



HYBRID WAR, INTERNATIONAL INTERFERENCE USING SOCIAL MEDIA



ONLINE TRAINING ON DIGITAL
COMPETENCES AND
CRITICAL THINKING



Erasmus+

© TeDiCom CC-by-SA

<https://kultur-life.de/projekte/tedicom>

Hybrid War - International Interference Using Social Media

2021 05 20

Darius Remeika

Questions:

What is Hybrid War?

Why Hybrid War works?

Why Social Media is perfect for Hybrid War?

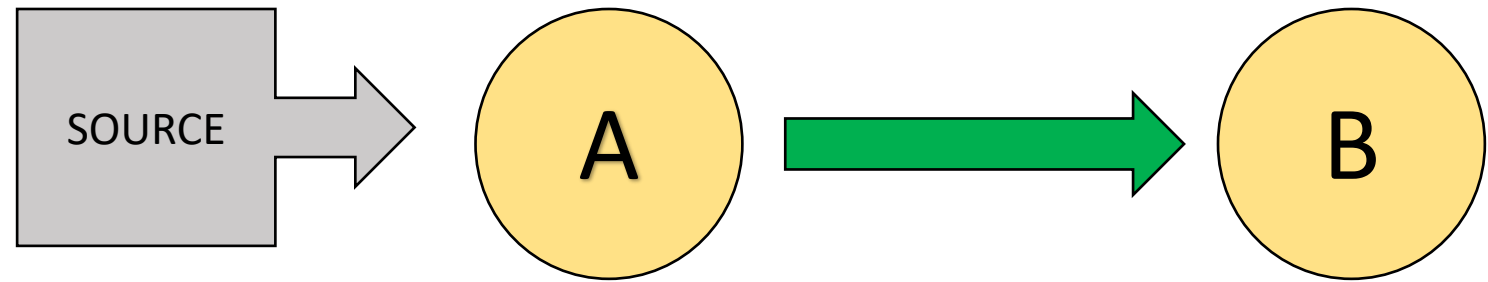
What can we do?

What is
Hybrid?

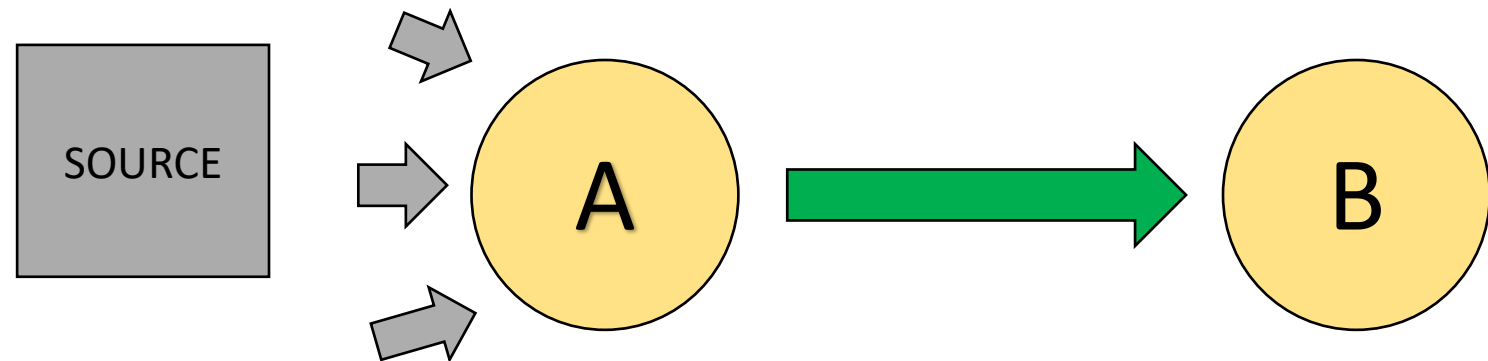


Hybrid Approach

Traditional approach



Hybrid approach



INFLUENCE

Hybrid War

“Synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects”

- ... ambiguity, uncertainty, criticism, dissatisfaction ...
- ... undermining public trust in democratic institutions ...
- ... below detection and response thresholds ...
- ... decision making process ...
- ... challenging the core values ...
- ... deepening unhealthy polarization ...

“Death by a thousand cuts”



Hybrid Environment: Critical Functions

Political

Military

Economic

Social

Information

Infrastructure

Political

The political domain encompasses the **actors**, **organizations** and **institutions** that exercise authority or rule within a territory through the application of various forms of political power and influence.

The political system is expected to be **representative** of the cultural, historical, demographic and sometimes religious factors that form the **identity of a society**.

Military

A country's military and defence capabilities constitute a **cornerstone** of its own **existence** and projection of power.

Compromising a country's military and defence capabilities can be a very effective means of influence, exerting pressure, and, in certain cases, preparing the ground for future military operation.

Economic

The objective of a hybrid threat action on the economy domain is to comprehensively **weaken** the **target state**, undermining public confidence in democracy and the government.

Social

Contentious issues, such as unemployment, poverty and education are always subject to debate in Western societies, and thus offer an easy target.

The use of **cultural** and civilizational themes in an effort to define fundamental elements of **national identity**.

Information

Anything of significance that happens in the real world, including every political and military conflict, will also take place in cyberspace.

The tools of this domain seek to shift the political discourse, to create or **promote narratives**, and to **manipulate public** opinion and sentiment.

Infrastructure

An asset, system or part which is essential for the maintenance of **vital societal functions**, health, safety, security, economic, or social well-being of people, and the distribution or destruction of which would have a significant impact.

Hybrid is always a combination of tools but
not all combinations are hybrid

Hybrid Source

State actor:

- Russia

Non-state actor:

- Daesh (ISIS)

- States operating through non-state entities
- No attribution
- Weak vs Strong
- Covert vs Overt
- Order's effects
- "Usefull idiots"

How it works?

1. Objective
2. Analysis
 - System of System
 - Target audience analysis
3. Execution
 - Proactive
 - Reactive
4. Evaluation



Social Media role in Hybrid War

The New Information Environment

- **Governments** and traditional media are no longer the most important players in the information space; they now have to **compete** for their place amid all the other actors.
- The amount of **information** we face every day makes it difficult to track and differentiate between useful information and **'noise'**.
- The virtual environment is an unregulated environment in which **anonymity** provides more **opportunities** than ever to disseminate **extreme views**, deliberate **misinformation**, and create **hoaxes** without revealing the person or organisation behind the creation of the content.

The “Weaponization” of Social Media

- ‘social cyber attacks – deliberate and organised actions to spread rumours, hoaxes, and manipulative messages in the virtual environment aimed at raising the fear and panic.
- To create Cognitive Dissonance.
- To attack the Identity



Techniques

Increase the visibility of the message:

- Automatically generated content
- Saturating the information environment
- Hijacking of trending hashtags

Targeting and distracting the opponent:

- Distribution of misinformation and rumours
- Attacking through the administrator
- Social engineering
- Deception

Trolling

- Aggression
- Labeling
- Use of historical references
- Demonstrating civilization or moral superiority
- Use of irony and sarcasm
- Conspiracy theories
- Blaming others
- Diverting discourse
- Social proof
- Dehumanization

A large orange circle on the left side of the slide, partially cut off by the edge.

HOW to identify Trolls?

Large amount of comments

Consistently pro-adversary content

Repeat, repost

Does not engage in conversation

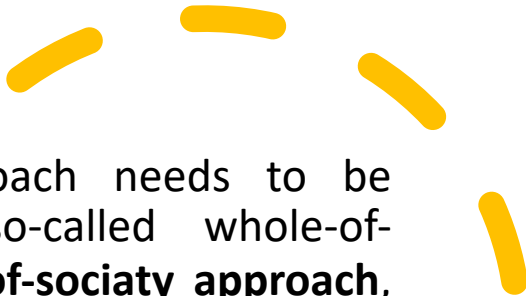
Illiterate in foreign languages

Politically motivated

Emotions



Resilience



A comprehensive and holistic approach needs to be adopted. This should reflect a so-called whole-of-government or, even better, a **whole-of-society approach**, bringing civil, military and political actors together, and duly leading to a new security ecosystem.

- Assessment of critical functions and vulnerabilities
- Specific indicators must be built, constant monitoring
- Identify and unmask disinformation
- Develop a unifying narrative
- Develop a network of credible voices
- Support for analytical journalism
- Respond with humour and satire
- Enhance critical thinking and media literacy



Questions

Darius Remeika
dariusopen@gmail.com
info@influenceq.lt