DAY 1: WEDNESDAY, JUNE 17

CRITICAL EFFECT 2026: RUN OF SHOW

	Track I: Critical Mass	Track II: Strategic Effect	Track III: Tactical Mastery
8:00–9:00	**BREAKFAST**		
9:00–9:25	**Welcome Remarks**: Disruptions: Taiwan, Typhoons, and Timelines with Bryson Bort & Josh Corman		
9:25–9:50	**Keynote**: Nick Andersen, CISA Acting Director		
10:00–10:30	Holding the Line: How States are Confronting Volt Typhoon and the Race to Harden Lifeline Infrastructure Before 2027 *Mike Klein (moderator), Craig Hunter, John Keefe, Michaela Lee, James Regan*	When the Internet Breaks: How to Keep Critical Infrastructure Alive at 5% Bandwidth *Caleb Queern*	Hidden in Plain Sight: AI-Augmented Defense for Rural Water Systems *Clement Danish and Stacey Myers*
10:30–11:00		From Military Prototype to Public Good *Johan Chamucero*	Your Nurses Are Hiding Infusion Pumps in Cabinets: What 300 Clinicians Won't Tell Your CISO *Ron Thompson*
11:00–11:30	Behind the Dais: Committee Staff Perspectives on OT Cybersecurity *Nicholas Leiserson (moderator), Kevin Block, Mireya Jurado, Alan McQuinn*	Measuring Catastrophe: Why Critical Infrastructure Cannot Survive Without a Disaster Scale *Munish Walther-Puri*	Stop Selling Ferraris to People Who Need Pickup Trucks: What OT Operators Actually Need from the Cyber Industry *Josh Ross*
11:30–12:00		Strengthening Cybersecurity in Water Utilities: What's Actually Working *Lessie Skiba*	Digital Strangelove or: How I Learned to Stop Worrying and Love Cyber Disruption Planning *Christopher Cruz*
12:00–12:30			
1:00–1:30	A Tale of 3 Cities: COOP vs. Continuity of the Economy vs. Public Safety *Josh Corman (moderator), Dean Ford, Mark Montgomery, Natalie Sullivan, Chuck Weissenborn*	"When YOU are your worst nightmare" — Thinking Like an Adversary in an OT Environment *Andrew Krapf*	1000 Ways to Die: The Convergence of IT/OT in Hospitals *Pedro Umbelino*
1:30–2:00		The Silent Storm: SLED, AI, and the OT/ICS Workforce Visibility Crisis *James Regan and Jeff Welgan*	Buying Time: How Intelligent Deception Could Give Under-Resourced Critical Infrastructure Operators a Fighting Chance *Nicholas Carroll*
2:00–2:30	A Fortnight without Water: Secure by Design *Lauren Zabierek*	Civilian Exposure Reduction in a Shared Digitally World *Jonathan Horowitz and Sergio Caltagirone*	Protracted Disruption: Lessons from the Longest Cyber Conflict *Oleg Shakirov*
2:30–3:00	CI Fortify *Matt Rogers*	AI Runs on Lifelines: Stress-Testing the Infrastructure Beneath the AI Economy *Bob Kolasky*	SECUREGRID: Because OT Vulnerability Management is Broken *Katrina Rosseini*
3:00–3:30	Your Data or your Life? Overcoming Biases, Blind Spots, & Muscle Memory *Cynthia Kaiser (moderator), Andrew Carney, Brian Mazanec, Adam Robbie*	Food for Thought: Current and Coming National Security Risks *Andrew Rose*	Residential Proxies and Critical National Infrastructure *Joseph Slowik*
3:30–4:00		UnDisruptable27's Cyber-Informed Engineering Mitigations *Josh Corman and Gus Serino*	Quantum Risk in OT: What Breaks, What Matters, What to Do Now *Shadya Maldonado*
4:10–5:00	**Press Panel: Are the Typhoon Narratives Failing: Why & How Not To?** Paul Roberts (moderator), Eric Geller, Sean Lyngaas, Maggie Miller, Kim Zetter		

DAY 2: THURSDAY, JUNE 18

CRITICAL EFFECT 2026: RUN OF SHOW

	Track I: Critical Mass	Track II: Strategic Effect	Track III: Tactical Mastery
8:00–9:00	**BREAKFAST**		
9:00–9:25	**Welcome Remarks**: Bryson Bort and Josh Corman		
9:25–9:50	**Keynote**: Philanthropy's role in cyber from Sesame Street to UnDisruptable27 | Craig Newmark		
10:00–10:30	Cyber Civil Defense Teamwork *Stephanie Ross (moderator), Matt Altomare, Paul Chang, Netta Squires*	Buying Blind: How Federal Acquisition Is Leaving Cyber-Informed Engineering on the Table *Virginia Wright*	Putting the E in P.A.C.E.: When Satcom Is Not Enough *Mark Bristow*
10:30–11:00		The Case for a Tech Regulator of Last Resort *Andrea Matwyshyn*	*The First EMB3d Tiering Rollover: Meeting the Anthropic Mythos Moment* *Niyo Little Thunder Pearson*
11:00–11:30	A Wolff at the Door (and his super-friends) *Evan Wolff (moderator), Charles Carmakal, Steve Elovitz, Megan Stifel*	The Electrotech Stack at Risk: China, AI, and America's Energy Supply Chains *Phoebe Benich and Emma Stewart*	OT/ICS Incident Response Capacity: The Good, the Bad, and the Ugly *Chuck Weissenborn*
11:30–12:00		OT Security Policy in Emerging Markets: Why It Matters and What We Can Learn *Sheila Casserly*	
12:00–12:30	**LUNCH**		
1:00–1:30	**Cyber Policy Shark Tank** Hosted by Beau Woods		
2:00–2:30	**Wrap Up** Bryson Bort and Josh Corman		

Track 1: Critical Mass

9:00 AM: Welcome Remarks

Bryson Bort and Josh Corman

9:25 AM: Keynote

CISA Acting Director Nick Andersen

10:00 AM: Holding the Line: How States are Confronting Volt Typhoon and the Race to Harden Lifeline Infrastructure Before 2027

Mike Klein (moderator), Craig Hunter, John Keefe, Michaela Lee, James Regan

- The intelligence is no longer ambiguous: PRC-linked actors have pre-positioned themselves inside American critical infrastructure. When Target-Rich, Cyber-Poor sectors lack basic IT staff, a single failure can cascade into devastating consequences. How do we defend the defenseless? This panel convenes senior leaders from state cyber offices, state cyber commands, and the National Guard to examine what states are actually doing — and what more they can do — in response to this documented, pre-positioned threat. The conversation will focus not just on detection and defense, but on resilience: the ability to absorb a hit, sustain operations, and protect human life when systems fail.

11:00 AM: Behind the Dais: Committee Staff Perspectives on OT Cybersecurity

Nicholas Leiserson (moderator), Kevin Block, Mireya Jurado, Alan McQuinn

- You've seen Congressional hearings on TV or read about them in the press. You've seen the impact of laws Congress has passed. But what's it like behind the scenes, especially on a niche, technical issue like operational technology cybersecurity? Hear directly from House committee staff on how they approach national security challenges at the interface of connectivity and physical systems, their priorities today, and how they keep up with a rapidly changing threat environment.

1:00 PM: A Tale of 3 Cities: COOP vs. Continuity of the Economy vs. Public Safety

Josh Corman (moderator), Dean Ford, Mark Montgomery, Natalie Sullivan, Chuck Weissenborn

2:00 PM: A Fortnight without Water: Secure by Design

Lauren Zabierek

2:30 PM: CISA's CI Fortify

Matt Rogers

3:00 PM: Your Data or Your Life? Overcoming Biases, Blind Spots, & Muscle Memory

Cynthia Kaiser (moderator), Andrew Carney, Brian Mazanec, Adam Robbie

4:10 PM: Press Panel: Are the Typhoon Narratives Failing: Why & How Not To?

Paul Roberts (moderator), Eric Geller, Sean Lyngaas, Maggie Miller, Kim Zetter

Track 2: Strategic Effect

10:00 AM: When the Internet Breaks: How to Keep Critical Infrastructure Alive at 5% Bandwidth

Caleb Queern

- How can IT systems operate when networks degrade or fail? This talk shows practical techniques to design resilient systems that function under extreme bandwidth constraints and disrupted conditions.

10:30 AM: From Military Prototype to Public Good

Johan Chamucero

- DAF CROCS debuts OT Cyber Defender training pipeline. Discover actionable, hands-on training pathways that empower engineers and cyber teams to protect critical infrastructure. Join the mission!

11:00 AM: Measuring Catastrophe: Why Critical Infrastructure Cannot Survive Without a Disaster Scale

Munish Walther-Puri

- Cyber incidents in critical infrastructure are hybrid "technological disasters" that combine the speed of software failure with devastating, physical, cascading outages. Crucially, the lack of standardized, quantifiable metrics for these large-scale cyber events is the single greatest inhibitor to fast, coordinated response and clear communication during a crisis. We have long struggled to communicate "how bad" and "how wide/broad" an incident is, leading to communication paralysis and under-resourced recoveries. This talk introduces the need for a technology disaster scale focused on critical infrastructure. Drawing inspiration from established natural disaster scales (like Richter and Volcano Explosivity Index), the Tech Disaster Scale provides the critical precision and standardized language needed to accelerate communication among emergency and incident responders, government officials, media, and security practitioners.

11:30 AM: Strengthening Cybersecurity in Water Utilities: What's Actually Working

Lessie Skiba

- Water utilities face rising cyber risk, but adoption lags. Learn how coaching, trust, and public-private collaboration are scaling real-world cyber readiness in critical infrastructure.

1:00 PM: "When YOU are your worst nightmare" — Thinking Like an Adversary in an OT Environment

Andrew Krapf

- Attendees of this presentation will be challenged to apply their knowledge of OT systems to realize what could happen when adequate Prevention, Detection, Isolation, and Recovery abilities are not present. Although fictitious in nature, the conversation will highlight the need to engage a consequence-driven, risk-based thought exercise and how they would respond. The goal is to show that a knowledgeable adversary is not just an abstract concept.

1:30 PM: The Silent Storm: SLED, AI, and the OT/ICS Workforce Visibility Crisis

James Regan and Jeff Welgan

- Federal agencies and SLED entities lack reliable data on the cyber workforce, especially in OT/ICS. This session offers a roadmap using Workforce Intelligence and AI to validate specialized skills and close the effectiveness gap.

2:00 PM: Civilian Exposure Reduction in a Shared Digital World

Jonathan Horowitz and Sergio Caltagirone

- Modern digital infrastructure is often designed to support both civilian and military users without a clear separation. As a result, these interconnected systems create dependencies where civilian populations rely on infrastructure that may also serve military purposes. During armed conflict, attacks targeting military components can unintentionally or intentionally disrupt services critical to civilians. This proposal provides the space to unpack this issue and explain a new research project that will research, develop, and advance practical solutions for segregating civilian and military users on shared digital infrastructure during times of armed conflict, with the ultimate goal of improving civilian protection.

2:30 PM: AI Runs on Lifelines: Stress-Testing the Infrastructure Beneath the AI Economy

Bob Kolasky

- This presentation will connect AI infrastructure risk to lifeline critical functions, with particular attention to cross-sector dependencies (energy, water, cloud, communications). It will emphasize pragmatic resilience actions that can be implemented within 6–18 months and that are relevant not only to hyperscale operators but also to smaller organizations that depend on shared infrastructure.

3:00 PM: Food for Thought: Current and Coming National Security Risks

Andrew Rose

3:30 PM: UnDisruptable27's Cyber-Informed Engineering Mitigations

Josh Corman and Gus Serino

Track 3: Tactical Mastery

10:00 AM: Hidden in Plain Sight: AI-Augmented Defense for Rural Water Systems

Clement Danish and Stacey Myers

- Micro, low-visibility disruptions in under-resourced systems represent one of the fastest paths to disproportionate national-level impact. Adversaries targeting U.S. critical infrastructure increasingly operate below detection thresholds, using automation, legitimate tools, and long dwell times to probe and persist inside industrial control systems. These campaigns do not announce themselves. They blend into normal operations. Rural water and wastewater utilities represent a critical exposure point. When a small wastewater system fails, the impact is not gradual; it is immediate. This session focuses on what can be put in place now to prevent small, local disruptions from scaling into 2027-style multi-region cascade events.

10:30 AM: Your Nurses Are Hiding Infusion Pumps in Cabinets: What 300 Clinicians Won't Tell Your CISO

Ron Thompson

- Security controls aren't built for clinical reality. We asked 300+ clinicians what actually happens at the bedside when systems fail.

11:00 AM: Stop Selling Ferraris to People Who Need Pickup Trucks: What OT Operators Actually Need from the Cyber Industry

Josh Ross

- Borrowing from modern software's MVP framework, this talk introduces "Minimum Viable Security Posture" as a first-principles approach to OT resilience for under-resourced critical infrastructure.

11:30 AM: Digital Strangelove or: How I Learned to Stop Worrying and Love Cyber Disruption Planning

Christopher Cruz

- Perfect security is a myth and your IR plan won't save you. We must learn to operate in a degraded environment and build for disruption planning before the "doomsday machines" activate.

1:00 PM: 1000 Ways to Die: The Convergence of IT/OT in Hospitals

Pedro Umbelino

- Hospitals are a complex System of Systems. Their infrastructure is like a small city, with multiple, independent, operationally distinct systems that interact to deliver healthcare services to users at the end of the day. No single system controls the whole – instead, clinical services emerge from the coordinated behavior of clinical, administrative, and logistical subsystems. This also means multiple single points of failure. And the convergence of IT and OT in these small cities we call hospitals is ramping up their cascading risk profiles. In this talk, we will explore 1000 ways to die, from delayed surgeries caused by a ransomware attack on the scheduling software to patient evacuation from HVAC systems, from infusion pumps being manipulated to target kill to medical data exfiltration to some country in Asia, from backup generator damage to DICOM clinical image manipulation. We will marathon through many different scenarios, protocols, and technologies, highlighting as much as possible about the challenges hospitals face in this world where everything seems connected, online, and at the reach of a button.

1:30 PM: Buying Time: How Intelligent Deception Could Give Under-Resourced Critical Infrastructure Operators a Fighting Chance

Nicholas Carroll

- Minot’s water system was struck by ransomware and the SCADA systems went offline three weeks ago. Volt Typhoon mapped Littleton’s grid for 10 months. Intelligent offline honeypots could buy defenders the time resilience requires well before the cascade.

2:00 PM: Protracted Disruption: Lessons from the Longest Cyber Conflict

Oleg Shakirov

- While policymakers and media warn of a single, catastrophic attack on critical infrastructure, the Russia–Ukraine war shows a less spectacular threat: smaller, opportunistic incidents that still cause real damage.

2:30 PM: SECUREGRID: Because OT Vulnerability Management is Broken

Katrina Rosseini

- SECUREGRID shifts OT security from vulnerability management to real-time behavioral adaptation designed for systems that can’t afford disruption.

3:00 PM: Residential Proxies and Critical National Infrastructure

Joseph Slowik

- Adversaries continue to target critical national infrastructure (CNI) via cyber means, and have improved their technical and OPSEC mechanisms in doing so. Key to this evolution is leveraging proxies of compromised network devices, often in residential or small office settings, to facilitate communication from adversary to victim space. In this discussion we will analyze the technical nature of these networks, their implications for monitoring and defense, and policy and ethical considerations for response and mitigation. In doing so we will review current intrusion activity associated with PRC and Russian entities, and the risks associated with continued operations.

3:30 PM: Quantum Risk in OT: What Breaks, What Matters, What to Do Now

Shadya Maldonado

- VPNs, remote access gateways, jump servers, OPC UA servers, and encrypted tunnels crossing the IT/OT boundary at Layer 3 run quantum-vulnerable cryptography. As your organization plans its next move, you need to know: what actually breaks, what to prioritize first, and which playbooks are delivering results now.

Track 1: Critical Mass

9:00 AM: Welcome Remarks

Bryson Bort and Josh Corman

9:30 AM: Keynote: Philanthropy's role in cyber from Sesame Street to UnDisruptable27

Craig Newmark

10:00 AM: Cyber Civil Defense Teamwork

Stephanie Ross (moderator), Matt Altomare, Paul Chang, Netta Squires

11:00 AM: A Wolff at the Door (and his super-friends)

Evan Wolff (moderator), Charles Carmakal, Steve Elovitz, Megan Stifel

1:00 PM: Cyber Policy Shark Tank

Beau Woods (host)

2:00 PM: Wrap Up

Bryson Bort and Josh Corman

Track 2: Strategic Effect

10:00 AM: Buying Blind: How Federal Acquisition Is Leaving Cyber-Informed Engineering on the Table

Virginia Wright

- The principles of Cyber-Informed Engineering (CIE) are clear: engineer out cyber risk at the design stage, bound the consequences of compromise, and eliminate the assumption that detection and response alone can protect critical systems. What is far less clear is how any of this gets bought. Drawing on an analysis of current cybersecurity standards, procurement language, and evaluation criteria, we identify where CIE requirements fall through the cracks — and what it would take to close them. We present a mock procurement exercise as a concrete use case, demonstrating how vendors and buyers are talking past each other on engineered security and provide targeted modifications to requirements language and evaluation factors that could change outcomes without requiring wholesale regulatory overhaul.

10:30 AM: The Case for a Tech Regulator of Last Resort

Andrea Matwyshyn

11:00 AM: The Electrotech Stack at Risk: China, AI, and America's Energy Supply Chains

Phoebe Benich and Emma Stewart

- The United States is entering a generational energy buildout, but as billions go towards modernizing our electrical infrastructure, our systems remain dependent on China for the underlying "electrotech stack." A new paper by the Carnegie Mellon Institute for Strategy and Technology examines how this reliance creates severe supply chain vulnerabilities and threatens the security advantages a modernized grid is supposed to deliver. This session will draw from that research to explore how the U.S. can secure its energy future and achieve maximum strategic return.

11:30 AM: OT Security Policy in Emerging Markets: Why It Matters and What We Can Learn

Sheila Casserly

- Emerging market OT security policy is active, distinctive, and consequential for US competitiveness and security. A framework for practitioners and policymakers to engage and learn.

Track 3: Tactical Mastery

10:00 AM: Putting the E in P.A.C.E.: When Satcom Is Not Enough

Mark Bristow

- What happens to your situational awareness when both the grid and your networks go down and stay down for weeks? MITRE's Critical Infrastructure Risk-Informed Decision Analysis Platform (CIRIDAP) is designed to fill the current gap: there is no national Common Operating Picture (COP) for critical infrastructure in prolonged "dark sky" conditions, when power and IP-based, cellular, satellite, and landline communications are largely unavailable. This talk will cover how the system works, what we learned in our live demo about improving ICS resilience and decision-making during extended outages, and options for scaling CIRIDAP into an operational capability for long-duration, large-scale disruptions.

10:30 AM: The First EMB3d Tiering Rollover: Meeting the Anthropic Mythos Moment

Niyo Little Thunder Pearson

- Cybersecurity and critical infrastructure is at a critical juncture, Anthropic is on the verge of releasing an AI model that can potentially find vulnerabilities regardless of code base or operating system. In the face of a vulnerability tsunami, the EMB3D team will implement its first EMB3D Tiering rollover cycle, downgrading "Intermediate" mitigations to "Foundational" mitigations, "Leading" mitigations to "Intermediate" mitigations while identifying futureproofed "Leading" mitigations.

11:00 AM: OT/ICS Incident Response Capacity: The Good, the Bad, and the Ugly

Chuck Weissenborn