Cyber Influence Operations (ICOs): The Use of Cyber Attacks to Support Influence Operations

Published on 14/12/2025

Influence Operations and Information Warfare aim to spread one's message or prevent the adversary from doing so, focusing not only on the narrative but also on confusing, distracting, and demoralizing the adversary. In this context, cyberspace is seen as an ideal environment for conducting operations that have more **disruptive** than **destructive** outcomes.

The Emergence of Influence Cyber Operations (ICOs)

The authors of the document propose the term **Influence Cyber Operations (ICOs)** to describe actions in cyberspace where the primary goal is to influence the behavior of a target audience.

ICOs are defined as:

> "*Operations that influence the logical layer of cyberspace with the intention of affecting attitudes, behaviors, or decisions of the target audience*".

These operations are considered a subset of Influence Operations that qualify as **cyber attacks** . ICOs fall within the logical layer of cyberspace and are intrusive, as they gain unauthorized access to networks and systems to destroy, alter, or add information[7].

The document distinguishes ICOs from **Inform & Influence Operations (IIOs)**, which are content-oriented activities (such as propaganda and disinformation) aimed at creating an artificial information environment, operating at the semantic level of cyberspace.

Strategic Approaches: Russia vs. the West

Strategic approaches to Influence Operations differ significantly:

- **Russian Approach:** Russia considers Information Warfare as a tool of *hard power* and has developed a more **integrated and holistic** vision. The goal is to gain strategic advantages without provoking an armed response from NATO. ICOs are seen as **low-risk and low-cost** capabilities that contribute to destabilizing the adversary, fueling confusion, and undermining trust. The difficulty of attribution offers a high degree of "plausible deniability".
- **Western Approach:** Western democracies tend to adopt a more **compartmentalized** approach, maintaining a sort of "firewall" between the *soft power* of IIOs and the clandestine *hard power* of ICOs. The approach is based on maintaining **transparency and credibility**, principles that would be undermined by clandestine and coercive actions in peacetime. The use of ICOs is limited, in principle, to military operations or specific *intelligence* authorities.

Cyber Influence Operations (ICOs): The Use of Cyber Attacks to Support Influence Operations

Cyber Influence Operations (ICOs): The Use of Cyber Attacks to Support Influence Operations

Common Types of Influence Cyber Operations

The spectrum of ICOs is broad, and the techniques are often considered low-tech, easily automatable or outsourceable. Such activities, while not reaching the level of an armed attack in a legal sense, aim to influence attitudes and decisions:

- **Unauthorized access to an information system (Hacking):** Gaining access to modify data or undermine trust in national authorities. For example, compromising the computers of the Central Electoral Committee in Ukraine to damage the government's credibility.
- **False Flag Attacks:** Using specific techniques to deceive the adversary into believing the operation was conducted by another party. An example is the attack on TV5 Monde, initially attributed to an ISIS-affiliated group, but later linked to Russian *hackers*.
- **Distributed Denial of Service (DDoS) Attacks:** Attacks to overwhelm the target's resources, affecting only availability and not confidentiality or integrity. They aim to undermine credibility and are still widely used to embarrass governments or organizations (e.g., attacks on NATO sites or in Estonia in 2007).
- **Website Defacement:** Similar to graffiti or vandalism, these attacks primarily cause embarrassment and aim to spread disinformation or undermine trust. Their effectiveness lies in the media reaction.
- **Doxing:** The revelation and publication of private or classified information obtained through *hacking* or other sources, with the aim of embarrassing or shaming the target, potentially creating divisions among allies.

Conclusions

ICOs will remain a source of disruption, contributing to an already existing sense of insecurity and supporting a broader narrative of Influence Operations.

To counter them, the article suggests:

- **Increasing cyber awareness** among the population and the political/bureaucratic elite.
- **Transparency** from governments and companies in managing attacks and *leaks*.
- A proper understanding of the **nature and impact** of these attacks, avoiding labeling everything as "cyber war".

News link: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf