START
NATIONAL CONSORTIUM FOR THE
STUDY OF TERRORISM AND RESPONSES TO TERRORISM

RESEARCH BRIEF

Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) Dataset

As a part of an ongoing effort to better understand adversaries' multi-domain behavior and motivations, the Unconventional Weapons & Technology Division (UWT) of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) has completed the initial development of the Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) dataset, a first of its kind. The dataset, collected only using publicly available information, currently contains 130 cyber-physical and cyber-operational incidents carried out against critical infrastructure worldwide from January 1, 2009, to November 15, 2019.

The Inclusion Criteria for SMICI Dataset

1. The attack must have originated from the cyber domain;
2. The attack must target a critical infrastructure sector as defined by Presidential Policy Directive 21 (PPD-21), dated February 12, 2013; and,
3. The attack must be a disruptive cyber-physical incident OR disruptive cyber-operational incident.

Definitions of Disruptive Cyber-Physical and Disruptive Cyber-Operational Incidents

Disruptive Cyber-Physical Incidents

An incident where a threat actor – state or non-state – executes malicious action(s) in the cyber domain that have a disruptive kinetic effect(s) in the physical domain. The threat actor is able to cause disruption to operational technology (OT) by bridging the information technology (IT) and OT gap. In general, this type of incident occurs when a threat actor targeting critical infrastructure (CI) compromises Industrial Control Systems (ICS). [1]

Disruptive Cyber-Operational Incidents

An incident where a threat actor executes malicious actions through the cyber domain that have a disruptive kinetic effect in the physical domain. However, these incidents do not involve direct action(s) against ICS. Rather, these attacks are designed to disrupt the IT systems that are connected to the ICS or Internet-of-Things (IoT) systems and devices. [2] For this dataset, we include espionage incidents as cyber-operational incidents because remediation of systems after detection disrupts operations, and much of the cyber espionage in CI is interpretable as either a) conducting reconnaissance for intelligence preparation of the battlefield (IPB) or stealing intellectual property (IP) for economic purposes.

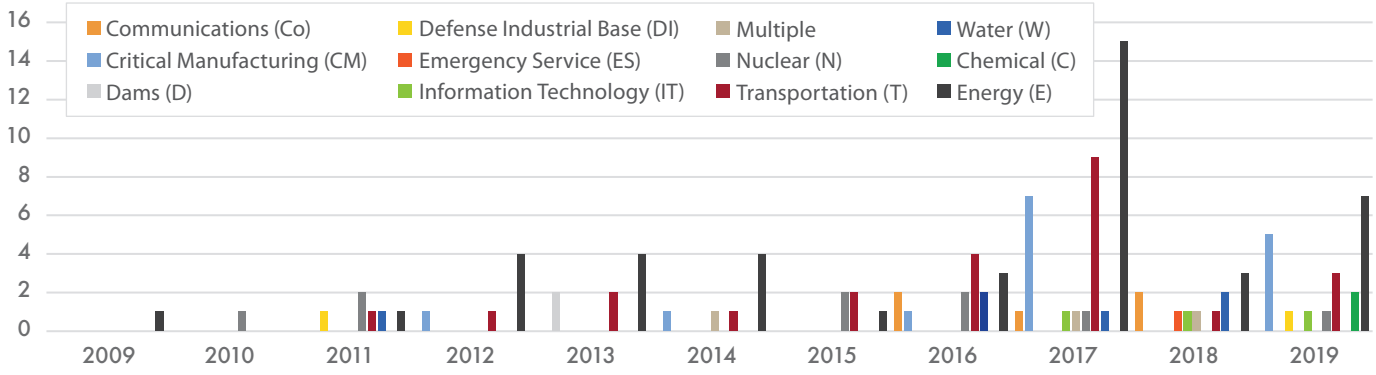
[1] ICS is the aggregation of various OT systems, devices, and process (e.g. HMIs, PLCs, RTUs, SCADA, DCUs, etc.); therefore, malware that targets OT is reported as ICS malware. To date, ICS malware is exceptionally rare and only five types of ICS malware have been publicly reported as involved in disruptive cyber-physical incidents: Stuxnet, Havex, BlackEnergy (BE3 in particular), Industroyer/CRASHOVERRIDE, and Triton/Trisis. Havex and BlackEnergy (BE2 AND BE3) interacted with ICS systems, but did not directly cause cyber-physical disruption. The original design of BlackEnergy malware was for cybercrime.

[2] Ransomware and wiper malware are particularly effective in these incidents; however, sophisticated use of IoT malware such as BrickerBot and Mirai demonstrate the adaptability of the malware development and the vulnerability of our critical infrastructure to such threats.

PRIMARY TAKEAWAYS OF THE SMICI DATASET

1. Incidents by Critical Infrastructure Sectors, 2009-2019*

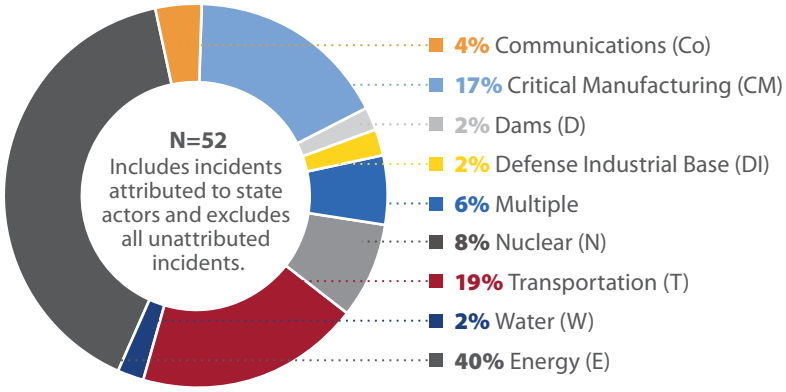
Of the critical infrastructure sectors observed, we noted a consistent targeting in two sectors, Energy (37%) and Transportation (23%). The Critical Manufacturing (13%) and Nuclear (7%) sectors followed as third and fourth, respectively. The spike for the Energy and Transportation sectors in 2017 is due to the worldwide disruptions brought on by the ransomware WannaCry in May 2017 and the wiper malware NotPetya in June. In continuing this research, we will expand the dataset to include other CI sectors, namely Financial Services.



N=115
Includes all incidents against identified CI sectors.
*Data collection endpoint: November 15, 2019.

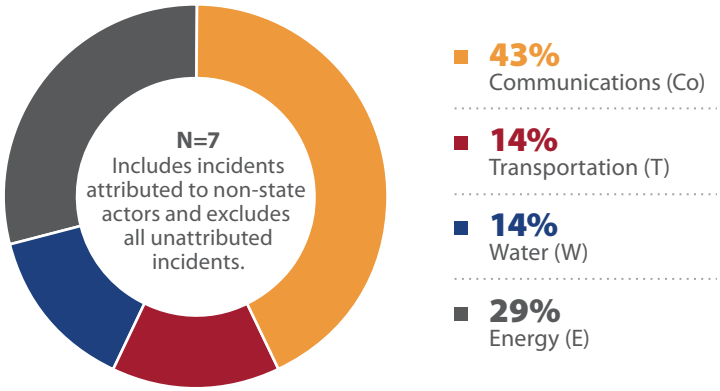
2. CI Sectors Targeted by State Actors

Top sectors targeted by state actors are Energy (40%), Transportation (19%), and Critical Manufacturing (17%). State actors, such as Russia, routinely execute campaigns in these sectors for either espionage or destructive objectives. We mention Russia in particular because it or threat actors tied to the Russian government have been attributed the most for targeting all of the CI sectors, especially Energy.



3. 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. [3] [4]

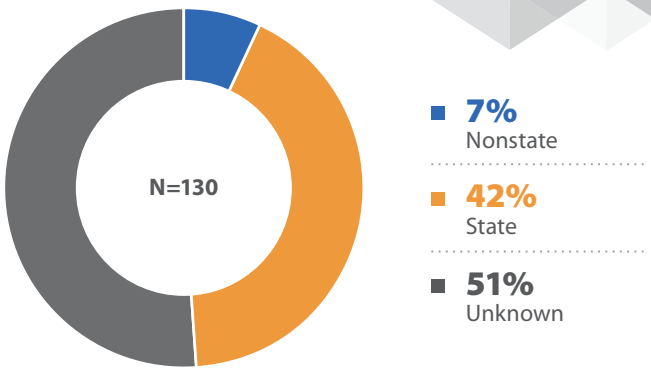


[3] Paul Roberts, 2017. "Mirai Attack Was Costly For Dyn, Data Suggests." The Security Ledger, February 3. https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/.

[4] Catalin Cimpanu, 2017. "US ISP Goes Down as Two Malware Families Go to War Over Its Modems." BleepingComputer, April 25. https://www.bleepingcomputer.com/news/security/us-isp-goes-down-as-two-malware-families-go-to-war-over-its-modems/.

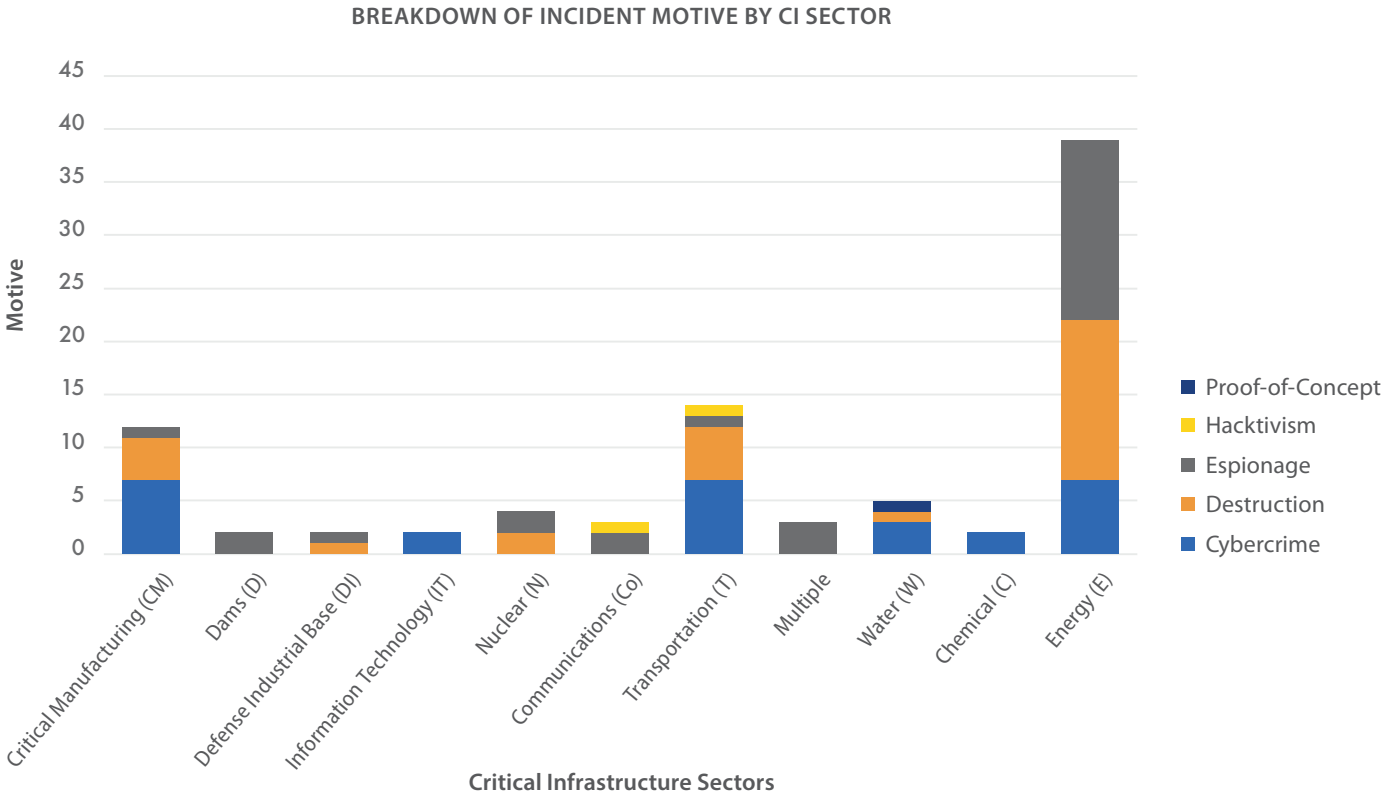
4. State/Non-state/Unknown Share of Incidents

Out of 130 incidents recorded, 64 where successfully attributed to either a state or non-state actor. As shown in the pie chart below, a little over 50% of the attacks were unattributed. State actors are attributed to 42% of incidents whereas non-state actors account for 7% of incidents.[5] Of the attributed state actors, Russia accounted for 60%, North Korea 20%, and Iran 12%.[6]



5. 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.



N= 88

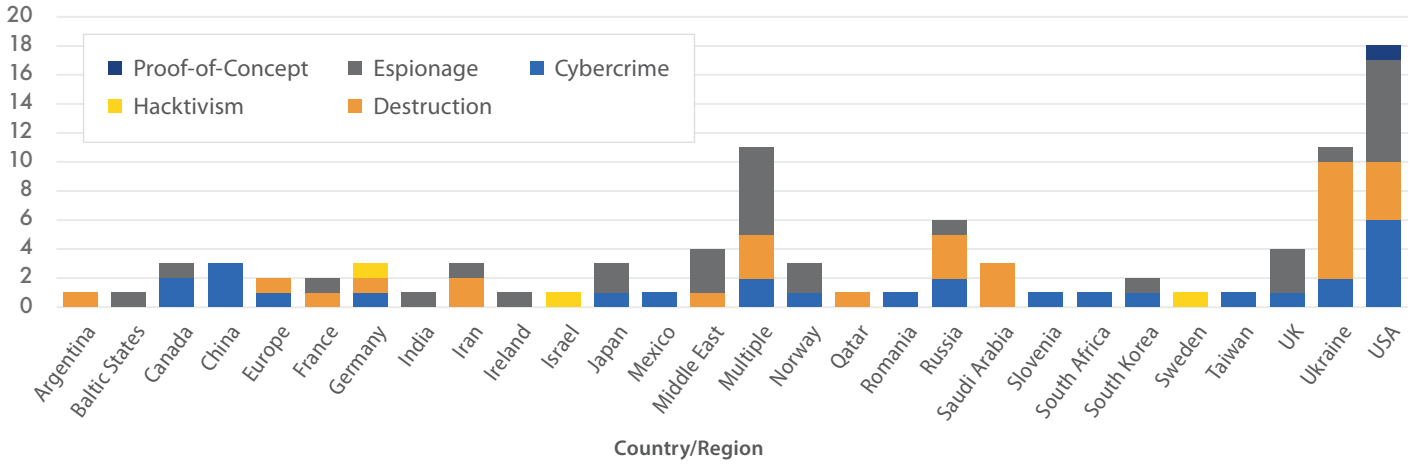
Excludes incidents with unidentified CI sector and incidents with unidentified motive.

[5] This breakdown is in line with the criteria for this dataset because we excluded incidents such as website defacement and most types of distributed denial of service (DDoS) which are mostly caused by non-state actors. Defacement and DDoS serve to disrupt operations for the victim; however, our definition of operational disruption focuses on incidents causing severe disruptions to critical infrastructure and/or having an effect in the physical domain. DDoSing a website is minimal in disruption, but attacking the Domain Name System (DNS) server infrastructure of a company, (e.g. Dyn 2016) that services tens of thousands of websites and online services from utility billing to social media is far more severe and disruptive.

[6] As we continue to build out the dataset, we anticipate the attribution share to decrease because of the inherent difficulty of ascribing attribution as well as the security and legal barriers associated with reporting cyber incidents in general.

6. 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.

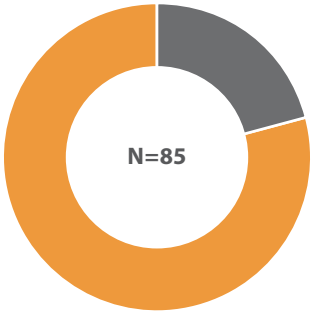


N= 93

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

7. Disruptive Cyber-Physical/Operational Share of Incidents

Of the 130 incidents collected in the dataset, we were able to clearly identify 85 cases as either disruptive cyber-physical (21%) or cyber-operational (79%). Of the cyber-physical incidents, 50% of the incidents were attributed to state actors, 11% to non-state actors, and 39% were unattributed/unidentified.[7]



21%
Cyber-Physical

79%
Cyber-Operational

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

[7] Of the incidents by unidentified actors, we assess with moderate confidence four of them were state actors. However, limited open-source information prevents us from coding those incidents with both or either "attributed" and "state actor" variables.

ABOUT THIS REPORT

UWT
UNCONVENTIONAL **WEAPONS AND TECHNOLOGY**

Project Lead: **Dr. Steve Sin**, UWT Director at START
Project Researcher: **Rhyner Washburn**, Cyber Intelligence Researcher at START

Please direct questions to Dr. Steve Sin at sinss@umd.edu, or Rhyner Washburn at rwburn@umd.edu.

START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based research, education and training center comprised of an international network of scholars committed to the scientific study of terrorism, responses to terrorism and related phenomena. Led by the University of Maryland, START is a Department of Homeland Security Emeritus Center of Excellence that is supported by multiple federal agencies and departments. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and effects of terrorism; the effectiveness and impacts of counterterrorism and CVE; and other matters of global and national security. For more information, visit www.start.umd.edu or contact START at infostart@umd.edu.