# LAST CHANCE:

## Communicating at the Nuclear Brink Scenarios and Solutions Workshop Synthesis Report

THE NAUTILUS INSTITUTE
STANLEY CENTER FOR PEACE AND SECURITY
TECHNOLOGY FOR GLOBAL SECURITY

May 14, 2020

**Authorship:** This report was prepared by staff of Nautilus Institute, Stanley Center for Peace and Security, and Technology for Global Security, with assistance from Randall Consulting and copy editing by Maureen Jerrett. Cover image is by Lauren Hostetter of Heyhoss Design.

**Acknowledgments:** The workshop was funded by the John D. and Catherine T. MacArthur Foundation. The Center for International Security and Cooperation at Stanford University co-hosted the workshop held on October 21–22, 2019, under the Chatham House Rule.



**Publication:** This report is published simultaneously by Technology for Global Security here and by Nautilus Institute here.

## CONTENTS

## EXECUTIVE SUMMARY

Nuclear war threatens the existence of humanity. Managing this risk depends on the ability of nine supreme nuclear commanders to avoid using nuclear weapons or to de-escalate rapidly after initial use, rather than drive toward full-scale nuclear cataclysm. Unfortunately, current nuclear command, control, and communications (NC3) systems to control nuclear weapons and communicate with one's own forces and those of adversaries—to step back from the brink of nuclear war, or to end it once it begins—may not be up to the task, in light of novel technical developments of the early 21st century. Today NC3 systems are in fact "systems of systems" that rely on legacy and modern technologies that are increasingly vulnerable to digital and other rapidly emerging, disruptive capabilities. This fact has been laid bare in recent years through U.S. government-sponsored research, including that of the U.S. Defense Science Board.[1] If and when NC3 systems fail under stress, however, leaders *must* have a way to communicate to step back from the brink.

In 2018, when he was the commander of U.S. nuclear forces, General John Hyten (now the U.S. vice chairman of the Joint Chiefs of Staff) made public that government planners and systems architects were requesting private sector contributions and innovations from outside routine acquisitions channels as part of designing and building the "NextGen" U.S. NC3 architecture.[2] This imperative is not uniquely American but is shared by other nuclear-armed states. As a result, this report outlines a vision for a novel "hotline" system,[3] devised through conversations between public and private actors from around the world, that would enable secure and verifiable communications between leaders during nuclear crises and other high-stakes scenarios. This unique, resilient system is designed for "radical simplicity" from the hardware up, with as few components as possible. The proposed system would augment but not replace hotlines currently used by governments around the world or provide such links where they do not already exist. Such a hotline system would also provide a communications option for rapid and reliable connectivity between heads of state and senior nuclear commanders.

We call this system CATALINK, from the terms "cataclysm" and "link." The CATALINK would rely on internationally driven open-source technology to maximize user integrity

---

[1] "...this Task Force concluded that the cyber threat is serious and that the United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities" (p. 4). "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat" (Washington, D.C.: Department of Defense, Defense Science Board, January 2013), https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

[2] On November 27, 2018, Strategic Command issued the "Next Generation NC3 Enterprise Challenge," the memorandum signed by General Hyten can be found here: https://www.tech4gs.org/uploads/1/1/1/5/111521085/memorandum-next_generation_nc3_enterprise-21nov2018.pdf

[3] Merriam-Webster defines what has historically served as a hotline as "a direct telephone line in constant operational readiness so as to facilitate immediate communication." See "Hotline," in Merriam-Webster, accessed May 1, 2020, https://www.merriam-webster.com/dictionary/hotline

and trust. This system would exploit redundant transmission capabilities to ensure that multiple parties could connect under extreme conditions, including loss of power and absence of cellular and internet connectivity. The endpoint devices would be designed for durability, availability, and ease of use, enabling parties to immediately connect with confidence amid crises. These devices will be built from the bottom-up through international collaborative efforts to ensure security, integrity, and resilience. If successfully developed, CATALINK might also inspire features of new "mainstream" command-and-control systems, building on existing capabilities as nuclear weapons states consider "NextGen" architectures.

The next step for this project is to create a prototype of this new system and to lay the administrative and political groundwork necessary for implementation. The long-term vision is to develop and deploy CATALINK as a voluntary communications tool to support crisis decision-making globally—one that is secure, survivable, and free from interference, spoofing, or jamming. The stakes could not be higher. A stable, secure hotline connecting nuclear states (and other nations) could ensure that leaders can negotiate, confirm information, or signal intentions to avoid escalation to nuclear war. CATALINK will justify its existence if the system helps to avert even one such conflict.

After extraordinary expenditures over the decades, it is possible and perhaps expected that mainstream NC3 systems could prove adequate. Yet, this project is motivated by the fact that prominent experts—including Andy Marshall, Ash Carter, and others—have for many years noted the persistent gap for communication between nuclear adversaries and even allies. As current STRATCOM Commander Admiral Chas Richard testified in February 2020, the U.S. NC3 system may now be approaching a point of no return.[4]

The initial concept for a new hotline system emerged at a January 2019 workshop at Stanford University focused on global nuclear command, control, and communication (NC3) systems, convened by Nautilus Institute, Technology for Global Security (Tech4GS), and the Preventive Defense Project. At this workshop, Eric Grosse, former VP of Security & Privacy Engineering at Google, suggested a new approach to hotlines that would take advantage of emerging concepts in hardware and software security and encryption.*

On October 21–22, 2019, Tech4GS and Nautilus Institute convened a follow-on workshop, co-organized with the Stanley Center for Peace and Security and hosted by the Center for International Security and Cooperation at Stanford University. At the workshop, experts from industry, government, and academia used scenarios to further refine the concept and specify design criteria and possible incubation strategies for a back-up hotline system for use in nuclear crisis communications. More information about the workshop and the scenarios can be found in the appendices to this document.

*See Eric Grosse, "SECURITY AT EXTREME SCALES", NAPSNet Special Reports, May 30, 2019, https://nautilus.org/napsnet/napsnet-special-reports/security-at-extreme-scales/ Eric Grosse's work on hotline cryptography is at: https://github.com/n2vi/hotline/blob/master/hotline cryptography.pdf

[4] Aaron Mehta, "Strategic Command Boss Warns of Nuclear 'Point of No Return,'" Defense News, February 28, 2020, https://www.defensenews.com/smr/nuclear-arsenal/2020/02/28/stratcom-head-warns-us-near-nuclear-point-of-no-return/

# 1. THE PROBLEM: WHEN COMMUNICATIONS BREAK DOWN DURING A NUCLEAR CRISIS

> Difficult as it is to provide reliable communications among American forces in nuclear war, communication with U.S. allies and with the Soviet Union is even harder. Yet some thought needs to be given to communications between the superpowers, since terminating a nuclear war before it escalates to all-out exchanges is a goal of U.S. strategy…. Explicit messages could be sent by normal connections moments before one side launched an attack, or later if communications systems were deliberately spared. (Ashton Carter, 1987)[5]

> In the future, especially as you get out into the 2050s and beyond, which is where we have to think now that we're building this new nuclear command and control architecture for the future…. The structure that we build has to be near infinite...that the adversary can never figure out how the message is getting through and it will always get through, therefore…. How do you certify something that you're looking 30, 40, 50 years in the future? Something that has a near infinite number of pathways? We don't know how to do that yet…." (General John Hyten, April 2019)[6]

In the United States and other nuclear weapons states, nuclear command, control, and communication (NC3) systems in many regards are outdated, vulnerable, and overly complex. All NC3 systems require constant modernization, and some are improvised under severe constraints—such as those in the DPRK. Even in the United States, as former U.S. STRATCOM Commander General John Hyten noted, no one knows how to make NC3 certifiably reliable in current, let alone future, technological conditions.

Experts familiar with methods of attacking modern network and communication technologies are concerned that it is not only possible, but even probable that elements of current NC3 systems will fail under real stress. These challenges call for a renewed focus on the "third C" in the NC3 framework: communication, not only within the command-and-control hierarchy, but also between parties in an escalating nuclear-prone conflict. The latter element is not often considered part of a nation's NC3 superstructure but, as noted by Ash Carter above, will serve a critical role between NC3 systems in moments of crisis. Currently, adversaries may not have a trustworthy means to communicate to avoid nuclear cataclysm, for a variety of technical and political reasons. Leaders of nuclear states urgently need new systems to ensure they have a

[5] Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, eds., Managing Nuclear Operations (Washington, D.C.: Brookings Institution, 1987), p. 604.
[6] General John E. Hyten, quoted in U.S. Strategic Command, "Space Symposium Media Roundtable" (Colorado Springs, Colorado, April 9, 2019), https://www.stratcom.mil/Media/Speeches/Article/1817618/space-symposium-media-roundtable/

communication link that they can rely upon during an escalating crisis—whether it is incorporated into NC3 or not.[7]

The risk of nuclear war has recently resurged. Nine countries possess about 14,500 nuclear weapons today, and even more countries (14) have NC3 systems. Another 25 states rely on nuclear weapons as part of extended deterrence agreements or contribute to their deployment. In the United States alone, legacy NC3 enterprises are decades-old patchworks of systems and subsystems with multiple layers of software and hardware. This patchwork character leads many experts to believe that these systems will not be resilient enough to overcome new threats arising from cyberwarfare, autonomous vehicles, and artificial intelligence—technologies that could dramatically accelerate the escalation of nuclear-prone conflicts and add uncertainty at the exact moments when commanders must make decisions with existential import.

Communications amid nuclear crises require the availability of secure, reliable networks that key decision-makers trust. The development and advocates of such a system cannot be centered on the United States nor solely focused on solving U.S. problems. If the actors in a nuclear crisis lack confidence that their communications will be reliable and secure, then it is more likely that their decisions could be driven by panic or uncertainty. As a result, insecure communications could motivate preemptive launch of nuclear weapons—a modern version of the historical concern about use-it-or-lose-it postures. The gravity of nuclear risk demands collaborative and internationally orchestrated solutions.

Systems for communications, indications and warning, and response capabilities are likely to be among the first attacked early in a crisis.[8] These systems are force multipliers and their early loss could degrade forces accordingly. The amount of time for decision-making was already terrifyingly short in the nuclear age, but—is arguably tightening even further in the digital age. Already,

> The biggest vulnerability in a nuclear posture is communications. This makes it a prime target, but one which at a strategic level no one admits to. 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 such attacks on further escalation." - From "Communication Disruption Attacks in NC3," Paul Bracken, Yale University, October 2019

[7] Some have argued that the concept for CATALINK (and the idea for a novel hotline system generally) should be separated completely from "NC3," which they say is specifically about positive and negative control of nuclear weapons. Acknowledging there is no global or agreed meaning to the term NC3, we believe that nations' NC3 and communications systems are inextricably intertwined with each other's NC3 systems, a condition we call "global NC3 interdependence." Hotlines, such as that between the U.S. and Russia, are born of recognition at the political level of this interdependence, as was recognized by Ash Carter and others decades ago. Thus, any conceptualization of a "nuclear communication" system should include international communications considerations and hotlines.

[8] As argued cogently in Daryl K. Press, "NC3 and Crisis Instability–Growing Dangers in the 21st Century," NAPSNet Special Reports, October 17, 2019, https://nautilus.org/napsnet/napsnet-special-reports/nc3-and-crisis-instability-growing-dangers-in-the-21st-century/ and

there is little or even no time for decision-making, much less de-escalation with an adversary or deconfliction of one's own forces. In an era of highly public communications and threat signaling—compounded by the emergence of social media—the possibility of a catastrophic nuclear incident continues to grow.[9]

Digital technology raises major concerns about compromise at the level of chips, core software, or applications. Today's systems comprise elements from myriad sources, many of which could plausibly be malicious. Many elements are also so complex that verification of the absence of malice is difficult or impossible to achieve. We should understand this intuitively, as even world-class companies regularly experience failure or compromise.

Although communications among global leaders could be decisive in averting a nuclear crisis, developing a communications system that is highly trusted and reliable in nearly every situation is a major technical challenge. Efforts to develop a shared communications system may be hampered by a lack of mutual trust among stakeholders, particularly as adversaries may be reluctant to adopt a system they fear could be compromised. Similarly, governments may be reluctant to use solutions developed by other countries or by the private sector, which could be regarded as lacking sufficient security compared to home-grown NC3.

> The leaders of the United States and the Soviet Union would of course communicate through the violent actions they ordered. But it is less clear how other messages could be sent between surviving elements of the two governments. For the existing Washington-Moscow hotline to have a chance at functioning in a nuclear war, both sides would have to withhold attack on national capitals. Such restraint may occur. But in exchanges of such ferocity that emergency communications within the national chains of military command become difficult, international communications can be only still more difficult. Similar considerations apply to communications among NATO and Warsaw Pact nations or with other allies. —Ash Carter, 1987[10]

Requirements for a solution to these challenges must account for various scenarios to elucidate practical necessities. The table below is an illustrative initial conception of what some of those scenarios may look like, based on potential crises involving the

---

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] Paul Davis argues that this challenge of ever-increasing time compression does not need to actually be the case in the 21st century, and that this is a policy decision well before it is a technical one. Policy choices to dial back launch on warning postures, for example, and agreements between nuclear states in advance to assume such revised postures, would greatly reduce the time constraints imposed on decision makers. See Paul K. Davis, "What Do We Want From the Nuclear Command and Control System?" NAPSNet Special Reports, October 24, 2019, https://nautilus.org/napsnet/napsnet-special-reports/what-do-we-want-from-the-nuclear-command-and-control-system

[10] Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, eds., Managing Nuclear Operations (Washington, D.C.: Brookings Institution, 1987), p. 226.

United States, Russia, China, and the DPRK. As indicated in this chart, a CATALINK-style solution is necessary for situations such as cases 3, 4, 6, and 7. In some of these scenarios, long-range and high-bandwidth communications are not available, networks are badly compromised and therefore neither effective nor trustworthy, or leadership has lost trust in those who control the communications.

### Table 1: Possible CATALINK use cases

| State of comms system | Physical | Environmental | Demand for crisis communications* | Network security | Operational | Trust in official system's controllers |
|---|---|---|---|---|---|---|
| | **U.S. Conflicts with Russia, China, or DPRK** | | | | | |
| 1 | Normal | Normal | Normal | Normal | Normal | Yes |
| 2 | Space Systems Down | Noisy Atmosphere | Very High | Normal | Normal | Yes |
| 3 | Long-range systems down or dubious (satellites, undersea cables) | Noisy Atmosphere | Very High | Badly degraded (external, internal, including emergent hardware-level threats) | Degraded due to problems of management, competence, and chaos | Yes |
| 4 | Long-range systems down or dubious (satellites, undersea cables) | Noisy Atmosphere | Very High | Badly degraded (external, internal, including emergent hardware-level threats) | Degraded due to problems of management, competence, and chaos | No (internal schisms and intrigues, or distrust of an adversary's system) |
| | **Regional conflicts (e.g. India-Pakistan)** | | | | | |
| 5 | Normal | Normal | Normal | Normal | Normal | Yes |
| 6 | Normal Except Regionally | Noisy Atmosphere | High | Badly degraded (external, internal, including emergent hardware-level threats) | Degraded due to multiple reasons | Yes |
| 7 | Normal Except Regionally | Noisy Atmosphere | High | Badly degraded (external, internal, including emergent hardware-level threats) | Degraded due to multiple reasons | No (internal schisms and intrigues, or distrust of an adversary's system) |

*Demand for communication services may be measured: (1) technically; for example, in bits of information/second, which varies by media (text, voice, images, video); and (2) relative to the capacity of the communication network to reliably achieve transmission of the information. The combination of the two parameters may exceed the capacity of

the communication system to transmit the information reliably. In general, the demand for communication may increase dramatically in a crisis and overwhelm transmission capacity, degrading or collapsing the communication system. Thus, “very high” and “high” levels of demand are relative to the level of normal (non-crisis) demand for specific information services, on the one hand, *and* the capacity of the communication system to provide the communication service to a specified level of reliability in specific use scenarios on the other.
Source: Paul Davis, RAND, used with permission.

## 2: THE SOLUTION: CATALINK

Leading experts concur on the need for a high-assurance,[11] additional consultative layer of communications between decision-makers and Nuclear Command Authorities in nuclear-armed states—called CATALINK—that would be designed through a deliberately open process to generate and merit buy-in and mutual trust. CATALINK would be resilient to various types of attacks, including cyberattacks and other electronic forms of warfare, that could disrupt military and civilian systems on a massive scale. Most importantly, this system would enable decision-makers to communicate in the midst of an array of interacting problems—such as breaches of sensor and early warning systems, corruption or failure of intra-military communications, false alarms, or the collapse of power systems and networks—that cloud decisions in a fog of uncertainty and confusion at critical moments in conventional war, let alone nuclear war.

> With existing certified-secure technology, it sometimes happens that government officials want to securely communicate with partners that they can't totally trust and their best option is to use obsolete crypto devices from years ago, still secure enough for the purpose, a bit clunky, but not a catastrophic loss if one gets into enemy hands. Because of open-source and comparatively low-cost we target, one can imagine a variant of our hotline system being able to meet that need" —From "Hotline Cryptography," Eric Grosse, 2019

The highest priority of the CATALINK system is to help avoid or quickly terminate nuclear war. Once CATALINK is found to be reliable and secure in nuclear crisis communications between adversaries, it might be deployed within the national NC3 infrastructure as well as for multi-party communications in other non-nuclear but catastrophic situations, such as natural disasters, global pandemics, nuclear-plant meltdown, or other circumstances where existing communications systems may be compromised or unavailable. The implementation of CATALINK will be country specific. There are nations that have highly unique, entirely stand-alone NC3 systems that are in no way tied to these other emergency response systems. Through the research of this project, it has become clear that some nations—including the United States—do connect these systems, and thus this project will endeavor to adjust its parameters for each international use case. In addition, a communications system that can work under high-stress conditions could be valuable for an enterprise incident-response team whose infrastructure and credentials have been compromised.

[11] By “high-assurance,” we mean functionally correct and highly resistant to external attack, biasing engineering tradeoffs in favor of security to an extent greater than ordinary defense software. Ideally, this includes formal methods that result in machine-checked proofs.

CATALINK design specifications are based on conditions judged likely to prevail before, during, and after a crisis occurs. These include:

- **Usability/Low Latency:** The system must be available and easy to use under a wide range of conditions, and it should offer secure message transmission or reception.
- **Resilience:** The system must be resilient under nearly all imaginable circumstances, including electromagnetic pulses,[12] power failures, cellular network failures, solar storms, and volcanic eruptions. The system must be reliable enough that parties are confident they and other nuclear commanders trust they can use it during crises.
- **Redundancy:** The supporting network that connects the devices in the network must be sufficiently redundant to ensure multiple means of connection and a high probability that the link is available at all times.
- **Interoperability:** The system must operate across global networks and systems without restriction to a single nation's communications standards.
- **Mobility:** Ideally, the system should be designed to work in any location, at any time, including in remote geographic areas on any continent, on a high-altitude aircraft, or on a vessel deep below the ocean's surface. In practice, achieving intercontinental range may be a minimum performance requirement to connect with supreme nuclear commanders, with some nuclear forces beyond the range of the initial system.
- **Bandwidth:** The hotline system should enable, at a minimum, "thin-line" (low-bandwidth) communications to enable transmission of text. A higher-bandwidth system could enable faster message delivery and enhance the diversity of communication channels.
- **Accessibility:** The system must be scalable and accessible to global leaders.
- **Trustworthiness:** The design and development process must merit and instill assurance that the system is secure and reliable. The system itself must have strong protocols in place for validation and verification of users—in other words, a demonstrated usable and effective means of confirming the right person is "at the keyboard."

## Components of CATALINK: Puck and ROCCS

CATALINK will be designed to satisfy all these requirements. This hotline will be a simplified and resilient communication system that includes at least two secure endpoint

[12] A high-altitude electromagnetic pulse (HEMP) caused by nuclear weapons bursts in the upper atmosphere or near space could potentially disable communications systems. HEMP may not be a major concern for nuclear attacks from the DPRK; but any major nuclear power would be capable of executing a HEMP attack that could cause systems to fail. Developing a communications link that is resilient in the face of such attacks could have the side benefit of protecting the capability from space weather-induced EMP effects, such as the 1859 Carrington event. See "Solar Storm of 1859," in Wikipedia, April 16, 2020, https://en.wikipedia.org/wiki/Solar_storm_of_1859

devices: the “Puck,” named for their relatively small size and durability, and the “Resilient Omni-frequency Crisis Communication System,” (ROCCS)—an associated relay device and redundant networking system. Each of these elements is described below.

## Endpoint Devices: The “Puck”

Each “Puck” would be a bare-bones computer designed for a single purpose: enabling the encryption and transmission of short, text-based chat, and possibly images and voice. Puck devices would have as few component parts as possible to maximize resilience and security.

A key feature of the Puck is its “radical simplicity.” These devices would effectively be ultra-modern versions of the two-way digital pagers used in the 1980s and 1990s, but with firmware built-in, state-of-the-art security. The highly simplified device would be “open source down to the silicon” in design. That is, the software, firmware, operating system, and hardware would all rely on secure, reliable, and proven open-source technologies.[13] The use of open-source technology will help ensure transparency and increase justified trust among users that there are no inherent or hidden vulnerabilities. The system would employ new and emerging technologies that make communications systems more secure and stable than previously possible. The following are additional design specifications for the Puck, which will continue to evolve:[14]

- **Processor:** The Puck would use *RISC-V* (pronounced "risc-five,” which is short for “reduced instruction set computer”), an open-source hardware instruction set architecture (ISA).[15] All parties seeking a trustworthy processor for their Puck can design a suitable processor for themselves or select from among existing open-source designs. Then, parties can fabricate the processor at the foundries they find most trustworthy, which allows for domestic sourcing. Additionally, the device makeup could consider starting with an FPGA, and use the 32-bit architecture to save space/power/effort.
- **Data transmission:** The device would have a single HDMI input to enable the transfer of data and display of images or other graphic content.
- **Power:** The Puck would be powered with 12-volt DC electricity delivered through a battery, generator, or external power supply.
- **Text Input:** The device would include a single micro USB input to allow a keyboard or screen connection.
- **RAM:** The Puck would have 1GB of RAM, which would be relatively inexpensive and likely suffice for the purposes of the device.

[13] The details of these requirements are further elucidated below, but best summarized in the submission for the workshop by Ron Minnich.
[14] These specifications were proposed in the October 2019 workshop. See Appendix I for more details.
[15] “RISC-V Foundation | Instruction Set Architecture (ISA),” RISC-V International, accessed May 1, 2020, https://riscv.org/

- **Firmware:** The Puck would use OREBOOT ("coreboot without 'c'"),[16] which is designed to support Linux payloads and to target truly open systems requiring no binary blobs.[17] The booting process would use a "root of trust" (RoT)—a hardware-validated boot process that verifies on a step-by-step basis, starting with an anchor that cannot be modified.
- **Kernel:** For the core operating system, the Puck would use seL4, which has end-to-end proof of implementation correctness and security enforcement.
- **Encryption:** The Advanced Encryption Standard (AES-256-GCM) could be used for encryption, but to encourage international participation we would not exclusively adopt this aging National Institute of Standards and Technology (NIST) standard. Rather, each sender would choose their favorite AEAD cipher, with symmetric rather than public keys to dispel worries about quantum resistance. The system would require users to exchange keys via an in-person encounter in advance of any potential crisis. (A more complete description of the encryption process and key exchange can be found in Eric Grosse's paper, "Hotline Cryptography."[18]) More widely used versions of the system could use an expanded system of public key cryptography whereby users can determine that a sender really is who they purport to be in a crisis context.
- **User Verification:** For confirming endpoint operator identity and authorization in a pragmatically secure fashion, the current state-of-the-art is password plus FIDO U2F Security Key. However, it could be reasonable to talk with an independent group that wants to make PIV / CAC cards and foreign analogs, which are well-supported substitutes for U2F.

There is another requirement, which is arguably implicit, but perhaps worthy of being called out separately. This has to do with the quality of the communication—for example, no missing words, no erroneous spellings, no erroneous translations similar to the errors introduced by smart phones as they "auto-correct" spelling and choice of words.

## The Network: "ROCCS"

The "Puck" will allow users to enter and encrypt a message containing text and ideally images. These devices would then connect to a transmission node within the ROCCS, which could convey the message using one of a variety of redundant networks, depending on the availability of options and the type of message sent.

Although the Puck would not necessarily be powered on continuously, ROCCS would always be connected and awaiting a signal. A read receipt would not be sent until the recipient's Puck decrypts the message. The Puck and ROCCS would connect only

[16] Oreboot/Oreboot, Rust (2019; repr., oreboot, 2020), https://github.com/oreboot/oreboot
[17] See "Binary Large Object," in Wikipedia, March 20, 2020, https://en.wikipedia.org/w/index.php?title=Binary_large_object&oldid=946463002
[18] See Eric Grosse, "Hotline Cryptography" (GitHub, 2019), https://github.com/n2vi/hotline

periodically. The time for booting the Puck, entering a message, sending the message, and decrypting and reading the message would take roughly 10 minutes. This timeframe is a best-case scenario, when the receiving Puck and its operator happen to be ready to receive a message. It is intended as an estimate of the time it takes for low-bandwidth radio delivery and initial human translation. This time might be reduced greatly by having each Puck-user dyad create sets of prearranged, pre-translated "anticipatory" messages—with understood meaning in all languages and military contexts—stored in advance.

ROCCS would operate primarily as a minimal, low-data-rate network, with the possibility of adding a switch or software to use other networks as needed—for example, satellites, commercial networks, fiber-optic lines, and high-frequency or low-frequency radio bands. ROCCS would necessarily operate in a range of conditions, including at the brink of nuclear war and after the world has gone over the brink and is in free fall into a nuclear cataclysm. The ROCCS must be available for the following three scenarios, which illustrate various stages of a nuclear crisis.

**1. Routine non-crisis world of multiple nuclear-prone conflicts**

In this world, nuclear weapons states are in a general, but not immediate state of deterrence. States have the capacity to use nuclear weapons against an adversary but have no immediate intention of doing so. In this context, the Puck would require only basic network support to test readiness and establish the system is available and working. With this baseline, allow nuclear commanders could train on the Puck devices, and establish confidence that Puck-based communications will be available as needed.

In this relatively stable context, CATALINK can be supported by a variety of existing channels including the commercial internet, ideally with enhanced quality of service achieved by tactics such as prioritizing certain types of data or reserving bandwidth from commercial internet-service providers.

**2. Crisis world of nuclear-prone conflict**

In this world, two or more nuclear weapons states are on alert and are either poised to use nuclear weapons or are engaged in a conventional war that could escalate to nuclear war. In such a pre-nuclear war crisis, the primary purpose of CATALINK would as a mechanism for states to back away from the brink of nuclear war. In such cases, ROCCS could rely on one or more channels, including commercial communications systems, space satellites, digital-over-fiber-optic cables, and radio.

ROCCS could also rely on private communication networks deployable if other systems are failing or are no longer available. These networks could be established at the intercontinental level (for example, between the United States, United Kingdom, France, Russia, and China) or to facilitate shorter-range communications at a regional level—for example, between India and Pakistan or South Korea and North Korea.

## 3. Nuclear war world

In the event of a nuclear war, the primary purpose of ROCCS would be to enable communications among nuclear commanders to terminate the conflict—regardless of whether the conflict is limited and local, or a global, all-out nuclear war. In this situation, other communications systems are likely to be interrupted: space satellites may be lost, radio signals may be degraded as the atmosphere is perturbed by nuclear detonations, fiber-optic cables may be severed, human network operators may be incapacitated, and nuclear commanders and command posts may already be annihilated.

To survive in an ongoing or post-launch scenario, ROCCS would need to be geographically resilient, autonomously operating, available round-the-clock, and survivable against all credible attempts to destroy it. Commercial networks alone would be insufficient for an ongoing or post-launch context as they are engineered to favor efficiency over survivability and tend to be over-reliant on other systems that may be compromised. In addition, commercial networks for wireless and satellite communications also tend to use narrow and well-known frequency bands that can be easily jammed with low-quality, high-power radio frequency noise generators and cheap antennae.

In these dire circumstances, *ad hoc*, improvised meshed networks could connect surviving Pucks through existing or new relay nodes. The effort could be supplemented by specific emergency relays and measures, such as balloons, drones, emergency rockets, emergency cubesats (miniature satellites), smart phones, high-frequency radio, very low-frequency radio, and other channels.

Mesh networks could present a promising alternative in a degraded environment. For example, a wireless mesh network was the only network available in New Orleans following Hurricane Katrina,[19] and a mesh network aided communications at Ground Zero following the 9/11 attacks.[20] Such a network would have to be designed at a global level. Capacity to implement such a system is already available in the private sector.[21] Options for mesh networks that could help send signals across oceans could include ship-to-ship, air-to-air, and ship-to-air connections.

A variety of options are available to keep ROCCS operational in an ongoing or post-launch scenario:

---

[19] Tim Greene, “New Orleans’ Wi-Fi Network Now a Lifeline,” Computerworld, March 17, 2006, https://www.computerworld.com/article/2562696/new-orleans--wi-fi-network-now-a-lifeline.html

[20] See Mitchell L. Moss and Anthony Townsend, “Response, Restoration, and Recovery: September 11 and New York City’s Digital Networks,” in Crisis Communications: Lessons from September 11, ed. by Michael A. Noll, Kindle (Lanham, Maryland: Rowman & Littlefield, 2003), p. 63.

[21] Existing private-sector solutions for mesh networks, such as GotennaMesh, could serve as models. See “GoTenna Mesh | Text & GPS on Your Phone, Even without Service,” goTenna Mesh, accessed May 1, 2020, https://gotennamesh.com/

- Ultra-low frequency (ULF) and very low-frequency electromagnetic waves can transmit low data-rate signals
- Ultra-wideband or “omni-frequency” transmissions require little energy to transmit short-range, high-bandwidth signals
- Highly directional, “smart” antenna arrays connected through a mesh network of antennae that could be ground-based (either fixed or mobile), sea-based on ships or rigs, or possibly on Loons (polyethelene balloons developed by Google X)[22] operated over international waters.

Of these options, a sea-based mesh network would likely present the least regulatory resistance and would have maximum resilience during a nuclear, biological, cyber, and conventional attacks. Air-based radios on planes likely would encounter regulatory pushback from the Federal Aviation Administration (FAA) and other agencies and would be more vulnerable during an offensive. Ground-based systems would be subject to regulation by the Federal Communications Commission (FCC) and also would be considerably less resilient in a nuclear exchange. Satellites will have limited options for size and power consumption and could be cost-prohibitive to launch and operate non-commercially. Finally, undersea wireless and acoustic transmission may be limited by distance but should not be discounted without further investigation.

The ROCCS would be an “always-on solution” with a constellation of continuously operating assets rather than a system that requires humans or autonomous systems to deploy a surge of new physical assets in an emergency. Network nodes such as balloons, drones, and cubesats would be unpredictable in real-world settings if they sit idle most of the time without constant testing, to be deployed only in an emergency. Like a nuclear submarine that never leaves the dock or fire engine that never leaves its station, an emergency network that is unused on a regular basis is unlikely to work when the time comes. Feedback from an always-on network permits continual network verification and optimization and limits the potential for adversaries to analyze traffic and usage patterns: anomalous traffic may be quickly analyzed if it bursts up on-demand, but if the encrypted traffic is constant then there is no information revealed about the timing of communication in a constant stream.

An important dimension of developing CATALINK is that this iterative process will continue to revisit new and tougher use scenarios that redefine technical requirements—and therefore the design and implementation—of the Puck and ROCCS, even as they are developed. A set of possible test cases is provided below.

## Developing Norms and Protocols

Effective systems require clear protocols for usage. CATALINK will also need well-established norms to ensure that users deploy and use it when crisis erupts. If users

[22] See “X - Loon: Expanding Internet Connectivity with Stratospheric Balloons,” X, the moonshot factory, accessed May 1, 2020, https://x.company

ignore or forget the system exists—or they are not confident about using it when the need for communication is most urgent—the system will be useless. Governments using the network will need to invest time for training, develop programs and protocols to build familiarity and trust between users and operators, and conduct regular "rehearsal" exchanges between senior-level decision-makers and staff outside of crisis, so that operators become familiar with operations. Protocols may be necessary to:

- Facilitate the exchange of cryptographic keys among users of the system;
- Ensure continuous availability to senior-level decision-makers. Just as the U.S. President is always accompanied by a person who carries the nuclear codes, so too the Puck needs to be immediately available wherever the supreme nuclear commanders are located;
- Verify the identity of the person on the other end;
- Ensure the system's technical integrity and validate it is always on through regular testing, a daily "ping," and rehearsed exchanges under various conditions;
- Update the system and add or remove users from the network;
- Establish prearranged messages with associated codes that can be understood instantly on the other end and to minimize the need for interpretation and risk of misinterpretation and/or mistranslation, including "distress codes" to warn of potential compromise of the system's integrity; and
- Set expectations for speed of response. If a user sends a message and is required to wait for an extended period, it can create distress and confusion and that can feed into escalatory dynamics.

Countries using the CATALINK network will need to create confidence and breed familiarity within their own bureaucracies through trainings and regular exchanges between users at the staff and senior decision-maker levels. Ideally, users and staff from different countries will regularly convene to discuss the system, ensure it is verifiably secure, make any required upgrades, and plug the system back into their respective bureaucracies.

Governments may be reluctant to implement the CATALINK system if they lack trust that the devices were designed as promised using open-source methods. As a result, they may want to have control over the actual fabrication of the Puck. Thus, the finalized schematics for the Puck could be shared with users for them to oversee production in their own trusted manufacturing facilities. Necessary processor chips could be fabricated in domestic semiconductor fabrication plants. If countries are not able to manufacture or fabricate the components required, it may be necessary to establish an independent, neutral fabricator that could be subject to verification and audit.

## 3. CATALINK NEXT STEPS

The next steps in developing the CATALINK crisis communications system will be to secure funding to develop a prototype, while continuing to engage with technologists and policymakers to vet the concept, technical specifications, protocols, and norms. It will also be necessary to engage senior-level government officials and industry leaders from a range of countries including both nuclear and non-nuclear weapons states. There is no reason to assume the United States will be the first user.

### Developing the CATALINK System

The projected timeline below for prototyping of the Puck is a process that will require hiring a team of full-time employees to manage and direct the system's design. The roughly estimated cost would be between $10-12 million for development of an initial prototype over 12 months. The core team of engineers would include:

- A hardware expert to select which RISC-V SoC to use, review system schematics, and work with a vendor to review the manufacturing line;
- A firmware expert who understands what to code and what not to code;
- Kernel expert;
- Software expert;
- Cryptography expert;
- An integrator to integrate the other components and to ensure validation; and
- A project leader/coordinator.

Development of ROCCS would flow from development of the Puck. At the outset, it is assumed that the network would comprise up to nine Pucks, one for each national supreme nuclear commander. If the five NATO nuclear delivery states are included the system could include up to fourteen nodes. Designing for a nine-endpoint network would enable the team to make rapid progress on a network architecture. Subsequent iterations could include additional nodes if desired.

The following proposed development plan to build ROCCS is designed to operate in the most demanding case—a post-nuclear war environment. We could accelerate this process depending on the size of the team and availability of funding.

**Months 0-6 (estimated budget: $1-2M)**

1. Investigate and verify regulatory feasibility of chosen wireless mesh network (for example, sea-based).
2. Design the software and hardware for the ROCCS wireless mesh router.
3. Build a mesh network software simulator without ROCCS radio.
4. Build a limited function prototype with fewer than 10 nodes.

**Months 6-12 (estimated budget: $7-10M)**

1. Develop the network with software-based radio.
2. Test ROCCS in varying conditions.
3. Pilot the network on a small network of 100 nodes.

**Months 12-24 (proposed budget $10M)**

1. Optimize the network in global field tests with 1000 nodes.
2. Estimate investment and operating budget based on prior stems.
3. Launch ROCCS with support of nine to fourteen nuclear states.

The processes of designing the hardware, firmware, and software could begin simultaneously. Additional time would be required for final review and running schematics. Each component would have to go through a quality check before it is integrated. Following initial development, an iterative process of red-teaming and open hacking could be used to test and refine the security and stability of the system.[23] Simulations could also be useful for testing the system in a variety of circumstances, though participants noted there are limits to the degree to which simulations can effectively replicate all the variables and dynamics of a real-world crisis situation.

## Building a Community of Interest

Engaging governments to participate in this new hotline system is a critically important challenge, particularly if their countries do not already have hotlines or understand their potential value. Even if commanders are convinced that CATALINK is necessary and effective, they may face skepticism within their leadership and staff about the suitability of a system built with open-source technologies. Other practical factors must be addressed in each user context, such as legal infrastructure, organizational and technical capacities, and funding, all of which will be needed to participate in this new crisis communications network. Managing CATALINK's implementation and governance process will require strategic planning and strong leadership.

A high-level international governance board could be helpful to lead the development of the system and engage key decision-makers. Organizations noted as possible prospects for collaboration include the BSI Group (British Standards Institution), the NIST, the Hewlett Foundation, and Open Philanthropy.

Identifying a small set of "first adopters" will help build a base of champions for the project. Given the potential mistrust that might result if the project emerges in only one state or originates in one of the large nuclear powers, non-nuclear nations could be

[23] Workshop participants stressed the importance of finding the right balance in managing an open-source process. It was noted that open-source processes sometimes lack effective coordination and fail because they are too decentralized; on the other hand, having too strong a leader (a "benevolent dictator") can also be detrimental to the process. Ultimately, it was decided that, although the technologies used in developing the "Puck and ROCCS" system should be open-source, the development of a prototype should be closely directed. An open-source competition could be useful at a later stage for stress-testing or penetration-testing the device and network once they are built.

ideal candidates to help spearhead this process because they have a stake in the outcome and sufficient resources and influence to make a difference. Germany could be a strong contender, as its government is already pushing advanced technical systems for official use that are based on open-source technologies. South Korea and Japan are also potential champions for the effort. Another potential approach could be a governance grouping from states that are not part of the extended nuclear weapons umbrella, such as Australia, Brazil, Sweden, South Africa, and Switzerland.

The implementation process could build upon existing programs and processes, such as the post-pandemic Nuclear Non-Proliferation Treaty review process. It may also be useful to connect the project with the Joint Data Exchange Center (JDEC), set up between Russia and the United States for the exchange of information related to missile and space launches. Another model for this globally integrated system is the international monitoring system, a network of 321 standardized stations around the world that all connect into an international data center for tracking nuclear explosions.

## CONCLUSION

Limiting the threat of nuclear war remains one of the most important challenges facing humanity. This challenge will become more difficult as NC3 systems confront artificial intelligence, cyberattacks, and other emerging technologies. NC3 systems face these new pressures even as the strategic context in which they operate becomes more complex, less stable, and more chaotic, all of which will only accelerate with continued urbanization, globalization, and the proliferation of nuclear weapons in new countries and, potentially, non-state actors.

We envision CATALINK as a solution to a global problem that requires global participation. We welcome feedback and input on the concept for CATALINK. We have also opened a Slack channel that you can request to join. Please send requests, thoughts, or ideas via email to CATALINK@tech4gs.org

# APPENDIX 1: "ANTIDOTES FOR EMERGING NC3 TECHNICAL VULNERABILITIES" SCENARIOS WORKSHOP

## Origins of the Workshop

To explore emerging issues associated with modernization of global NC3 systems, Technology for Global Security (Tech4GS)—together with diverse partner organizations—hosted a series of multi-sector discussions between October 2018 and October 2019. These workshops brought together a cross-section of participants who would otherwise not typically converge, including experts from fields such as nuclear policy, law, engineering, computer science, and security.

The first workshop, *Social Media Storms and Nuclear Early Warning Systems,* was held in October 2018 to examine the possibility that social media could inadvertently or purposefully trigger nuclear war.[24] Former government officials and current global industry leaders discussed how social media might interact with the early warning systems of nuclear-armed states, and how the potential changes in the propensity of leaders could potentially lead to war. Officials from the U.S. situation rooms at the state and federal level, as well as top leadership at private entities, identified the scope and impact that social media has on international strategic stability. The workshop resulted in a four-part special report series focused on the underlying themes discussed. This discussion was hosted by Technology for Global Security and held at the Hewlett Foundation campus. The workshop was co-sponsored by the Nautilus Institute and the Preventive Defense Project - Stanford University, and funded by the MacArthur Foundation.

The second workshop, *NC3 Around the World*, was held at the Hoover Institute in January 2019 to focus on the impact of NC3 systems on global security.[25] This workshop featured discussions based on over 30 readings and presentations by practitioners, academics, experts, and opinion-makers in the field with specific skills-sets.[26] The workshop focused on the potential for emergent effects within the highly complex "meta-system" of NC3 systems, particularly given the superimposition of emerging technologies such as artificial intelligence and quantum computing. The workshop revealed that, under stress, NC3 systems may (and some will) fail robustly, which could in turn lead to a nuclear war.

---

[24] Nautilus Institute, Technology for Global Security, Preventive Defense Project, "Social Media Storms and Nuclear Early Warning Systems: A Deep Dive and Speed Scenarios Workshop Report," NAPSNet Special Reports, January 08, 2019, http://nautilus.org/wp-content/uploads/2019/01/Social-Media-Nuclear-War-Synthesis-Report-Final-Jan8-2019.pdf

[25] Peter Hayes, Binoy Kampmark, Philip Reiner, and Deborah Gordon, "Synthesis Report–NC3 Systems and Strategic Stability: A Global Overview," NAPSNet Special Reports, May 05, 2019, https://nautilus.org/napsnet/napsnet-special-reports/synthesis-report-nc3-systems-and-strategic-stability-a-global-overview/

[26] All these papers have been posted at www.nautilus.org and www.tech4gs.org

At this workshop, Eric Grosse, former VP of Security and Privacy Engineering at Google, presented the initial concept of a radically simplified communications system—a private, highly secure "thin line" that might enable connectivity for nuclear commanders. Built on the idea that "complexity is the enemy of security," the concept for a new, highly secure communications built on open-source technologies became the focus of a third workshop, *Antidotes for Emerging NC3 Technical Vulnerabilities*. This workshop was held October 21-22, 2019, on the Stanford University campus in Palo Alto, California. This addendum draws on the dialogue, notes, and records of the workshop and on the ten expert presentations delivered on October 21. (These will be published separately after this report is published).

## Workshop Objectives

Attendees of the October 21-22 workshop refined the plan for the development of a secure, reliable, trusted communications capability that could augment existing systems, which are potentially vulnerable to failure in future situations. The proposed open-source option would be designed, developed, and proven by private and public actors. In other words, participants were tasked with determining whether open-source technology solutions could be used to bridge the gap between technologies that are in place and technologies that need to be in place to enable crisis communications and avert nuclear disaster.

The stated objectives of the workshop were as follows:

1. Explore a range of risks and vulnerabilities of today's NC3 communications systems and clarify the stakes of failure.
2. Identify a set of design criteria for a simplified, secure, reliable, trusted hotline that could enable direct communications for heads of state, as well as other use cases such as lower level state-to-state communications, intra-military communications, engagement with non-state actors, and disaster response in different scenarios.
3. Ensure the approach increases the credibility of NC3 postures globally, particularly in the face of risks introduced by emerging technologies like cyberwarfare and artificial intelligence.
4. Ground the solution in learnings from the private and global sector, with a view to striving for technical simplicity and global participation.
5. The solution in learnings from the private and global sector.
6. Identify next steps to bring forward a vision for an augmented communications system that would help de-escalate conflict.

Over the course of two days, the workshop's participants focused on learning about elements of the challenge—including NC3 vulnerabilities, hotlines, and nuclear communications—before working collaboratively toward a technical solution with specifications for hardware, software, encryption, and network. In addition, participants

identified a framework for practical implementation with norms of operation and a process for engaging with potential stakeholders. As a focal part of the workshop, participants broke into groups to engage with four scenarios that were designed to highlight different communications challenges likely to emerge among adversaries and allies—including leaders, commanders, and interlocutors—in the course of nuclear and conventional crises, with the goal of refining the concept of a global crisis communication system.

The workshop brought together a diverse group of stakeholders with expertise in a variety of domains, who were chosen for their potential to tackle the question from a variety of perspectives. A key goal was to facilitate the integration of concepts and emerging technologies from the private sector and to narrow in on a communications solution that various stakeholders such as heads of state and military leaders would consider to be trustworthy.

Through the workshop, participants collaborated to “wind-tunnel” the concept of an integrated, alternative crisis communication system that would be developed from the “ground up” using open-source methods and technologies. The workshop used Eric Grosse’s proposal as the foundation to explore the development of a secure, reliable, and trusted communications capability that could augment existing systems that are potentially vulnerable to failure under stress.

**NC3 Overview**

A series of brief presentations grounded participants in some of the potential vulnerabilities in existing NC3 systems. Despite the complex technical components of NC3, humans are ultimately responsible for decision-making in nuclear crises, and senior decision-makers may not train sufficiently in considering the pragmatic and ethical dilemmas likely to arise in a nuclear crisis. Another challenge is that crises or conflicts could potentially magnify existing gaps and weaknesses, which result from streamlining the development and deployment of NC3 resources to increase efficiency in periods of peace. In some cases, the quest for efficiency has led to the development of systems that are used for both conventional and nuclear conflict. This entanglement could add to confusion and vulnerability during an escalating crisis. Dual-use systems could also add to the risk because they may be viewed as legitimate targets during a conflict.

An overview of the NC3 system in the United States noted the infrastructure comprises more than 200 different systems. Only 102 systems are known in the unclassified world. These systems are housed across different agencies and branches of the military, and roughly 39 percent of systems could be possible candidates for integration of artificial intelligence (AI). The rapid advancement of AI is another major concern for the stability of NC3 systems as leaders are increasingly turning to machine learning and other algorithm-based systems that may behave unpredictably or be vulnerable to cyberattack. In a nuclear crisis, AI might be used to support important roles like dynamic

targeting; for example, choosing targets based on real-time assessments of weather patterns, traffic patterns, casualties, and other variables. AI can be integrated into communications; for example, it can be used to pull signals out from transmissions that are difficult to parse and could allow for the continuation of communications in denied environments.

Of concern in the emerging AI space are deep neural networks—consisting of more than two layers of neural networks—that are programmed to learn by themselves. Many of the processes involved in NC3 could be clear use cases for neural networks, including sensing, computing, and communication. Yet these systems have been known to produce false positives and require rigorous testing and continuous quality control. Neural networks must be retrained and redeployed, which requires not only structured organizational processes, but also the ability to generate and input large amounts of training data. The integration of deep neural networks into key decision-making inputs—including modulation recognition (encoding data from one signal to another for transmission), image recognition, transcription, anomaly detection, and voice recognition—could add to uncertainty in escalating crises. As military commanders grow more likely to turn to AI-based decision-making under time pressure, it reinforces the need for robust communications systems that can help verify information or ascertain the accuracy of AI-based assessments.

**Nuclear Communications Overview**

A second panel featured a series of presentations on communications in the context of nuclear crises, including how and why adversaries use hotlines to communicate. While few unclassified details are available about the operations of existing nuclear hotlines, in general, hotlines serve as a direct communications link between the top leadership of governments. They generally operate on a point-to-point basis from a fixed location (though this need not be the case). Their primary purpose is to decrease the risk of conflict under tense political circumstances.

Hotlines also help with the signaling of power and resolve that typically takes place during conflicts. They can reinforce or clarify other signals that may be sent by the military or other sources. These systems can also help with the exchanging of offers necessary for resolving crises. Hotlines play a key role in providing clarity when information is scarce; for example, helping to avoid misperception of adversary's actions or to clarify actions taken that may appear dangerous to the other side. Key features of hotlines include speed—if events are spinning out of control rapidly, it is valuable to be able to connect directly to an adversary—and secrecy—particularly if there are domestic or international audiences from whom negotiations should be kept private. Although direct communications are the primary objective, the decision to use a hotline may itself send tacit messages; some may say the choice to use a hotline signals weakness.

The use of hotlines in the past has relied in part upon a degree of pre-established trust and familiarity. Norms play a key role in the nuclear sphere broadly, as countries have developed a range of shared practices designed to minimize the risk of inadvertently triggering the launch of nuclear weapons, for example, separating missiles from warheads. Norms are important because they help bridge the gap between major states and smaller states that may come into possession of nuclear weapons. It can be challenging to establish norms across cultures, however, and how norms are interpreted can vary across contexts, thus, clearly defined systems and standards can also help reduce differences of understanding.

As part of this discussion, a presenter noted the importance of distinguishing between nuclear attacks that are intended to disrupt communications and those that have a degrading effect on communications as a byproduct. Even small attacks can have large communication impacts. For example, the attacks of September 11, 2001, (a relatively small attack by nuclear standards) led to a chain of events that crippled communications systems aboard Air Force One and led to confusion among U.S. military leaders. The presentation emphasized the importance of senior leaders practicing, researching, and anticipating potential threats and placing themselves in empathetic position vis-a-vis their rival(s).

**Designing a Solution**

To help set a baseline understanding of the proposed crisis communications system, workshop attendees read and discussed "The Pitch," a proposal for the network rooted in Eric Grosse's paper that included initial design considerations and a rough project plan. A discussion about this proposal identified the importance of distinguishing the concept of hotlines from the broader NC3 framework, which typically focuses on intra-military communications—receipt and transmission of early warning, decision-making, and distribution of command orders.

Following this "stage-setting" discussion, a third panel focused on various elements that would be required for the development of the proposed crisis communications system. Part of this conversation included an overview of the open competition-based process used to develop the Advanced Encryption Standard (AES) in the late 1990s. This process successfully led to the development of a widely accepted global standard that is used in an array of highly sensitive daily operations. AES was the result of a multi-year, open, transparent, and international design competition led by NIST. This model was considered useful because a clear vision statement drove it, which called for "an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century."[27] The project's success was rooted in part in a high level of pre-established trust among participants, who came from an

[27] National Institute of Standards and and Technology, Department of Commerce, "Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard" (Federal Register, January 2, 1997), p. 93, https://www.govinfo.gov/content/pkg/FR-1997-01-02/pdf/96-32494.pdf

existing community of interest and saw the process as fun and rewarding. Notably, the National Security Agency (where many of the world's best cryptographers work) intentionally did not participate in the process except to review and give feedback, to ensure the new encryption scheme would maintain credibility globally. Two lessons from this example are particularly salient: first, that the time invested in norms building and socialization imbued the final outcome with a high level of trust in the outcome; and second, that involving stakeholders from the beginning of the process is key to success.

Following this overview came a technical deep dive on secure communications systems, including a description of the trade-offs and potential solutions. A talk on communications networks noted the trade-off between bandwidth and speed laid out in Shannon's Law, which says the maximum reliable speed of a communication link is proportional to the width of the band and also depends on the received signal power divided by interference (or noise). Wireless mesh networks were introduced as a possible solution for networking because they can operate at any scale. Low-frequency signals, which are already used in some NC3 systems, can travel farther and can pass through obstacles, but also generate more interference that slows down the network. Although antennae used to send low-frequency signals have traditionally been very large, new technologies have led to the development of smaller antennae for extremely low-frequency (ELF) and very low-frequency (VLF). It was noted that naval ships could in theory host a resilient mesh network, and that satellites, radios on ships, and other solutions have different survivability constraints.

A presentation on the importance of designing systems to be secure "down to the silicon" stressed that malware can be introduced into firmware (the permanent software programmed into a computer's read-only memory) in most modern computing devices. Many of the components associated with commercial providers, such as Lenovo and Asus, have been found to include code with "bad hygiene." Exploits can be added at any level, so it is important to build systems from the "atoms up." New initiatives such as RISC 5 enable open-source silicon development,[28] and new firmware options like OREBOOT (written in a language called RUST and eliminating potential vulnerabilities associated with the C++ coding language) provide more assurances and fewer problems compared to traditional options.

An expert presentation on the importance of verification explained how mathematical proofs can be used to provide certification and ensure a system meets critical security properties. Some means of verification would be more appropriate than others in the context of a crisis communications system. For example, a verification approach that requires continual testing and refinement—sometimes referred to as "test, patch, and pray"—would be ill-suited for NC3 because it is used so rarely: "You send one packet every five years, but it had better get there." Certain proofs, like an executable

[28] See "LowRISC: Collaborative Open Silicon Engineering," accessed May 1, 2020, https://www.lowrisc.org/

specification, might be an appropriate choice for an international protocol as they are based in mathematics rather than a specific language, so they translate well.

### Use Cases: Crisis Communications in Different Scenarios

As part of refining the concept of the proposed communication system, attendees engaged with a set of four use case scenarios detailing different variations of escalating crises. The purpose of the scenarios was to help participants think through questions such as who might need to use a communications system in different contexts, what the nature of the communication would be, how much bandwidth would be necessary for the transmission of information, whether multiple parties would have to engage simultaneously, how much encryption would be necessary, and whether it would need to be designed for one-way or two-way communication.

The scenarios were designed to encourage broad thinking about when a hotline or other back-up crisis communications system might be necessary, based on different pressures and conditions. The scenarios were developed around two key parameters likely to have an impact on the design of the communications system: the *form* of the communication, ranging from one-way information sharing to two-way or multi-party negotiations, and the *nature* of the situation requiring the system's use, ranging from conflict to crisis. The four quadrants formed from the intersection of these two variables were used to develop four scenarios requiring:

- Communication among two nuclear powers, despite kinetic attacks and NC3 breakdown;
- Communication throughout command and warning centers, to make sense of kinetic activity suspected to be a result of an AI error;
- Communications with a violent non-state actor during a high-stakes crisis; and
- Communications among interlocutors to avert regional conflict.

Attendees fleshed out each of these situations into a scenario (see Appendix 2). Below are some key findings from the scenarios discussion that fed into the CATALINK design reported above.

- In contexts when cellular networks are available, encrypted apps like Signal likely offer sufficient levels of encryption for many communication needs, even in a crisis context. For example, in the scenario "The Hunt is On," in which the CIA seeks to make contact with a violent non-state actor threatening to detonate dirty bombs, the urgency of a stable connection would override the need for privacy.

- "Thin line" communications would be sufficient for most leader-to-leader exchanges because it could transmit text and possibly images. A system that integrates both voice and text would be ideal; telephone calls can be freewheeling, but text messages are relatively limiting and can lack nuance and a human connection. It was noted that voice is latency intolerant—that is, a delay

in transmission makes it difficult to converse—but for communications between leaders from different countries, a built-in delay may be acceptable as messages need to be translated.

- The network would not require video conferencing, which would require transferring large amounts of data. While this medium has value through interactivity and body language, it also presents risks such as the misinterpretation of body language, particularly among speakers from different cultures. Yet the use of images on the system may be useful if leaders want to communicate some proof an attack was an accident, for example, an image of a radar track or flight recorder information. In a situation where countries are trying to correct an error, it may be more important to share data.

- As any single path might be degraded,[29] a crisis communications system among heads of state should use different channels—including satellite, ground networks, high-frequency bands, ultra-low bandwidth, and VLF, which can propagate long distances but is relatively slow. The group proposed developing software or a form of "switch" that sends messages over different channels based on their relative length and data payload. The use of ground-based assets such as ships and airplanes, as well as commercial assets, could enhance the capacity of the network. A key question is ensuring the availability of sufficient bandwidth for necessary communications.

- A solution specifically designed for one situation would be difficult to use in other situations. For example, a communications network that requires the exchange of encryption keys might not be appropriate for engagement with violent non-state actors.

- The most effective use case for the initial demonstration of CATALINK would be in the context of leader-to-leader communications at the nation-state level. Given the parameters of the proposed system, establishing prior relationships would be essential for adoption, and for willingness and ability to use in a nuclear crisis. A communication system between top leaders would have to be used with enough frequency that individuals become comfortable to pick it up and use it. The system should be readily available and something stakeholders are willing to turn to in a fraught situation. There is a tension between having a system that is only to be used in extremis, while also making sure it is used frequently enough that people feel comfortable using it.

Based on insights from these discussions, the participants identified four key areas for further group development: the hardware requirements, the software requirements, the

[29] Examples of a highly degraded environment include periods of time following a nuclear explosion or solar storm, when the atmosphere becomes opaque to high-frequency communications for several hours.

protocols that would be necessary to ensure the network is used properly, and the steps required to generate political buy-in necessary for the system's deployment. While discussing the scenarios, the group determined that, although the system might eventually be useful in a variety of contexts, a thin-line, highly secure *leader-to-leader communications* system is the initially narrow application that is most likely to yield global benefits.

Engaging with specific examples allowed attendees to test concepts and understand the boundaries of thinking around the proposed system. The groups were asked to consider a variety of questions related to understanding the needs of a new crisis communications system and realizing the project. Questions included: How would the design criteria for the system be different from that spelled out in "The Pitch"? What is common across the different use cases—and what is different? How would you engage stakeholders to use the system? What are the threat environments? What are frameworks within which this system gets adopted? How would one engage the right people? What is the playbook to see this project move from conception to development to product launch? What practices or behaviors would have to be adopted for system implementation?

A wide variety of insights emerged from this debate. For example, while discussing the question of video conferencing, participants noted that this medium has value through interactivity and body language, yet requires transferring large amounts of data and presents risks—body language can be misinterpreted, particularly among speakers from different cultures. This insight helped determine that the communications system only needs to deliver text and possibly images.

The scenarios discussions also highlighted that, assuming cellular networks are available, encrypted apps like Signal could be sufficient for many communications needs, even in a crisis context. For example, participants determined that for a scenario focused on negotiations with a non-state actor, the urgency of a stable connection would override the need for security and the strongest possible encryption. One group considered an enhancement that could be added to existing cell phones that could reduce the operation of the device to a single function; that is, an "I Care Extra" button that would shut off everything but Signal or another encrypted communications app. Such an approach could limit the possibility that other apps or elements of the device could capture or transmit information. (A model for this is Tails, an operating system based on Linux designed to be used exclusively for secure anonymous communications.[30]) It was also noted that there are existing and commercially available devices that prioritize privacy and security, including Purism.[31] However, while solutions like Signal may be useful for some contexts, these apps may not work in China or other locations.

[30] See "Tails - Privacy for Anyone Anywhere," accessed May 1, 2020, https://tails.boum.org/
[31] See "Beautiful, Secure, Privacy-Respecting Laptops & Phones," Purism, accessed May 1, 2020, https://puri.sm/

Participants also noted that, while Americans tend to think about U.S. systems and vulnerabilities, a hotline network could be most valuable for countries that do not already have hotlines or secure communications capabilities. A global communications system could have broader diplomatic benefits by allowing the inclusion and connection of countries that are widely viewed to be untrustworthy or unsophisticated. Hotlines also have implications within governments; decision-makers may want a trusted system they can use without other parts of the bureaucracy knowing about their use.

Groups also noted there were numerous trade-offs in developing systems. A solution specifically designed for one situation might be difficult to use in others. For example, a communications network requiring the exchange of encryption keys would be inappropriate for engagement with non-state actors. Participants also weighed the importance of having the capability to link together multiple parties involved in complex negotiations.

Discussants considered how different media affect communications and how user interfaces can affect trust. They considered the trade-offs of voice versus Text exchanges. Telephone calls can be freewheeling, but text messages are limiting. Moreover, if leaders do not speak the same language, they could miss nuance, and it can be difficult to establish a human connection. On the other hand, groups noted the potential for increased efficiency by having pre-rehearsed moves that can be communicated in a succinct way; for example, “I intend to stand down.” In a situation where countries are trying to correct an error, it may be more important to share data than to text back and forth.

The scenarios shed light on the cultural and institutional factors that help shape communications. The technical aspects of the connection are less important than the norms determining whether two people can connect in the first place. Technology will not resolve issues of trust, and use of a different technology will not affect how the message is received. Successful communication is embedded in existing relationships. If you send a message via phone, you send it to someone you know or who knows you. Creating opportunities for people to connect with appropriate government officials could facilitate communications. (One group proposed the “I have a dirty bomb hotline.”) Groups also considered whether a highly secure system could have “dual-use” implications; in other words, whether terrorists or other nefarious actors might employ it for criminal intent. Addressing concerns about the dual-use potential will be necessary to ensure the political viability of the project.

Key insights emerged from the discussion:

- A communication system between top leaders would have to be used with enough frequency that individuals become comfortable picking it up and using it. (This point led to a robust discussion around norms and protocols summarized in the main body of this report.)

- Existing communications infrastructure is more fragile than commonly understood to be, because so much rides over one infrastructure and there are dependencies on power infrastructure.
- The question of verification was raised across the scenarios, as the parties exchanging messages need a way to confirm the identity of the people they are speaking with and that the messages they are receiving are the messages being sent.
- Security is not always an important consideration. For example, when engaging with a non-state actor threatening to detonate a nuclear device, having strong cryptography is less important than the speed and reliability of the connection.
- If facsimiles of the CATALINK become widely available, simply having the system installed could be a signal that someone intends to do something dangerous.
- An inherent challenge in a hotline system is that it would not be used frequently enough to ensure the quality control that usually comes with open-source development.
- A highly secure communications system could be attractive for criminals and may also be adopted by militaries for internal communications. The potential dual-usages of the system could hinder political adoption.
- A bad actor who wanted to use a radio-based transmission system might choose to hide in an urban area with lots of radio noise to avoid detection.

The system should be readily available so that stakeholders are willing to turn to in a fraught situation. There is a tension between having a system that is only to be used *in extremis*, while also making sure it is used frequently enough that people feel comfortable using it.

The teams then reconvened and considered what changes they would make to their team's solution, including how it might be used for intra-country communications and non-nuclear global crises. Each team then presented the scenarios and their solutions to the other teams through an "around-the-world" format (moving from table to table, with one spokesperson staying behind to explain the solution to the other groups). These conversations aimed at probing how their solutions could be improved.

Overall, the group was positive about moving forward, and each participant made individual commitments to advance from the drawing board to tangible project development. Workshop participants appreciated that conversations focused on a specific question with direct application to a real-world problem. Some noted they would bring back the concept to their respective communities of interest, while others said they would focus on researching answers to questions that emerged in the discussion about CATALINK.

## APPENDIX 2: SCENARIOS

Participants in the workshop used scenarios to explore how communications among actors might vary in different types of escalating conflicts and identify the trade-offs required for the design of a global crisis communications system depending on how, when, and in what context it is used. These scenarios became starting points for discussions around how the design and operation of a global communications system might vary based on different use cases. Note that these scenarios were considered flexible and some were changed during conversation.

### Scenario A: Kinetic Escalation

Long-simmering tensions between the United States and China come to a head in the Taiwan Straits when a clash involving a transiting U.S. aircraft carrier battle group results in the loss of a U.S. frigate and two Chinese attack submarines. Recently deployed machine learning-based automated response systems appear to have played a role in the initiation of kinetic activity. Each side deploys search and rescue operations in the same zone, with constant risk of collision or other inadvertent engagement. The crisis escalates as a U.S. C3 satellite-based communication link fails without clear reason; a Chinese cyberattack is suspected but cannot be proven. Meanwhile, U.S. intelligence receives reports that Chinese mobile intercontinental ballistic missiles are receiving possible fire orders over dual-use communications links. The United States signals its resolve to China's leaders by issuing a "clear to air" alert and flying nuclear-capable bombers to the region. Concerned about the risks of further escalation leading to nuclear first-use, U.S. and Chinese leaders want to negotiate, but neither leader wants to be the first to make a call, fearing the move will show weakness.

### Scenario B: Red Sky in Morning

U.S. and ROK commanders are alarmed when the Korean People's Army (KPA) forces deployed along the demilitarized zone go to their highest alert level with no warning or apparent reason. U.S. signals intelligence detects signs of troop and heavy vehicle movement in some provincial cities, but the entire country seems to be on lockdown or underground. DPRK-controlled social media channels transmit threats to attack the ROK, Japan, and the United States with nuclear weapons. The DPRK shuts down all diplomatic channels in Pyongyang and all traffic in and out of the DPRK by land, sea, or air. The DPRK UN Mission in New York does not answer its phone. South Korea's president issues a warning that it will take "all necessary measures to protect its security." UN Command, headed by a U.S. general, requests that his Korean People's Army counterpart explain the alert and, receiving no response, sends this request via the inter-Korean hotline, to which the KPA does not respond. No single state is sufficiently trusted to orchestrate the collection and pooling of disparate information collected by each state's HUMINT and national technical means. Machine learning-based analytical tools are available, but system opacity and releasability prevent collaborative use. A private network mobilizes to establish secure communication back

channels with key North Koreans inside and outside of the DPRK, as well as through counterparts in companies that have algorithmic means for OSINT analysis. The network shares this critical deep insight with trusted interlocutors, who then need to convey that information via secure communications links back to trusted intermediaries in key capitals.

### Scenario C: A Bad Model

Tensions with the Russian Federation mount as a NATO aircraft inadvertently launches multiple AGM-158 air-to-ground missiles, striking Russian 9K720 Iskander batteries within the enclave of Kaliningrad Oblast. Russian leaders had long expressed concern about the intentions behind the NATO exercises that caused the launch, and Moscow interprets the incident as a purposeful escalation toward seizing Russian territory. As Russia alerts conventional and nuclear forces in theater, a U.S. early warning system designed to detect anomalous signals of an imminent nuclear attack—relying on a stack of AI-enabled decision support systems—reports an increasing and unprecedented probability of counterattack. As the engineers who manage the system struggle to understand the causes of the alerts within the deep learning systems, private company intelligence suggests that a Russian cyberattack in the past may have corrupted the AI models by manipulating the training data sets. There is a growing belief that the warnings of increased alert and dispersal of Russian strategic nuclear forces may be false positives, but no one can immediately resolve the uncertainty. Operations, warning, and signals assessment centers seek verification and validation to understand what's happening to avoid chaos, but there are no established lines of communications or protocols for resolving this type of crisis—much less a reliable means for doing so given the current uncertainty. In the context of heightened tension between European states, NATO, the United States, and Russia, there is an urgent desire to understand the nature of the warning, Russia's true intentions, and any opportunities to de-escalate the situation. A secure communications capability between operational-level leaders is needed, as well as for leader-level communications to relay urgent messages between the adversaries to decrease the diplomatic pressure.

### Scenario D: The Hunt is On

The Five Eyes intelligence consortium picks up multiple credible indicators that a violent non-state actor (VNSA), possibly an al-Qa'ida affiliate, possesses dirty bombs and may have placed them in multiple global capitals. The precise identity and location of the VNSA, and the type and targets of the bombs, are uncertain. Some indicators suggest the VNSA commander is located in Pakistan and that China, Japan, or the ROK are the targets, maybe Israel. U.S. officials quickly deduce that if the VNSA is ideologically, not apocalyptically motivated, then it may take cities hostage rather than destroy them with no warning. It is imperative to establish a communication channel with the VNSA to initiate bargaining before a city is taken hostage. Working through allies, the CIA enlists Saudi and Turkish leaders through a liaison to make a connection through an intermediary. Given the extraordinary sensitivity of communicating and bargaining with

terrorists, the CIA is concerned about using existing messaging apps to communicate due to the risk of leakage to third parties, including the media. The United States and its allies believe the negotiation must happen within 48 hours to avoid VNSA action. First contact with the VNSA must happen in a way that does not lead the VNSA to immediately order its fielded units to execute their plan.

## APPENDIX 3: EXPERT PRESENTATIONS AT THE WORKSHOP

The revised workshop presentations listed below will be published separately to this report.

Thomas A. Berson, “The AES Project: Any Lessons for NC3?”

Paul Bracken, “Communication Disruption Attacks in NC3”

Brendan Green, “Hotlines in Theory and History”

Eric Grosse, “Security At Extreme Scales”

Ron Minnich, “Open Source Down to the Silicon”

Salma Shaheen, “Building Communication Norms Across Nuclear C2”

Devabhaktuni “Sri” Srikrishna, “Secure Comms Deep Dive”

Alexa Wehsener, “NC3 Meets Deep Learning”

Adam Wick, “Modern Formal Verification in Practice”