A Diamond is an Analyst’s Best Friend:
The Diamond Model for Influence Operations Analysis
Charity Wright
@CharityW4CTI
Threat Intelligence Analyst
Insikt Group, Recorded Future

Current:
❖ Influence operations
❖ Geopolitical intelligence
❖ Strategic intelligence

Previously:
❖ US Government
   ➢ Mandarin Linguist
   ➢ Military Intelligence Analyst
❖ Enterprise CTI (Hilton, EY)
❖ CTI Vendors: Cybercrime, strategic intelligence
Agenda

- What is “influence ops” vs “disinfo” vs “fake news”?
- IO as a threat to public and private sector
- Existing frameworks: What we have been doing
- The Core: Narrative warfare
- The Future: The Diamond Model for IO
  - Technical Axis
  - Socio-political Axis
- Example 1: Corporate disinformation
- Example 2: State-sponsored political influence operation
## Important Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>misinformation</td>
<td>“false information that is spread, regardless of whether there is intent to mislead.”</td>
</tr>
<tr>
<td>disinformation</td>
<td>“deliberately misleading or biased information; manipulated narrative or facts; propaganda.”</td>
</tr>
<tr>
<td>fake news</td>
<td>&quot;purposefully crafted, sensational, emotionally charged, misleading or totally fabricated information that mimics the form of mainstream news&quot;</td>
</tr>
</tbody>
</table>
BREAKING: COUNTLESS PEOPLE ON FACEBOOK

STILL SHARING FAKE NEWS SITES, DISREGARDING ANY USE OF LOGIC OR CRITICAL THINKING
Influence Operations

Organized attempts to achieve a specific effect among a target audience.

Attempts to affect the decision-making, beliefs, and opinions of a target audience.
Previous Analysis Revolved Around:

Content = The NARRATIVE (story)

Voice = The accounts involved

Dissemination = The way the information spreads across platforms
Citizens will find themselves in the digital crossfire of international conflicts that exploit online platforms with convincing disinformation campaigns.

1 Reconnaissance
An adversary identifies target attributes and monitors online platforms.

2 Weaponization
Realistic false content is created with AI-enabled software.

3 Attack
False content is planted in promising online venues (e.g., groups, hashtags, messages).

4 Infection
Bots and algorithms share and drive engagement with false content.

5 Impact
False narratives overcome factual ones and spur beliefs and actions favorable to the adversary.

Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation
<table>
<thead>
<tr>
<th>TA01 Strategic Planning</th>
<th>TA02 Objective Planning</th>
<th>TA03 Develop People</th>
<th>TA04 Develop Networks</th>
<th>TA05 Microtargeting</th>
<th>TA06 Develop Content</th>
<th>TA07 Channel Selection</th>
<th>TA08 Pump Priming</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0001 5Ds (dismiss, distort, distract, dismay, divide)</td>
<td>T0005 Center of Gravity Analysis</td>
<td>T0007 Create fake Social Media Profiles / Pages / Groups</td>
<td>T0010 Cultivate ignorant agents</td>
<td>T0016 Clickbait</td>
<td>T0019 Generate information pollution</td>
<td>T0029 Manipulate online polls</td>
<td>T0039 Bait legitimate influencers</td>
</tr>
<tr>
<td>T0002 Facilitate State Propaganda</td>
<td>T0006 Create Master Narratives</td>
<td>T0008 Create fake or imposter news sites</td>
<td>T0011 Hijack legitimate account</td>
<td>T0017 Promote online funding</td>
<td>T0020 Trial content</td>
<td>T0030 Backstop personas</td>
<td>T0040 Demand unsurmountable proof</td>
</tr>
<tr>
<td>T0003 Leverage Existing Narratives</td>
<td>T0009 Create fake experts</td>
<td>T0012 Use concealment</td>
<td>T0018 Paid targeted ads</td>
<td>T0021 Memes</td>
<td>T0031 YouTube</td>
<td>T0041 Deny involvement</td>
<td></td>
</tr>
<tr>
<td>T0004 Competing Narratives</td>
<td>T0013 Create fake websites</td>
<td>T0022 Conspiracy narratives</td>
<td>T0032 Reddit</td>
<td>T0042 Kernel of Truth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0005 Distort facts</td>
<td>T0010 Create fake videos and images</td>
<td>T0023 Leak altered documents</td>
<td>T0033 LinkedIn</td>
<td>T0043 Use SMS/WhatsApp/Chat apps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0006 Create Master Narratives</td>
<td>T0012 Use concealment</td>
<td>T0018 Paid targeted ads</td>
<td>T0021 Memes</td>
<td>T0031 YouTube</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0007 Create fake Social Media Profiles / Pages / Groups</td>
<td>T0011 Hijack legitimate account</td>
<td>T0017 Promote online funding</td>
<td>T0020 Trial content</td>
<td>T0030 Backstop personas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0008 Create fake or imposter news sites</td>
<td>T0012 Use concealment</td>
<td>T0018 Paid targeted ads</td>
<td>T0021 Memes</td>
<td>T0031 YouTube</td>
<td>T0041 Deny involvement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0009 Create fake experts</td>
<td>T0013 Create fake websites</td>
<td>T0022 Conspiracy narratives</td>
<td>T0032 Reddit</td>
<td>T0042 Kernel of Truth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0010 Cultivate ignorant agents</td>
<td>T0016 Clickbait</td>
<td>T0019 Generate information pollution</td>
<td>T0029 Manipulate online polls</td>
<td>T0039 Bait legitimate influencers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0011 Hijack legitimate account</td>
<td>T0012 Use concealment</td>
<td>T0018 Paid targeted ads</td>
<td>T0020 Trial content</td>
<td>T0030 Backstop personas</td>
<td>T0040 Demand unsurmountable proof</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0013 Create fake websites</td>
<td>T0022 Conspiracy narratives</td>
<td>T0032 Reddit</td>
<td>T0042 Kernel of Truth</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0014 Create funding</td>
<td>T0023 Distort facts</td>
<td>T0033 LinkedIn</td>
<td>T0043 Use SMS/WhatsApp/Chat apps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T0015 Use fake experts</td>
<td>T0025 Leak altered documents</td>
<td>T0034 Twitter trolls amplify and manipulate</td>
<td>T0053 Tertiary sites amplify news</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Narrative = Assigns MEANING and IDENTITY to information.

1. Narrative is NOT truth or lies.
2. The audience is targeted with multiple layers of meaning and identity.
3. Narrative MAKES it TRUTH to the audience because it relates to their unique experiences.
The Original Diamond Model for Intrusion Analysis

We adapted this for the particulars of influence campaigns.
Large scale or small?
Bots, trolls, automation, deepfakes, forgeries, budgets

Influencer
nation - state, criminal, political, proxy companies

Fringe websites, social media platforms, specific accounts, news agencies, IP addresses, digital artifacts, etc.

Capabilities
Global, national, local, small groups, political constituencies, consumers

Infrastructure

Audience

Technical axis
Socio-political axis
The Technical Axis: Capabilities and Infrastructure

Capabilities

Large scale or small?
Bots, trolls, automation, deepfakes, forgeries, budgets

Narrative

Fringe websites, social media platforms, specific accounts, news agencies, IP addresses, digital artifacts, etc.

Infrastructure
The Socio-political Axis: Influencer and Audience

❖ An individual or organization that is conducting malign influence activity.
❖ Purposefully engage in sharing false information in order to create chaos or panic, criticize, divide, or defame.
❖ They range from overt agents like outspoken politicians to more covert, low-quality inauthentic accounts, called “trolls”.

❖ The intended target of the influence operation.
❖ Can range in size from a single individual to a large international audience, but is likely somewhere in between.
❖ The most effective and resourced influence campaigns will likely target a specific demographic using a customized narrative.
Corporate Example: Auto Company

Influencer

Criminal disinfo -as-a-service hired by foreign competitor

Capabilities

Deepfake, altered photos, inauthentic profiles, fake news coverage

Narrative

Streaming media platform, mainstream social media, fringe news websites hosted on foreign IPs and domains

Audience

US and European audiences where competitor launched new vehicle, adults ages 25-55

Infrastructure
Example 2: Fictional State - sponsored group

Inauthentic social media accounts, fringe social media used by audience, local town hall building

Country H's intelligence agency, local police

T0053 Trolls amplify and manipulate, T0055 Use hashtag, T0057 Organize rallies and events

Country G's cultural minority

Country G's cultural minority

Technical axis

Socio-political axis
Let's keep in touch!

charity.wright@recordedfuture.com

@CharityW4CTI