Defining Influence and Disinformation

Olga Belogolova
Policy Lead, Influence Operations
“Fake News” and other Lies

Source: European Parliament Research Service
A cacophony of terms

Figure 1: Number of returned articles mentioning keywords as searched on 15 July 2019 via the New York Times landing page featuring articles on “Russian Hacking and Influence in the U.S. Election”

Disinformation

Source: “Captain of the Soviet Country Leads Us From One Victory to Another,” Boris Efimov, 1933
Misinformation and “MDM”

Source: First Draft News
Content based terminology

Source: First Draft News
Content Responses to Content Problems

- **Remove**: content and accounts that violate our Community Standards
- **Reduce**: distribution of low quality content (including false news)
- **Inform**: people by giving them more context, so they can decide what to read, trust, and share
### Information Operations Integration into Joint Operations (Notional)

<table>
<thead>
<tr>
<th>Core Supporting Related Information Activities</th>
<th>Activities</th>
<th>Audience</th>
<th>Target</th>
<th>Objective</th>
<th>Information Quality</th>
<th>Primary Planning Integration Process</th>
<th>Who does it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Warfare</td>
<td>Electronic Attack</td>
<td>Physical</td>
<td>Information</td>
<td>Physical</td>
<td>Electronic Attack</td>
<td>Joint Operation Planning and Execution System (OPE/EF)</td>
<td>Individuals, Governments, Militaries</td>
</tr>
<tr>
<td></td>
<td>Electronic Protection</td>
<td>Physical</td>
<td>Informational</td>
<td>Protect the Use of Electro-Magnetic Spectrum</td>
<td>Security</td>
<td>JOPES/Defense Planning</td>
<td>Individuals, Businesses, Governments, Militaries</td>
</tr>
<tr>
<td></td>
<td>Electronic Warfare Support</td>
<td>Physical</td>
<td>Informational</td>
<td>Identify and Locate Threats</td>
<td>Security</td>
<td>JIE/Intelligence Preparation of the Battlespace/JPES/SGINT Collection</td>
<td>Militaries</td>
</tr>
<tr>
<td></td>
<td>Computer Network Defense</td>
<td>Physical</td>
<td>Informational</td>
<td>Protect Computer Networks</td>
<td>Security</td>
<td>JIE/Intelligence Preparation of the Battlespace/JPES/SGINT Collection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Computer Network Exploitation</td>
<td>Informational</td>
<td>Informational</td>
<td>Gain Information From and About Computer Networks</td>
<td>Security</td>
<td>JIPES/SGINT-6 Vulnerability Analysis</td>
<td></td>
</tr>
<tr>
<td>Psychological Operations</td>
<td>Psychological Operations</td>
<td>Cognitive</td>
<td>Influence</td>
<td>Cognitive</td>
<td>Influence</td>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>Military Deception</td>
<td>Military Deception</td>
<td>Cognitive</td>
<td>Mislled</td>
<td>Cognitive</td>
<td>Mislled</td>
<td>Accuracy</td>
<td></td>
</tr>
<tr>
<td>Supporting Capabilities</td>
<td>Information Assurance</td>
<td>Informational</td>
<td>Protect Information and Information Systems</td>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Security</td>
<td>Physical</td>
<td>Secure Information and Information Infrastructure</td>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Attack</td>
<td>Physical</td>
<td>Destroy, Disrupt</td>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counterintelligence</td>
<td>Cognitive</td>
<td>Masked</td>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Combat Camera</td>
<td>Physical</td>
<td>Inform/Document</td>
<td>Usability, Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Capabilities</td>
<td>Civil Military Operations</td>
<td>Cognitive</td>
<td>Influence</td>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public Affairs</td>
<td>Cognitive</td>
<td>Inform</td>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public Diplomacy</td>
<td>Cognitive</td>
<td>Inform</td>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Nathaniel Gleicher @ngleicher Jan 9**

What underlies your desire to describe based on the activity (Inf0 v the goal (influence)? And actually, isn’t it reasonable to say that influence is both the goal (the noun form) and the activity (the verb form)?

---

**Yoel Roth @yoyoel Jan 9**

Decidedly NOT the verb form! That presumed the activity is successful - which is an empirical question that needs to be answered (and which we generally overestimate, I think). But that’s a separate issue.

---

**Nathaniel Gleicher @ngleicher Jan 9**

Hmmm. Saying they’re attempting to influence doesn’t grant that they are successful. And I agree it shouldn’t — public debate 100% overestimates the impact of IO. But see the risk there — that’s definitely a trap to avoid.

---

**Nathaniel Gleicher @ngleicher Jan 9**

As we discuss this, I think I prefer “influence” b/c it defines IO by the actions of threat actors, as opposed to their payload. And the payloads are often unremarkable. Overemphasis/analysis of fascination with IO payload is a recurring problem.

---

**Alicia Wanless @ageneralista Jan 9**

I can see @yoyoel and Twitter’s point on that. And it also highlights the challenges of definitions being universally applicable. What might work for policy in one context might not make sense elsewhere. Lately I’ve been leaning towards terms borrowed from ecology...
Historical Terms: Political Warfare and “Active Measures”
Propaganda and Public Diplomacy
Influence Operations

Influence Operation (IO)
Coordinated efforts to manipulate or corrupt public debate for a strategic goal.

Overt IO
State media, official government actors, etc.

Covert IO
Coordinated Inauthentic Behavior, foreign interference

Global CIB disruptions, 2017-2021
(by country of origin)
How did we go from influence ops to CIB?
A long trail of deception and influence
Deterrence in the IO space

**deterrence**

/daˈtərəns/
noun

the action of discouraging an action or event through instilling doubt or fear of the consequences.

Disruption (removal of networks / fake accts, blocking domains)
PNG (persona non grata)
Disclosure (public sharing of threat research and analysis, including attribution when possible)
Transparency (labels, informational notifications)
Notification (User alerts)
Information sharing (industry, government, civil society)
**Soft action to bring violators back in compliance** (demotion, warnings, etc.)
Deterrence in the IO space
Signals of Success?

- Threat actors forced into better opsec/adapt
- Threat actors shift to use other platforms
- Threat actors get caught before they can build an audience
- Threat actors cannot get real-world traction
- Civil society more aware of threat actor tactics
- Increased whole-of-society lead sharing