IST Institute for SECURITY + TECHNOLOGY

The Institute for Security and Technology *is a critical action think tank dedicated to uniting technology and policy leaders to create actionable solutions to emerging security challenges. The CATALINK initiative at IST advocates for an internationally-driven, secure, resilient communications solution that has the potential to avert catastrophes amidst rising tensions among adversaries.*

For more information, visit securityandtechnology.org/catalink

Image credit: Lauren Hostetter of Heyhoss Design

STRENGTHENING NUCLEAR CRISIS COMMUNICATIONS

STEPS TO IMPLEMENT MESH NETWORKS TO ENHANCE RESILIENCE & SECURITY

NOVEMBER 15, 2024 | WASHINGTON, DC

Summary Report

Christian Steins

In November 2024, the Institute for Security and Technology (IST) hosted a technical workshop in Washington, DC, that brought together participants from diverse fields to discuss potential avenues for improving the resilience of crisis communications networks used by military leaders and heads of state to prevent or de-escalate nuclear crises or conflicts. Discussions throughout the day focused on identifying technical vulnerabilities to existing communication networks, making policy recommendations to enhance trust and interoperability, and exploring the potential of integrating mesh and satellite-based networks into the design of IST's CATALINK project—a secure, resilient international communications solution designed to ensure crisis communication between nuclear powers. The workshop was held under the Chatham House Rule, and consequently, this report does not attribute any part of the summary to specific individuals or organizations. IST is grateful for the political and financial support from the German Federal Foreign Office and the Swiss Federal Department of Foreign Affairs that makes this work possible.

The objectives of the workshop were threefold:

1. To foster understanding and collaboration between technical and policy experts on the benefits provided by novel technical approaches, such as mesh networking for crisis communications.
2. Identify and address current and potential technical vulnerabilities to international crisis communications.
3. Define and map the next steps for IST's development of the ROCCS network and CATALINK concept through in-depth technical discussions.

Critical takeaways from the workshop included:

- **IST should engage with the international technical community from Nuclear and Non-Nuclear Weapons States (NNWS), including Russia and China, to build trust and incorporate their technical feedback into the CATALINK and ROCCS network blueprints.**
- **IST should explore the feasibility of integrating orbital-based mesh networks, such as the Starlink satellite constellations (only as an example, not suggesting the use of Starlink for the ROCCS network), into a secure communication infrastructure for crisis scenarios where conditions on the ground may be degraded.**

About the CATALINK Initiative

In 2019, IST launched the CATALINK initiative, an additive multilateral crisis communication concept designed to enhance the resiliency and reliability of existing bilateral crisis communication channels linking nuclear-armed states. Faced with the question of how to improve the resilience of existing channels, the CATALINK team's technical advisors looked to the unique capabilities of mesh networks, which are a series of wirelessly connected devices—or nodes—that work together to relay data from one node to the next.

Mesh networks originated as a technology developed by the U.S. military in the 1960s. As the technology continued to prove a useful signal carrier, mesh networks soon evolved to become integrated as key elements of the modern Internet's network infrastructure, demonstrating their importance as small and large-scale options to provide reliable commercial communications.[1] If an existing node fails, the network self-corrects, making it possible for mesh networks to maintain functionality during disruptions and failures. Based on their level of resilience and utility, IST designed the Resilient Omni-Frequency Crisis Communications System (ROCCS) network as a key element of the CATALINK concept, with mesh networks as a primary potential technical option for implementation.[2] The ROCCS would be a permanently active global mesh network to provide the crisis communication channels with an additional layer of network connection, ensuring redundancy and resilience.[3]

1. Lessons from the Space Industry and Private Sector

At the workshop, participants discussed viable networks to facilitate crisis communications, including space-based mesh networks like the U.S. Space Surveillance Network (SSN). Commercial satellite-based solutions, like Starlink, were proposed as models for accessible yet secure global crisis communication, providing resilient communication capabilities in areas where ground infrastructure may be vulnerable.

The group offered examples of ground-based mesh networks to illustrate their versatility and trustworthiness in connecting anywhere. One example was Google's Wi-Fi mesh network, which provided connectivity for the entire Mountain View, California area and served as a model for large-scale, efficient mesh networks in commercial applications.[4] The discussion also highlighted military applications of mesh networks, showcasing their utility in complex, high-stakes environments, such as their facilitation of emergency responder communication channels after the attacks on September 11th disabled the primary communications infrastructure in lower Manhattan. As technical participants explained, mesh networks' core advantage lies in their ability to function at varying scales—from small, localized setups, to expansive, city-wide or even regional networks. This adaptability in scale also contributes to the critical role mesh networks have played in providing resilient connections and facilitating secure communication during crises when traditional communication infrastructures are overloaded or disrupted, including during natural disasters and unpredictable catastrophic events like the September 11th attacks.[5]

2. Developing the ROCCS and CATALINK Systems

Participants explored the technical requirements and logistical elements of existing mesh networks and NC3 systems and identified possible implementation pathways for the ROCCS network. A key takeaway was the importance of building redundancy and geographic diversity into crisis communication networks, which can be achieved using numerous, widely distributed nodes to ensure reliable transmission even if some fail or are disrupted.

Discussing the technical challenges, the group noted the importance of interoperability standards across

1 Meshmerize, "Wireless Mesh Networking Intricacies," July 14, 2023, https://meshmerize.net/wireless-mesh-networking-intricacies-let-s-talk-about-mesh-baby/.

2 Glenn Fleishman, "Wireless mesh networks: Everything you need to know," *PC World*, May 5, 2020, https://www.pcworld.com/article/407165/mesh-network-explained.html.

3 Institute for Security and Technology, "CATALINK Project - ROCCS Network," last accessed May 2025, https://securityandtechnology.org/catalink/.

4 Mikhail Afanasyev, Tsuwei Chen, Geoffrey M. Voelker, and Alex C. Snoeren, "Analysis of a Mixed-Use Urban WiFi Network: When Metropolitan becomes Neapolitan," Google Research, October 2008, https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/34430.pdf.

5 Meshmerize, "Emergency Network Deployment: Mesh Networks Lifesaving Power in Disaster Management," October 19, 2023, https://meshmerize.net/emergency-network-deployment-mesh-in-disaster-management/.

communication systems, ensuring these systems speak the same language. The panel noted that diverse, spread-out networks may struggle to connect seamlessly without standard protocols, negatively impacting or risking their operability entirely.

Participants offered insights into the importance of personalized communication channels, like direct lines between military commanders, such as the former US-Russia deconfliction hotline in Syria, highlighting the need for robust and adaptable protocols tailored to the nuances of specific nuclear dyads.[6]

3. Countering Emerging Threats to Crisis Communication Systems

During the discussions on the vulnerabilities of crisis communications systems and the threats posed by emerging disruptive technologies (EDTs), participants raised various offensive and defensive applications of EDTs. These included electromagnetic pulses (EMPs), artificial intelligence (AI), advanced offensive cyber capabilities, and autonomous weapons and targeting systems that could increase risks to NC3 systems and communications.

A representative with experience at the National and Nuclear Risk Reduction Center (NNRRC) in the United States shared insights on the importance of maintaining technical resilience within the NNRRC's operations. The discussion highlighted ongoing efforts to adapt and strengthen systems through AI tools, including threat monitoring and enhancing translation capabilities. The broader conversation emphasized the potential of mesh networks to bolster communication resilience, particularly in wartime or during natural disasters, when traditional systems like radios or telephones may be compromised or unavailable.

Next Steps

The insights and recommendations from this workshop will continue to guide IST's ongoing efforts to enhance nuclear crisis communication infrastructure and reach the next stages in our technical development of the CATALINK concept and its accompanying ROCCS network. Future work will focus on network design, international collaboration, and engagements with technical experts. IST continues to strive to unite the technical and policy communities on the importance of nuclear risk reduction through secure crisis communications.

6 Robert Hamilton, "The Weirdest War: Lessons from US-Russia "Deconfliction" in Syria," Stanley Center for Peace and Security, April 17, 2023, https://riskreduction.stanleycenter.org/hamilton-syria-deconfliction/; Leah Walker and Andrew Facini, "Atlas of Crisis Communications: Nuclear States," Institute for Security and Technology, July 2022, https://securityandtechnology.org/wp-content/uploads/2022/07/Atlas-of-Crisis-Communications-Nuclear-States.pdf.