Department of the Air Force

Identifying Ways to Reduce Risk to Control Systems / Operational Technology – event 211

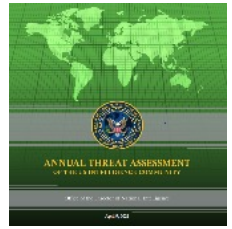
Mr. Daryl Haegley, SL, GICSP, OCP

DAF Technical Director, DAF Control Systems Cyber Resiliency

28 August 2023, 1500-1550

Montgomery Performing Arts Center, Main Stage

Director of National Intelligence – Annual Threat Assessments 2021-23



Control systems/critical infrastructure are top "cyber" threats

- Russia continues to target **critical infrastructure**, including underwater cables & industrial control systems, in US /allied / partner countries, as compromising such infrastructure improves -and sometimes demonstrate -its ability to damage infrastructure during a crisis
- China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to **critical infrastructure** within US
- Iran has ability to conduct attacks on **critical infrastructure**, as well as to conduct influence and espionage activities. Iran was responsible for multiple cyber attacks between Apr-Jul'20 against Israeli water facilities that caused unspecified short-term effects (*press reporting*)
- North Korea probably possesses expertise to cause temporary, limited disruptions of some **critical infrastructure** networks and disrupt business networks in US, judging from its operations during the past decade, and it may be able to conduct operations that compromise software supply chains

Adversaries persistently look for any weak link … Which is ours?

Importance of Public-Private Partnerships

2023 National Cybersecurity Strategy (under 'Securing Cyberspace')

"Together, industry and government must drive effective and equitable collaboration to correct market failures, minimize the harms from cyber incidents to society's most vulnerable, and defend our shared digital ecosystem."

CYBERCOM Executive Director (Sept 2022)

"What we need from the private sector is early warning, essentially. If they see anomalies that we need to know about, we can prepare to conduct an offensive operation or conduct defense of DoD's networks. **Valuable information can be gained by the private sector. And of the flip side, we have a lot of information to offer"**

CISA

"Public-private partnerships are foundation for effective critical infrastructure security and resilience strategies, and timely, trusted information sharing among stakeholders is essential to the security of the nation's critical infrastructure."

Ways to Reduce Risk to Control Systems / Operational Technology

Joyce Hunter
Institute for Critical Infrastructure Technology (ICIT)

Executive Director of ICIT, a non-profit think tank, providing objective research, advisory, and education to legislative, commercial, and public-sector cybersecurity, national security and critical infrastructure stakeholders

Jason Christman
Johnson Controls International

Vice President and Chief Product Security Office, leading cybersecurity strategy and risk management across a diverse portfolio of smart building technologies and cloud connected solutions

Danielle Jablanski
Atlantic Council Fellow / Nozomi Networks

OT Cybersecurity Strategist at Nozomi Networks, responsible for researching global cybersecurity topics and promoting OT and ICS cybersecurity awareness throughout the industry

Fred Gordy
Building Cyber Security

Director, OT Risk Assessment. Smart building industry expert and thought leader with over 22 yrs of experience in secure CS development and implementation for Fortune 500 companies throughout the US, Canada, and abroad