Unified Model and Dataset for Cyber-Enabled Influence Operations

Jim Morris* **Lucia Falzon**** **Lucy Fidock*** **Hung Nguyen***

{jim.morris, hung.nguyen, lucia.falzon, lucy.fidock}@adelaide.edu.au

***University of Adelaide, **Consunet Pty Ltd**

INTRODUCTION

Cyber-enabled influence operations (CEIOs) are influence operations *that integrate sophisticated hacking techniques with influence campaigns*. **We build a unified model and an open-source database of CEIOs**. Our model combines the MITRE ATT&CK and DISARM frameworks, which denote cyberattack and influence components, respectively. Users can construct CEIO data using our framework through a GUI builder.

There are currently **15 real-world** CEIOs in our dataset.

Model, code and data are available at: https://github.com/ceios/ceios

MOTIVATION

- Prevalence of CEIOs has been rapidly increasing over the last few decades.[1]
- There is a need to monitor, analyse, prevent, predict, and disrupt CEIOs.
- **No** standardised, comprehensive framework to describe and model CEIOs
- **No** centralised resource dedicated to collating all publicly available information on CEIOs.

→ Urgent need for a unified model and appropriately sized datasets for CEIOs.

CHALLENGES AND CONTRIBUTION

Challenges:

- Lack of available, accessible, and quality data and analyses to help discover, research, and model CEIOs.
- Lack of standardised model and terminology for CEIOs.
- No program currently which models a unified framework of ATT&CK and DISARM in STIX format.

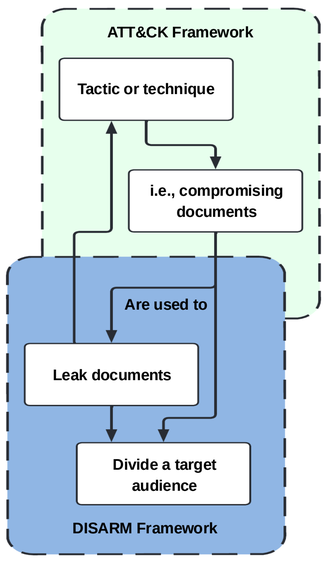
Contribution:

- A standardised model for CEIOs – combining ATT&CK and DISARM in STIX format
- An open-source software CEIO attackflow builder for constructing CEIO data
- A **centralised database** to collate and **model** available information on **CEIOs**.
- **Use cases:** Our data can be analysed to gain insights into CEIOs including common procedural actions, common procedural styles of threat actors, etc. All to better predict, prevent, and disrupt future CEIOs.

UNIFIED FRAMEWORK

We propose a unified framework that can be used to model and analyse cyber-influence operations. To **enhance** the **collaboration and interoperability** of the threat intelligence, the framework models can be exported into the standardized STIX format.

- The individual frameworks are **MITRE ATT&CK**[2] (cyber-attack components) and **DISARM**[3] (influence operation components).



- These frameworks are a suitable solution because they share a similar language and format, and both cover a sufficiently broad scope of their respective operations.
- ATT&CK has a well-established knowledge base with a large and actively contributing community.
- DISARM builds on existing frameworks and efforts to understand disinformation campaigns.
- DISARM was designed through a collaborative effort that included MITRE with STIX compatibility. Thus, it **integrates easily** into the ATT&CK ecosystem.

ATTACK FLOW BUILDER MODIFICATIONS

Current Application

Cyber-attack modelling with the ATT&CK framework but no support for Influence operations.

Modified Application

Integrates the DISARM framework.
Enables **CEIO** modelling with the unified framework.

https://github.com/ceios/ceios/builder

OUR OPEN-SOURCE CEIO DATASET

Documentation

- A **summary, timeline and context** of the incident or operation.
- The operations described using the **unified framework**, with tactics and techniques categorized as cyber-attack or influence.

Resources

The entry contains the resources used to produce the documentation, captured as found during research. This is to ensure **reproducibility** and preserves information.

Disarm-Attack Flow Model

Each entry has an **interoperable and visual model** of the operation in STIX format.

- Each action (node) represents a tactic or technique
- The connections (edge) show the procedural sequences and relationships between tactics and techniques.

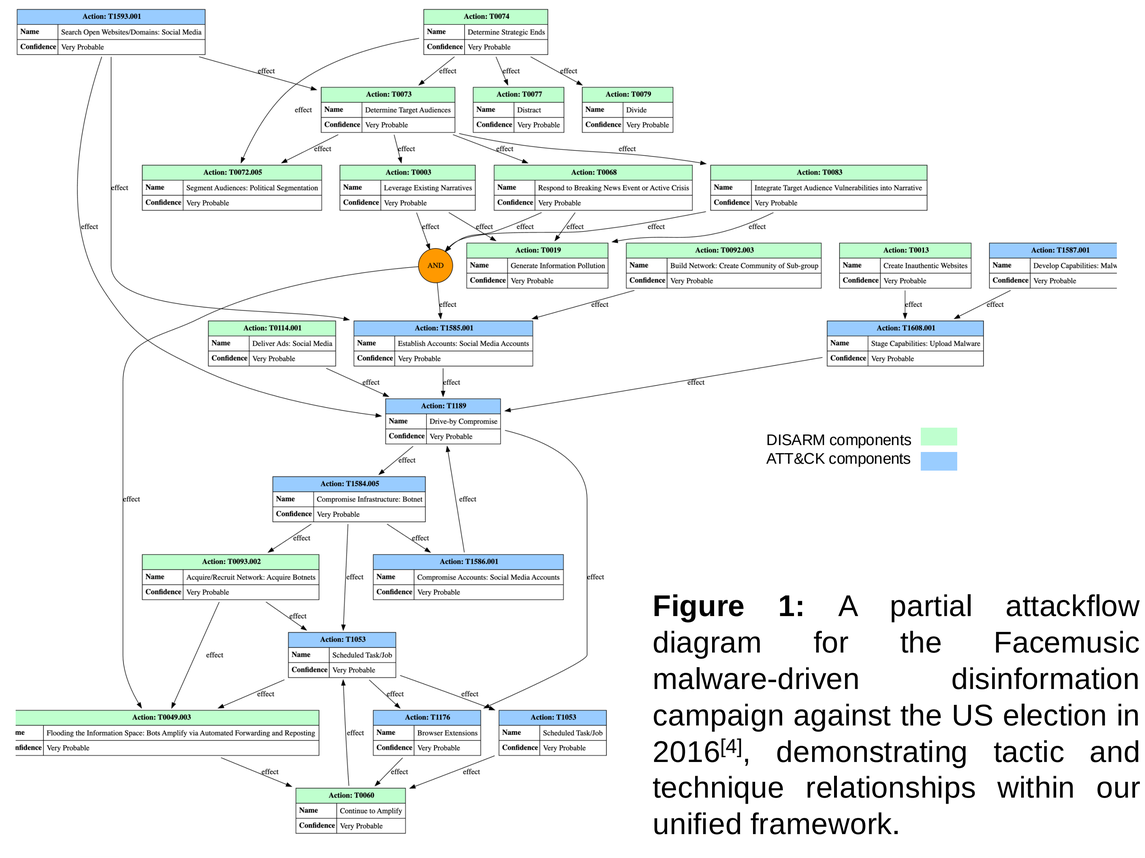


Figure 1: A partial attackflow diagram for the Facemusic malware-driven disinformation campaign against the US election in 2016[4], demonstrating tactic and technique relationships within our unified framework.

Figure 2: The comprehensive diagram for the FaceMusic disinformation campaign. This highlights the sophistication that CIOs can achieve.

CEIOs IN 2024

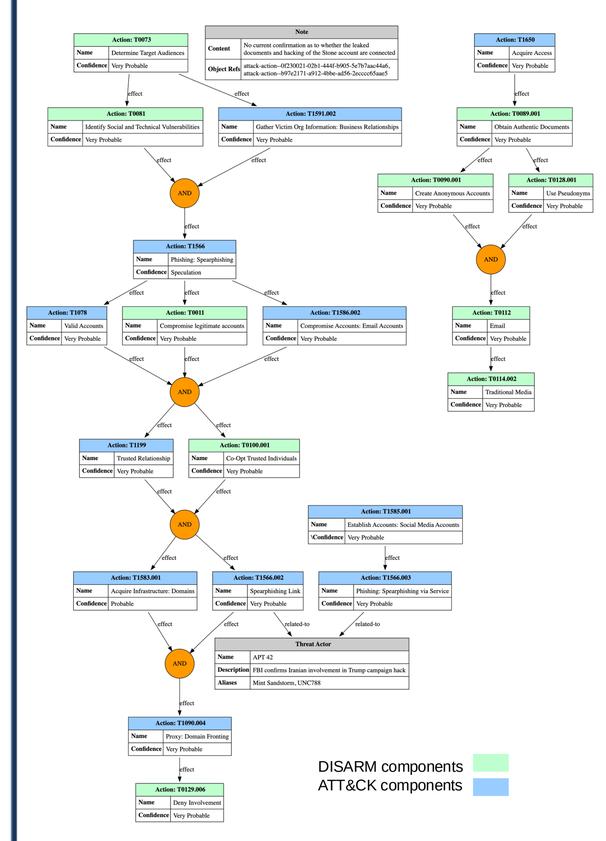


Figure 3: Attackflow diagram of the on-going Iranian CEIO campaign against US 2024 election.

ANALYSIS

Exploratory Data Analysis

- Common **successful attack avenues**
- Preferred disinformation **dissemination mediums**
- **Motives** of threat actors and CEIOs
- **Common relationships** between tactics, techniques, and procedures.

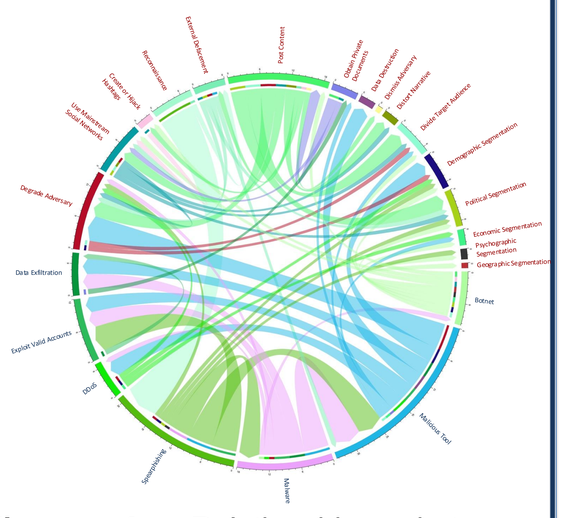


Figure 4: Relationships between DISARM (red) and ATT&CK (blue) tactics and techniques in our dataset.

[1] Vićić, J. and Harknett, R. (2024). *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspace.* Intelligence and National Security, 39(5), pp. 897–914. doi: 10.1080/02684527.2023.2300933.
[2] *MITRE ATT&CK Get Started* (2024) *Get Started | MITRE ATT&CK®*. Available at: https://attack.mitre.org/resources/.
[3] *What is the DISARM Framework*. Available at: https://www.disarm.foundation/framework.
[4] Etudo, U., Whyte, C., Yoon, V. and Yaraghi, N., 2023. *From Russia with fear: fear appeals and the patterns of cyber-enabled influence operations*. Journal of Cybersecurity, 9(1).