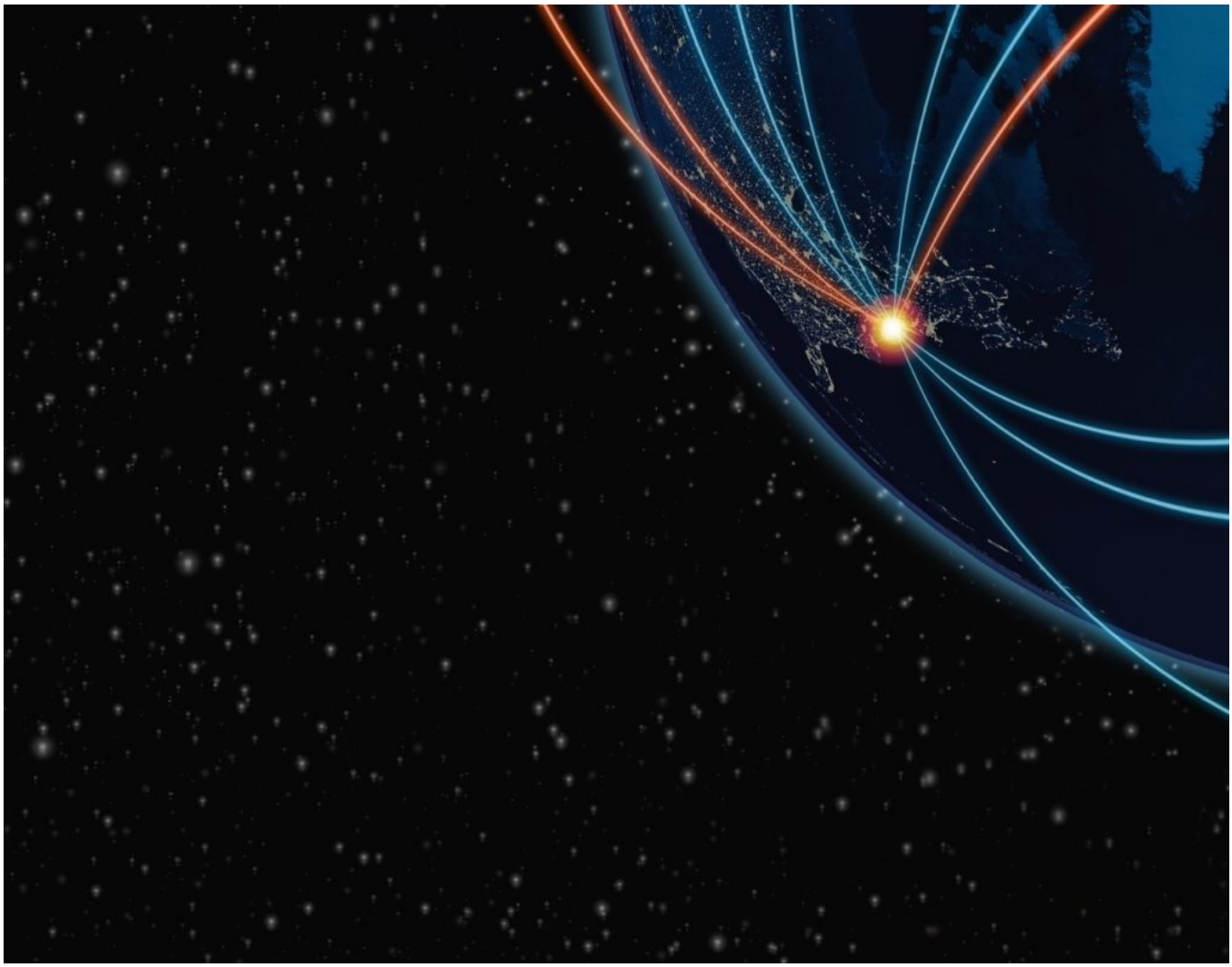
SECURITY THROUGH SIMPLICITY PODCAST



Recommended Citation

Eric Grosse, "SECURITY THROUGH SIMPLICITY PODCAST", NAPSNet Special Reports, July 07, 2020, https://nautilus.org/napsnet/napsnet-special-reports/security-through-simplicity-podcast/

ERIC GROSSE

JULY 7 2020

I. INTRODUCTION

In the podcast "**Security Through Simplicity**," Eric Grosse, former Vice President of Security and Privacy Engineering at Google, explains the technical cryptographic choices for **CATALINK** "a system strong enough to resist well-resourced adversaries, yet simple enough to be reviewed and adopted by skeptical international competitors."

This podcast is a companion to his technical paper "**Hotline Cryptography**" which is currently open for comment to the public on GitHub, in turn, a follow-on from his 2019 paper on NC3 "**SECURITY AT EXTREME SCALES**."

The Fourth Leg podcast series with its companion papers on NC3 and hotlines resulted from from *the Antidotes for Emerging NC3 Technical Vulnerabilities, A Scenarios-Based Workshop* held October 21-22, 2019 and convened by The Nautilus Institute for Security and Sustainability, Technology for Global Security, The Stanley Center for Peace and Security, and hosted by The Center for International Security and Cooperation (CISAC) Stanford University.

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

The views expressed in this report do not necessarily reflect the official policy or position of Technology for Global Security or the Nautilus Institute. We seek a diversity of views and opinions on significant topics to identify common ground.

Banner image is by Lauren Hostetter of Heyhoss Design

II. NAPSNET SPECIAL REPORT: PODCAST WITH ERIC GROSSE

SECURITY THROUGH SIMPLICITY PODCAST

JULY 7 2020

The problem is the complexity that besets legacy nuclear command, control, and communications. In a confrontation, the leaders of nuclear-armed states must always have the ability to communicate with their adversary in order to de-escalate. All nuclear-armed states must have a secure and reliable crisis communications system with the leaders of other nuclear-armed states.

CATALINK is a concrete proposal to make hotlines between nuclear-armed states secure, reliable, and trustworthy, yet functional and open-source down to the silicon. The goal is that leaders are confident that they can communicate securely in order to avert war.

The solution, Grosse suggests in the podcast, lies in radical simplicity.

In the podcast "**Security Through Simplicity**," he details the trade-offs between security, reliability, and efficiency in the proposed CATALINK system. He provides a primer on how a sender and receiver will exchange cryptographic keys to ensure they are communicating securely and provides the reasoning for his proposed technical baseline solutions as outlined in his paper "Hotline Cryptography" which is currently open for comment to the public on GitHub.

The paper not only details the technical cryptographic choices for the CATALINK system, but argues for choices to make the CATALINK "strong enough to resist well-resourced adversaries, yet simple enough to be reviewed and adopted by skeptical international competitors."

For more information about CATALINK, contact catalink@tech4gs.org

III. NAUTILUS INVITES YOUR RESPONSE

Nautilus invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/security-through-simplicity-podcast/

Nautilus Institute
2342 Shattuck Ave. #300, Berkeley, CA 94704 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org