Operazioni Cyber di Influenza (ICOs): L'uso degli Attacchi Informatici a Supporto delle Operazioni di Influenza

Pubblicato il 14/12/2025

Le Operazioni di Influenza e la Guerra dell'Informazione mirano a diffondere il proprio messaggio o a impedire all'avversario di farlo, concentrandosi non solo sulla narrazione, ma anche sul confondere, distrarre e demoralizzare l'avversario. In questo contesto, il cyberspazio è visto come un ambiente ideale per condurre operazioni che hanno esiti più **disruptive** (dirompenti) che **distruttivi**.

La Nascita delle Influence Cyber Operations (ICOs)

Gli autori del documento propongono il termine **Influence Cyber Operations (ICOs)** per descrivere le azioni nel cyberspazio in cui l'obiettivo principale è influenzare il comportamento di un pubblico target.

Le ICOs sono definite come:

> "*Operazioni che influenzano lo strato logico del cyberspazio con l'intenzione di influenzare atteggiamenti, comportamenti o decisioni del pubblico target*".

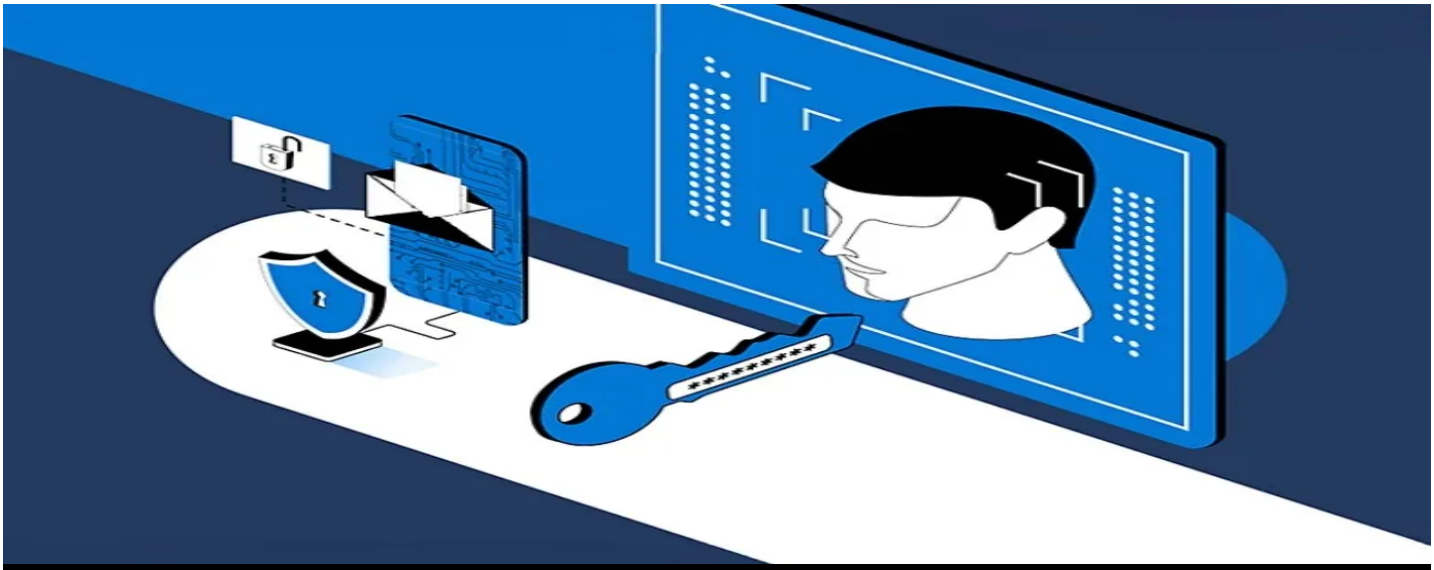
Queste operazioni sono considerate un sottoinsieme delle Operazioni di Influenza che si qualificano come **attacchi informatici**. Le ICOs rientrano nello strato logico del cyberspazio e sono intrusive, poiché ottengono accesso non autorizzato a reti e sistemi per distruggere, alterare o aggiungere informazioni[7].

Il documento distingue le ICOs dalle **Inform & Influence Operations (IIOs)**, che sono attività orientate al contenuto (come propaganda e disinformazione) che mirano a creare un ambiente informativo artefatto, operando a livello semantico del cyberspazio.

Approcci Strategici: Russia contro Occidente

Gli approcci strategici alle Operazioni di Influenza differiscono notevolmente:

- **Approccio Russo:** La Russia considera la Guerra dell'Informazione come uno strumento di *hard power* (potere duro) e ha sviluppato una visione più **integrata e olistica**. L'obiettivo è ottenere vantaggi strategici senza provocare una risposta armata della NATO. Le ICOs sono viste come capacità a **basso rischio e basso costo** che contribuiscono a destabilizzare l'avversario, alimentando confusione e minando la fiducia. La difficoltà di attribuzione offre un alto grado di "plausible deniability" (ragionevole negabilità).
- **Approccio Occidentale:** Le democrazie occidentali tendono ad adottare un approccio più **compartimentalizzato**, mantenendo una sorta di "firewall" tra il *soft power* delle IIOs e l'*hard power* delle ICOs clandestine. L'approccio si basa sul mantenere la **trasparenza e la credibilità**, principi che sarebbero minati da azioni clandestine e coercitive in tempo di pace. L'uso di ICOs è limitato, in linea di principio, alle operazioni militari o a specifiche autorità di *intelligence*.



Operazioni Cyber di Influenza (ICOs): L'uso degli Attacchi Informatici a Supporto delle Operazioni di Influenza

Tipi Comuni di Influence Cyber Operations

Lo spettro delle ICOs è ampio, e le tecniche sono spesso considerate a bassa tecnologia, facilmente automatizzabili o esternalizzabili. Tali attività, pur non raggiungendo il livello di un attacco armato in senso legale, mirano a influenzare gli atteggiamenti e le decisioni:

- **Accesso non autorizzato a un sistema informativo (Hacking):** L'ottenimento di accesso per modificare dati o minare la fiducia nelle autorità nazionali. Ad esempio, la compromissione dei computer del Comitato Elettorale Centrale in Ucraina per danneggiare la credibilità del governo.
- **Attacchi False Flag:** L'uso di tecniche specifiche per ingannare l'avversario e far credere che l'operazione sia stata condotta da un'altra parte. Un esempio è l'attacco a TV5 Monde, inizialmente attribuito a un gruppo affiliato all'ISIS, ma poi collegato a *hacker* russi.
- **Attacchi Distributed Denial of Service (DDoS):** Attacchi per sopraffare le risorse del bersaglio, influenzandone solo la disponibilità e non la riservatezza o l'integrità. Mirano a minare la credibilità e sono ancora molto diffusi per mettere in imbarazzo governi o organizzazioni (es. attacchi ai siti NATO o in Estonia nel 2007).
- **Defacement di siti web:** Simili ai graffiti o al vandalismo, questi attacchi causano principalmente imbarazzo e mirano a diffondere disinformazione o minare la fiducia. La loro efficacia risiede nella reazione mediatica.
- **Doxing:** La rivelazione e pubblicizzazione di informazioni private o classificate ottenute tramite *hacking* o altre fonti, allo scopo di imbarazzare o mettere in imbarazzo il target,

potendo creare divisioni tra alleati.

Conclusioni

Le ICOs rimarranno una fonte di disturbo, contribuendo a un senso di insicurezza già esistente e supportando una narrazione più ampia di Operazioni di Influenza.

Per contrastarle, l'articolo suggerisce:

- **Aumento della consapevolezza cyber** tra la popolazione e l'élite politica/burocratica.
- **Trasparenza** da parte dei governi e delle aziende nel gestire gli attacchi e le *fughe di notizie* (leaks).
- Una corretta comprensione della **natura e dell'impatto** di questi attacchi, evitando di etichettare tutto come "guerra cyber".

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