pad with quantum key distribution, dramatically complicating attempts to decrypt messages for adversaries in a nearly unbreakable imple mentation. The quantum key distribution demonstration has proven the concept in an operation environment but has yet to be developed for military applications.

Improvements From Resilient Communications and Datalinks on Strategic Situational Awareness

The current NC3 communications links used by DoD forces already provide worldwide range and vantage, have sufficient data rates to transport orders and status messages within seconds (speed), have high availability (persistence) and data protection features, and are resilient in stressing conditions of nuclear war.[34] All of the current efforts being pursued by the Air Force NC3 PEO are modernization efforts to sustain current capabilities. Improvements to resilience can be made by integrating the technologies of spectrum sensing cognitive radios and MANET in the NC3 communications architecture. Instead of waiting for preselected wireless frequencies to become available in a trans-attack or post-attack environments, spectrum sensing will allow for wireless nodes within the NC3 architecture to scan the EME and select frequencies that are uncongested and recovered from nuclear weapons effects to reduce the duration of any blackout periods. The fixed network architectures with multiple point to point links would also be improved by layering on the capability of forming ad hoc networks of surviving nodes through the use of MANETs that leverage spectrum sensing cognitive radios. Last, securing the links with post-quantum cyphers will ensure that the integrity and confidentiality of messages can be maintained as the current encryption cyphers become inadequate against attacks using quantum computers.

Effects from Resilient communications and datalinks on Strategic Stability

Resilient communications are an essential capability that contribute to strategic stability through the maintenance of a credible counterforce strike. Improving the resiliency of the communications of the NCCS only enhances strategic stability, as increased confidence in the resilience of communications for NC2 may reassure decision makers that they will be able to launch surviving nuclear assets after absorbing a nuclear first strike, thus reducing the incentive to launch on warning. Similarly, if one country was aware of its opponent's resilient

---

[32] Tom Simonite, "NSA Says It "Must Act Now" Against the Quantum Computing Threat", MIT Technology review, February 3, 2017, https://www.technologyreview.com/s/600715/nsa-says-it-must-act-now-against-the-quantum-computing-threat/.

[33] "Chinese satellite uses quantum cryptography for secure video conference between continents", MIT Technology Review, January 30, 2018, https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/.

[34] Extent to which technology can continuously operate or is available to operate in a contested environment; Position or distance from which new information can be ascertained; Shortening in the time between an adversary's action and the ability to act on the information.

NC3 systems, it might be less likely to attempt a disarming first strike because the victim would retain the ability to retaliate even in a post-nuclear use environment.

However, the use of newer technologies such as spectrum sensing cognitive radios, MANETs, and post-quantum cryptography are all developments that would be difficult for opponents to detect. Spectrum sensing is an entirely passive process and not detectable by opponents. Furthermore, switching between various frequency bands among cognitive radios would require an adversary to have multiple ultra wideband sensors spanning multiple frequency bands—this would be difficult to host on weapons systems due to size, weight, and power constraints of such a capability. Whereas fixed networks have static interfaces and paths, a MANET is constantly adjusting to operational environment. This highly dynamic behavior increases the difficulty for an adversary to infiltrate, monitor, or deny the use of the communications network. As with the use of modern encryption techniques and cyphers, the use of quantum cryptography to encrypt data over communications networks would render the data unreadable by adversaries but would dramatically increase the computational demands of successfully breaking the cypher through brute force methods over modern 64-bit cyphers.

Spectrum sensing cognitive radios, MANETs, and post-quantum cryptography technologies and techniques are all dual-use and will also be implemented by tactical forces using many of the same type of wired and wireless links used by NC3 communications systems. Furthermore, in order to have any chance of determining the network topology or spectrum utilization, an opponent would first have to determine what portion of the spectrum to attack, then defeat the transmission security of the links, whether frequency hopping and spread spectrum techniques, and finally defeat any encryption within the link to start analyzing the network data and link layer data. The only exception would be the use of the VLF/LF link that is only used to communicate to nuclear forces and is impossible to use covertly as it sends out signals at kilowatt of output power in an omnidirectional pattern.

As a result, nuclear-armed countries will have to develop messaging strategies to alert opponents of their capability to assure communications for NC3 amongst leadership and nuclear forces through all phases of a nuclear attack to maintain or bolster nuclear deterrence. Something as simple as field exercises of a capability that cannot be covertly used, such as the VLF/LF link, can be used as part of the messaging and to establish the use of the link in non-crisis situations.

Conclusion

The NCCS is an essential element to ensure crisis stability; deter attack against the United States and its allies; and maintain the safety, security, and effectiveness of the U.S. nuclear deterrent. Enhancing the communications systems within the NCCS only serves to improve strategic stability by providing leadership and nuclear forces with the option to allow for more time to develop information in an evolving crisis situation that involves nuclear weapons or other weapons of mass destruction. The benefits provided by MANET techniques, spectrum sensing cognitive radios, and post-quantum encryption do not have any escalatory drawbacks, and they also do not increase the first mover incentive to opponents. On the contrary, the ability to retain C2 of nuclear forces may provide leadership with a longer time frame to make decisions in a nuclear crisis since leadership would possess a high degree of confidence that a retaliatory strike would be possible after absorbing some adversary attacks.

ABOUT CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic in-sights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy in-stitutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).