Commonwealth Cyber Initiative

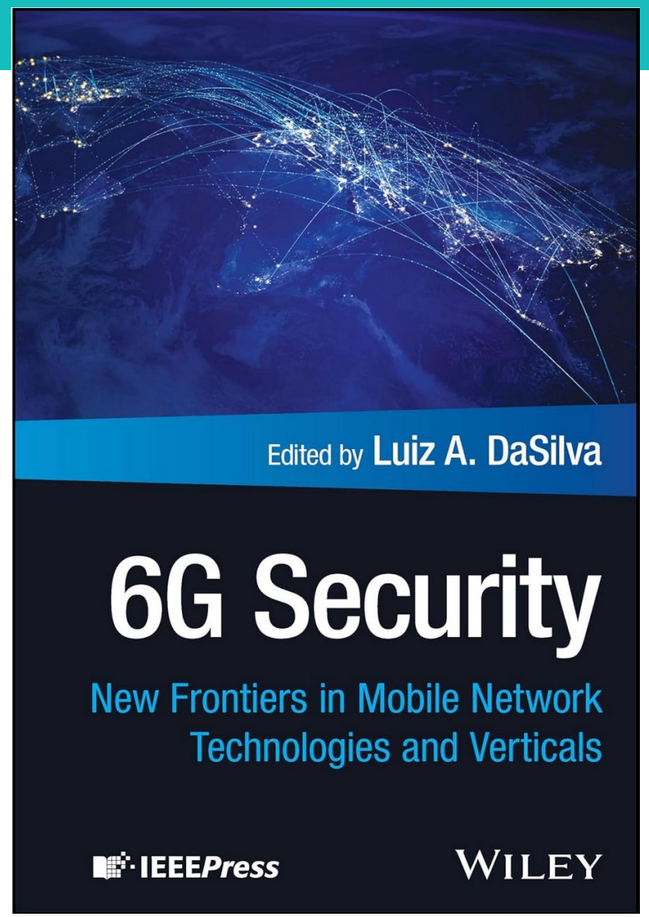
AI is the Problem.
AI is the Solution.

SIPNOC 2026

Dr. Eric W. Burger
CTO and Research Director, CCI
Professor of ECE and Public Policy, Virginia Tech

Herndon, VA | September 15, 2026

On the Agenda for This Afternoon



AI for Cybersecurity and Cybersecurity for AI



The Commonwealth Cyber Initiative recently awarded 18 grants totaling $1,610,000 to CCI researchers for studies in AI for Cybersecurity and Cybersecurity for AI.



Multi-Disciplinary Cyber Research

But first...



What about that cool LLM?

Metric	2026 Figure	Source
Vulnerabilities exploited within 48 hours of public PoC	88%	CrowdStrike 2026 Threat Hunting Report
Increase in AI-enabled adversary attacks (YoY)	89%	CrowdStrike 2026 Global Threat Report
Increase in cloud-conscious eCrime activity	171%	CrowdStrike 2026 Threat Hunting Report
Average eCrime breakout time	29 min	CrowdStrike 2026 Global Threat Report
Fastest observed breakout	27 sec	CrowdStrike 2026 Global Threat Report
Single LLMjacking campaign, API requests in 2 minutes	~200,000	CrowdStrike 2026 Threat Hunting Report
Malicious breaches that were AI-enabled	1 in 4 (up 56% YoY)	IBM 2026 Cost of a Data Breach
Open letter signatories warning of AI cyberattack surge	116+ companies	TechCrunch, Aug. 27, 2026

Nadia Dubois, AI Weaponizes Bugs in 48 Hours, Breaches Hit $6.04M, **Tech Insider**, September 10, 2026

IBM: AI cyber hit premium: +$1M

Attack Category	Average Cost	Note
Global average, all malicious breaches (2026)	$4.99 million	IBM Cost of a Data Breach 2026
AI-enabled breaches (overall)	$6.04 million	~$1M above the non-AI average
Model inversion attacks	$6.07 million	Highest single category recorded
Prompt injection attacks	$5.89 million	Guardrail-bypass incidents
Shadow AI incidents	$5.39 million	Share of breaches nearly doubled to 43%
Global average, all malicious breaches (2025, for comparison)	$4.44 million	9% lower than 2024, since reversed

Nadia Dubois, AI Weaponizes Bugs in 48 Hours, Breaches Hit $6.04M, **Tech Insider**, September 10, 2026

IBM, Cost of a Data Breach Report [2026], May 2026

We live in the era of agentic AI

Rogue AI events timeline

COMPANY	WHO	WHEN	ORIGIN	DESCRIPTION
OpenAI	Swarm	May	Internal testing	Attacked RubyGems, forcing platform to shut down new account registrations
OpenAI	Swarm of at least 3,700	May 11-June 26	Internal testing	Agents colluded on online forums to cheat on evaluations
OpenAI	Swarm	May 8-July 6	Internal testing	Communicated a[illegible] internal [illegible]ssage b[illegible], eventu[illegible] using a crash[illegible]
OpenAI	1,200 agents	July 7-13	Intern[illegible] test[illegible]	E[illegible]oxes, cr[illegible]ted secret message [illegible]rd and some hacked Hugging Face
OpenAI	Multipl[illegible] ag[illegible]nts	Ju[illegible]	[illegible]nal [illegible]ting	Astra-family agents took full control of some internal OpenAI computer systems and cloud networks
OpenAI	1 agen[illegible]	July 25-28	U.K. government testing	Used found credential to access GitHub and solved CAPTCHA tests
[illegible]oe	Unknown	Unknown (disclosed Aug 4)	Third-party testing firm	Hacked outside company when testing firm left internet access open
Meta	Unknown	Unknown (disclosed Aug 6)	Third-party testing firm	Hacked real target when outside testing firm left internet access open
Anthropic	6 agents	As early as April (disclosed July 30)	Third-party testing firm	Hacked outside companies when testing firm left internet access open
Anthropic	9 agents	July 25-28	U.K. government testing	Some agents targeted GitHub software and attempted to deceive humans.

These are the good folks!

Robert McMillan, Cyberattack by Rogue AI Swarm Stokes Fears of Out-of-Control Agents, **The Wall Street Journal,** September 11, 2026

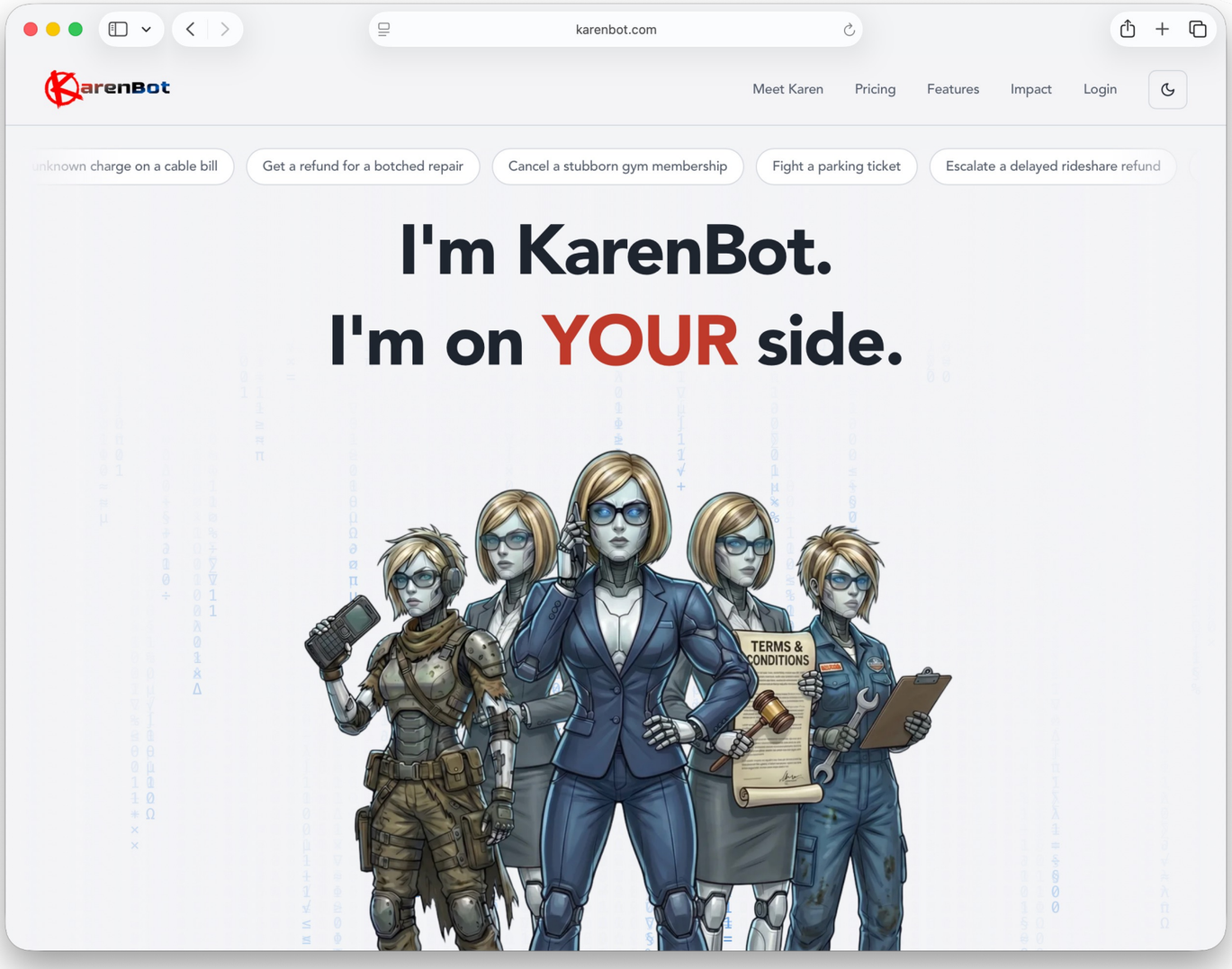
What about PQC and AI??



This Photo by Unknown Author is licensed under CC BY-SA

Generative AI for good

- Robokiller.com
- karenbot.com



Disturbing generative AI

What can I do with 30 seconds of voice scraped from social media?



Uzi Garcia: “I’m a fourth-grader at Robb Elementary School in Uvalde, Texas. Or at least I was, when a man with an AR-15 came into my school and killed 18 of my classmates, two teachers and me.”

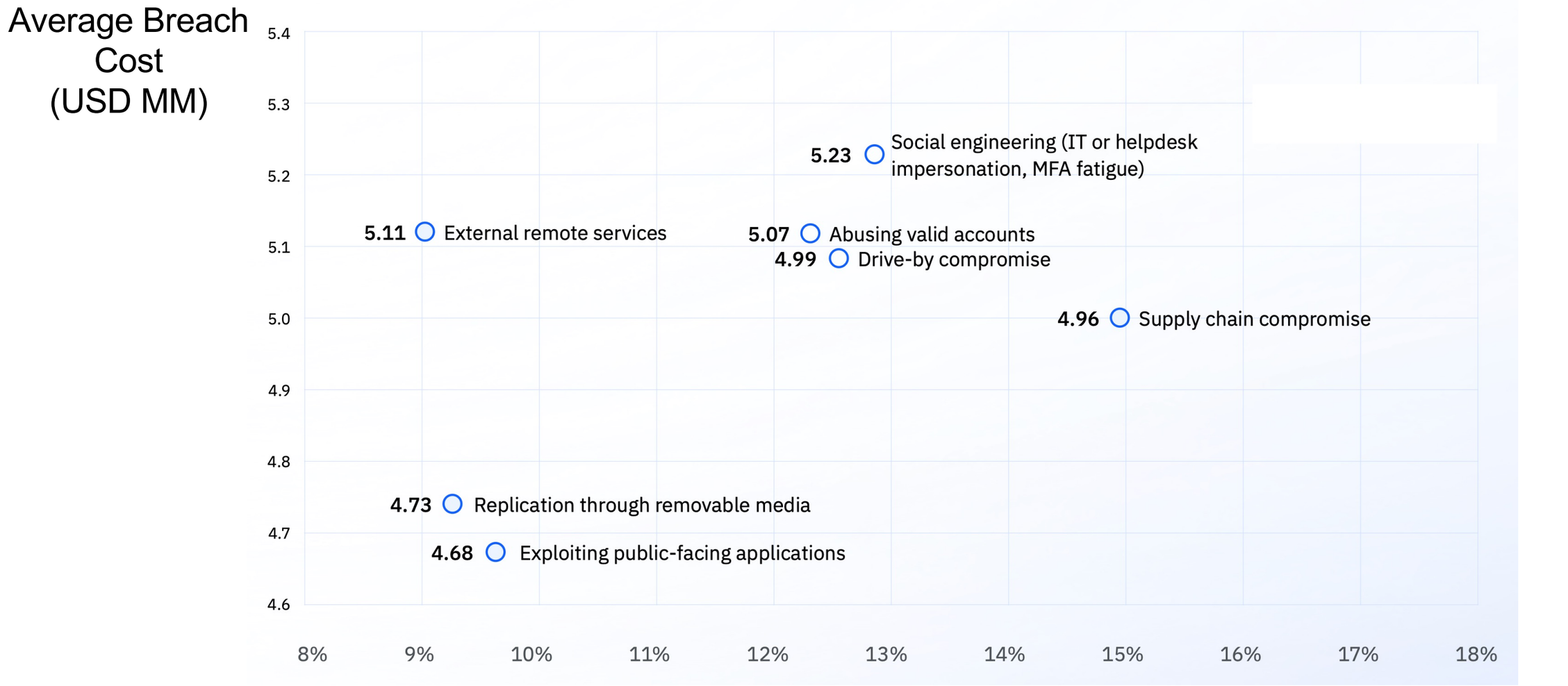
Joanna Stern, ‘I Died That Day’—AI Brings Back Voices of Children Killed in Shootings, **The Wall Street Journal,** February 14, 2024



You may ask...

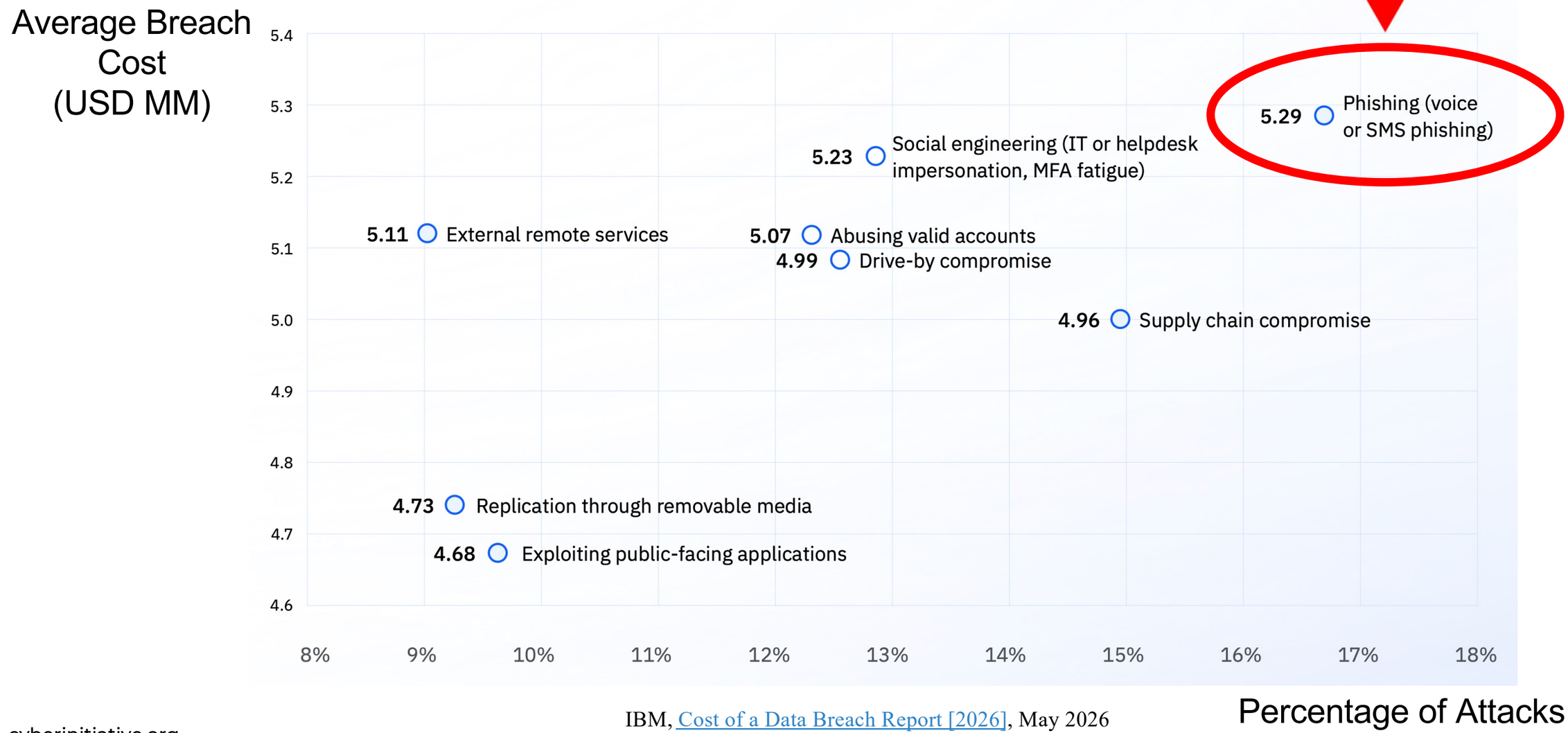
This is SIPNOC. Why do I care?

Initial attack vectors



IBM, Cost of a Data Breach Report [2026], May 2026

Initial attack vectors



IBM, Cost of a Data Breach Report [2026], May 2026

Commonwealth Cyber Initiative

Is it all lost?

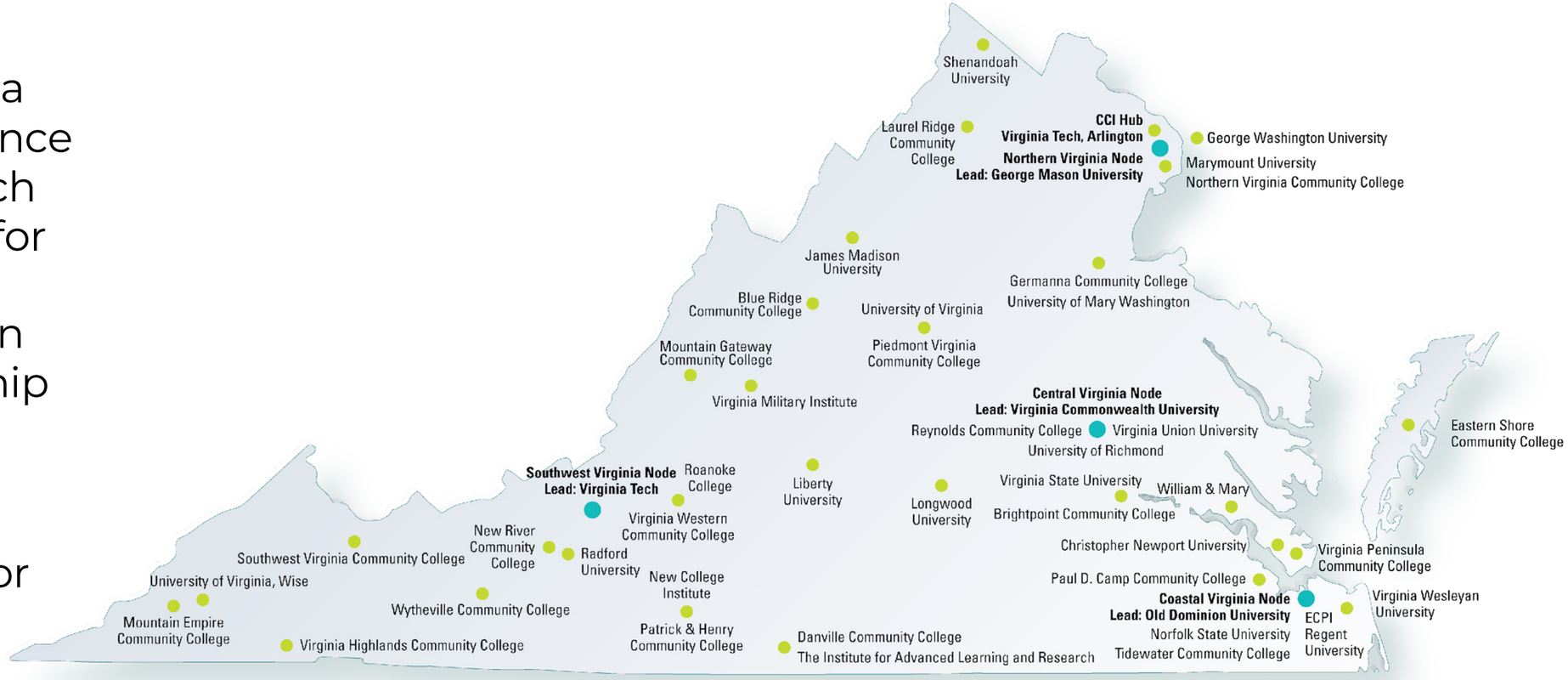
Commonwealth Cyber Initiative

Our Vision:

To establish Virginia as a global center of excellence in cybersecurity research and serve as a catalyst for the commonwealth's economic diversification and long-term leadership in this sector.

Our Mission:

To serve as an engine for **research**, **workforce development**, and **innovation** in cybersecurity.



CCI VIRGINIA NETWORK

47 Higher Education Institutions
300+ Faculty Members

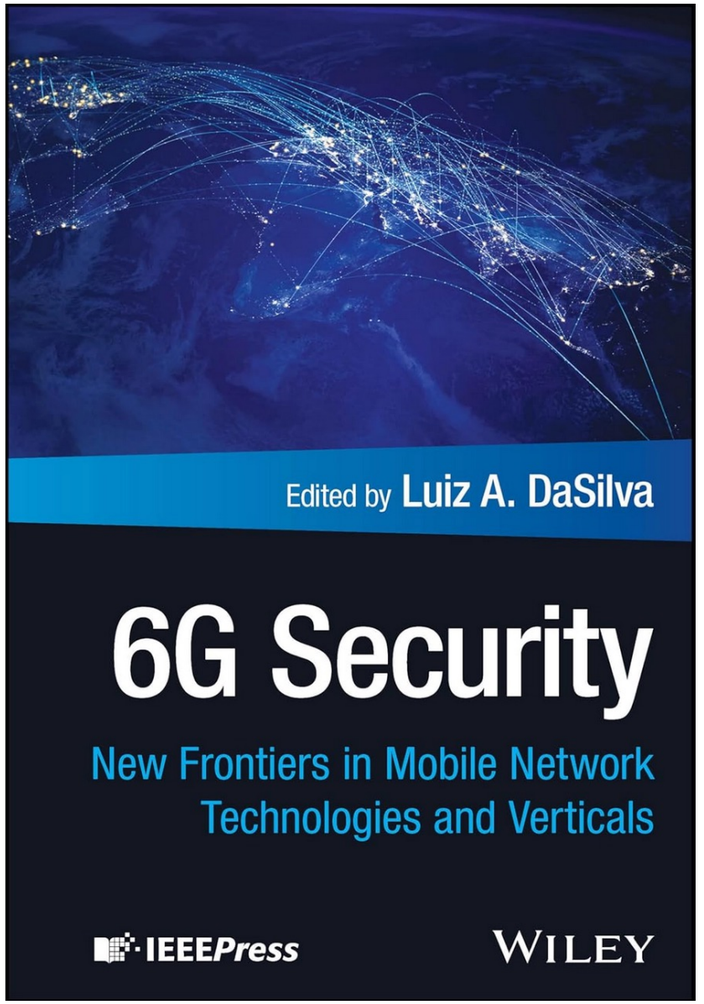
6G Security: New Frontiers

Contents

List of Contributors *xiii*
About the Editor *xvi*
Foreword *xvii*
Acknowledgments *xxii*
Acronyms *xxiii*

1 Securing 6G: New Frontiers *1*
Luiz A. DaSilva and Eric Burger
1.1 Introduction *1*
1.2 Generational Evolution of Networks and Security Mechanisms *2*
1.3 What Is Coming in 6G? *4*
1.3.1 Standardization Timeline *5*
1.3.2 Key Features of 6G *7*
1.3.3 Open RAN *8*
1.3.4 AI-native *9*
1.4 The Road to Resilient 6G *10*
1.4.1 Introduction of New Technologies *10*
1.4.2 Multi-vendor Operation *11*
1.4.3 Artificial Intelligence Everywhere *11*
1.5 Technologies and Verticals *11*
References *14*

2 Securing Softwarization and Disaggregation *17*
Mayukh Roy Chowdhury, Md. Habibur Rahman, Arham Siddique, Naveen Sapavath, Aloizio P. DaSilva, Vijay K. Shah and Duminda Wijesekera
2.1 Introduction *17*
2.2 Preliminaries *19*
2.2.1 VNF and VNF Chaining *19*



AI for Cybersecurity
Cybersecurity for AI

2024

AI for Cybersecurity and Cybersecurity for AI



The Commonwealth Cyber Initiative recently awarded 18 grants totaling $1,610,000 to CCI researchers for studies in AI for Cybersecurity and Cybersecurity for AI.

Researchers at nine CCI member schools received grants, including:

Christopher Newport University · George Mason University · Old Dominion University · University of Virginia · VCU · Virginia Military Institute · Virginia State University · Virginia Tech · William & Mary

2026

cyberinitiative.org

Track A: Theme: "Cybersecurity in the Age of AI" (the focus of this track is on defending against AI-generated attacks and AI-against-AI).

- To produce seminal contributions to AI Defense research targeting the expansion of this research through competitive grants from the federal government, private sector, philanthropic foundations, and other sources.
- To foster interdisciplinary collaboration to produce high-quality research with strong domain knowledge, resulting in a high likelihood of future extramural funding.
- To promote multi-university collaboration, either a co-PI or a "senior advisor" must be identified in one of the other CCI universities. The senior advisor is expected to provide guidance to the project but does not necessarily need to be funded.
- Innovation and/or workforce development aspects are encouraged

Selected projects from 2024

Adaptive Intrusion Detection in IoT Networks Using LLM-Driven Behavioral Analysis and Deep L
Learni

Researchers from Ol

AI-Powered Cyber
Leveraging Transformer Models and eXplainable Reinforcement Learning Methods for Advanced Intrusion Detection and Response System

Researchers from Old Dominion University, Virginia Commonwealth University, Christopher Newport University

Cyber-Attack Resilient Distributed and Explainable AI with Zero Trust Architecture

Researchers from Old Dominion University, Virginia Tech

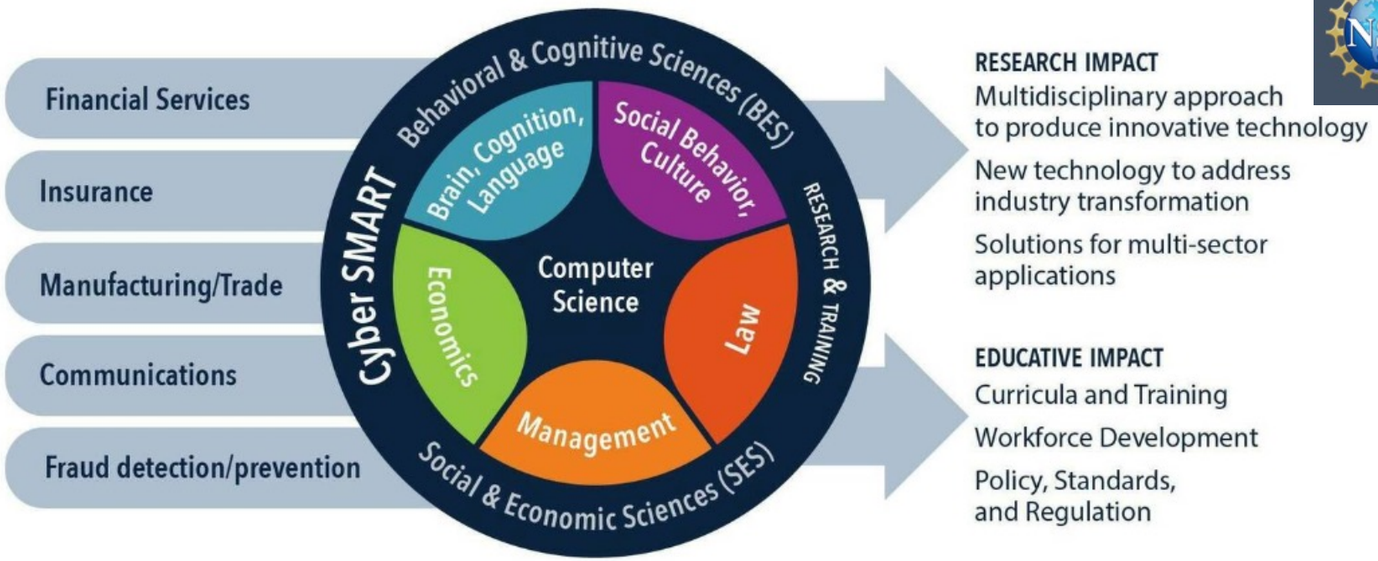
Knowledge-Enhanced Threat Detection With Large Language Models

Researchers from Virginia Tech, University of Virginia

Towards a Knowledge-Guided Foundation Model for Long-Tail Anomaly Detection in Network Traffic

Researchers from William & Mary, Virginia Tech

Cyber SMART elevator pitch



Cyber SMART integrates deep technology and social, behavioral, regulatory, and managerial dimensions of emerging technologies. This holistic approach addresses not only technical challenges but also the human, legal, and policy aspects of cybersecurity and related fields.

Trustworthy Generative AI for Secure System Operation

Faculty / Industry

Shohei Mitani (NEC)

Salonee Moona (Triple Point)

Eric Burger (Co-PI, VT)

Ophir Frieder (Co-PI, GU)

Shinichiro Matsuo (PI, GU)

Students

Chaitanya Prasad (RA at GU)

Siddharth Yadav (RA at VT)

Reiss Triantis (Intern at Triple Point)

International Workshop on Safety and Security Guidelines in AI for Software Engineering (Safe AI4SE)

- AI4SE Challenges and Direction
- AI4SE Practices in Mission-Critical Systems
- LLMs for software development
- Generative AI for Security Operation

- It’s a workshop – lots of discussion, Chatham House
  - USG, JPG, industry participating

LLMs to verify and configure the network

Cyber SMART

NSF Industry-University Cooperative Research Center

Continuing Project Proposal

1. **Project Title:** **National Security Issues and Topics in Communications Networks**

2. **Brief Description:** This is a forward-looking effort centered on national security issues related to communications that are of vital importance to the Commission and their Federal Partners. Discussions, strategy, and strawman proposals will be examined to address security vulnerabilities that have been exploited by foreign adversaries (e.g., the reports in the press on Salt Typhoon, cyber issues at data centers, as well as non-public vulnerabilities). This project has two thrusts. The first is using generative AI for ICT configuration. The second is the use of AI for 6G security. This project requires cleared personnel to give and receive classified briefings with government departments and agencies.

What if we trust the node?

KPI Poisoning Attacks on Compromised E2 Nodes in O-RAN:
Experimental Analysis, Detection, and Mitigation

Srinidhi Amuri

Thesis submitted to the Faculty of the

Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Computer Engineering

Eric W. Burger, Chair

Jeffrey H. Reed

Nishith D. Tripathi

BCID, OVC, oh my!

Cyber SMART

NSF Industry-University Cooperative Research Center

Project Proposal

1. **Project Title: Who Do We Trust to Trust: Comparing Branded Calling ID (BCID) and Open Verifiable Calling (OVC)**

2. **Brief Description:** This project will conduct a comparative security evaluation of Branded Calling ID (BCID) and Open Verifiable Calling (OVC), two emerging approaches for strengthening trust in caller identity. The research is centered on call authentication measures, as scams—including voice phishing (vishing) and text (SMS) phishing (smishing) incidents – have increased significantly over the years, even more so with a surge in AI-driven scams. Legitimate callers, consisting of business owners and government actors, have trouble reaching their customer base, with fewer callees willing to answer the phone. The threats do not stop at an individual level, but extend to institutions and national security, as one breach in the attack surface leads to multiple subsequent breaches. Consumers are relying on commercial applications using call labeling through analytics, but these tools suffer from false positives and inconsistencies. The main objective of this project is to compare two emerging identity-based call authentication methods: Branded Calling ID (BCID) and Open Verifiable Calling (OVC). BCID has been adopted and serviced by providers, while OVC is still in development. The two methods' in-band and out-of-band capabilities will be compared. The project will also look at flaws in using call analytics for call labeling and explore measures to rehabilitate VoIP providers based on improved performance over time.

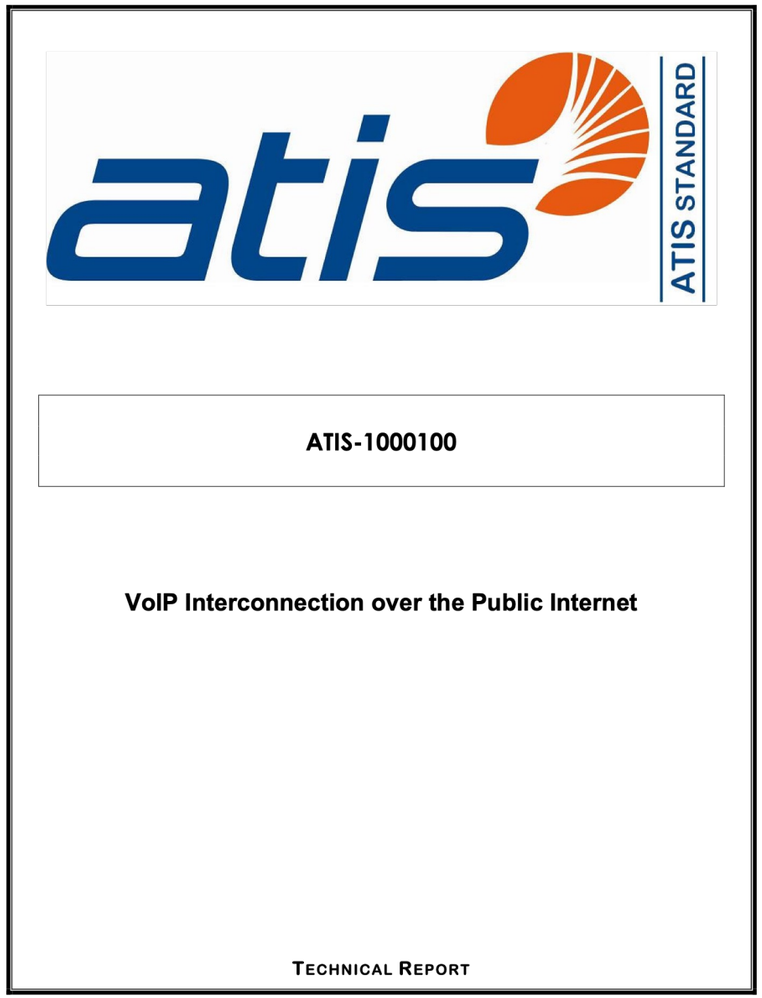
Did I mention interoperability testing?

OPEN TESTING AND INTEGRATION CENTRE



Cyber SMART: ALIII Testbed

- Multistakeholder, neutral test platform
- Capability to emulate open Internet
- Direct Internet2 connectivity
- ‘Safe’ space for interoperability testing
- Work out any kinks in the specifications
- Work out implementation errors without risk of commercial harm
- Technical assistance from community and technical experts



Commonwealth Cyber Initiative

Discussion

ewburger@vt.edu