Information Warfare and Critical Infrastructure: The Combined Power of Information Warfare Threats

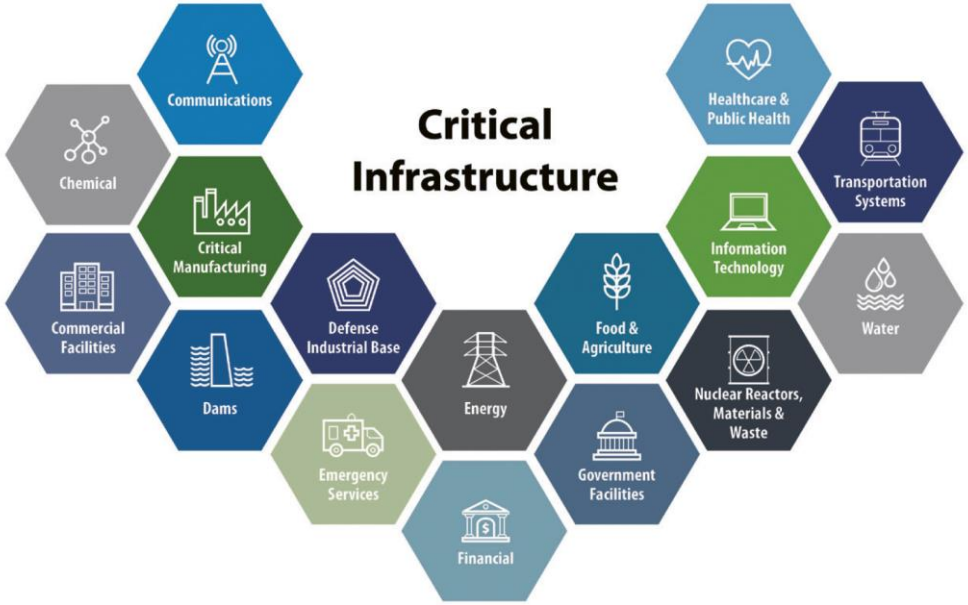
Dr. Josh Sipper
Professor of Cyberwarfare Studies
Air Force Cyber College
jasipper@gmail.com

Biographical Sketch

- Dr. Joshua Alton Sipper is currently assigned to the Air Force Cyber College as a Professor of Cyberwarfare Studies. He completed his Doctoral work at Trident University in September of 2012, earning a Ph.D. in Educational Leadership (emphasis, E-Learning Leadership). Dr. Sipper's previous degrees were obtained from Troy University (M.Ed. Education) and Faulkner University (B.S. English). Dr. Sipper is a veteran who served honorably in the U.S. Air Force in the intelligence career field and worked for Lockheed Martin in a similar capacity on the U2 program. More recently, Dr. Sipper shifted his focus into the cyber realm as a Systems Engineer for General Dynamics at the Air Force's 26th Network Operations Squadron, followed by a nine-year stint as a civil servant in the Air Force cyber career field at the Curtis E. LeMay Center for Doctrine Development and Education. Dr. Sipper currently serves as a Professor of Cyber Warfare Studies at the Air Force Cyber College, Air University, Maxwell AFB. Dr. Sipper's research interests include cyber operations, ISR, electromagnetic warfare, and cyber warfare.

Information Warfare and Critical Infrastructure

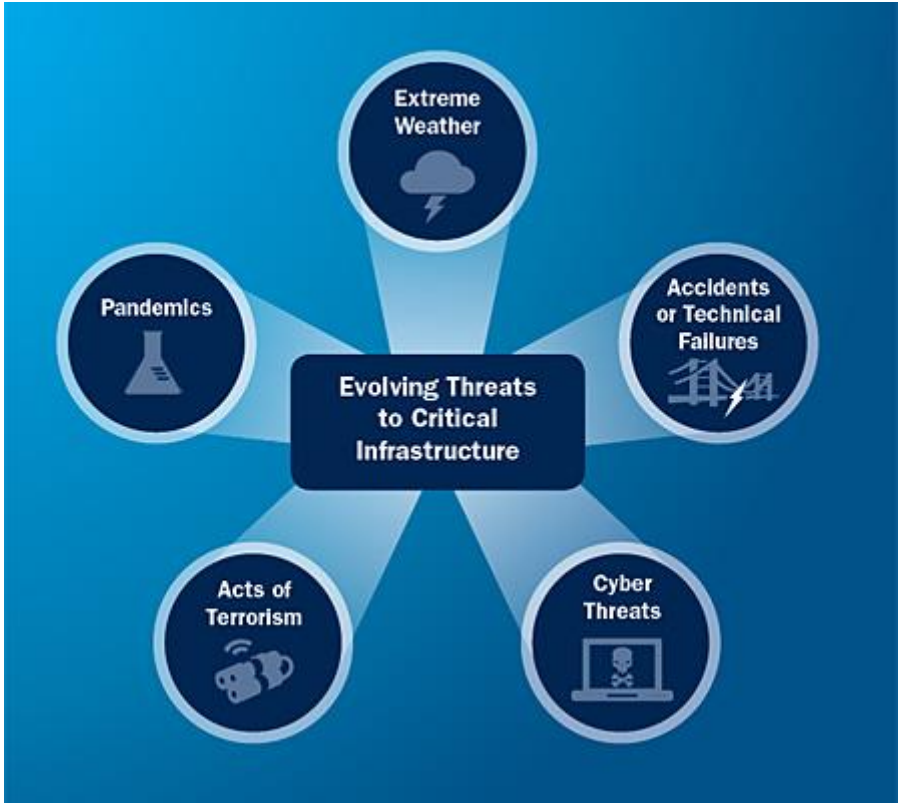
- Introduction
- IW Threats to CI
- Cyber Operations CI Threats
- Electromagnetic Warfare CI Threats
- ISR CI Threats
- IO CI Threats
- CI Vulnerabilities
- IW Adversaries to IC
- Conclusion



© US Cybersecurity & Infrastructure Security Agency (CISA)

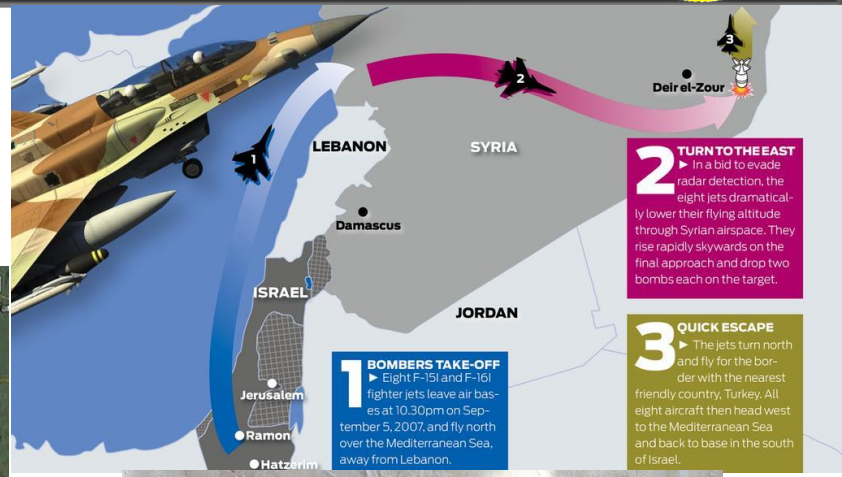
Introduction

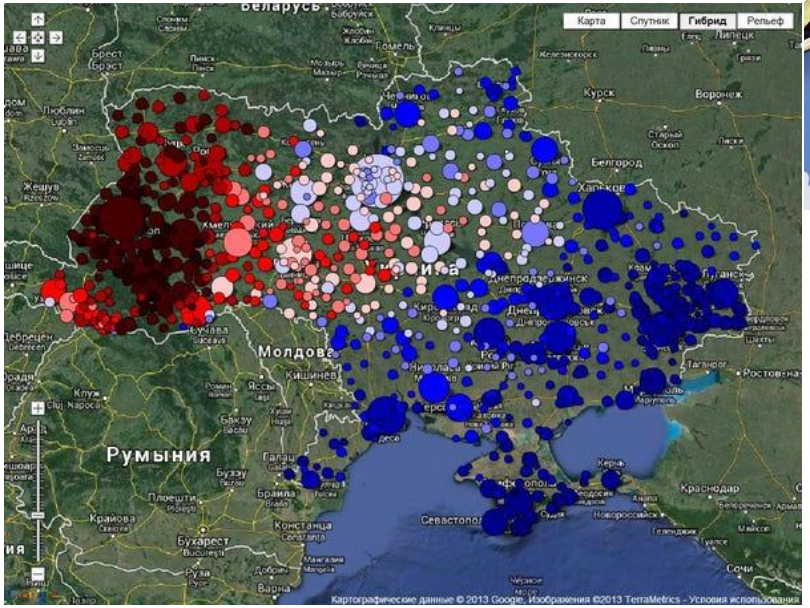
- Pressure exerted by peer adversaries such as China and Russia on critical infrastructures (CI) across the globe has increased markedly
- Not just cyber threats, but information warfare threats (electromagnetic warfare (EW), intelligence, surveillance, and reconnaissance (ISR), and information operations (IO)
- Peer threats (China/Russia) and near peer threats (North Korea/Iran)



IW Threats to CI

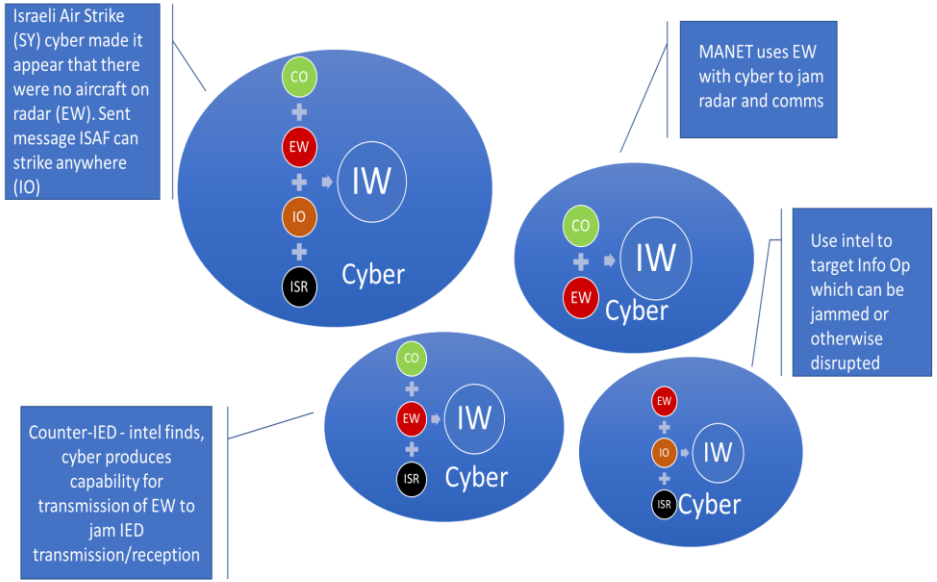
- OPERATION ORCHARD
- Russia in Ukraine and eastern Europe
- *Ever Given*





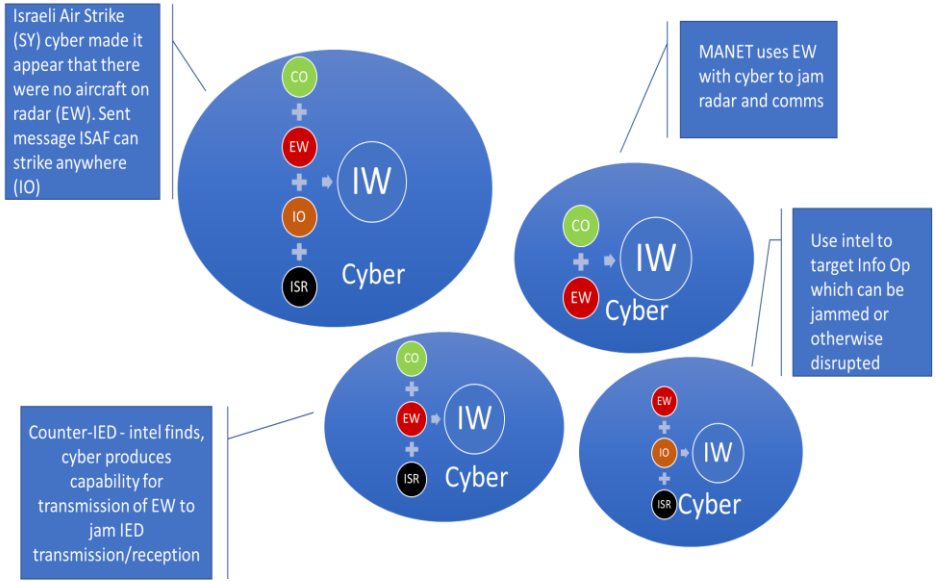
Cyber Operations CI Threats

- Crucial for cyber as the key enabler to be present in each of these and other IW activities
- During the 2020 COVID-19 pandemic where everything from hospitals to the World Health Organization (WHO) experienced cyberattacks and ransomware against a wide range of CI including health, food, fuel, and information systems
- China (Halfnium Hack) and Russia (Solarwinds Hack)



Electromagnetic Warfare CI Threats

- The recent move to 5G technologies has increased not only the EMS attack structure, but also the types of aggressive EW possible within the EMS and IE
- There are challenges extant in the advancement of 5G including allocation of the EMS and peer competition from China specifically who is already leading the way in 5G infrastructure internationally
- Use of an EMP has long been regarded as literally the nuclear option for the degradation and destruction of CI



ISR CI Threats

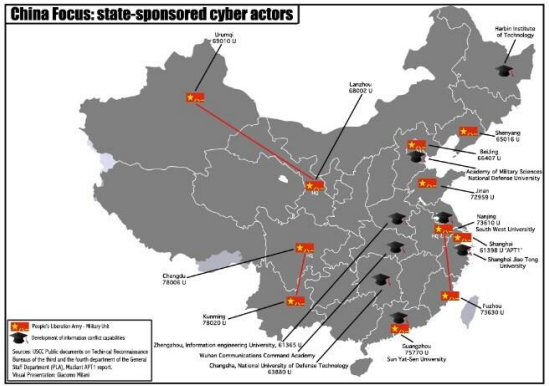
- Recent Solarwinds supply chain espionage event is a prime instance of how adversaries (in this case Russian actors) can use intelligence gathering to break into numerous systems at the government and private level simultaneously
- One-dimensional understanding of network defense and cyber intelligence
- The more information from multiple sources gathered, the greater the chance of breaking in and stealing data or implanting malware

IO CI Threats

- Influence is a large part of IO
- Government, private, and societal decision makers are often affected as well in many adverse ways
- IO against CI can also be used to shape perceptions, affect command and control capabilities, and test the steel of the tactical workforce through influencing decision making and perceptions of individual and group usefulness and morale

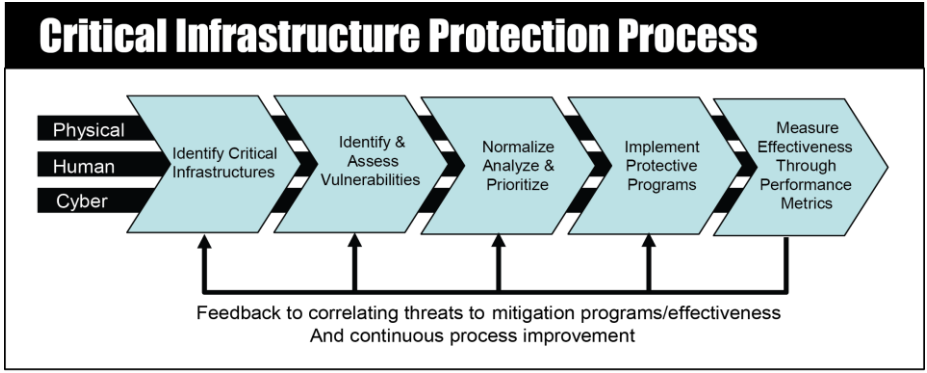
IW Adversaries to IC

- Often a criminal element not formally sponsored by the governments that commits the acts
- The European Commission recognizes the importance of 5G specifically to its sovereignty in relation to Chinese threat against CI
- Complex operations using EW, ISR, CO, and IO against Ukraine and its citizens as well as other European nations have allowed Russia to test these capabilities to their fullest degree, adding the potential to use them against Western targets



CI Vulnerabilities

- In the risk equation (Threat +Vulnerability = Risk) vulnerabilities inhabit the part of risk that CI organizations can actually directly affect
- Many CI communications, radars, and navigation systems operating within the EMS are directly vulnerable to jamming and spoofing
- The first step to exploiting these types of vulnerabilities is in knowing about them in the first place



Ref: CTS1: The Counterterrorism, WMD & Hybrid Threat SMARTbook (www.TheLightningPress.com)

Conclusion

- Although a great deal of research has been conducted regarding the effects of CO on CI, the other IRCs within the greater IW framework pose critical threats to CI
- While IW combined IRCs have not been used to their fullest potential within CI yet, the likelihood of them being used soon by adversarial governments or their adherents is high

Source: GAO analysis of Department of Defense (DOD) information. | GAO 21-525T