START

NATIONAL CONSORTIUM FOR THE
STUDY OF TERRORISM AND RESPONSES TO TERRORISM

Significant Multi-Domain Incidents Against Critical Infrastructure (SMICI)

Dr. Steve Sin
Mr. Rhyner Washburn

CAOE/SMA Age of Disruption Speaker Series

14 February 2020

Cyber-Physical Attacks on Critical Infrastructure

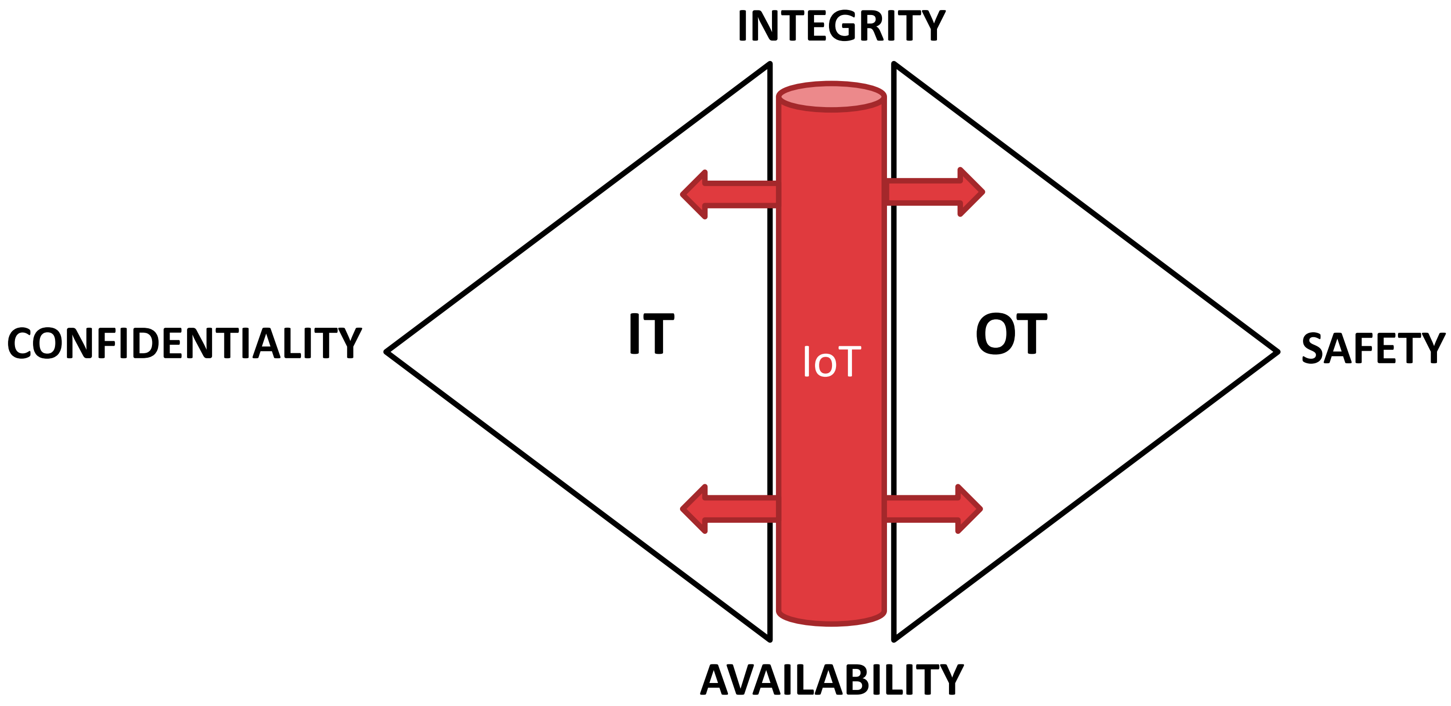
- Have the potential to damage physical infrastructure assets with widespread consequences
- One of the major homeland/national security challenges for the foreseeable future
- No dataset that aggregates publically available data on such attacks
  - Limits our ability to:
    - Gain a deeper understanding of the phenomenon
    - Hypothesize the behaviors and motivations of the attackers
  - Create a platform that can serve as a federated space for cyber incidents against critical infrastructure
- The dataset collects on 12 individual variables and currently contains 130 cyber-physical and cyber-operational incidents worldwide between January 1, 2009, and November 15, 2019

Inclusion Criteria

- Time frame:
  - Version 1: January 2009- November 2019
  - Version 1.1 and beyond: December 2019 forward

- Attack must:
  1. Originated from the cyber domain
  2. Target a critical infrastructure sector as defined by the Presidential Policy Directive 21 (PPD-21)
  3. A disruptive cyber-physical incident OR disruptive cyber-operational incident

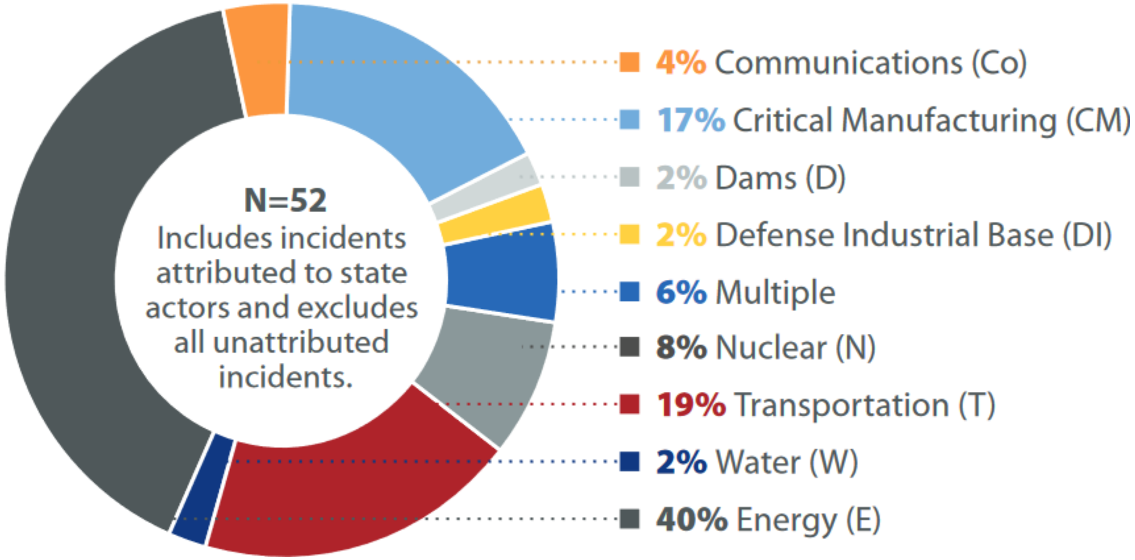
Keep it Secret (IT), Keep it Safe (OT)



CI Sectors Targeted by State Actors

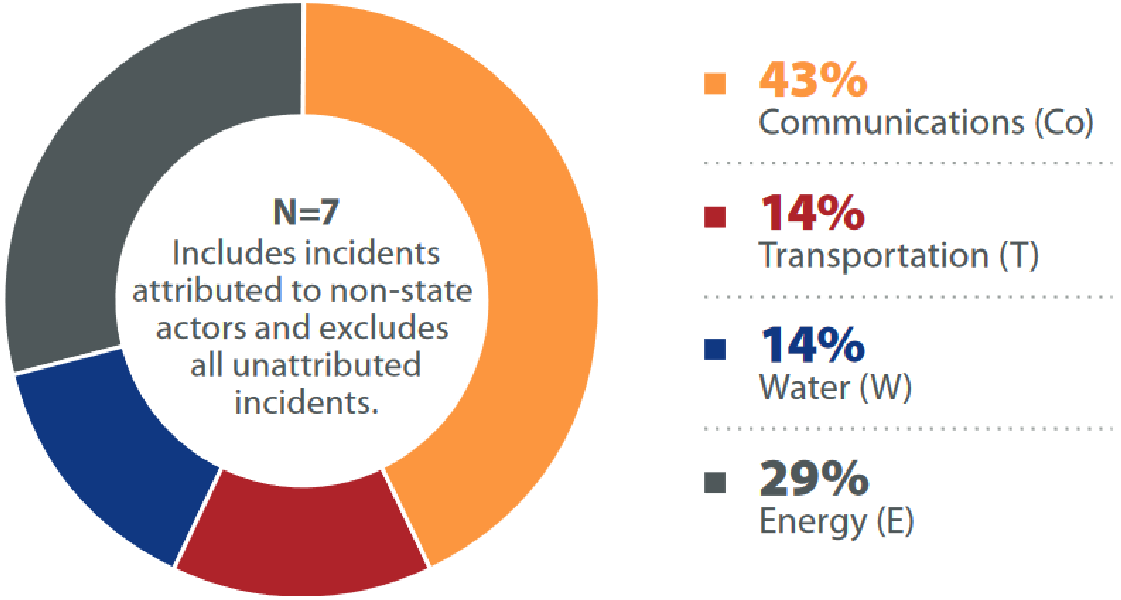
- Top sectors targeted by state actors:
  - Energy: 40%
  - Transportation: 19%
  - Critical Manufacturing:17%

- State actors, such as Russia, routinely execute campaigns in these sectors for either espionage or destructive objectives



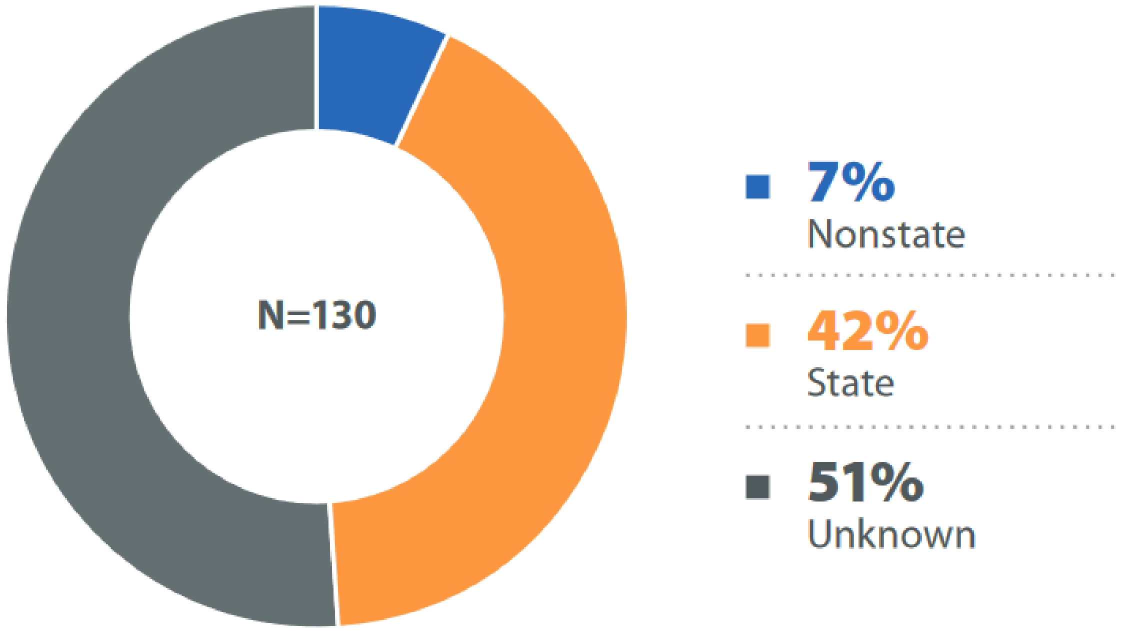
CI Sectors Targeted by Non-state Actors

- The *n* for sectors targeted by non-state actors is small, but that is expected given that the majority of non-state actor incidents in the cyber domain often remains unattributed
- It is particularly interesting that the most targeted sector is the Communications sector (43%)
- This result can be attributed to the 2016 Dyn attack involving the Mirai botnet and BrickerBot's targeting of Sierra Tel modems in 2017



State/Non-state/Unknown Share of Incidents

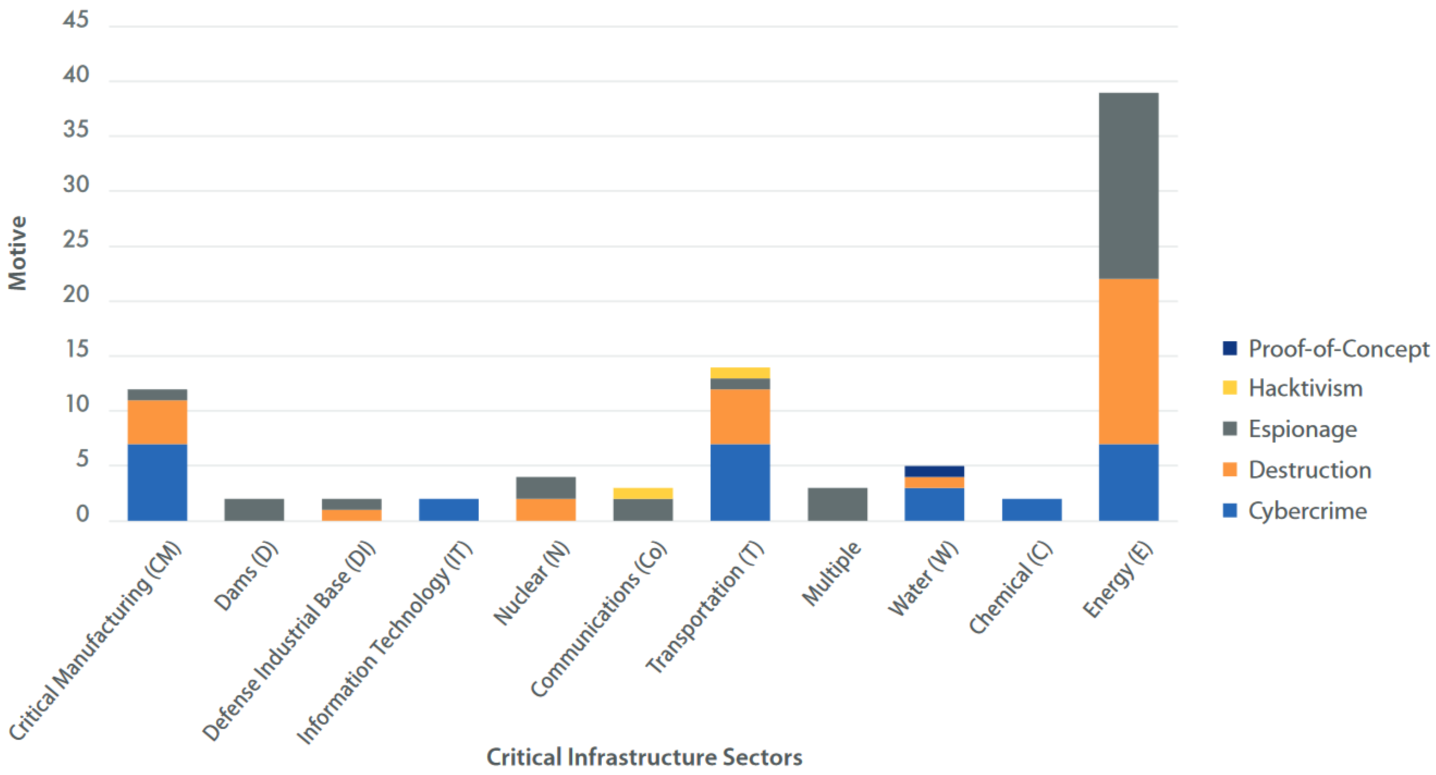
- Out of 130 incidents recorded, 64 where successfully attributed to either a state or non-state actor
  - State Actor: 42%
  - Non-state Actor: 7%
  - Unattributed/Unidentified: 51%
- Of the attributed state actors:
  - Russia – 60%
  - North Korea – 20%
  - Iran – 12%
- Mix of actors for incident attributed to non-state actors



CI Sector Targeted by Motive

Adversaries have a variety of motives for attacking critical infrastructure and the distribution of these motivations vary by sector. For example, within the Energy sector, 46% of incidents are Espionage, 39% Destruction, and 17% Cybercrime.

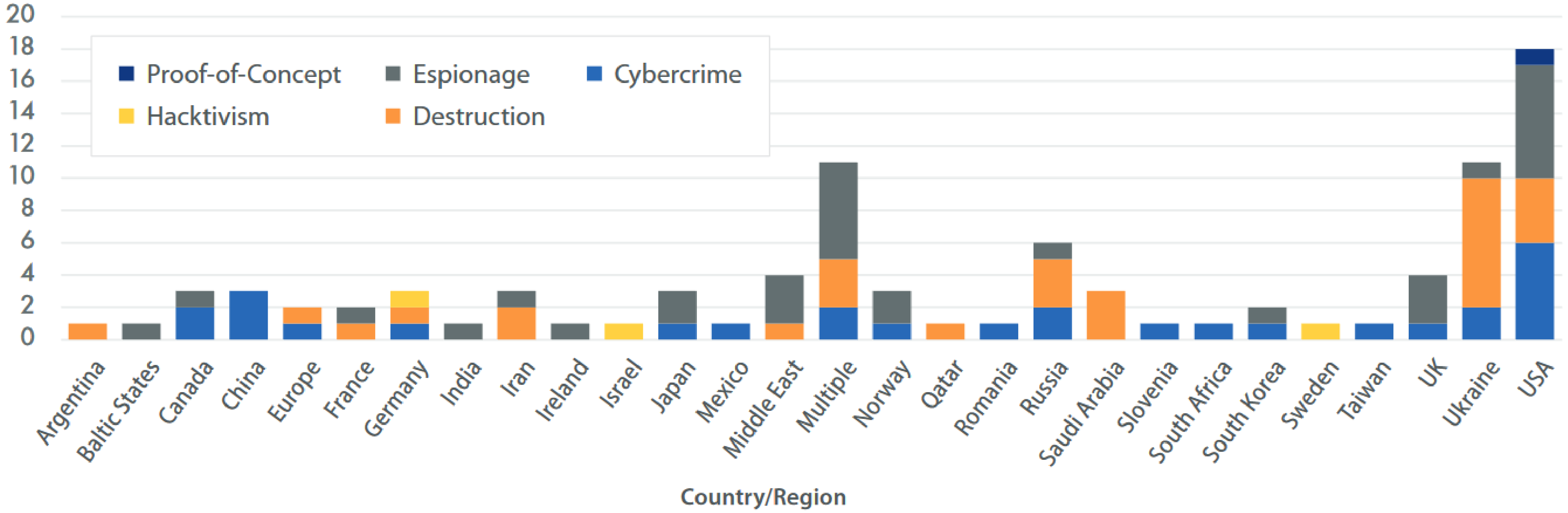
BREAKDOWN OF INCIDENT MOTIVE BY CI SECTOR



N= 88
Excludes incidents with unidentified CI sector and incidents with unidentified motive.

Countries Targeted by Motive

The United States shows to be the most targeted country regardless of motive, accounting for a little over 19% of the total incidents. Ukraine is the second most targeted country, accounting for a little less than 12% of the total incidents, ***but*** it is the most targeted country for CI destruction, accounting for approximately 28% of all destruction incidents.

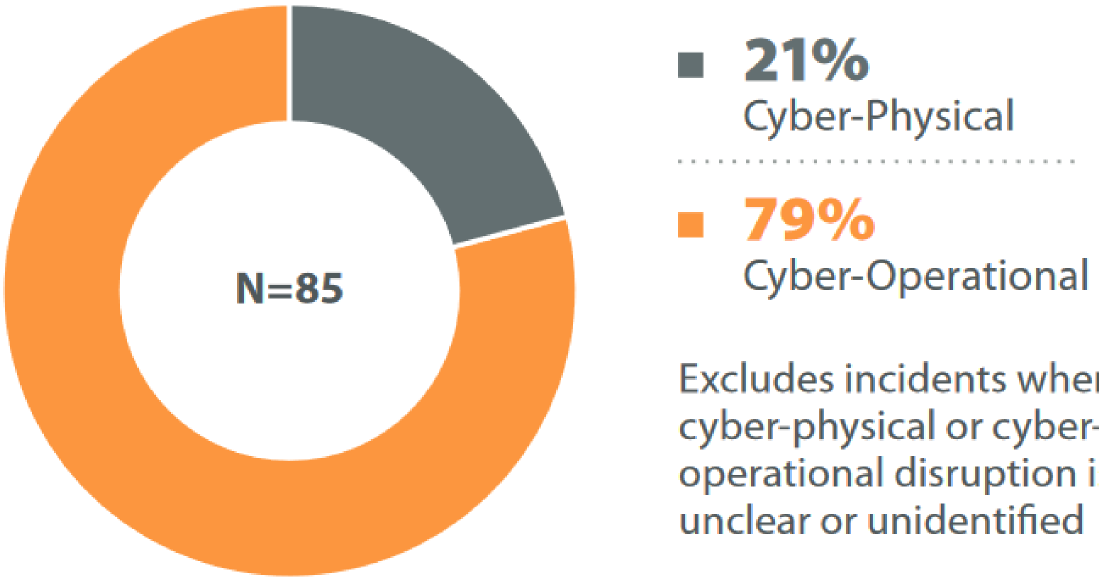


N= 93

Excludes incidents with unidentified Motive and incidents in unidentified country/region.

Disruptive Cyber-Physical/Operational Share of Incidents

- Of the 130 incidents, able to clearly identify 85 cases as either disruptive cyber-physical or cyber-operational incidents
  - 21% Cyber-physical; 79% Cyber-operational
- Cyber-physical incidents:
  - State Actor: 50%
  - Non-state Actor: 11%
  - Unattributed/unidentified: 39%
- Cyber-operational incidents:
  - State Actor: 45%
  - Non-state Actor: 7%
  - Unattributed/unidentified: 48%



Excludes incidents where cyber-physical or cyber-operational disruption is unclear or unidentified

Next Steps

- SMICI update (v1.1)
  - Complete 2019 collection and update other years with incidents missed in v1.0
  - Include more critical infrastructure sectors (Commercial, Healthcare, etc.)
- Enrich data set with new variables and features (v1.2–2.0)
  - Map incident TTPs to MITRE ATT&CK Framework
    - ATT&CK Enterprise and ICS
  - Inclusion of publicly available Indicator-of-Compromise (IoCs)
- SMICI v2.1 and beyond
  - Map incidents to National Vulnerability Database (NVD)

Thank You

Steve S. Sin, Ph.D.

sinss@umd.edu

Rhyner T. Washburn, MPS

rwburn@umd.edu