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

UWT
UNCONVENTIONAL WEAPONS AND TECHNOLOGY

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 expanded upon its initial development of the Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) dataset. The dataset, collected using only publicly available information, contains 524 cyber-operational and cyber-physical incidents carried out against critical infrastructure worldwide from January 1, 1992, to July 9, 2021.

Definitions of Cyber-Operational and Cyber-Physical Incidents

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 against operational technology (OT) such as Industrial Control Systems (ICS).[1] Rather, these attacks disrupt information technology (IT) that is assistive to business and operational processes.[2]

Cyber-Physical Incidents

An incident where a threat actor – state or non-state – executes malicious actions in the cyber domain that have a damaging kinetic effect in the physical domain. Threat actors can cause damage in OT environments by bridging IT/OT gaps or directly attacking OT.[3] ICS malware is exceptionally rare and only seven variants of ICS malware have been publicly reported as involved in cyber-physical incidents.[4]

DATA AND METHODOLOGY

The dataset collects information on 41 individual variables organized into eight categories: Actor, Target Country, Specific Target, Geographic, Malware/Technical, Temporal, Impact, and Miscellaneous. Collection of data is by publicly available sources only. Credible social media sources, news reporting, and industry briefs/reports are the primary sources used in the data collection. We intend to continue the collection effort, improve data granularity, and expand the dataset temporally, with current the collection effort focused on 2021 and 2022.

[1] ICS is the aggregation of various OT systems, devices, and process (e.g., HMIs, PLCs, RTUs, SCADA, DCUs, etc.)

[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.

[3] Malware that targets OT is coded as ICS malware.

[4] Stuxnet, Incontroller/PipeDream, Havex, BlackEnergy (BE3 in particular), Industroyer/CRASHOVERRIDE, Industroyer2, and Triton/Trisis. Havex and BlackEnergy (BE2 AND BE3) interacted with ICS systems, but they did not directly cause cyber-physical damage.

Inclusion Criteria

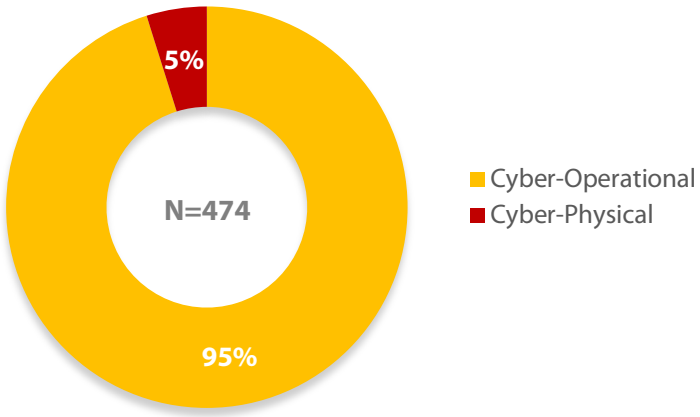
For an incident to be considered for inclusion in the SMICI dataset, the incident must meet the following base inclusion criteria:

1) Attack originated in the cyber domain.
2) Attack targeted a critical infrastructure sector as defined by Presidential Policy Directive 21 (PPD-21), dated February 12, 2013.
3) Attack must be cyber-physical OR cyber-operational.

TAKEAWAYS OF THE SMICI DATASET

Cyber-Operational and Cyber-Physical Share of Incidents

Of the 524 incidents collected in the dataset, we were able to clearly identify 474 incidents as either cyber-operational (95%) or cyber-physical (5%). Excludes incidents where cyber-physical or cyber-operational is unclear or unidentified.

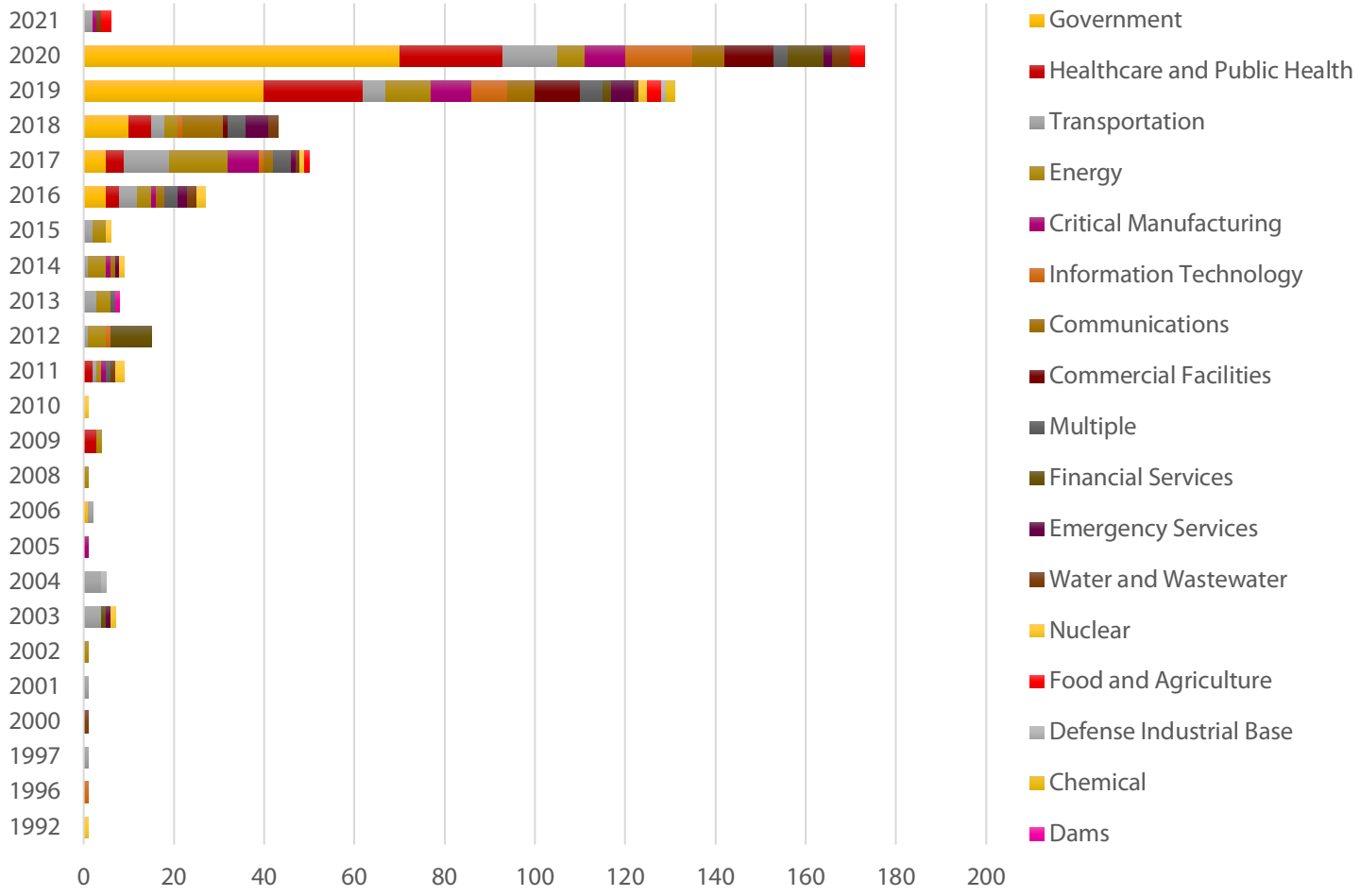


Incidents by Critical Infrastructure Sector, 1992-2021

Of the critical infrastructure sectors observed, Transportation (11%) and Energy (11%) sectors are consistently targeted over multiple years, with significant activity in 2017 due in part to the worldwide disruptions brought on by the ransomware WannaCry in May 2017 and the wiper malware NotPetya in June. The significant rise of coded incidents meeting SMICI criteria from 2016 to 2020 is due, in part, to:

- Diffusion of technology and technical instruction enabling more actors of lesser sophistication to conduct cyberattacks.
- Development and resiliency of illicit services and markets for and by threat actors motivated by financial gain (e.g., Ransomware as a Service, bulletproof hosting).
- Increased integration of new technologies and processes (e.g., cloud computing, IoT, A.I.) with less secure systems not originally designed to be connected to the Internet or information communication technology (ICT) in general.
- Increased quantity and quality of credible industry, government, and media entities reporting on cyber incidents as larger more disruptive and damaging cyberattacks occur, impacting tens of thousands of companies and millions of people across the world simultaneously.

With this research, we are continually expanding the dataset temporally with the current collection effort focused on 2021 and 2022. Additionally, we conduct end-of-year reviews of past years for potential incidents that may have been missed in the initial coding.

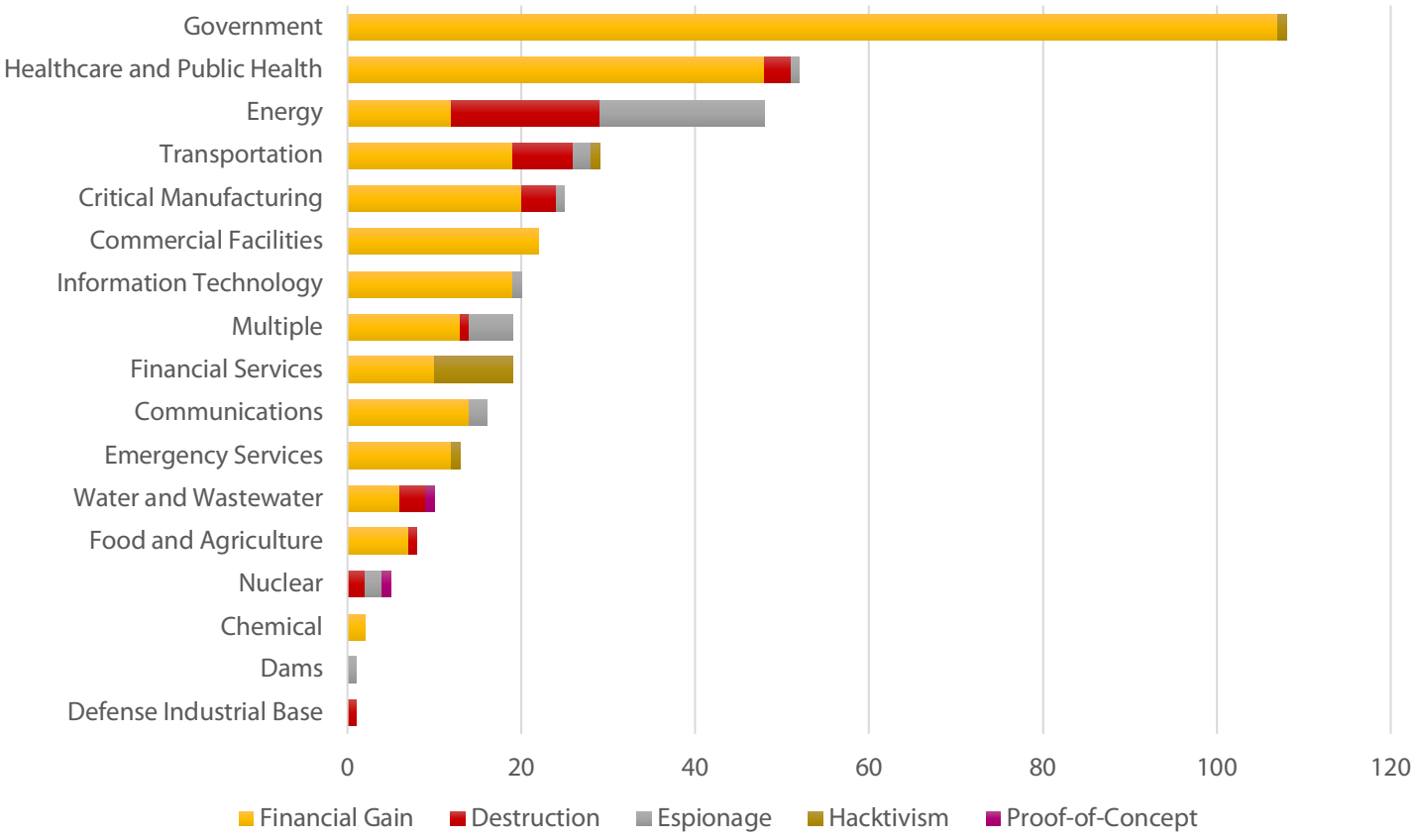


N=505

Excludes incidents with unidentified sectors.

Sectors Targeted by Motive

Adversaries have a variety of motives for attacking critical infrastructure and the distribution of these motivations varies by sector. For example, Government, and Healthcare and Public Health sectors account for 52% of all financially motivated incidents whereas Energy (45%) and Transportation (18%), and Critical Manufacturing (10%) account for 73% of destruction motivated incidents.



N=398

Excludes incidents with unidentified sectors and incidents with unidentified motive.

Financial Gain

Target selection can be opportunistic or targeted. These threat actors often extort and steal from victims who: have the most to lose, cannot remain inoperable for an extended time, or are visibly easy targets.

Destruction

No extortion or compromising. Target selection is rarely opportunistic. Threat actors pursuing destruction aim to cause maximum harm. Disrupt, degrade, and destroy.

Espionage

Focused, subtle, with the aim of exfiltrating as much data as possible. Threat actors engaging in espionage will not intentionally cause excessive damage or disruption unless it aids them (e.g., mitigating detection and attribution).

Hacktivism

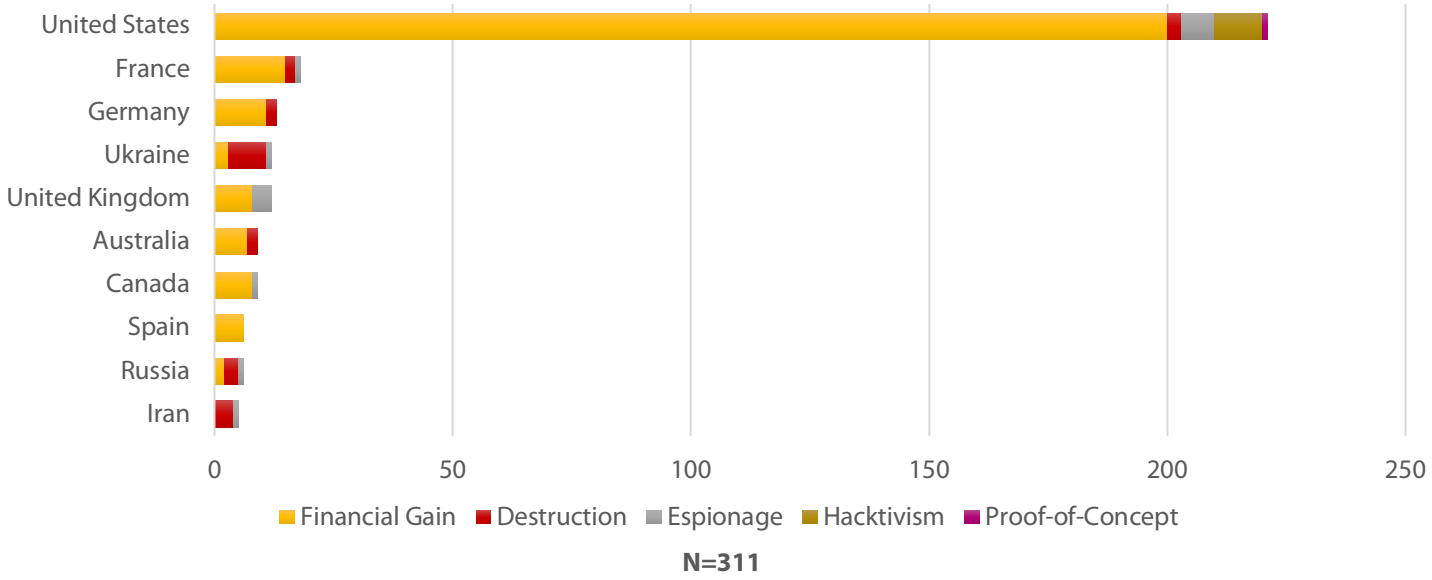
Influence public opinion, humiliate a target, make a political statement, or "do it for the lulz." For these threat actors, the message is the priority; any damage or disruption caused is often immaterial.

Proof-of-Concept

Not necessarily malicious but does have the capacity to cause damage or disruption (e.g., academic experiments that "got loose," or a grey hat demonstrating a security vulnerability without permission).

Top 10 Countries Targeted by Motive

The United States shows to be the most targeted country regardless of motive, accounting for over 77 percent of the total incidents.[5] Ukraine is the fourth most targeted country, but it is the most targeted country for destruction, accounting for approximately 33 percent of all destruction incidents.

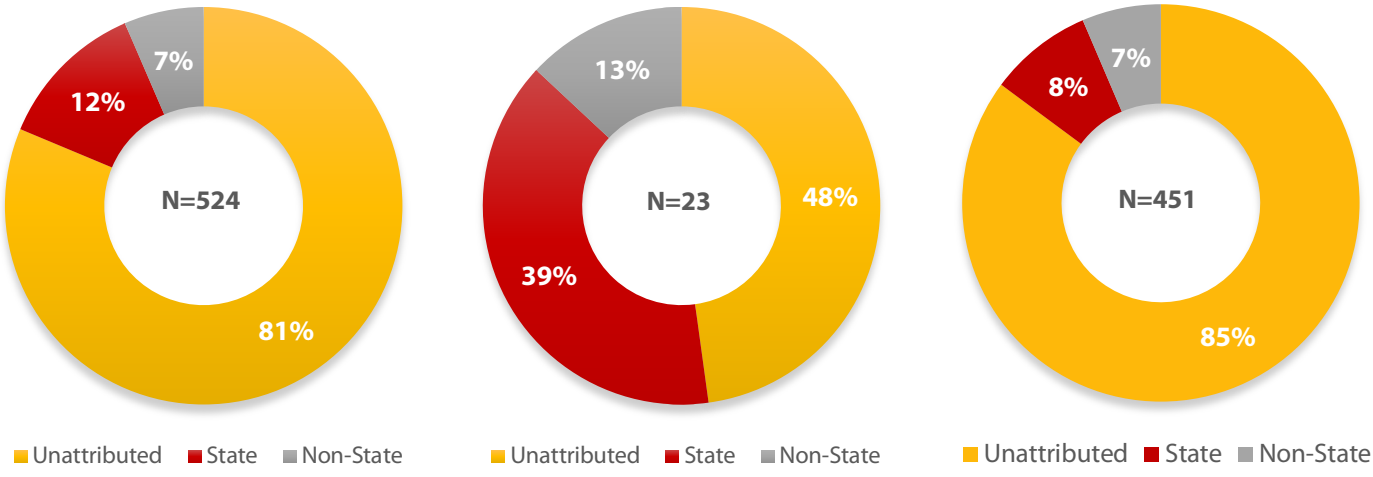


N=311

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

Breakdown of Actor Share of Incidents

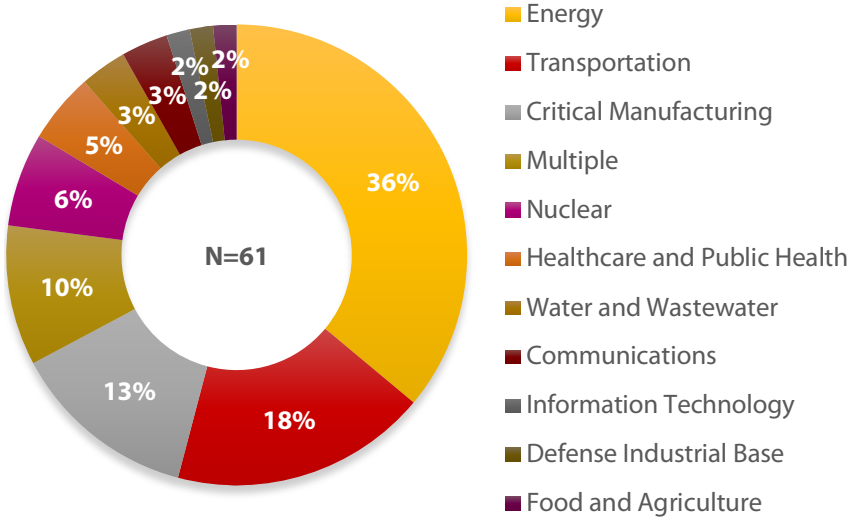
Out of 524 incidents recorded, 12 percent were successfully attributed to state actors and 7 percent to non-state actors. As shown in the pie chart, 81 percent of the incidents were unattributed. Of the cyber-physical incidents (*n*=23), 39 percent were attributed to state actors and 13 percent to non-state actors. In contrast, 8 percent and 7 percent of cyber-operational incidents (*n*=451) were attributed to state and non-state actors, respectively. This subset of incidents also had the largest percentage, at 85 percent, of unattributed incidents.



[5] Language and source credibility are partially the reason the United States is heavily represented in the database. In particular, the searchability and accessibility of U.S. local, state, and national news reporting significantly aids in identifying and verifying incidents quickly and efficiently. We are in the process of improving our collection and verification of incidents outside the United States.

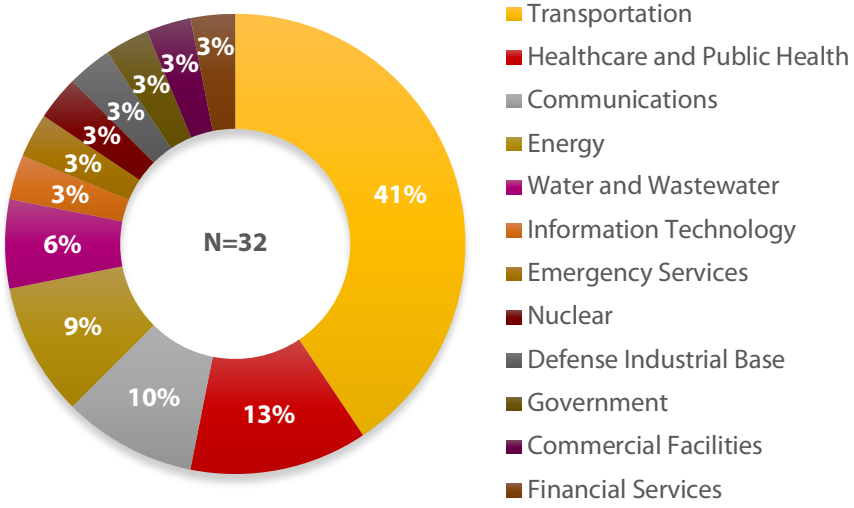
Sectors Targeted by State Actors

The top sectors targeted by state actors are Energy (36%), Transportation (18%), and Critical Manufacturing (13%). State actors, such as Russia, routinely execute campaigns in these sectors for either espionage or destructive objectives. We mention Russia specifically because it or threat actors tied to the Russian government have been attributed the most for targeting all of the CI sectors, especially Energy. Of the attributed state actors, Russia accounted for 54 percent, North Korea 19 percent, and Iran 16 percent.[6]



Sectors Targeted by Non-State Actors

The most targeted sector is the Transportation sector (41%), and many of those incidents involved disgruntled (ex)employees. The n for sectors targeted by non-state actors is small because attribution is difficult to ascertain. For example, attribution is often obtained through identifying the TTPs and the IOCs during remediation efforts of an incident. This can aid in attributing an incident to a threat actor. Actor type in SMICI is coded for non-state when an individual(s) has been identified namely through a) public arrest notification, or b) self-identification/admission.



[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 incidents in general.

ABOUT THIS REPORT

Principal Investigator: **Dr. Steve Sin**, UWT Director at START
Project and Data Collection Manager: **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.

This material is based upon work supported by the Department of Defense Basic Research Office under Contract No. HQ003421F0481 and work supported by internal START resources. Any opinions, findings, and conclusions or recommendations expressed are those of the authors and do not necessarily reflect the views of the Department of Defense, the University of Maryland, or START.

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 start.umd.edu or contact START at infostart@umd.edu.