DOMINOES
digital resilience to disinformation

1.1

Conflict and its manifestation in the information environment: hybrid warfare/threats, cognitive and information warfare

Rubén Arcos | University Rey Juan Carlos

doi.org/10.5281/zenodo.10063841

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

DOMINOES
digital resilience to disinformation

Erasmus+

Rubén ARCOS | URJC

CONFLICT AND ITS MANIFESTATION IN THE INFORMATION ENVIRONMENT

This module 1.1. addresses the following contents:

1. Conflict and its manifestation in the information environment
2. Hybrid warfare/threats
3. Cognitive and information warfare

UNIT OBJECTIVES

- To gain a comprehensive perspective on the information environment from a point of view that focuses on the security of citizens and the state.
- To be able to recognise and make connections between the manifestations and development of the information field in general.
- To recognise the emerging threats associated with the emergence of new technologies.

DOMINOES
digital resilience to disinformation

1.1.1

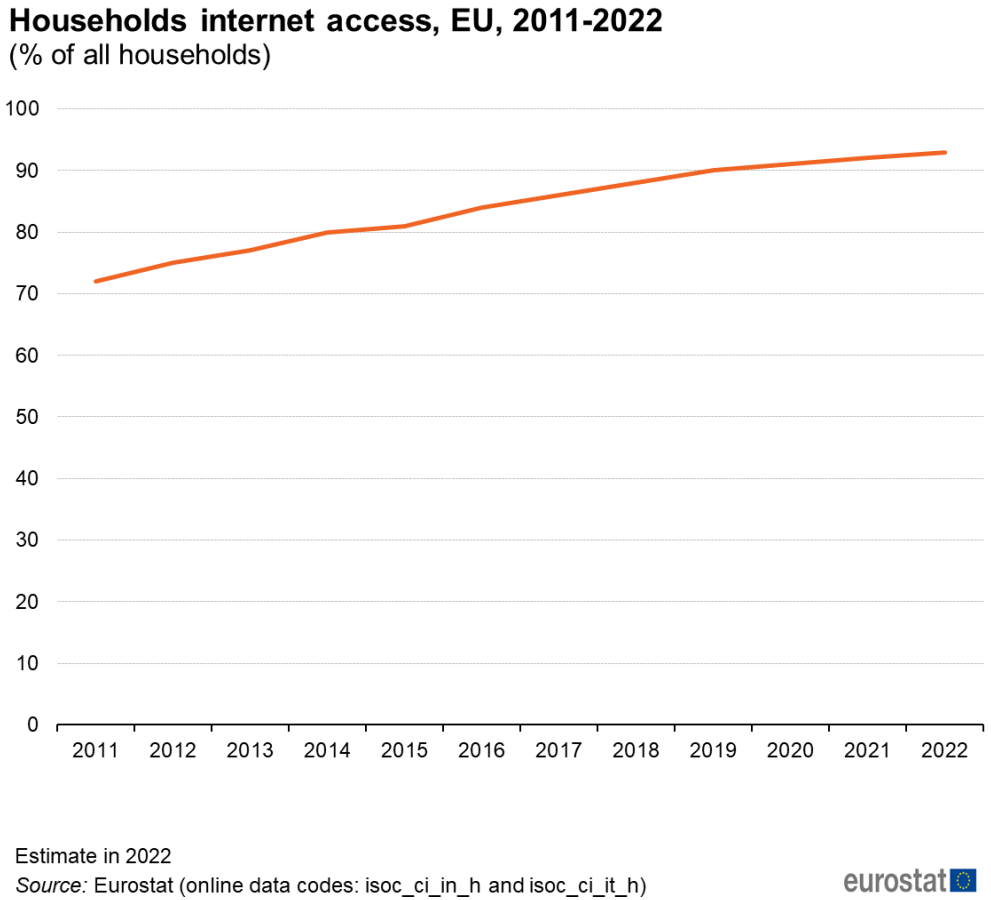
Conflict and its manifestation in the information environment

Digital cOMpetences INformatiOn EcoSystem

2021-1-RO01-KA220-HED-000031158

Conflict and its manifestation in the information environment

- The information environment has experienced enormous changes driven by an ongoing technological and digital revolution and the new ways humans produce, transmit and receive symbolic content.
- According to Eurostat, “in 2022, the share of EU households with internet access has risen to 93 %, up from 72 % in 2011” (Eurostat 2023). At the same time, the Reuters Institute Digital News Report 2022 has noted the “structural shifts towards a more digital, mobile, and platform-dominated media environment, with further implications for the business models and formats of journalism” (Reuters Institute for the Study of Journalism 2023: 10).

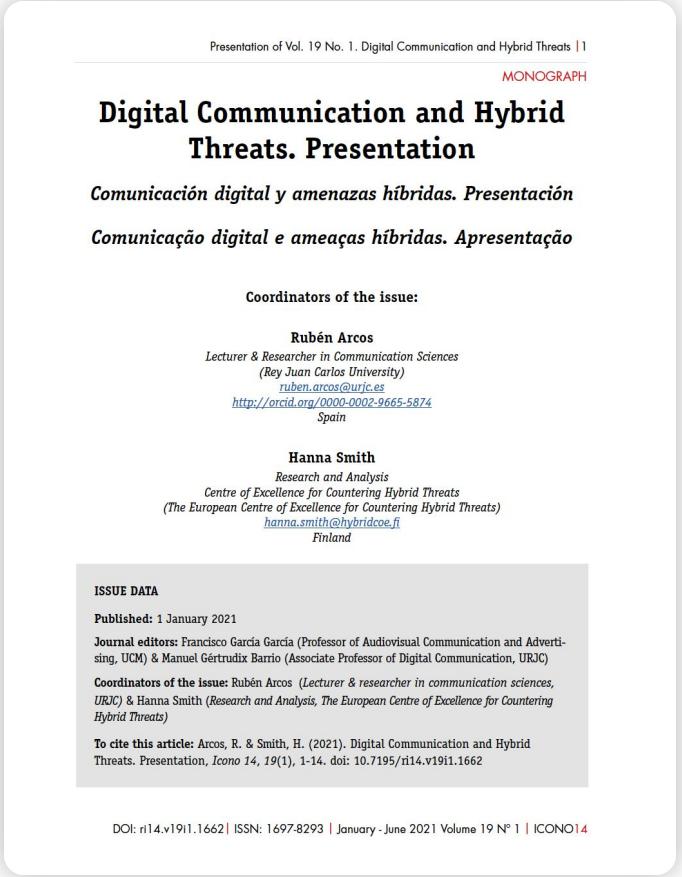


Conflict and its manifestation in the information environment

Unlike in the golden age of traditional media, in our overabundant information environment journalistic news reporting, news analysis and opinion pieces on international, national, and regional events and developments compete for the attention of an empowered audience that is now able as well to produce and disseminate content.

Since human beings developed situational awareness and “make decisions based on their representations about the world and the information available through interpersonal symbolic interactions and through the different media,” including social media platforms, information and digital content can me deliberately used with a malicious intent (Arcos & Smith 2021: 6).

Today, our digital communication environment and the communication tools that we Europeans employ for legitimate purposes are also being employed by foreign hostile actors for interfering in our democratic processes like elections, erode trust in our institutions, divide and destabilize our societies (Ibid).



Presentation of Vol. 19 No. 1. Digital Communication and Hybrid Threats | 1

MONOGRAPH

Digital Communication and Hybrid Threats. Presentation

Comunicación digital y amenazas híbridas. Presentación

Comunicação digital e ameaças híbridas. Apresentação

Coordinators of the issue:

Rubén Arcos
Lecturer & Researcher in Communication Sciences
(Rey Juan Carlos University)
ruben.arcos@urjc.es
http://orcid.org/0000-0002-9665-5874
Spain

Hanna Smith
Research and Analysis
Centre of Excellence for Countering Hybrid Threats
(The European Centre of Excellence for Countering Hybrid Threats)
hanna.smith@hybridcoe.fi
Finland

ISSUE DATA

Published: 1 January 2021

Journal editors: Francisco García García (Professor of Audiovisual Communication and Advertising, UCM) & Manuel Gértrudix Barrio (Associate Professor of Digital Communication, URJC)

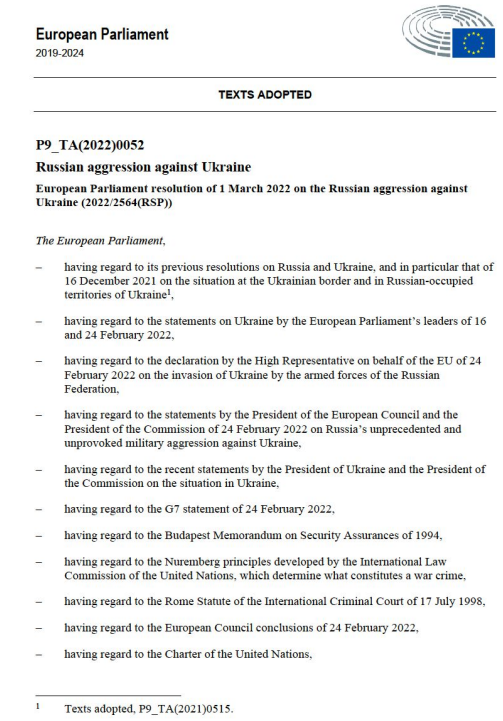
Coordinators of the issue: Rubén Arcos *(Lecturer & researcher in communication sciences, URJC)* & Hanna Smith *(Research and Analysis, The European Centre of Excellence for Countering Hybrid Threats)*

To cite this article: Arcos, R. & Smith, H. (2021). Digital Communication and Hybrid Threats. Presentation, *Icono 14*, *19*(1), 1-14. doi: 10.7195/ri14.v19i1.1662

DOI: ri14.v19i1.1662 | ISSN: 1697-8293 | January - June 2021 Volume 19 Nº 1 | ICONO14

Conflict and its manifestation in the information environment

- The European Parliament has condemned the use of information warfare by Russian authorities, their proxies, and state-funded media, in support of its military aggression against Ukraine, as well its employment of information manipulations and hostile narratives against the EU and NATO (See: European Parliament 2022).
- Mis- and disinformation, conspiracy theories and propaganda constitute symbolic tools that are targeted towards citizens abroad to produce cognitive, affective, and behavioral effects.



European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2022)0052

Russian aggression against Ukraine

European Parliament resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP))

The European Parliament,

– having regard to its previous resolutions on Russia and Ukraine, and in particular that of 16 December 2021 on the situation at the Ukrainian border and in Russian-occupied territories of Ukraine[1],

– having regard to the statements on Ukraine by the European Parliament's leaders of 16 and 24 February 2022,

– having regard to the declaration by the High Representative on behalf of the EU of 24 February 2022 on the invasion of Ukraine by the armed forces of the Russian Federation,

– having regard to the statements by the President of the European Council and the President of the Commission of 24 February 2022 on Russia's unprecedented and unprovoked military aggression against Ukraine,

– having regard to the recent statements by the President of Ukraine and the President of the Commission on the situation in Ukraine,

– having regard to the G7 statement of 24 February 2022,

– having regard to the Budapest Memorandum on Security Assurances of 1994,

– having regard to the Nuremberg principles developed by the International Law Commission of the United Nations, which determine what constitutes a war crime,

– having regard to the Rome Statute of the International Criminal Court of 17 July 1998,

– having regard to the European Council conclusions of 24 February 2022,

– having regard to the Charter of the United Nations,

[1] Texts adopted, P9_TA(2021)0515.

Conflict and its manifestation in the information environment

- The manipulation of public opinion processes and the degradation of the discussion on public issues through hostile influencing tactics in the information environment undermine the capability of democratic societies to make informed decisions. Manufactured confusion around international developments, political events, or hostile activities can damage a society's willingness and ability to respond to impending threats and pressing challenges.
- As Wanless and Pamment (2019) have pointed out, “relatively objective principles such as history, scientific knowledge, and territorial boundaries are being disputed in the information space by revisionist powers. More controversial fault lines such as cultural identity, migration, and politics are the subject of increasingly intense contestation”.

DOMINOES
digital resilience to disinformation

1.1.2

Hybrid warfare/threats

Digital cOMpetences INformatiOn EcoSystem

Erasmus+

ANIMV DARE. LEARN. INNOVATE.

Universidad Rey Juan Carlos

L-Università ta' Malta

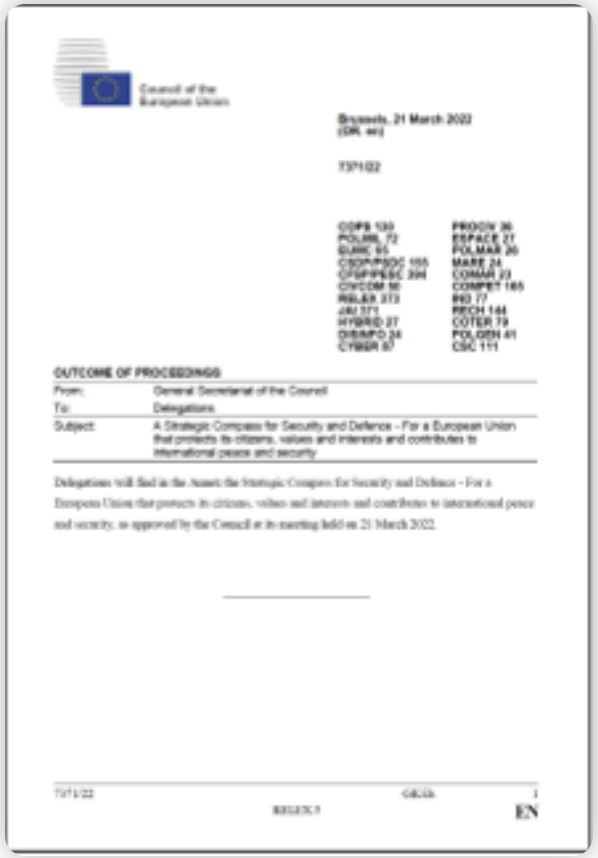
NEW STRATEGY CENTER

2021-1-RO01-KA220-HED-000031158

DOMINOES
digital resilience to disinformation

Erasmus+

Hybrid Operations/Threats in NATO and EU most recent and important concepts


Council of the European Union

Brussels, 21 March 2022

7371/22

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security

Delegations will find in the Annex the Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security, as approved by the Council at its meeting held on 21 March 2022.

EN

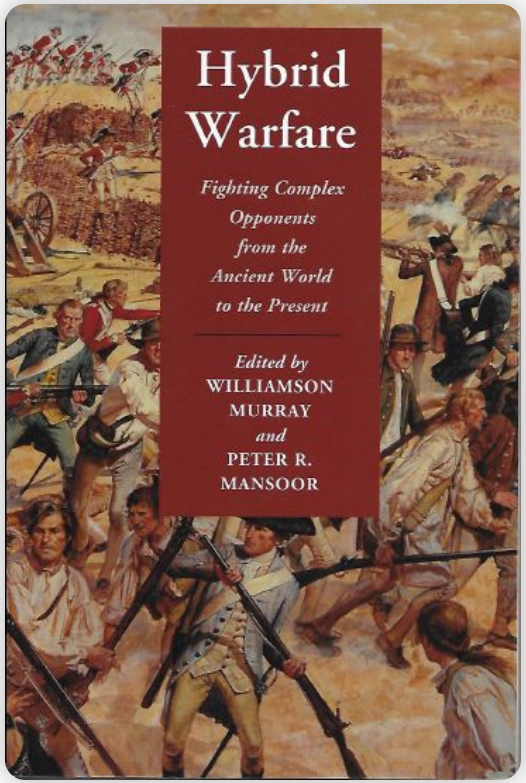
Hybrid Operations/Threats in NATO and EU most recent and important concepts

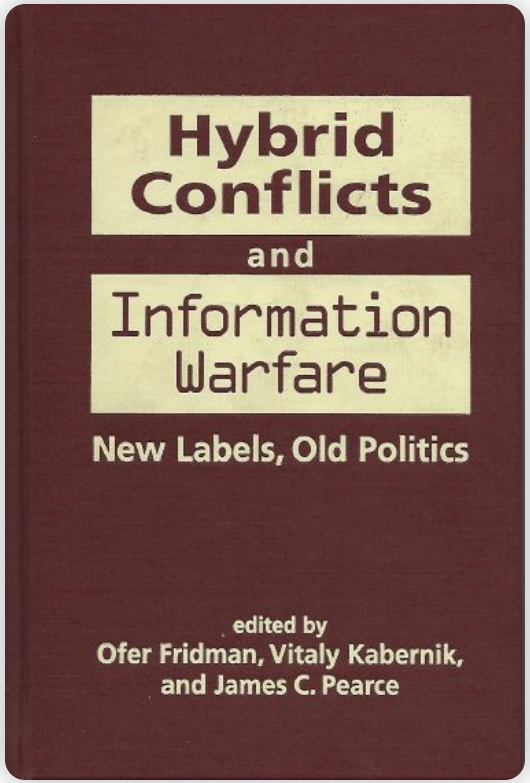
"**Authoritarian actors** challenge our interests, values and democratic way of life. They are investing in sophisticated conventional, nuclear and missile capabilities, with little transparency or regard for international norms and commitments. Strategic competitors test our resilience and seek to exploit the openness, interconnectedness and digitalisation of our nations. They interfere in our democratic processes and institutions and target the security of our citizens through **hybrid tactics**, **both directly and through proxies**. **They conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalise migration, manipulate energy supplies and employ economic coercion**. These actors are also at the forefront of a deliberate effort to undermine multilateral norms and institutions and promote authoritarian models of governance."

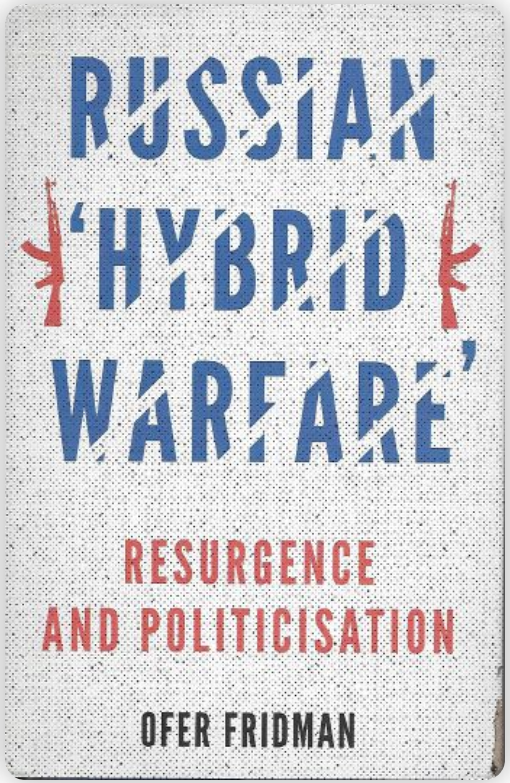
DOMINOES
digital resilience to disinformation

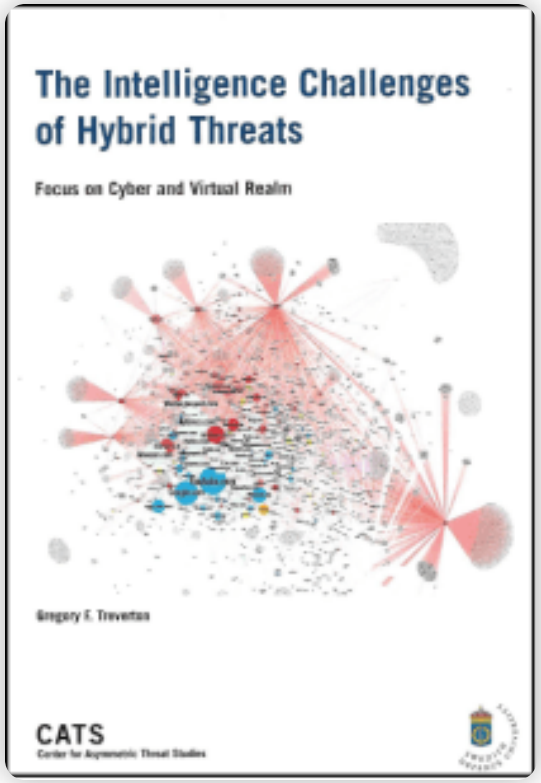
Erasmus+

Hybrid Operations/Threats in NATO and EU most recent and important concepts





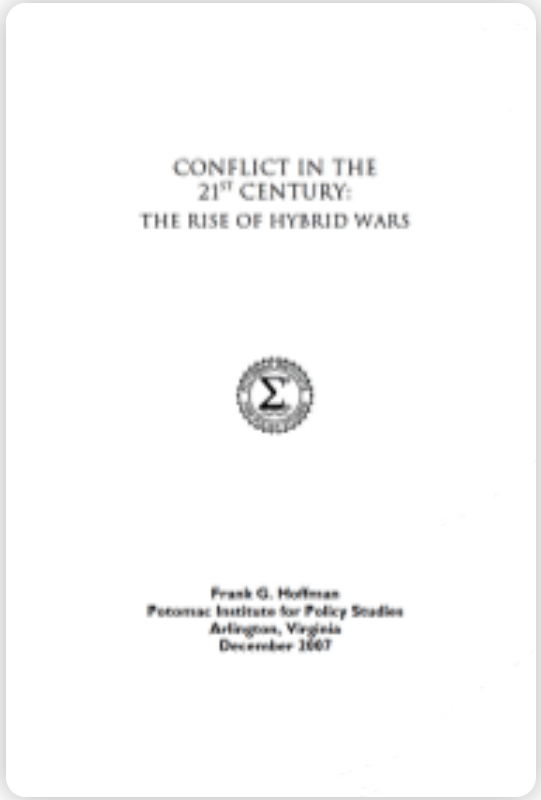




Hybrid Warfare: genealogy of the concept

- First public use by General Mattis at the Defense Forum sponsored by the Naval Institute and Marine Corps Association on September 8, 2005 (Hoffman 2007)
- Presented by LtGen James N. Mattis USMC and Frank Hoffman, **“Future Warfare: The Rise of Hybrid Wars**,” Naval Institute Proceedings, November 2005.

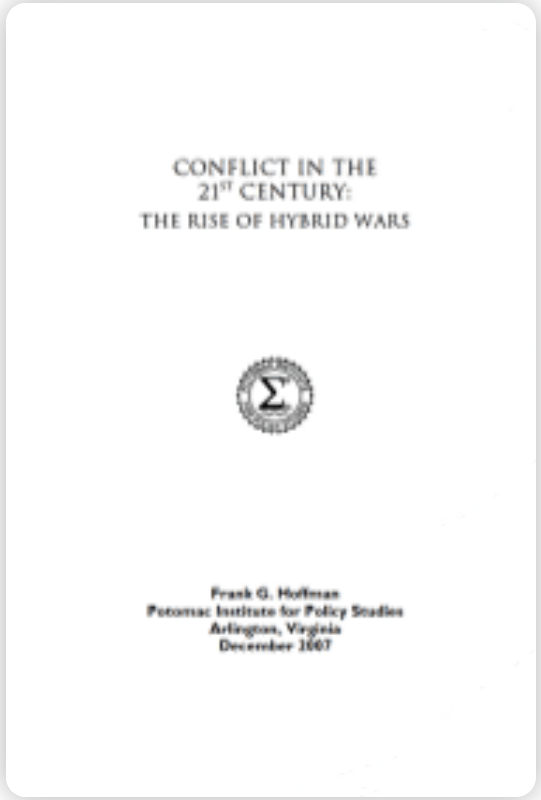
Hybrid Warfare: genealogy of the concept



- “Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder” (p. 8) [on p.14 Hoffman uses the term Hybrid Wars]

- The term “Hybrid” captures both their organization and their means. Organizationally, they may have hierarchical political structure, coupled with decentralized cells or networked tactical units. Their means will also be hybrid in form and application. In such conflicts, future adversaries (state, state-sponsored groups, or self-funded actors) will exploit access to modern military capabilities including encrypted command systems, man-portable air to surface missiles, as well as promote portracted insurgencies that employ ambushes, improvised explosive devices, and coercive assessinations” (p.28).

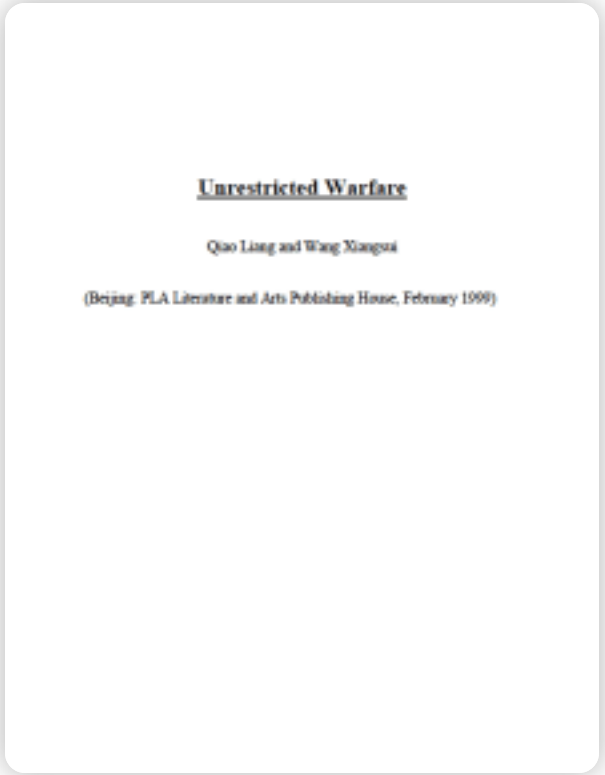
Hybrid Warfare: genealogy of the concept

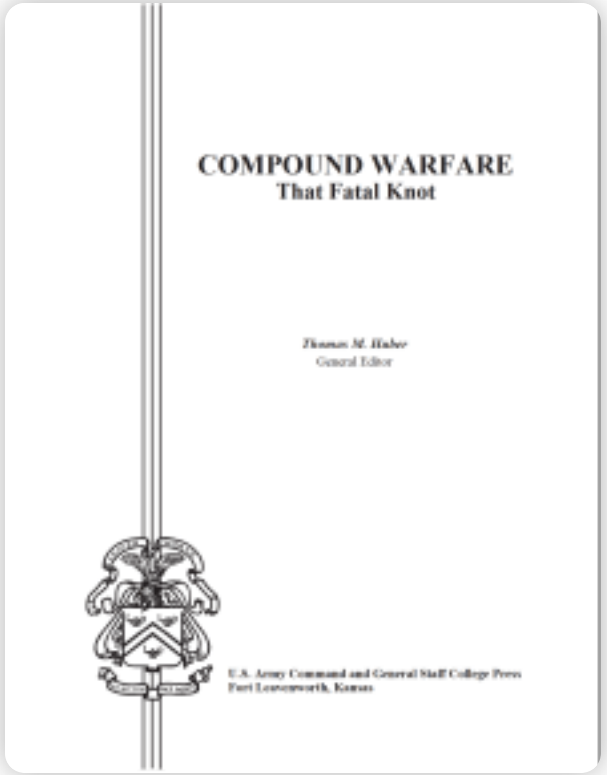


- “The blurring of modes of war, the blurring of who fights, and what technologies are brought to bear, produces a wide range of variety and complexity that we call *Hybrid Warfare*” (p. 14).

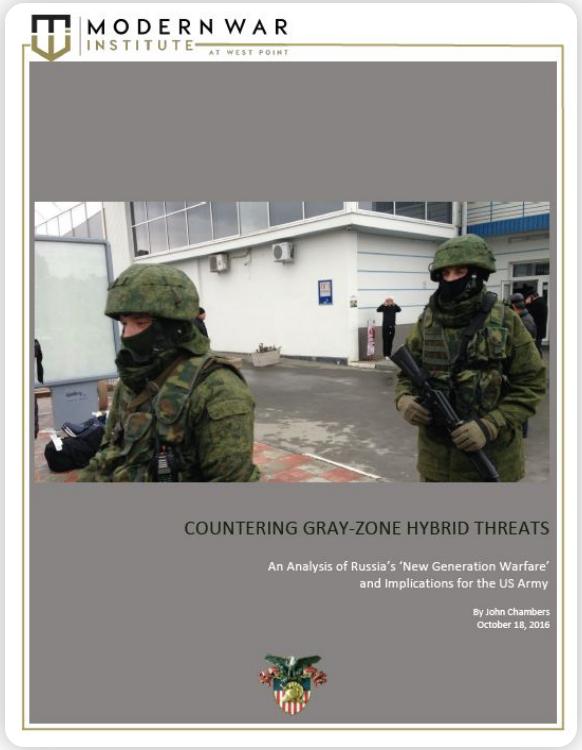
- The concept draws upon different “schools”: 4GW, Unrestricted Warfare, Compound Wars, Complex Warfighting, and others.

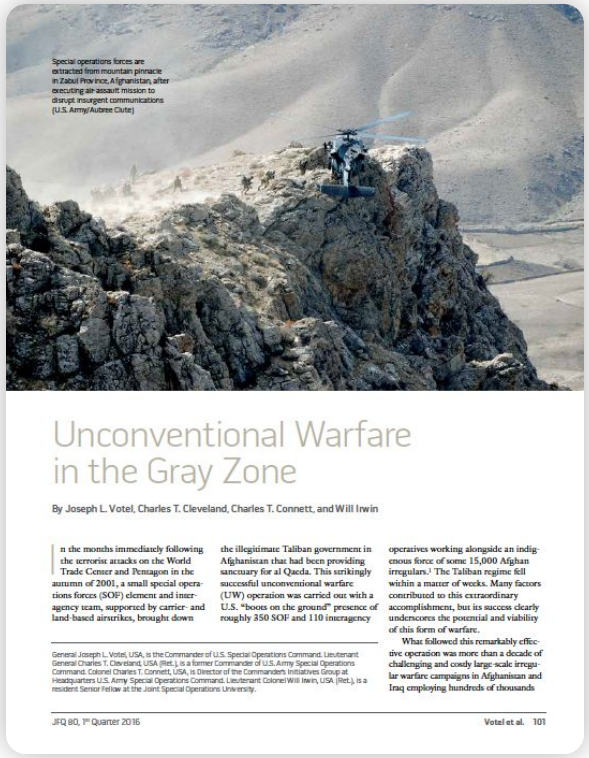
Different names, different perspectives?





Different names, different perspectives?





Hybrid Warfare: genealogy of the concept

- “Future challenges will present a more complex array of alternative structures and strategies, as seen in the summer of 2006 in the battle between Israel and Hezbollah”. (Hoffman 2007: 8)
- “Hezbollah clearly demonstrated the ability of non-state actors to study and deconstruct the vulnerabilities of Western style militaries, and devise appropiate countermeasures” (Ibid.)

Credit: Lynsey Addario for The New York Times

Hybrid Threats, according to F.G. Hoffman

- Hybrid Threats can be defined as: “any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battlespace to obtain their political objectives.” (2010: 443)

‘Hybrid Threats’:
Neither Omnipotent Nor Unbeatable

by F.G. Hoffman

F.G. Hoffman, a former Marine officer, has also served on the staff of the U.S. Commission on National Security/21st Century (Hart-Rudman Commission), was the National Security Analyst and Director, Marine Strategic Studies Group, at the Marine Corps Combat Development Command, Quantico, and served on the Professional Staff, Commission on Roles and Missions of the Armed Forces.

Abstract: Hybrid threats have now joined a growing suite of alternative concepts about the ever-evolving character of modern conflict. Here and abroad, the hybrid threat construct has found traction in official policy circles despite its relative novelty. It has been cited by the U.S. Secretary of Defense in articles and speeches, and by policymakers now serving in the Pentagon. Heretofore, the rapidly growing hybrid threat literature has focused on the land warfare aspects of the threat. Modern hybrid threats, including Hezbollah and Iran, have demonstrated the ability to employ irregular tactics and advanced naval capabilities along with illegal or terrorist activity. Thus, the hybrid threat is applicable to naval forces and the U.S. Navy needs to shed off lessons learned from its last experience in the Persian Gulf in the late 1980s to better prepare for an even more challenging future.

The purpose of this article is to provide an interpretation of what is commonly referred to as hybrid wars, and extends the research base of this emerging theory by exploring a maritime case study. Heretofore, the research base for this topic has been limited to conflicts primarily centered on ground operations. Such a narrow suite of cases has the potential to exclude the unique contributions that naval forces might bring to bear against adversaries exploiting hybrid combinations of capabilities and tactics. Even worse, it might leave our naval forces unprepared for the complexities of hybrid threats in their particular domain.

Over the past few years, a number of very interesting conceptualizations of conflict have emerged. Mary Kaldor's work on "new wars," John Robb's Open Source Warfare, and General Rupert Smith's modern wars

EU Definition

- “While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives **while remaining below the threshold of formally declared warfare.**
- There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats” JOIN(2016) 18 final


EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

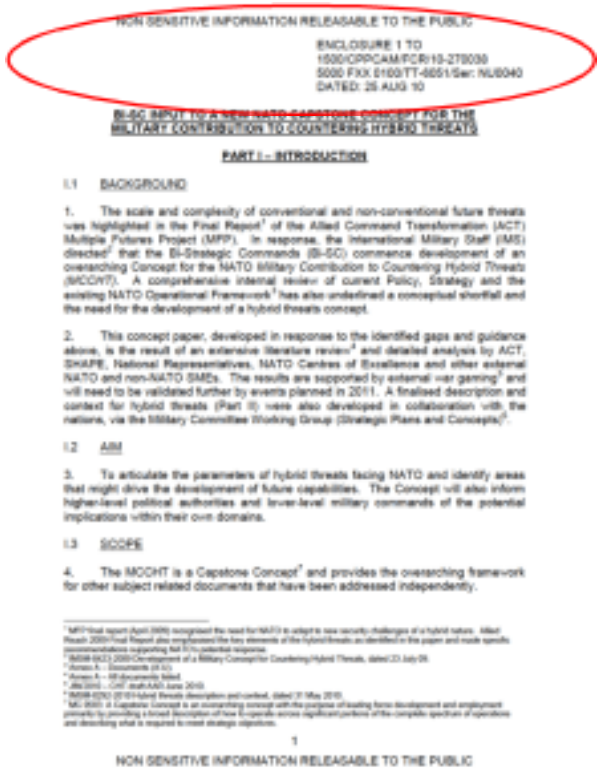
JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

EN EN

NATO Definition

- “Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives.” (NATO 2010).

- “Countering hybrid threats is not a new problem for NATO Nations as adversaries have sought regularly to operate up and down a scale of action, both in military and civil environments, depending on their level of expertise. **Hybrid threats involve adversaries (including states, rogue states, non-state actors or terrorist organisations) who may employ a combination of actions in an increasingly unconstrained operating environment in order to achieve their aims**”.



NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

ENCLOSURE 1 TO
1500/CPPCAM/FCR/10-270030
5000 FXX 0100/TT-6051/Ser: NU0040
DATED: 25 AUG 10

BI-SC INPUT TO A NEW NATO CAPSTONE CONCEPT FOR THE MILITARY CONTRIBUTION TO COUNTERING HYBRID THREATS

PART I – INTRODUCTION

I.1 BACKGROUND

1. The scale and complexity of conventional and non-conventional future threats was highlighted in the Final Report[1] of the Allied Command Transformation (ACT) Multiple Futures Project (MFP). In response, the International Military Staff (IMS) directed[2] that the Bi-Strategic Commands (Bi-SC) commence development of an overarching Concept for the NATO Military Contribution to Countering Hybrid Threats (MCCHT). A comprehensive internal review of current Policy, Strategy and the existing NATO Operational Framework[3] has also underlined a conceptual shortfall and the need for the development of a hybrid threats concept.

2. This concept paper, developed in response to the identified gaps and guidance above, is the result of an extensive literature review[4] and detailed analysis by ACT, SHAPE, National Representatives, NATO Centres of Excellence and other external NATO and non-NATO SMEs. The results are supported by external war gaming[5] and will need to be validated further by events planned in 2011. A finalised description and context for hybrid threats (Part II) were also developed in collaboration with the nations, via the Military Committee Working Group (Strategic Plans and Concepts)[6].

I.2 AIM

3. To articulate the parameters of hybrid threats facing NATO and identify areas that might drive the development of future capabilities. The Concept will also inform higher-level political authorities and lower-level military commands of the potential implications within their own domains.

I.3 SCOPE

4. The MCCHT is a Capstone Concept[7] and provides the overarching frame-work for other subject related documents that have been addressed independently.

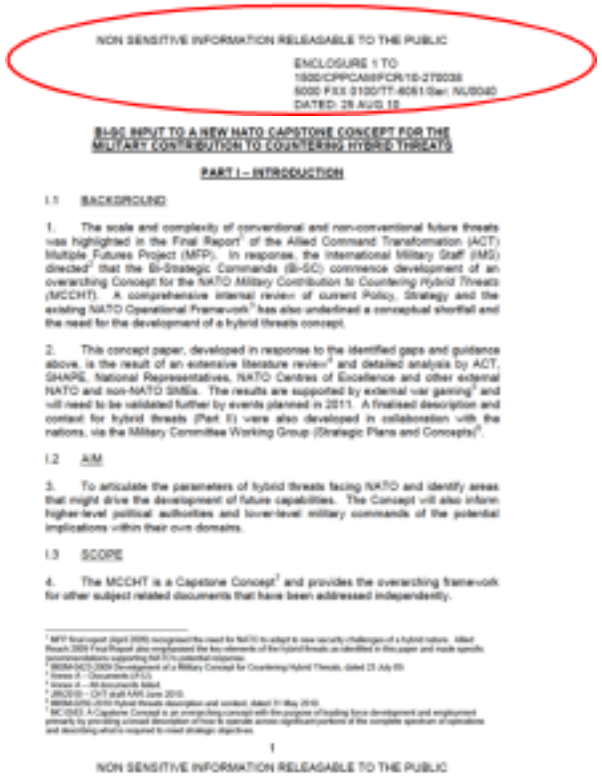
1

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

NATO Definition

- “Hybrid threats could be perpetrated by singular actors or a combination of states and non state actors with shared and diverse objectives, acting with different degrees of co-operation against NATO”.

- “Hybrid threats do, however, now present a significant challenge for the Alliance and its interests, whether encountered within national territory, in operational theatres or across **non-physical domains**” (including but not limited to cyber, information/media and financial environments).



NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

ENCLOSURE 1 TO

DATED: 28 AUG 10

BI-SC INPUT TO A NEW NATO CAPSTONE CONCEPT FOR THE MILITARY CONTRIBUTION TO COUNTERING HYBRID THREATS

PART I – INTRODUCTION

I.1 BACKGROUND

1. The scale and complexity of conventional and non-conventional future threats was highlighted in the Final Report[1] of the Allied Command Transformation (ACT) Multiple Futures Project (MFP). In response, the International Military Staff (IMS) directed[2] that the Bi-Strategic Commands (Bi-SC) commence development of an overarching Concept for the *NATO Military Contribution to Countering Hybrid Threats* (MCCHT). A comprehensive internal review of current Policy, Strategy and the existing NATO Operational Framework[3] has also underlined a conceptual shortfall and the need for the development of a hybrid threats concept.

2. This concept paper, developed in response to the identified gaps and guidance above, is the result of an extensive literature review[4] and detailed analysis by ACT, SHAPE, National Representatives, NATO Centres of Excellence and other external NATO and non-NATO SMEs. The results are supported by external war gaming[5] and will need to be validated further by events planned in 2011. A finalised description and context for hybrid threats (Part II) were also developed in collaboration with the nations, via the Military Committee Working Group (Strategic Plans and Concepts)[6].

I.2 AIM

3. To articulate the parameters of hybrid threats facing NATO and identify areas that might drive the development of future capabilities. The Concept will also inform higher-level political authorities and lower-level military commands of the potential implications within their own domains.

I.3 SCOPE

4. The MCCHT is a Capstone Concept[7] and provides the overarching framework for other subject related documents that have been addressed independently.

1

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

NATO’s response to hybrid threats and strategy of: prepare, deter, defend

Prepare

- “NATO continuously gathers, shares and assesses information in order to detect and attribute any ongoing hybrid activity”.
- Identifies national vulnerabilities and strengthen their own resilience,
- Training, exercises and education also play a significant role in preparing to counter hybrid threats.

Deter

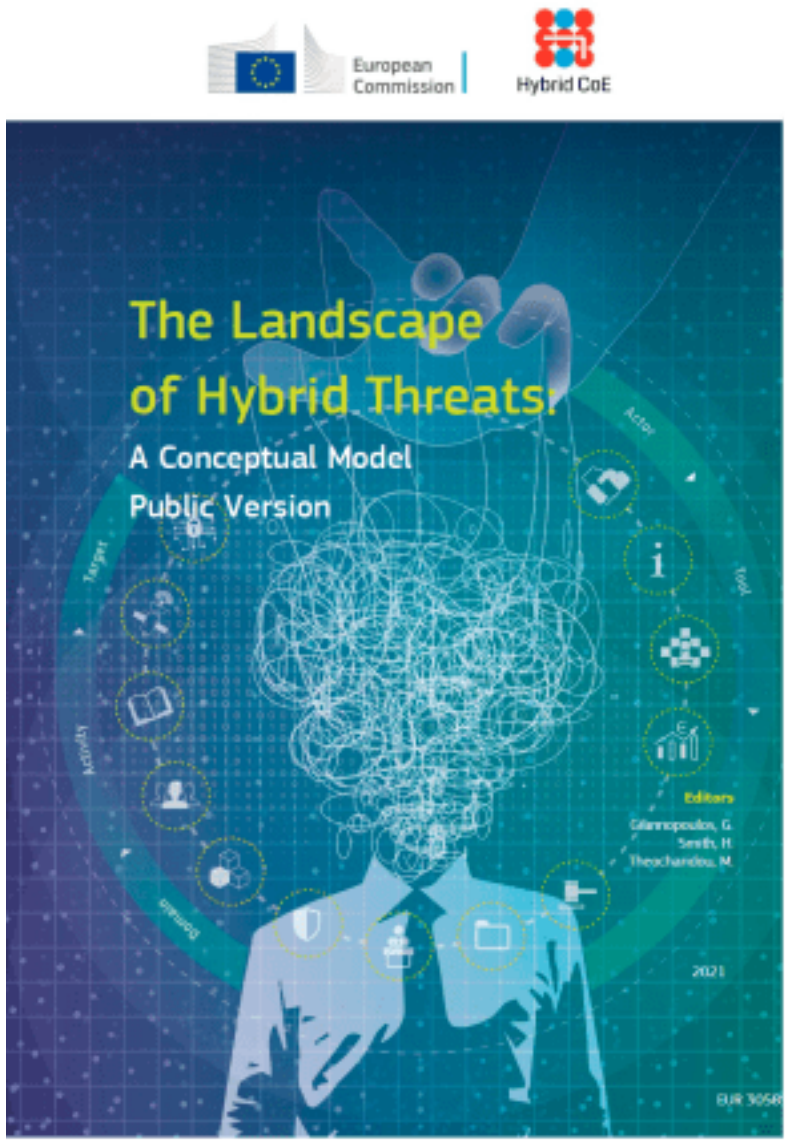
- Development of capabilities (political and military) and be resolved to act promptly
- Sending strong signals to adversaries through increasing readiness and preparedness of forces. Here StratCom is key

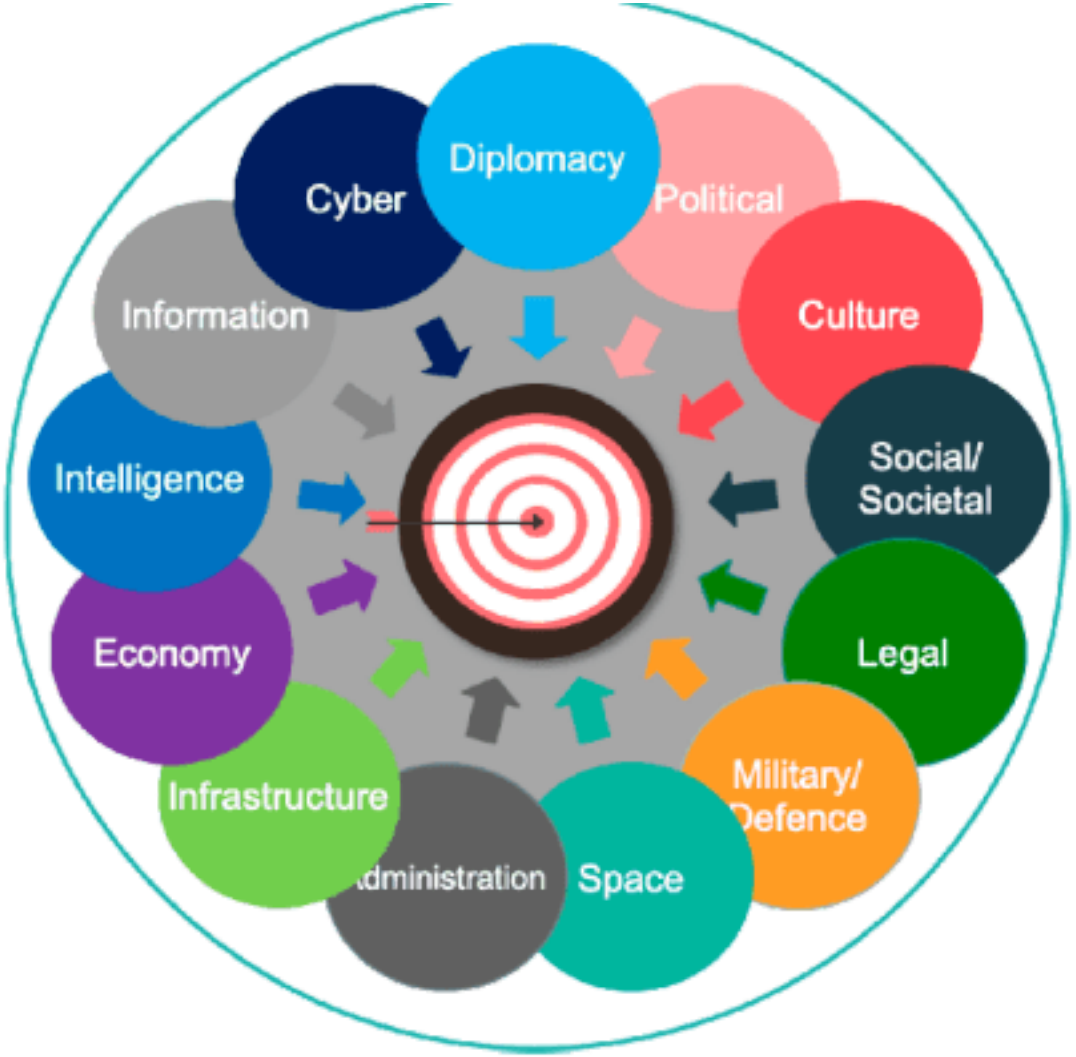
Defend

- “If deterrence should fail, NATO stands ready to defend any Ally against any threat. To this end, NATO forces have to be able to react in a quick and agile way, whenever and wherever needed.”

- “The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm the target by influencing its decision-making at the local, regional, state or institutional level.
- Such actions are **coordinated and synchronized and deliberately target democratic states’ and institutions’ vulnerabilities**.
- **Activities** can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and **designed to remain below the threshold of detection and attribution**.”

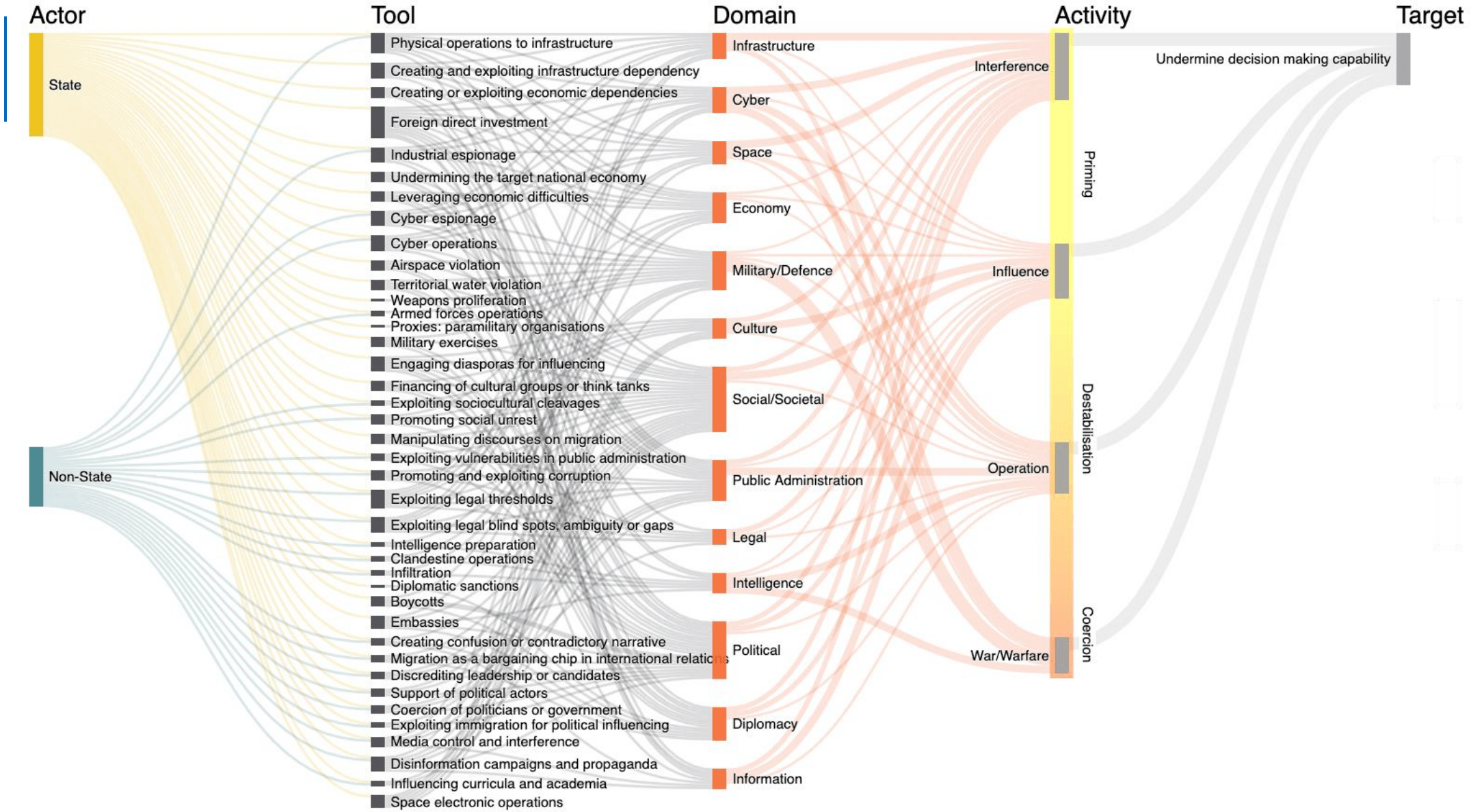
Source: Hybrid CoE https://www.hybridcoe.fi/what-is-hybridcoe/)


European Commission
Hybrid CoE
The Landscape of Hybrid Threats:
A Conceptual Model
Public Version
Actor
Tool
Target
Activity
Domain
Editors
Giannopoulos, G.
Smith, H.
Theocharidou, M.
2021
EUR 30585


Cyber
Diplomacy
Political
Information
Culture
Intelligence
Social/
Societal
Economy
Legal
Infrastructure
Military/
Defence
Administration
Space

JRC/Hybrid CoE conceptual model

- The **conceptual framework of hybrid threats**, developed by the Joint Research Centre (JRC) of the European Commission and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), is structured around four analytic pillars: actors, domains, tools and phases. The model considers 13 different domains –or "instruments of national power"– of hybrid threat activities: information, cyber, social, culture, political, diplomacy, infrastructure, legal, military, space, administration, economy, and intelligence. According to the conceptual model, hostile state and non-state actors target states in these different domains through a combination of tools for achieving their objectives. The spectrum of hybrid threats activities includes: interference, influence, operations/campaign, and warfare/war). These activities develop in a timeline that has three different phases: priming, destabilization and coercion. (See: Cullen et al. 2021).



Source: Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou 2021

Tools

- Propaganda
- Disinformation
- Leaks
- *Proxies*
- Paramilitary organizations
- Front organizations and covert funding of political parties
- Cyber attacks.
- Other.

The comprehensive resilience ecosystem (CORE) model

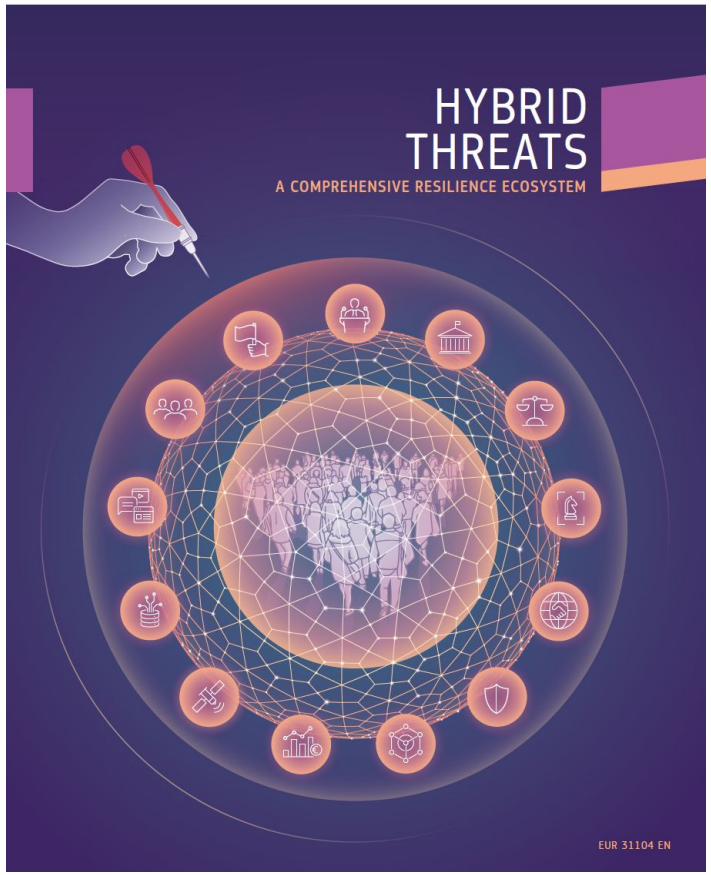
- The comprehensive resilience ecosystem (CORE) model developed by the JRC and the Hybrid CoE address hybrid threats through a systems approach representing democratic societies as a whole (Jungwirth et al. 2023). The 13 domains of the conceptual model are here considered to be “entry points or shields for/against hybrid tools” (Ibid.: 39) The CORE model is employed for analyzing and based on that analyses countering “hybrid threats that seek to undermine and harm the integrity and functioning of democracies, change decision-making processes, and create cascading effects” (Ibid.: 10). The CORE Model is based on the following key elements:

Foundations of Democratic Systems (7)	Domains of the Hybrid Threats Conceptual Model (13)	CORE model Ecosystem (3 spaces)	Layers of the ecosystem (3 layers)
Feeling of justice and equal treatment	information	Civic space	Local
Civil rights and liberties	cyber	Governance space	National
Political responsibility and accountability	social	Services space	International
Rule of law	culture		
Stability	political		
Reliability/availabili	diplomacy		
Foresight capabilities	infrastructure		
	legal		
	military		
	space		
	administration		
	economy		
	intelligence		

DOMINOES
digital resilience to disinformation

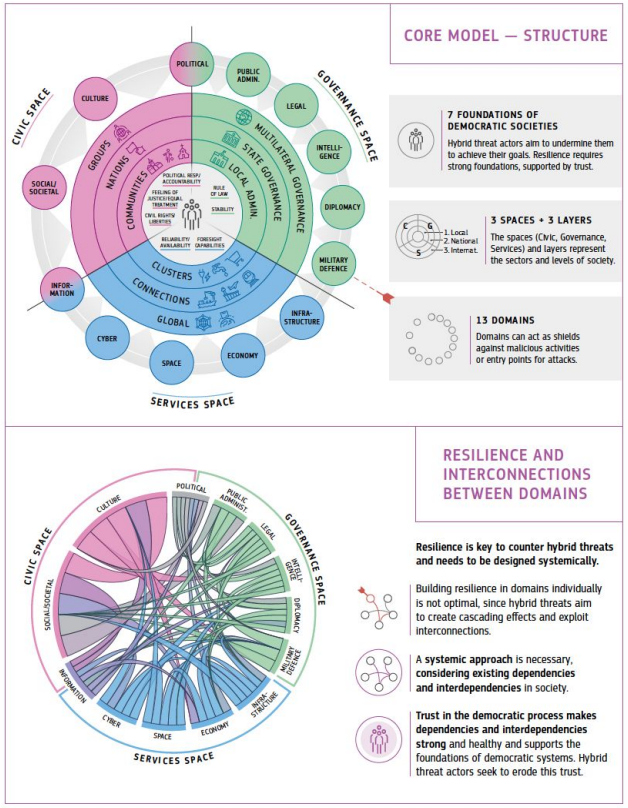
Erasmus+

European Commission | Hybrid CoE



CORE — A COMPREHENSIVE RESILIENCE ECOSYSTEM

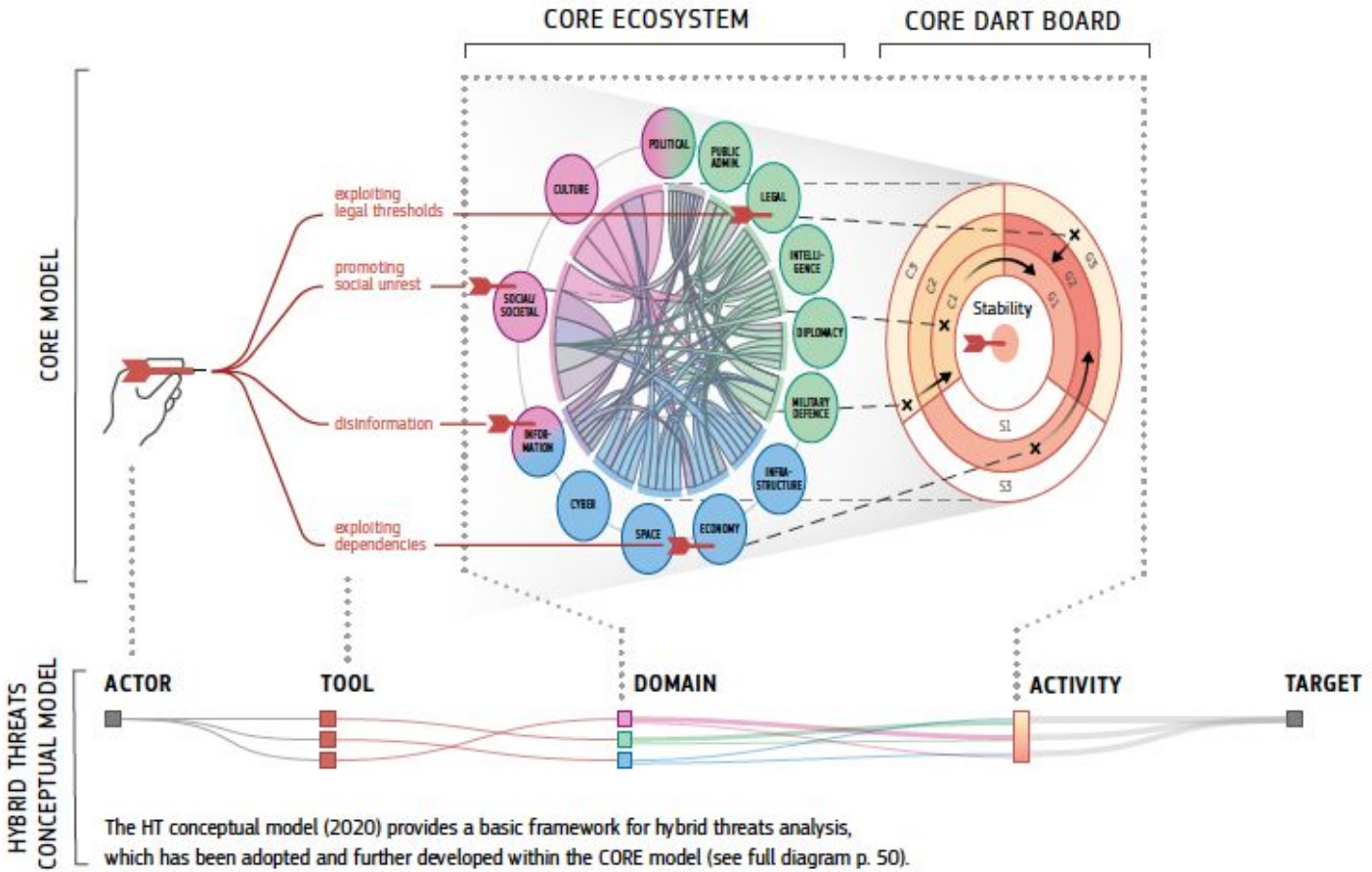
The comprehensive resilience ecosystem (CORE) model is a systemic representation of democratic society as a whole. It is used to analyse and ultimately counteract hybrid threats that seek to undermine and harm the integrity and functioning of democracies, change decision-making processes, and create cascading effects.



REPRESENTING THE IMPACT OF HYBRID THREATS

CORE can be used as a 'dart board' to map how actors use specific tools to attack different domains and create cascading effects to different spaces and layers.

It helps to analyse and understand impacts, developments/phases, and how intensely the spaces and layers are affected by hybrid threats and their dependencies.



The HT conceptual model (2020) provides a basic framework for hybrid threats analysis, which has been adopted and further developed within the CORE model (see full diagram p. 50).

DOMINOES
digital resilience to disinformation

1.1.4

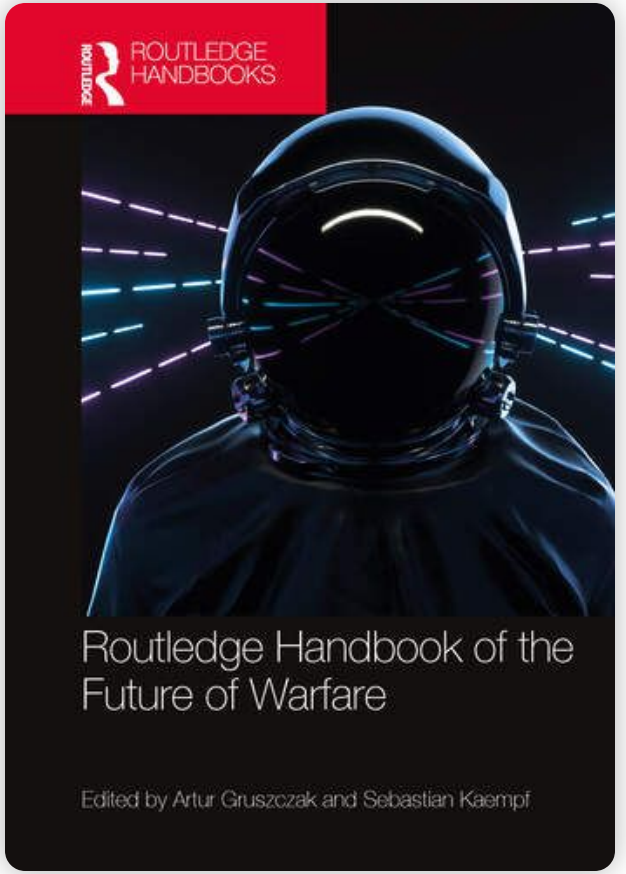
Cognitive and information warfare

Digital cOMpetences INformatiOn EcoSystem

2021-1-RO01-KA220-HED-000031158

Information Warfare

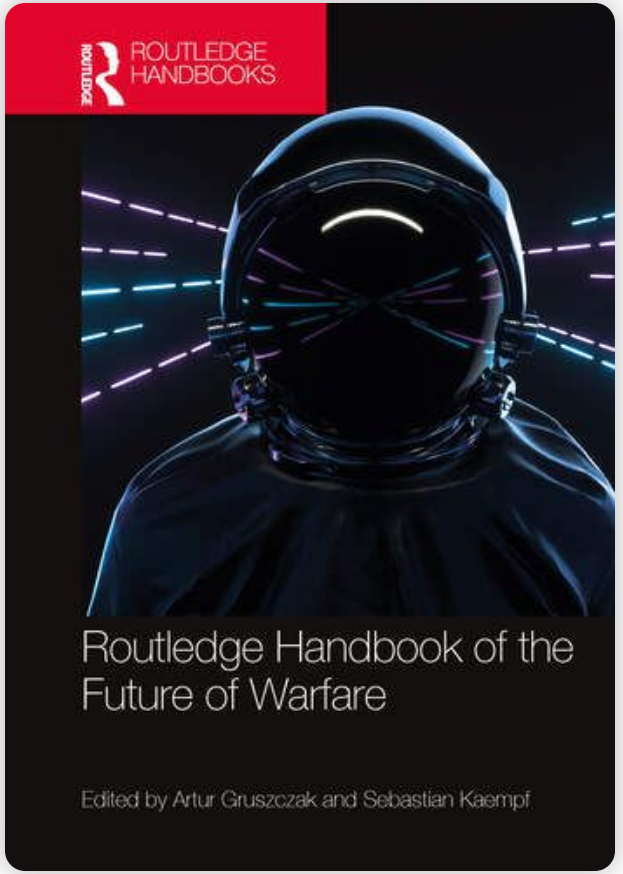
- During the last years, in the face of alleged unacknowledged interference activities against the West by authoritarian actors, the term information warfare has been used in the sense of weaponization of symbolic content (Arcos 2023)
- Digitalization and new technologies have created immense opportunities for adversaries to conduct hostile activities in the information environment and organize attacks against the cognitive domain through disinformation and information manipulations (Ibid).
- The basic underlying idea behind the term cognitive warfare is that in our digital information age the battlefield is not always and solely kinetic, a physical violent clash between armies, but involves wagging war at the cognitive level (Underwood 2017).



Source: Arcos, Intelligence and awareness, 2023

Information Warfare

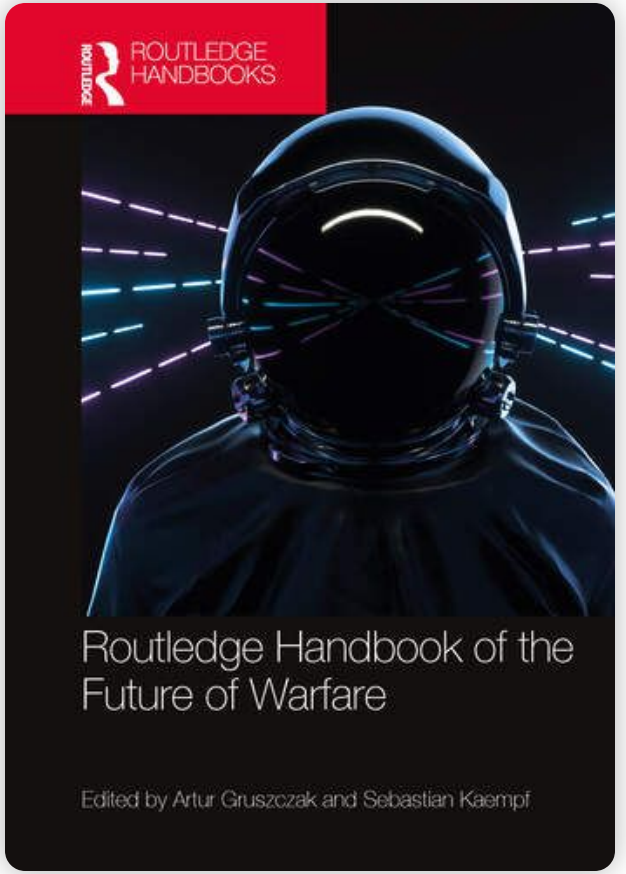
- Since humans make decisions based on our representations about the world emanating either from experience or from the information available through interpersonal symbolic interactions and through the different media – we cannot acquire direct experience on each and one of every international events and political development, and necessarily rely in the symbolic content transmitted by others – information can be weaponized or disseminated with a manipulative purpose for influencing our beliefs, understanding, attitudes or orientation toward objects (with positive or negative valence) and behaviors" (Arcos & Smith 2021).
- "Digitalization and the information revolution have produced an information environment that have transformed our societies and practices on the production, dissemination and consumption of symbolic content, with the effect of creating opportunities for adversaries to influence civilian populations of foreign countries through perception management, reflexive control and disinformation" (Arcos 2023).



Source: Arcos, Intelligence and awareness, 2023

Information Warfare

- As a concept, information warfare is problematic, since information can be instrumentalized against and adversary, or for the conduct of warfare, in distinct forms, activities and against different targets (military commanders, computer systems, intelligence systems, civilians); It involves “the protection, manipulation, degradation, and denial of information” (Libicki 1995, p. x).



Source: Arcos, Intelligence and awareness, 2023

Speaking at the U.S. Department of Defense Intelligence Information System 2017 Worldwide Conference, Lt. Gen. **Vincent R. Stewart** remarked:

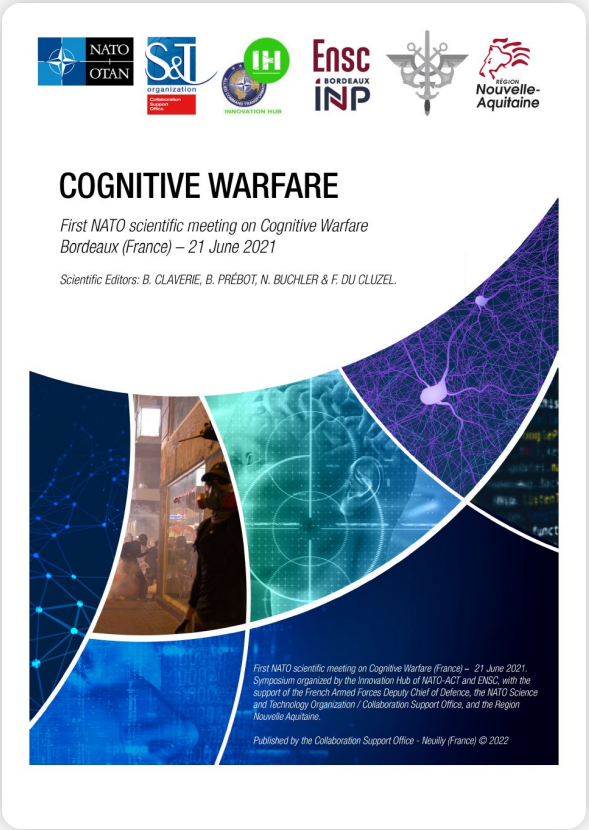
"Fifth-Generation Warfare. It will be cognitive warfare. In the 21st Century, warfare is about winning the information the decision space, either before or during a conflict. This is the deciding factor [...] Robbing our enemies of the decision space and the ability to think and act [...] A huge part of it is about information and how we collect, process, disseminate and protect that information and the systems that contain and deliver it" (Lt. Gen. Stewart

General Stewart used the illegal annexation of Crimea by the Russian Federation, as an example:

“What they actually did, as they shape the information environment proclaiming that they would defend ethnic Russians, was to sent the unidentified unidentifiable little green men to seize key location and used information warfare and cyber-attacks to communication channels and media outlets. By the time they held a referendum on Crimea annexation, Ukraine's decision space was gone. Russia already had control of the peninsula all without far many shots. Sun Tzu said to fight and conquer in all our battles is not supreme excellence. Supreme excellence consists in breaking the enemy's resistance without fighting”. (Ibid.)

Cognitive Warfare

- **Bernard Claverie** and **Francois Du Cluzel** have pointed out that the cognitive domain is a domain of modern warfare, together with land, maritime, air, space and more recently with the cyber domain,
- “It operates on a global stage since humankind as a whole is now digitally connected. It uses information technology and the tools, machines, networks, and systems that come with it. Its target is clear: our individual intelligences, to be considered both individually and as a group. Attacks are defined, structured, and organized to alter or mislead the thoughts of leaders and operators, of members of entire social or professional classes, of the men and women in an army, or on a larger scale, of an entire population in a given region, country or group of countries”. (Claverie and Du Cluzel 2022: 2-1).



DOMINOES
digital resilience to disinformation

Exercise in Groups

Erasmus+
2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Exercise in Groups

Running time:
1,5 hours

Participants split into **6 Groups of 5 members**

Each group should appoint **1 representative** for taking notes (in addition to engage in discussion) and present the results

- 2 Groups dealing with:
  - Malta
- 2 Groups dealing with
  - Romania
- 2 Groups dealing with
  - Spain

Method

Participants will engage in a structured discussion around the following questions:

- **How do you characterize the security environment?**
  - What are the main trends and drivers shaping potential scenarios for the region (Southern Europe and the Mediterranean)?
- **What are the main players** (state and non-state) **in the region from a political and security perspective?**
- **What are threats and most important challenges** (perspective of implications for Malta or Romania or Spain?)

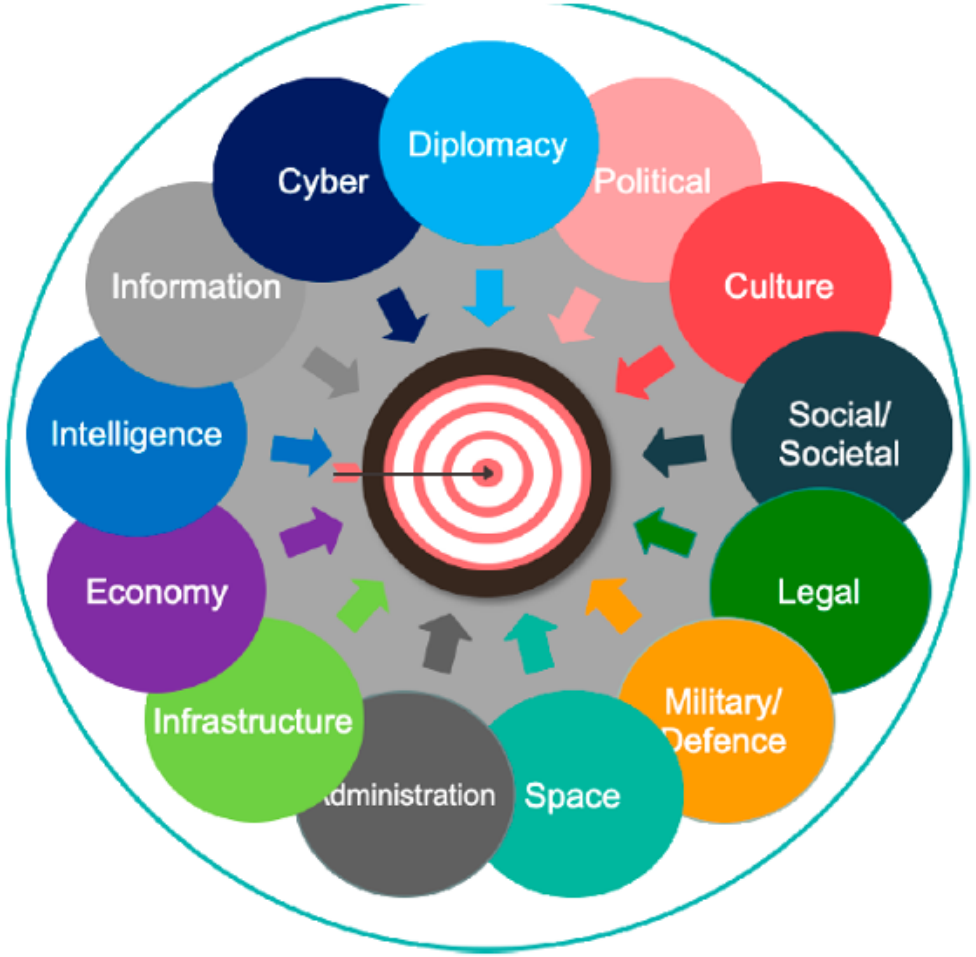
Method

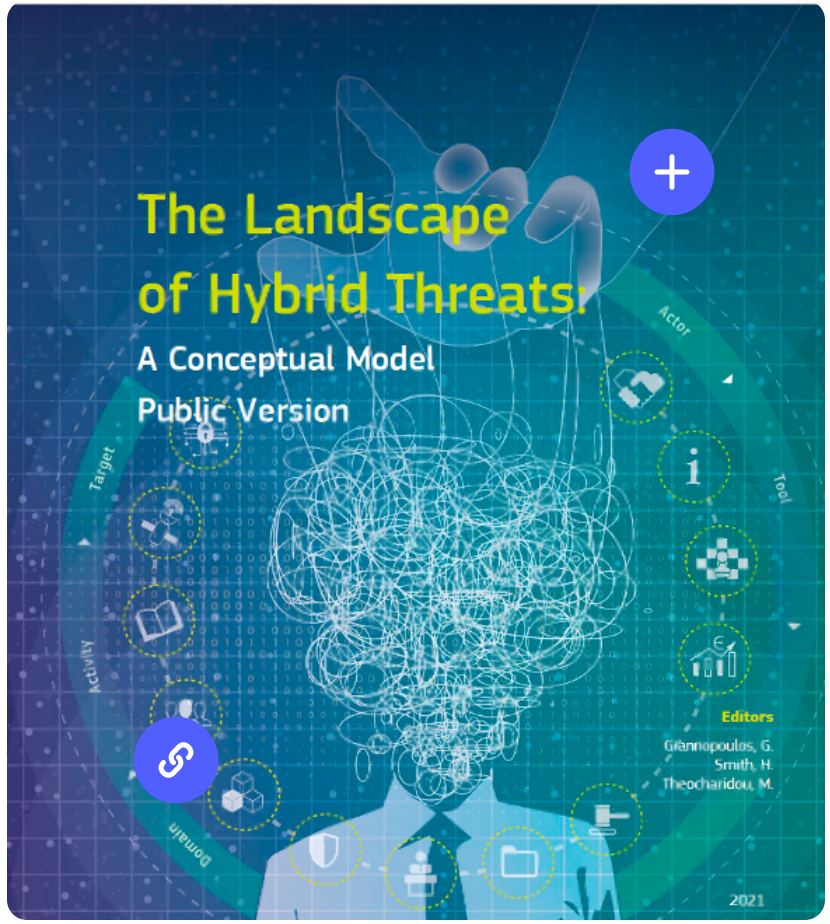
Participants will engage in a structured discussion around the following questions:

- **What vulnerabilities** (13 domains) **and opportunities** (local, national, transnational) **could be exploited by hostile actors through information manipulations and disinformation?**
- **What potential measures/initiatives could strengthen Malta/Romania/Spain's capability and competence to deal with those threats and with their potential manipulative activities in the information environment?**
    - (Consider not only government actors but also civil society)

Method

Use the **13 domains of hybrid threat activity of the JRC/Hybrid CoE conceptual framwework** when discussing on vulnerabilities and potential mitigation measures/initiatives



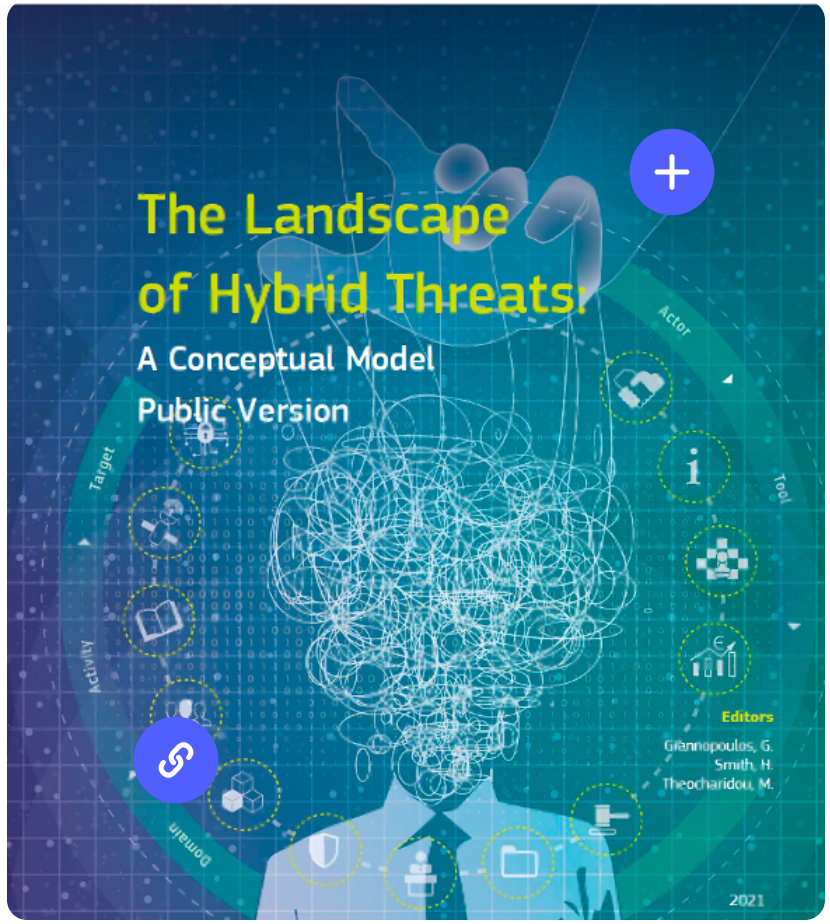


Lorem ipsum dolor

Method

1. **Discuss the results** of **your in-group discussion** with the other group that was assigned the same country.
2. **Agree on key points** to be presented to the whole classroom.
3. **Presentations** (5 minutes per country).

NOTE: You can use post-its and flipcharts to organize the inputs in your in-group discussion



Lorem ipsum dolor

DOMINOES
digital resilience to disinformation

References

Erasmus+
2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

References

- **Arcos, Ruben & Smith, Hanna** (2021). Digital Communication and Hybrid Threats. Presentation, Icono 14, 19(1), 1-14. doi: 10.7195/ri14.v19i1.1662.
- **European Parliament** (2022) European Parliament resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0052_EN.pdf
- **Eurostat** (2023). Digital economy and society statistics - households and individuals. Data extracted in December 2022. Last updated May last edited on 2 May 2023) https://bit.ly/3QeuS0D
- **Reuters Institute for the Study of Journalism** (2023). Digital News Report 2023. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023
- **Wanless, Alicia and Pamment, James** (2019). Editorial, Journal of Information Warfare, 18(3). https://www.jinfowar.com/journal/volume-18-issue-3/our-guest-editors

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Rubén Arcos (URJC)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Conflict and its manifestation in the information environment

1.1.1

10.5281/zenodo.10063880

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

The information environment has experienced enormous changes driven by an ongoing technological and digital revolution and the new ways humans produce, transmit and receive symbolic content

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

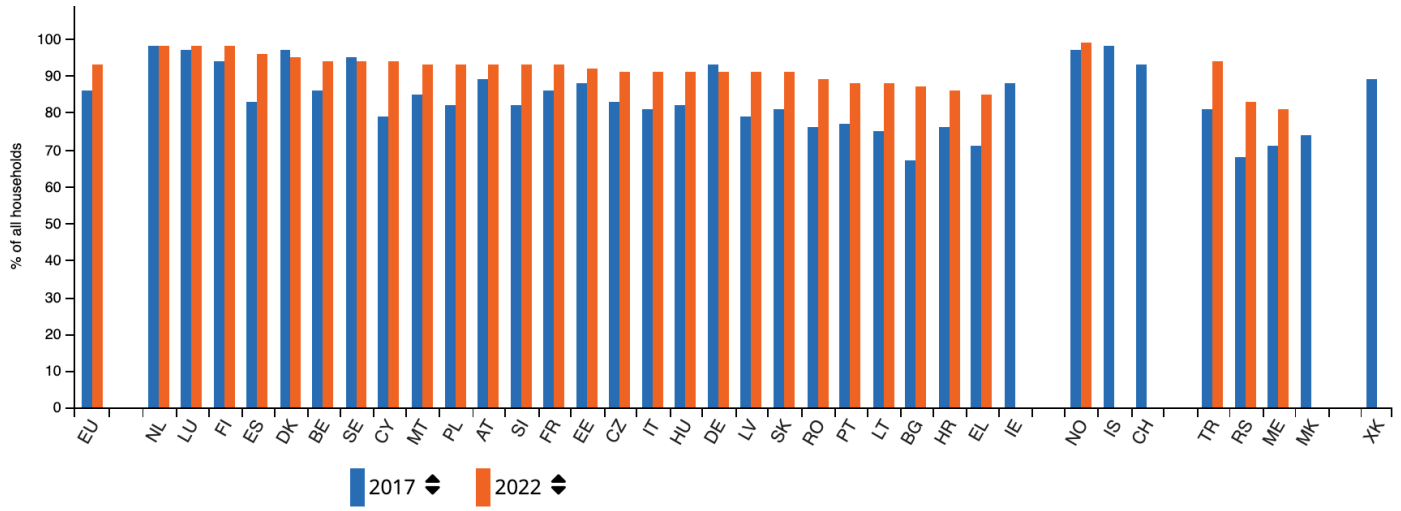
Growth of Internet access in Europe

DOMINOES

Tweet

In 2022, the share of EU households with internet access has risen to 93 %, up from 72 % in 2011.

Internet access of households, 2017 and 2022



EU estimate

*2022 not available: Ireland, Iceland, Switzerland, North Macedonia and Kosovo**

**Kosovo (XK) This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.*

Source: Eurostat (online data code: isoc_ci_in_h)

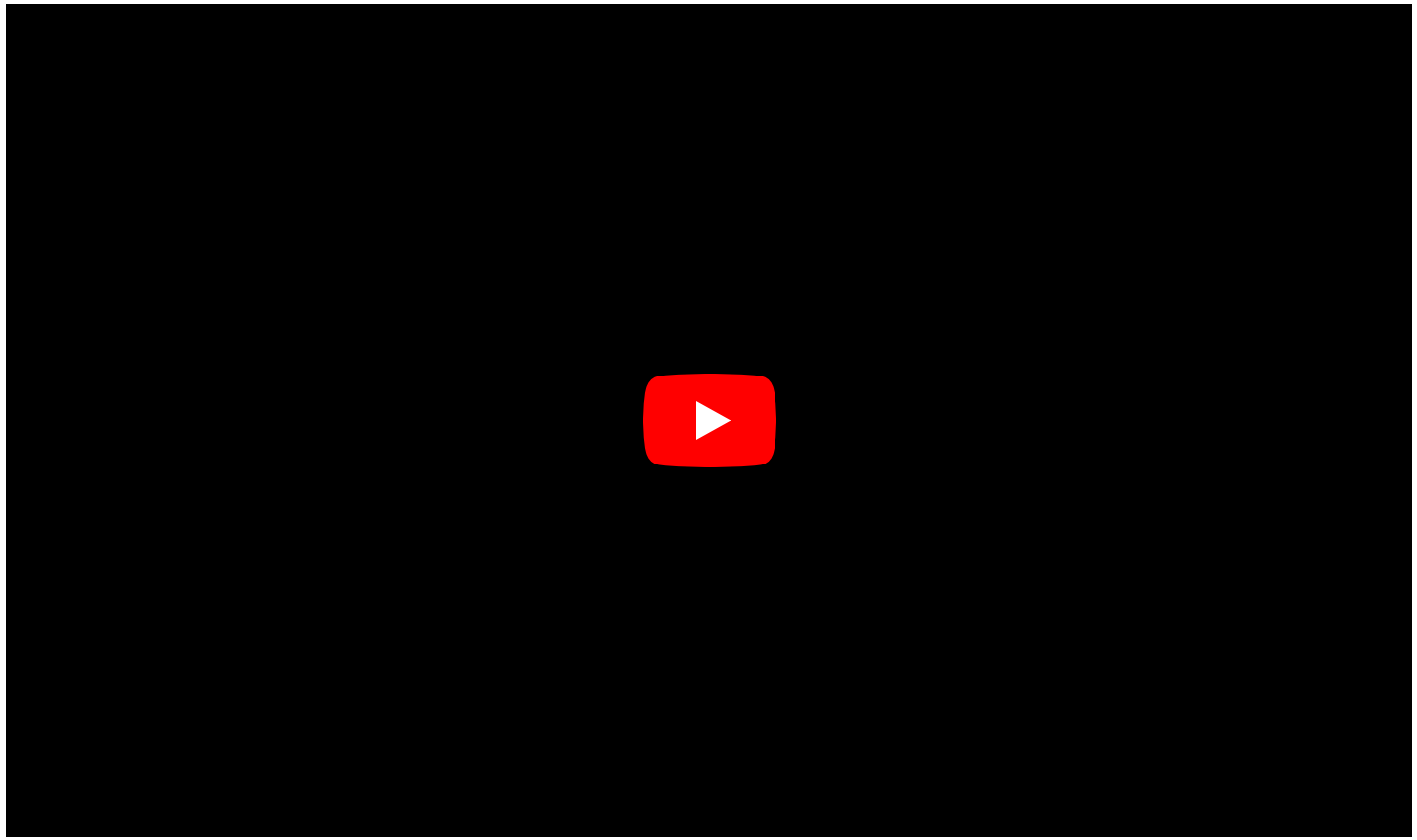
eurostat

According to Eurostat, “in 2022, the share of **EU households with internet access has risen to 93 %**, up from 72 % in 2011”

(Eurostat 2023)

Structural shifts in the informative ecosystem

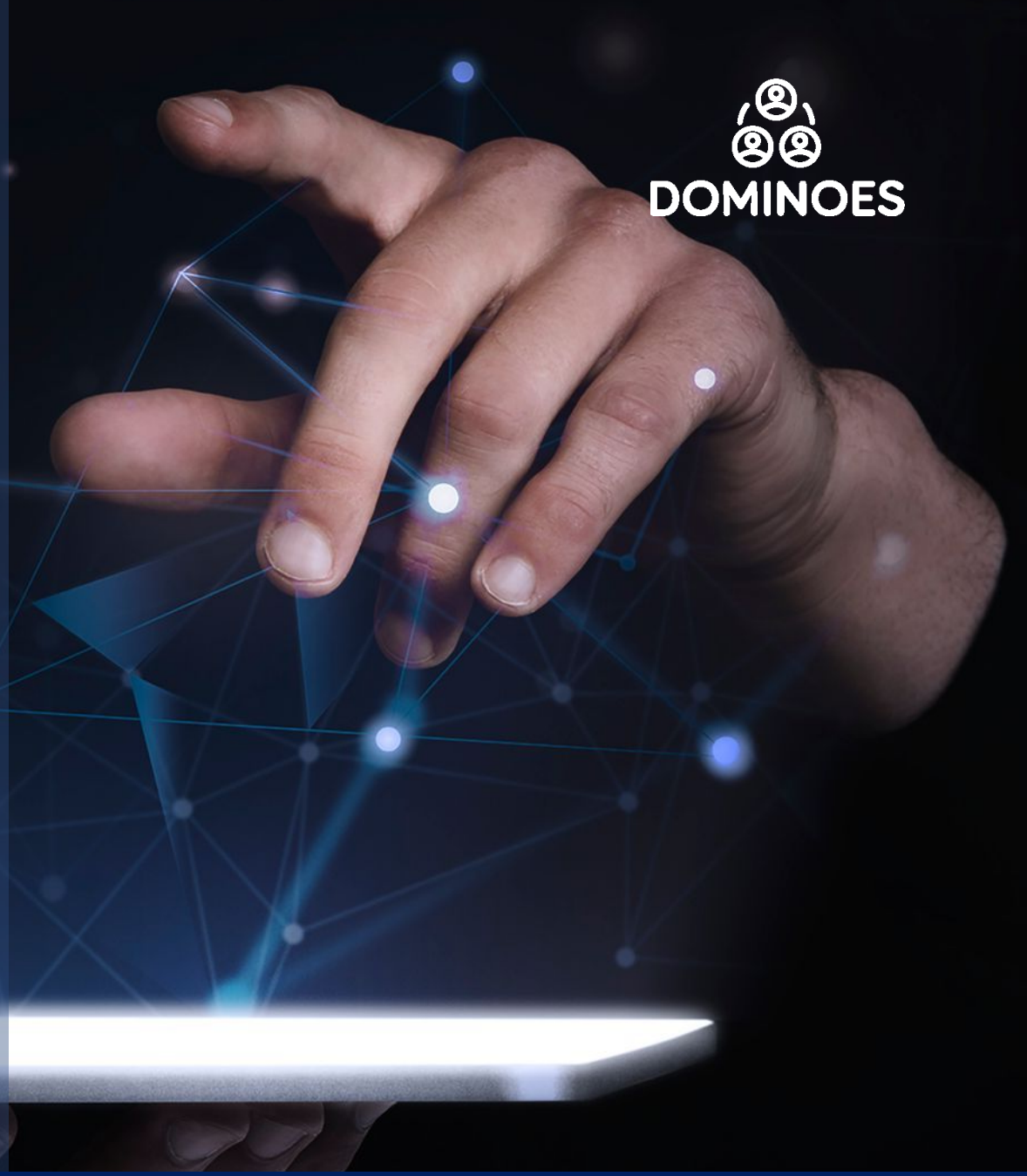
DOMINOES



The **Reuters Institute Digital News Report 2022** has noted the "**structural shifts towards a more digital, mobile**, and platform-dominated media environment, with further implications for the business models and formats of journalism"

(Reuters Institute for the Study of Journalism 2023: 10).

Unlike in the golden age of traditional media, in our overabundant information environment journalistic news reporting, news analysis and opinion pieces on international, national, and regional events and developments compete for the attention of an empowered audience that is now able as well to produce and disseminate content.



Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

Since human beings develop situational awareness and "make decisions based on their representations about the world and the information available through interpersonal symbolic interactions and through the different media," including social media platforms, information and digital content can be deliberately used with malicious intent.

(Arcos & Smith 2021: 6)

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DOMINOES

Today, our digital communication environment and the communication tools that we Europeans employ for legitimate purposes are also being employed by foreign hostile actors for interfering in our democratic processes like elections, erode trust in our institutions, divide and destabilize our societies.

(Arcos & Smith 2021: 6)

Co-funded by the European Union

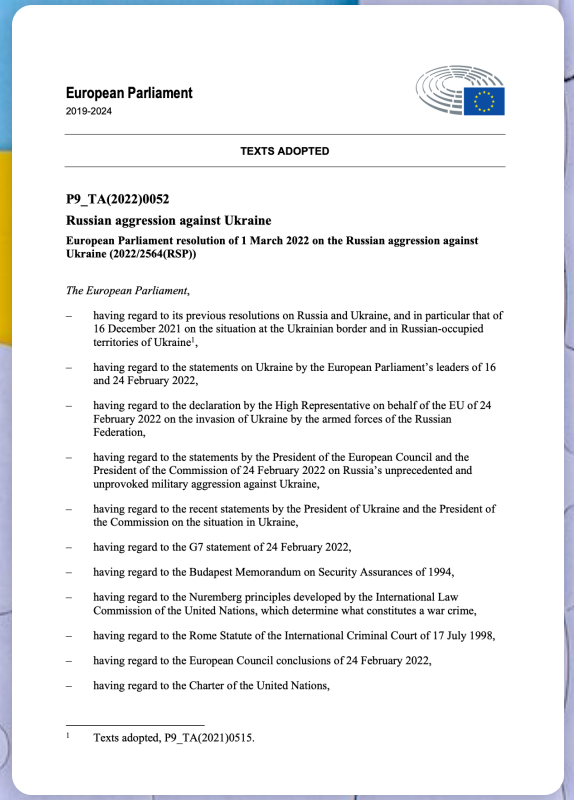
2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DOMINOES

The **European Parliament has condemned the use of information warfare by Russian authorities**, their proxies, and state-funded media, in support of its military aggression against Ukraine, as well its employment of information manipulations and hostile narratives against the EU and NATO

(Arcos, 2023)



European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2022)0052

Russian aggression against Ukraine

European Parliament resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP))

The European Parliament,

– having regard to its previous resolutions on Russia and Ukraine, and in particular that of 16 December 2021 on the situation at the Ukrainian border and in Russian-occupied territories of Ukraine[1],

– having regard to the statements on Ukraine by the European Parliament's leaders of 16 and 24 February 2022,

– having regard to the declaration by the High Representative on behalf of the EU of 24 February 2022 on the invasion of Ukraine by the armed forces of the Russian Federation,

– having regard to the statements by the President of the European Council and the President of the Commission of 24 February 2022 on Russia's unprecedented and unprovoked military aggression against Ukraine,

– having regard to the recent statements by the President of Ukraine and the President of the Commission on the situation in Ukraine,

– having regard to the G7 statement of 24 February 2022,

– having regard to the Budapest Memorandum on Security Assurances of 1994,

– having regard to the Nuremberg principles developed by the International Law Commission of the United Nations, which determine what constitutes a war crime,

– having regard to the Rome Statute of the International Criminal Court of 17 July 1998,

– having regard to the European Council conclusions of 24 February 2022,

– having regard to the Charter of the United Nations,

[1] Texts adopted, P9_TA(2021)0515.

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

Mis- and disinformation, conspiracy theories and propaganda constitute symbolic tools that are targeted towards citizens abroad to produce cognitive, affective, and behavioral effects.

The manipulation of public opinion processes and the degradation of the discussion on public issues through hostile influencing tactics in the information environment undermine the capability of democratic societies to make informed decisions.

Manufactured confusion around international developments, political events, or hostile activities can damage a society's willingness and ability to respond to impending threats and pressing challenges.

(Arcos & Smith 2021: 6)

As Wanless and Pamment (2019) have pointed out, "relatively objective principles such as history, scientific knowledge, and territorial boundaries are being disputed in the information space by revisionist powers. More controversial fault lines such as cultural identity, migration, and politics are the subject of increasingly intense contestation".

References

- **Arcos, Ruben & Smith, Hanna** (2021). Digital Communication and Hybrid Threats. Presentation, Icono 14, 19(1), 1-14. doi: 10.7195/ri14.v19i1.1662.
- **Arcos, Rubén** (2023). Intelligence and Awareness. In Routledge Handbook of the Future of Warfare (pp. 272-283). Routledge. https://doi.org/10.4324/9781003299011-29
- **European Parliament** (2022) European Parliament resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0052_EN.pdf
- **Eurostat** (2023). Digital economy and society statistics - households and individuals. Data extracted in December 2022. Last updated May last edited on 2 May 2023) https://bit.ly/3QeuS0D
- **Reuters Institute for the Study of Journalism** (2023). Digital News Report 2023. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023
- **Wanless, Alicia and Pamment, James** (2019). Editorial, Journal of Information Warfare, 18(3). https://www.jinfowar.com/journal/volume-18-issue-3/our-guest-editors

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Rubén Arcos (URJC)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Hybrid warfare/threats

1.1.2

doi.org/10.5281/zenodo.10063889

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.

Universidad Rey Juan Carlos

L-Università ta' Malta

NEW STRATEGY CENTER

According to Frank Hoffman, the concept of Hybrid Warfare was first publicly used “by General Mattis at the Defense Forum sponsored by the Naval Institute and Marine Corps Association on September 8, 2005”

HOFFMAN (2007: 14)

“

'We expect future enemies to look at the four approaches, irregular, catastrophic and disruptive] as a sort of menu and select a combination of techniques or tactics appealing to them.

We do not face a range of four separate challengers as much as the combination of novel approaches—a merger of different modes and means of war. This unprecedented synthesis is what we call Hybrid Warfare'

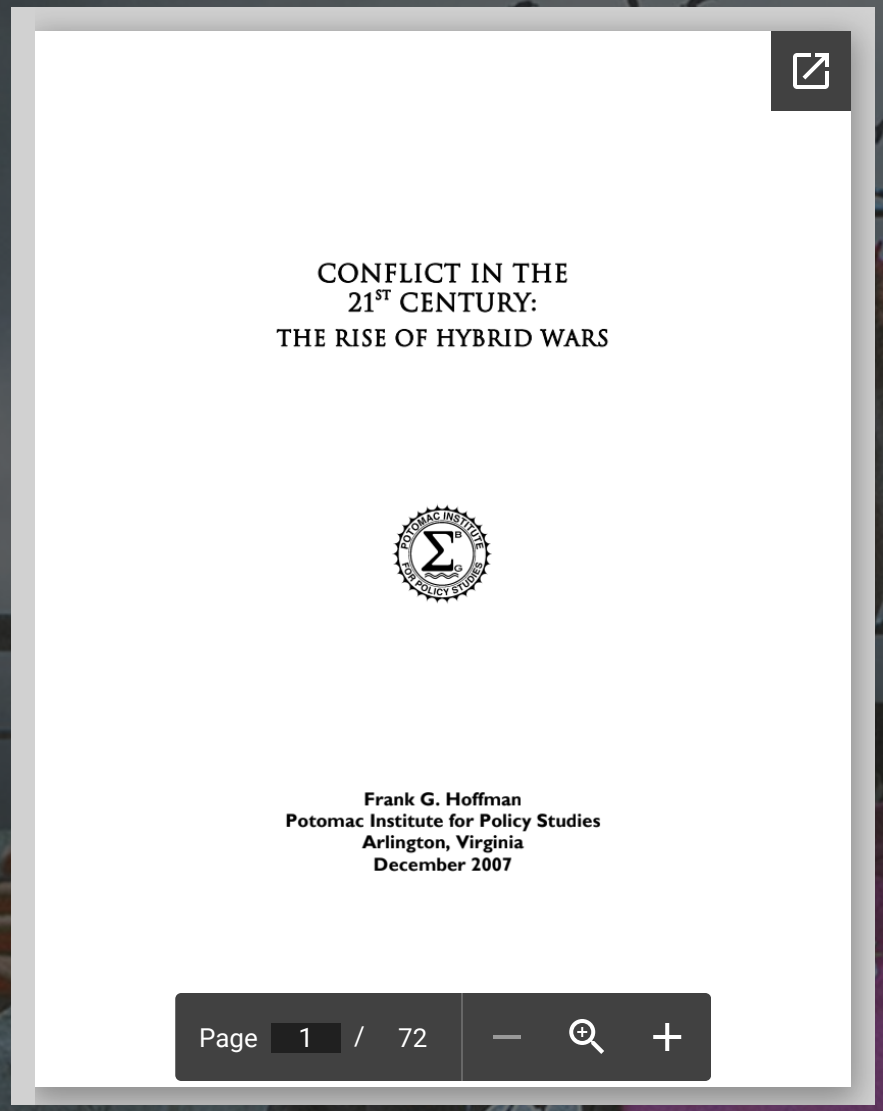
MATTIS AND HOFFMAN (2005)

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem



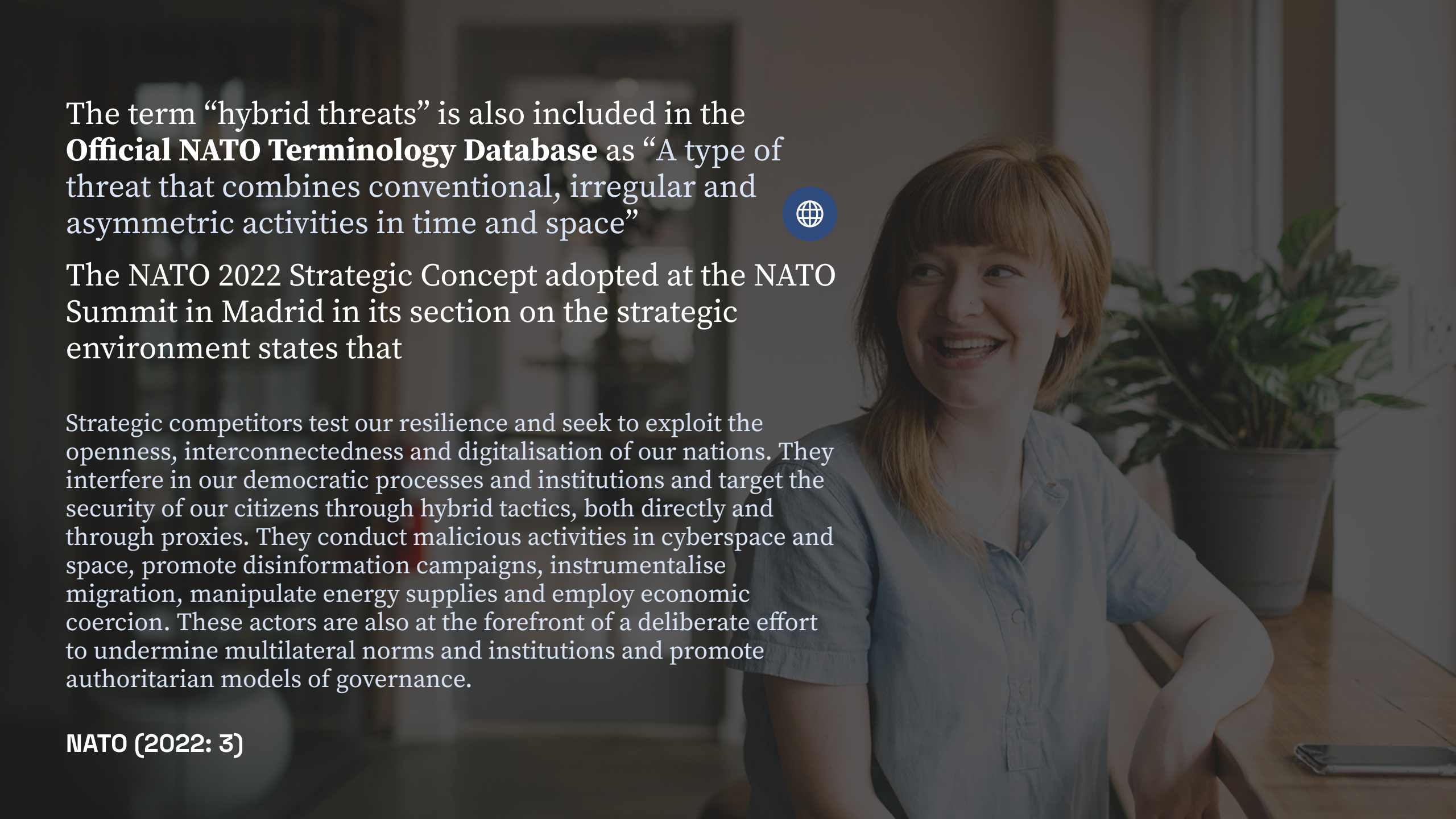
In his paper “Confict in the 21st Century: The rise of hybrid wars” (2007) Hoffman states

"Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid Wars can be conducted by both state and non-state actors.” (p. 8)

The 2016 EU Framework to Counter Hybrid Threats explained that the concept of hybrid threats

"aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats." (p.2)

EUROPEAN COMMISSION (2016, P. 2)

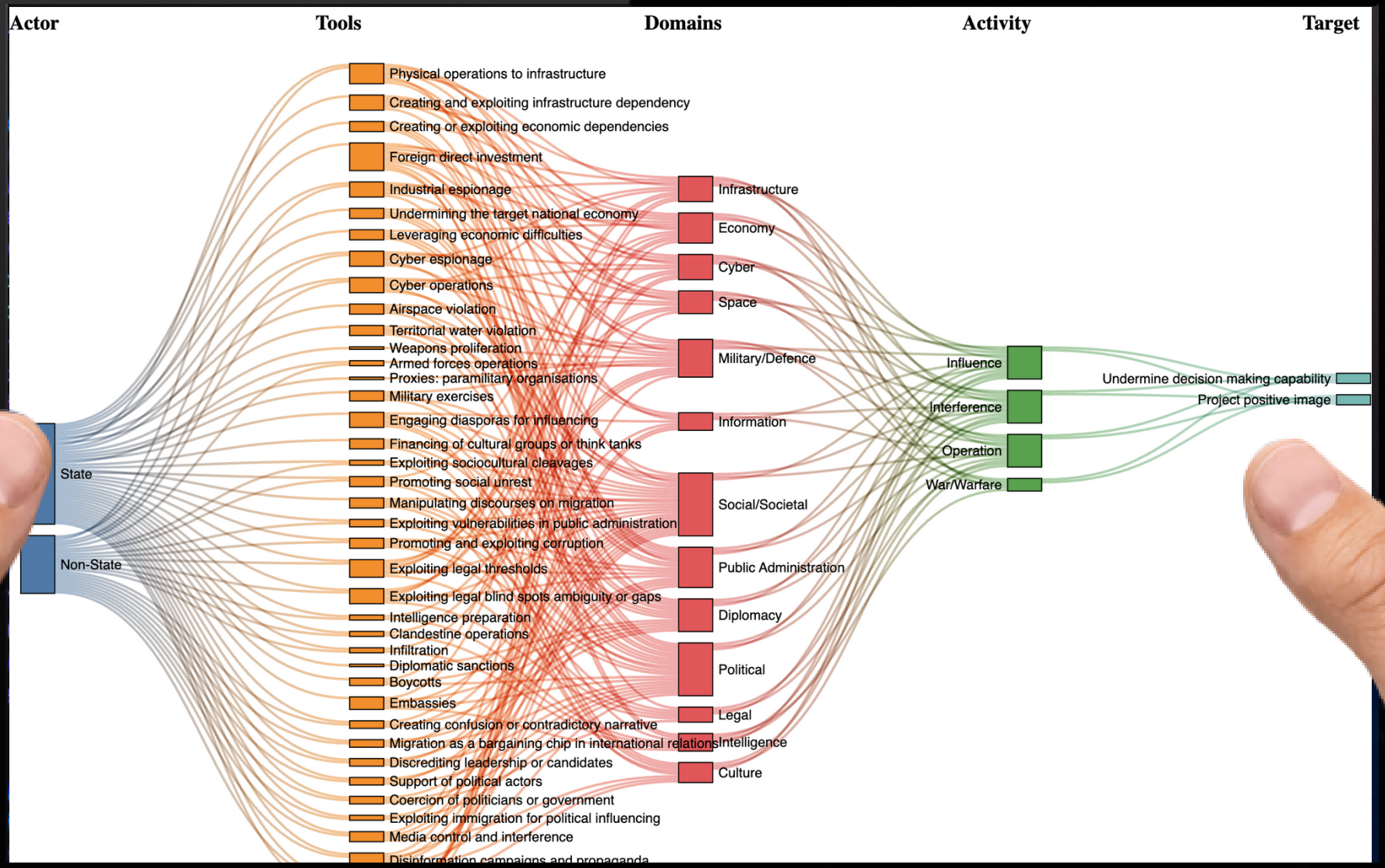


The term “hybrid threats” is also included in the **Official NATO Terminology Database** as “A type of threat that combines conventional, irregular and asymmetric activities in time and space”

The NATO 2022 Strategic Concept adopted at the NATO Summit in Madrid in its section on the strategic environment states that

Strategic competitors test our resilience and seek to exploit the openness, interconnectedness and digitalisation of our nations. They interfere in our democratic processes and institutions and target the security of our citizens through hybrid tactics, both directly and through proxies. They conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalise migration, manipulate energy supplies and employ economic coercion. These actors are also at the forefront of a deliberate effort to undermine multilateral norms and institutions and promote authoritarian models of governance.

NATO (2022: 3)



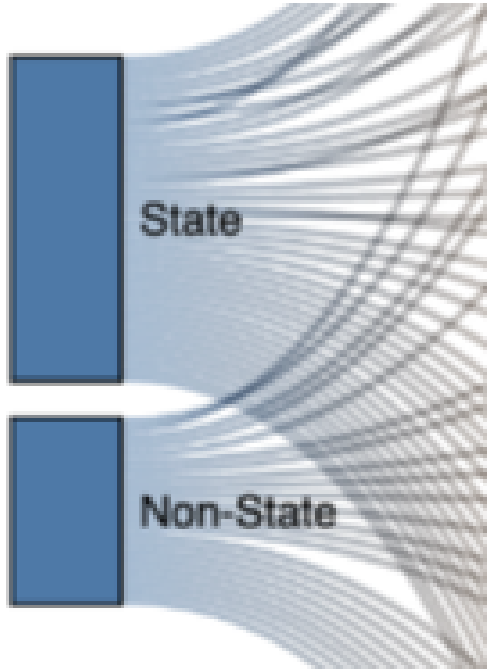
Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiO

Domains

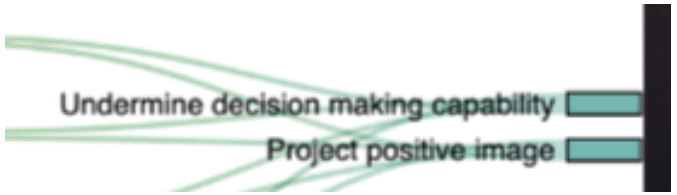
Tools


Physical operations to infrastructure
Creating and exploiting infrastructure dependency
Creating or exploiting economic dependencies
Foreign direct investment

Actors



Target


Undermine decision making capability
Project positive image

Activity

The comprehensive resilience ecosystem (CORE) model developed by the JRC and the Hybrid CoE address hybrid threats through a systems approach representing democratic societies as a whole (Jungwirth et al. 2023)

The 13 domains of the conceptual model are here considered to be "entry points or shields for/against hybrid tools" (Ibid.: 39)

The CORE model is employed for analyzing and based on that analyses countering "hybrid threats that seek to undermine and harm the integrity and functioning of democracies, change decision-making processes, and create cascading effects" (Ibid.: 10).

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

The CORE Model is based on the following key elements:

DOMINOES

7 Foundations of Democratic Systems

- Feeling of justice and equal treatment
- Civil rights and liberties
- Political responsibility and accountability
- Rule of law
- Stability
- Reliability/availability
- Foresight capabilities

13 Domains Hybrid Threats Conceptual Model

- Information
- Cyber
- Social
- Culture
- Political
- Diplomacy
- Infrastructure
- Legal
- Military
- Space
- Administration
- Economy
- Intelligence

3 CORE model Ecosystem

- Civil space
- Governance space
- Services space

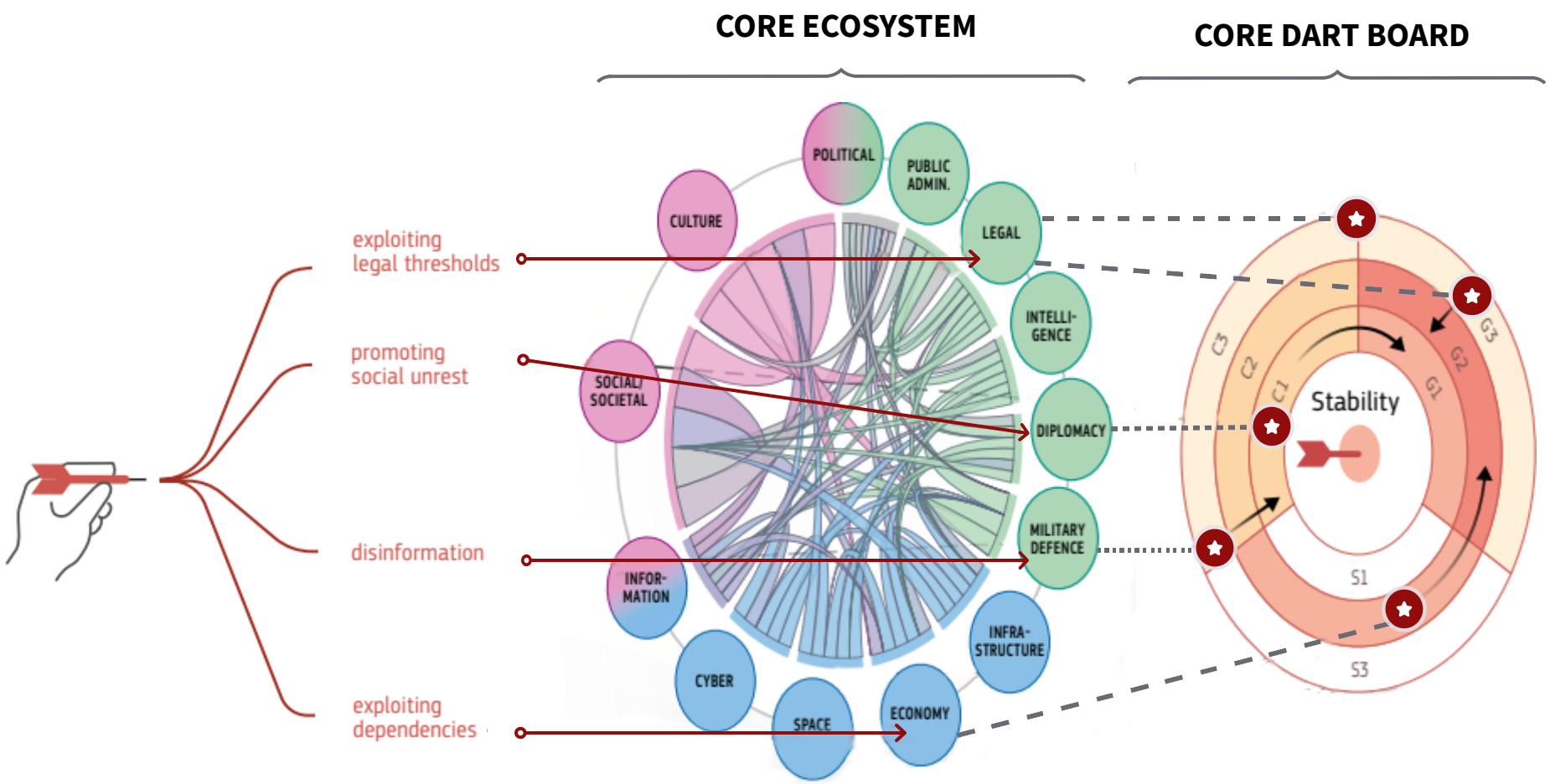
3 Layers of the ecosystem

- Local
- National
- International

As explained in the CORE model, **this framework can be used to map how hostile actors make use of specific tools for attacking democratic societie**s in the 13 different domains, understand their impacts, developments and how the three sectors of society or spaces and their layers are affected (Ibid.: 11).

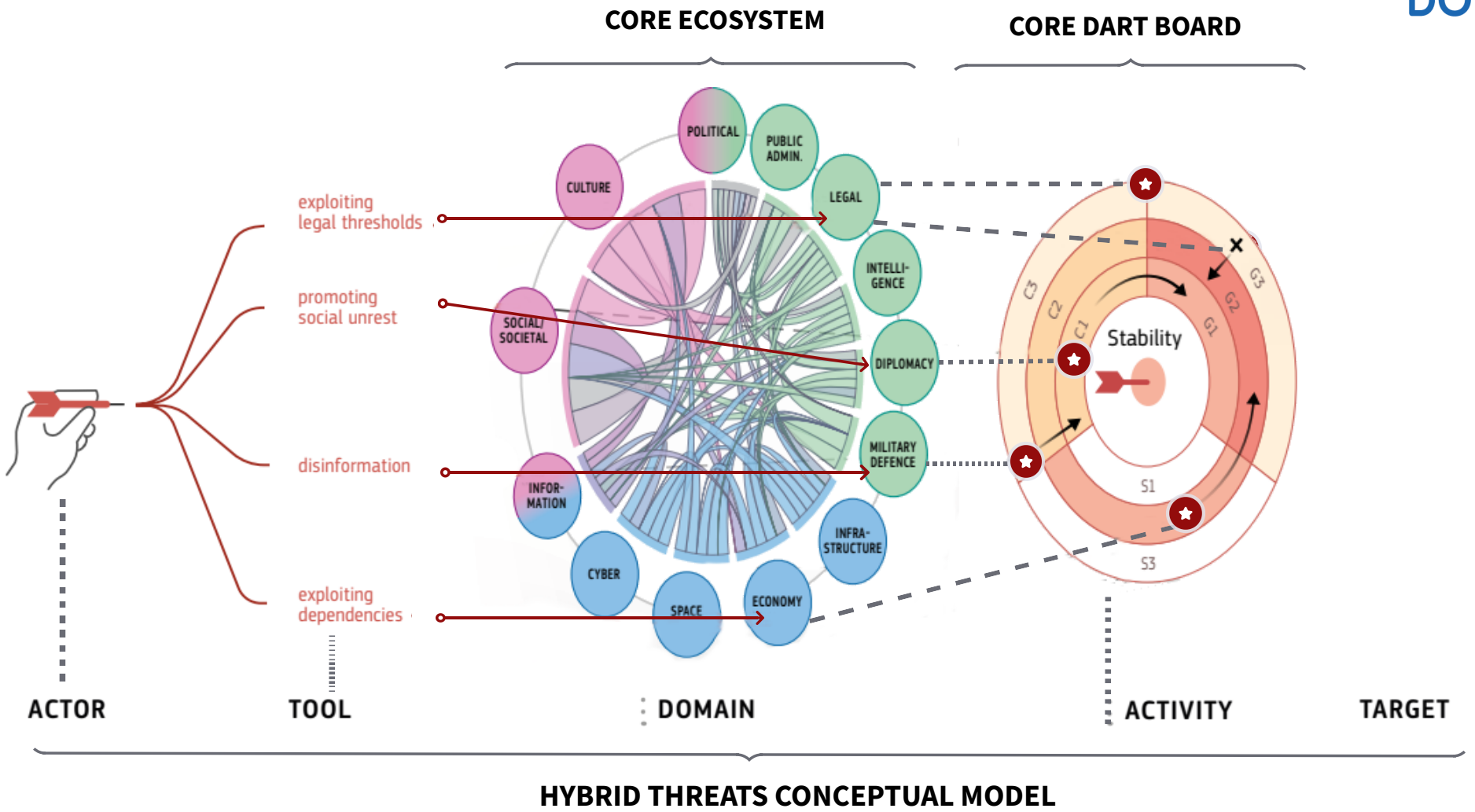
Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

The CORE Model

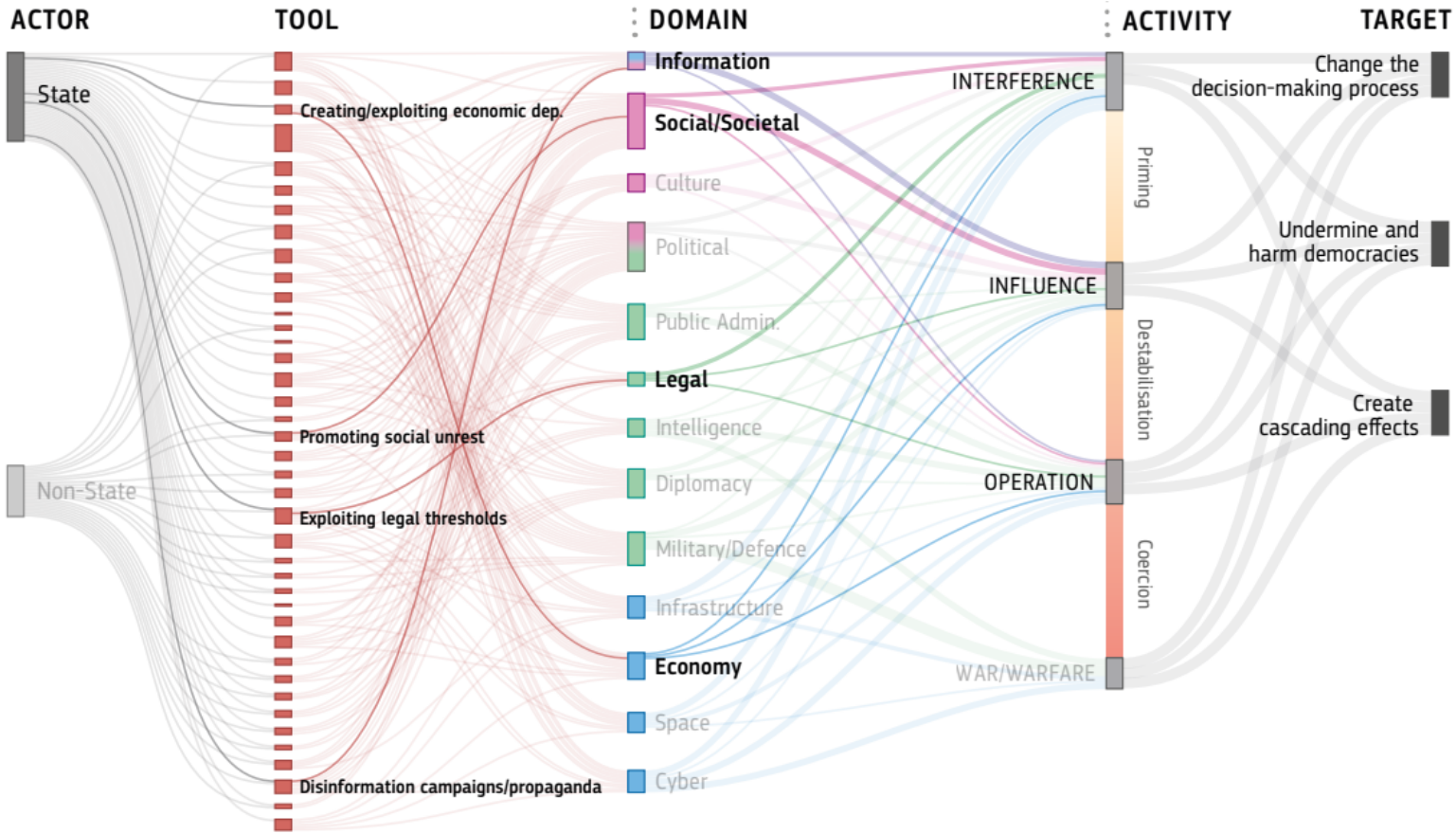


Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

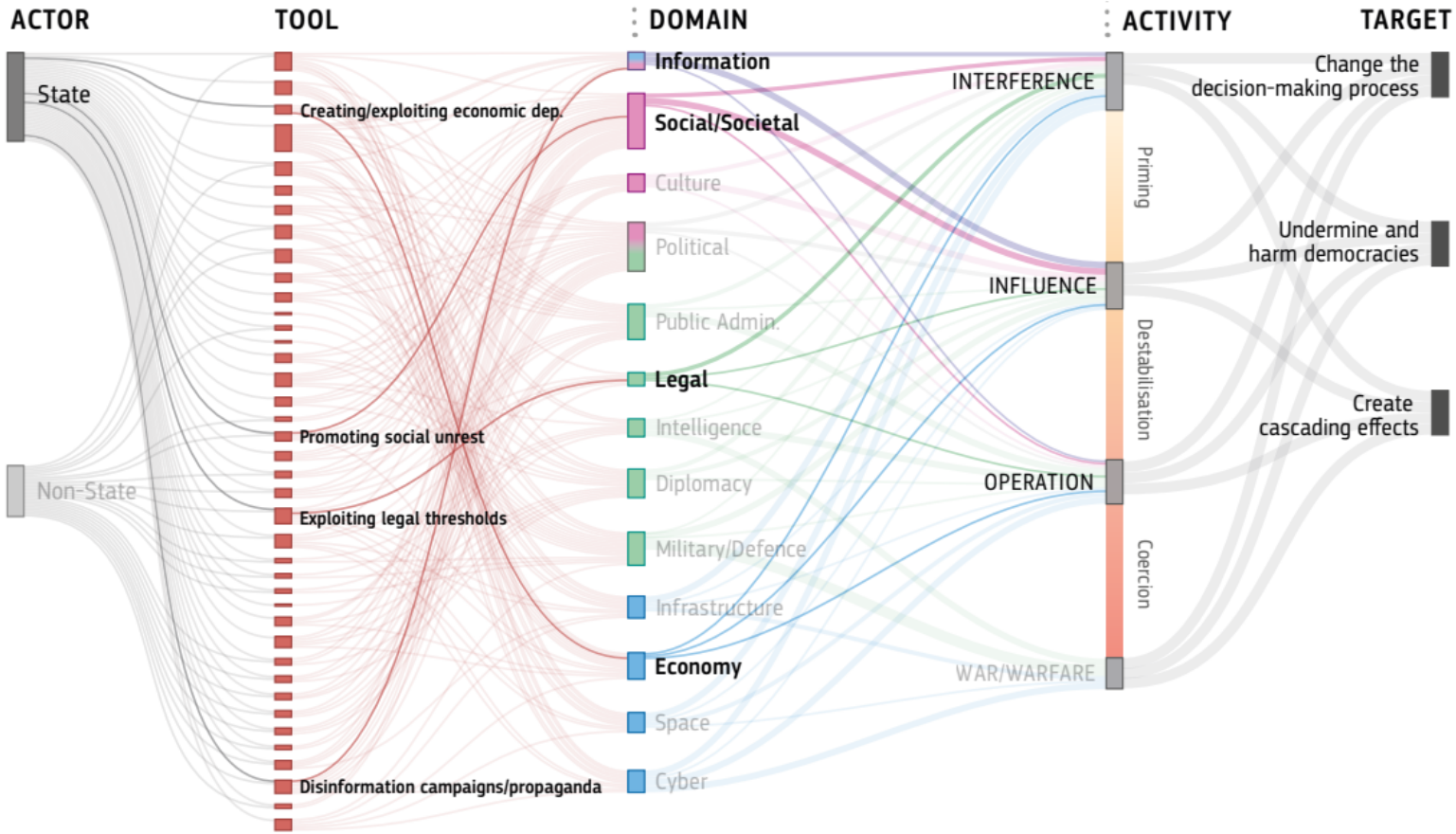
The CORE Model



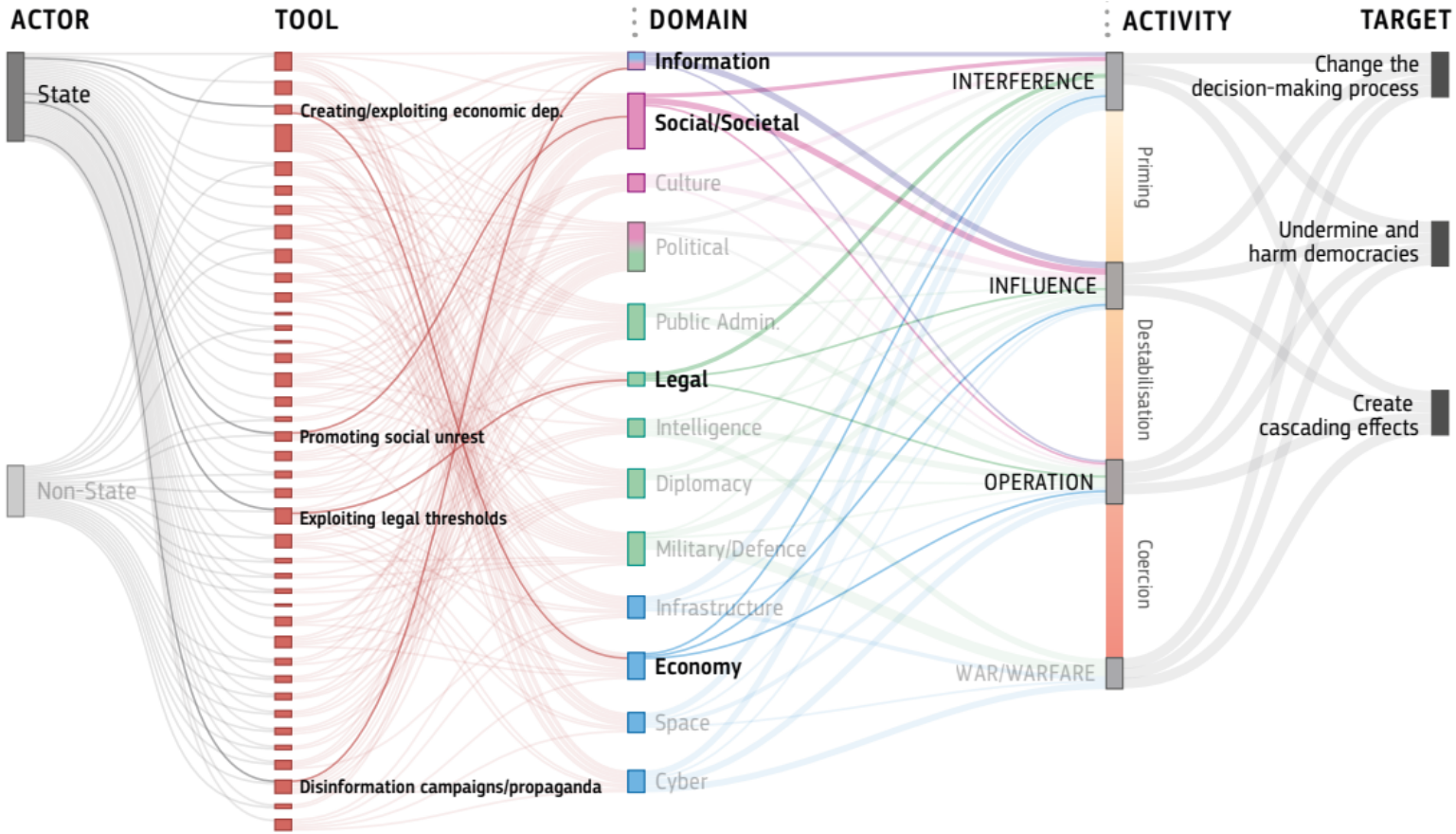
HYBRID THREATS CONCEPTUAL MODEL



HYBRID THREATS CONCEPTUAL MODEL



HYBRID THREATS CONCEPTUAL MODEL



Applying the CORE Model to the analysis of a case: The NORD STREAM CASE

DOMINOES

Compromised foundations: stability, reliability and availability, foresight

Following the Russian invasion of Ukraine in February 2022, Nord Stream 2 was stopped.
This case study analyses the situation up to the end of 2021 and hence does not directly take into account more recent events. It is not the intention of the case study to depict the influence of a war on an infrastructure project. However, the Russian invasion of Ukraine would also not influence the outcome of the case study. If anything, it supports the message that Nord Stream 2 led to a strategic dependency.

Analysed through hybrid threat lenses, the evolution of the Nord Stream 2 project reveals an adaptive targeting of the rule of law, reliability, and foresight foundations of the ecosystem. This case shows that the rule of law can be weakened by a structural confusion between public and private sectors from authoritarian regimes. The reliability of services provision would be dependent on geopolitical interests and political dynamics. Nord Stream 2 finally shows a failure of foresight and appreciation of the strategic implication of a decision perceived as non-geopolitical at the time it was made. It fell short of imagining the current context of heightened geostrategic tension between the EU and Russia, as well as failing to foresee the depth of divisions this would entail among the EU Member States in political terms.

Source: Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023)

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

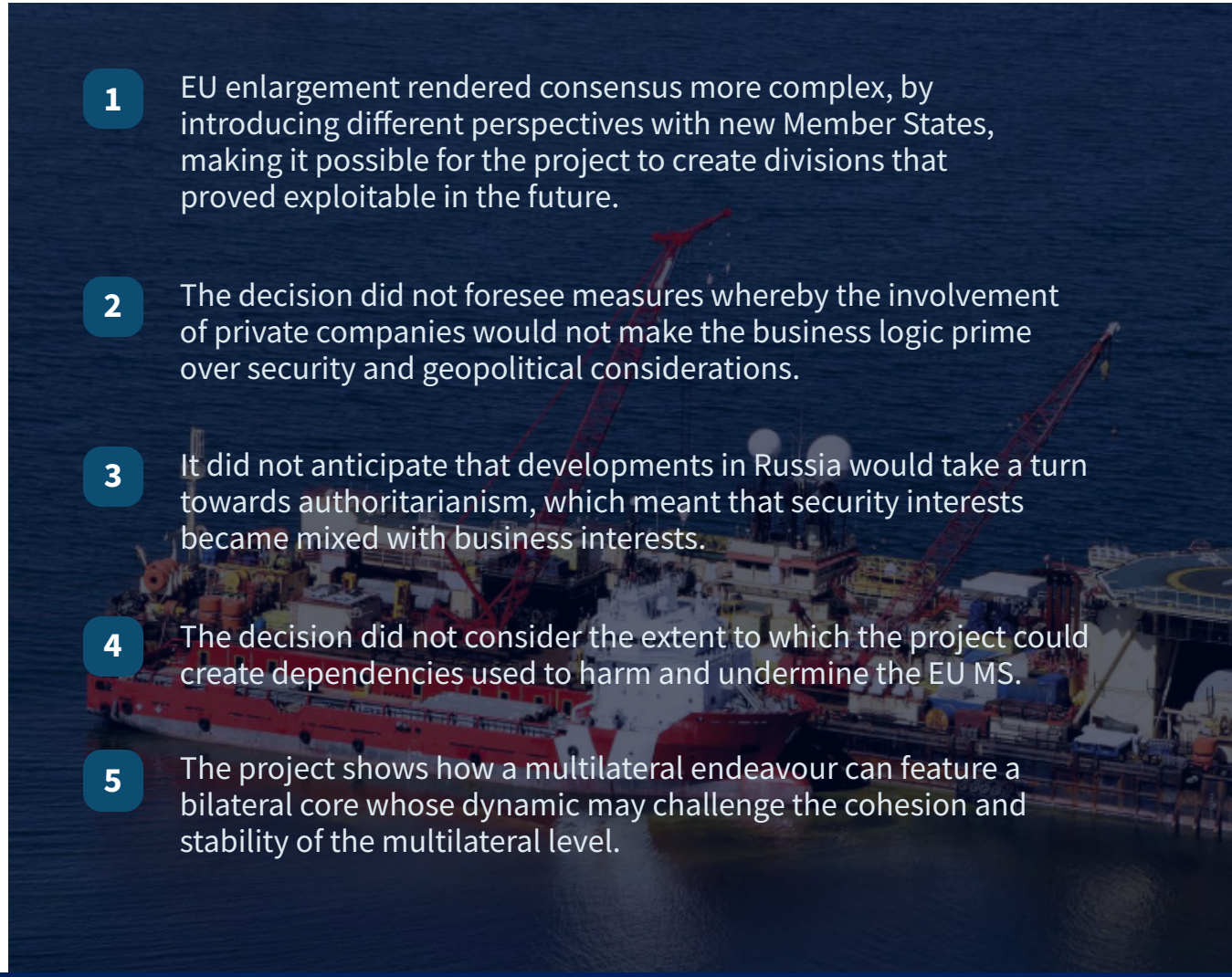
Applying the CORE Model to the analysis of a case: The NORD STREAM CASE

DOMINOES

The Nord Stream gas pipelines highlights the complexity and implications of decisions taken throughout the ecosystem. Although the EU has disclaimed the status of Nord Stream 2 as a common project, Nord Stream 1 took shape at the end of the 1990s as a pan-European project of common interest, with the aim of increasing the EU's energy security (Council of the European Union, 2006).

Within the framework of the EU-Russia energy dialogue, the overall objective of the energy partnership was to enhance the energy security of the European continent (European Commission, 2011)

The decision did not anticipate or consider a **series of connections and cascading effects** that impact the European security environment:



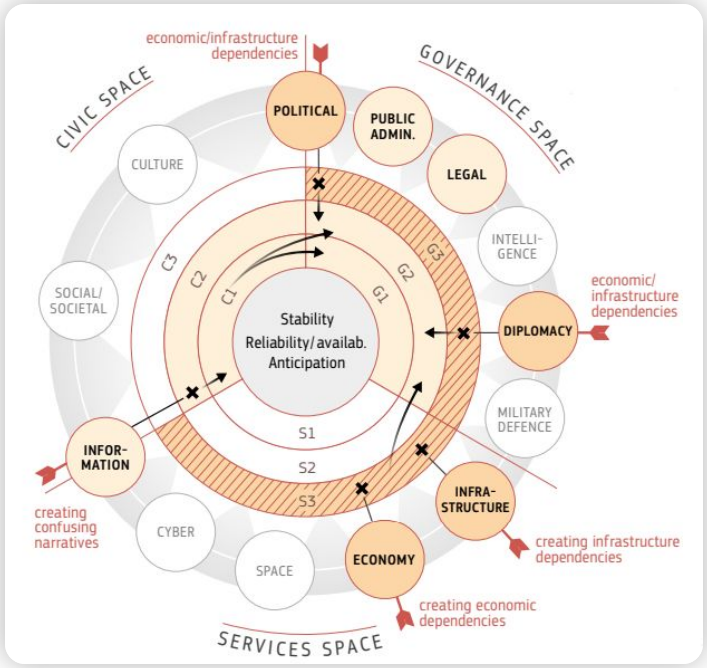
1. EU enlargement rendered consensus more complex, by introducing different perspectives with new Member States, making it possible for the project to create divisions that proved exploitable in the future.
2. The decision did not foresee measures whereby the involvement of private companies would not make the business logic prime over security and geopolitical considerations.
3. It did not anticipate that developments in Russia would take a turn towards authoritarianism, which meant that security interests became mixed with business interests.
4. The decision did not consider the extent to which the project could create dependencies used to harm and undermine the EU MS.
5. The project shows how a multilateral endeavour can feature a bilateral core whose dynamic may challenge the cohesion and stability of the multilateral level.

Source: Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023)

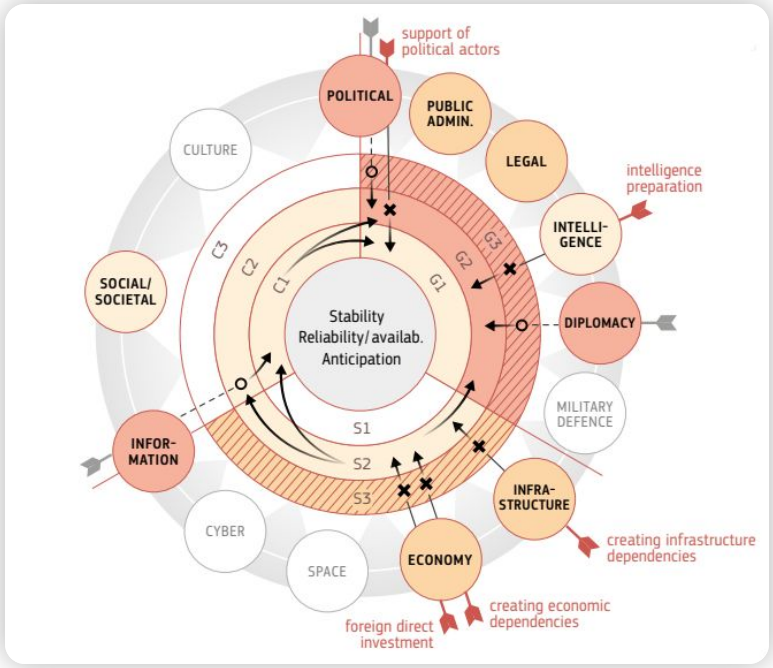
Applying the CORE Model to the analysis of a case:
The NORD STREAM CASE

DOMINOES

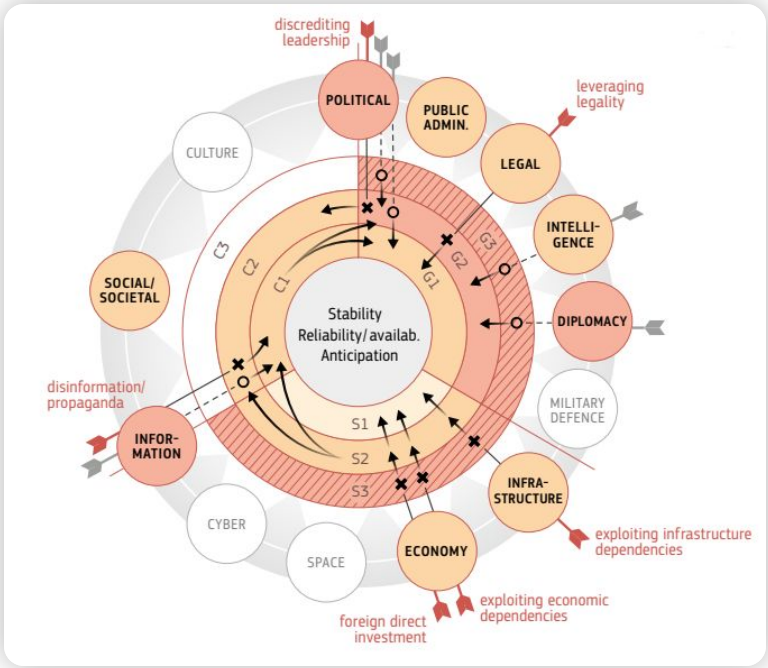
Russian hybrid threat activities within the EU (mainly Germany) develop over years into a gateway for interference/influence



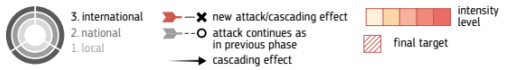
2005-2006



2014-2016



2021



Source: Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023)

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

Legend

3. international
2. national
1. local

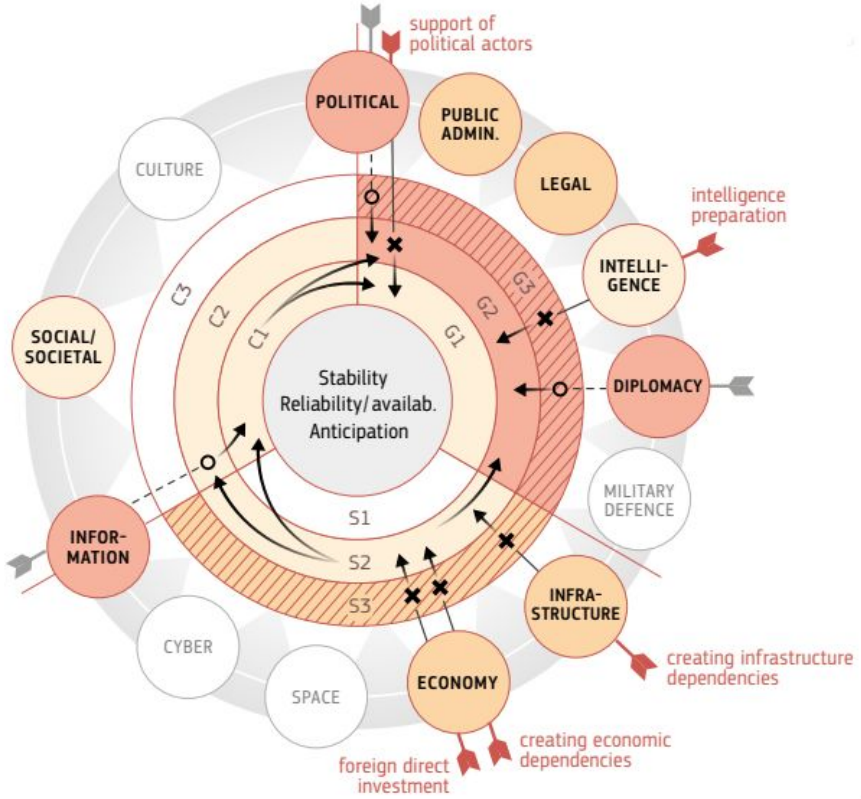
new attack/cascading effect

attack continues as in previous phase

cascading effect

intensity level

final target



2014-2016

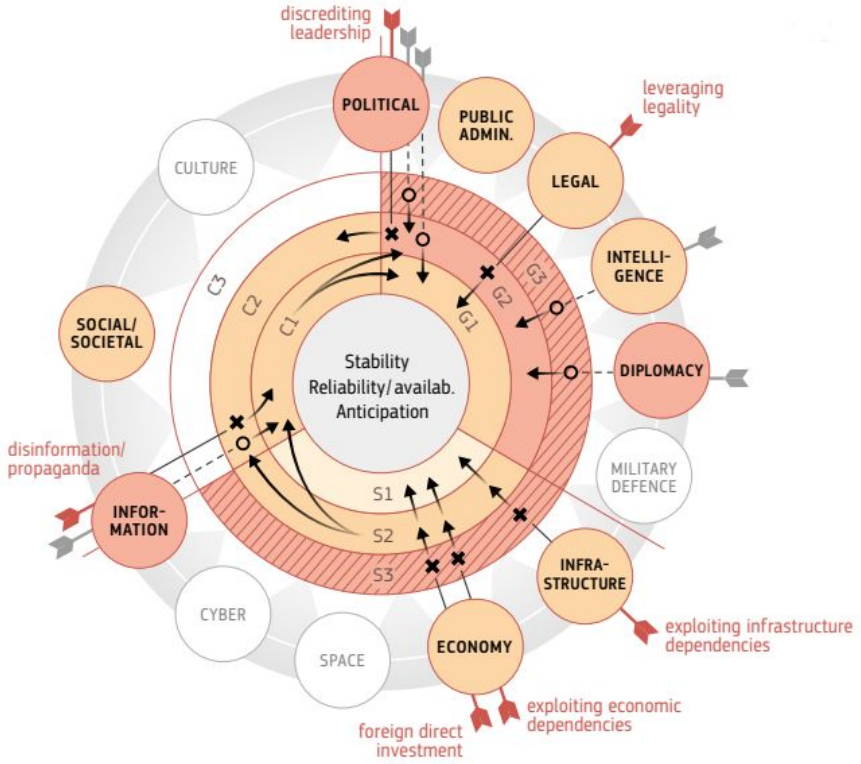
Interference

Creating infrastructure/economic dependencies
S3→S2 Some companies pulled out of the project, leading to stronger involvement of mainly Russian but also German companies.
S2→G2 Project became an object of national debate in Germany.

Foreign direct investors (Russian companies) targeted the energy supply sector in the EU, but especially in Germany.
S3→S2→C1/C2 Project business model affected (S2), sparking debates in societies of countries affected by the project (C1/C2).

Supporting political actors at state level that favour the project, especially in Germany.
G2→G1 Local German politicians are involved.

Intelligence preparation by Russia through intelligence operations around pipeline construction.
G3→G2 Concerns raised in national governments of the region.



2021

Interference

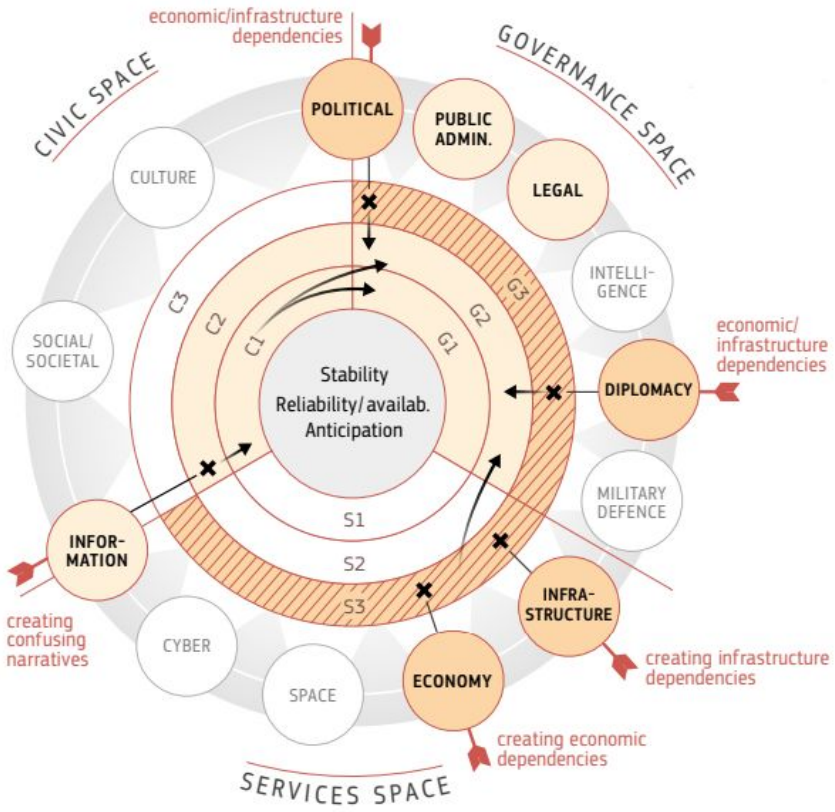
Exploiting infrastructure/economic dependencies: Dependencies created since 2005-2006 became exploitable by Russia.
S3→S2/S1 Regional German companies take on a more important role to ensure the completion of the project.

Foreign direct investment by Russia.
S3→S2/S1→C1/C2 Investments down to local level (S2/S1). New debates spark in societies of countries involved/affected (C1/C2).

Disinformation campaigns and propaganda were spread by Russia to convince decision-makers/public opinion in Germany to finish project.
C2→C1→G2/G1 Propaganda spread to local level (C1), and eventually affected public debate and election campaigns in Germany

Discrediting leadership/candidates during the 2021 federal election campaign in Germany to harm politicians opposing project.
G2→C2 Disinformation campaigns sparked debate in society.

Project managers leveraged legal rules, processes, institutions and arguments in Germany to complete the project threatened by sanctions.
G2→G1 This dubious approach led to political controversy at local level, where legal deceptions were applied.



2005-2006

Interference

Creating infrastructure/economic dependencies divided EU Member States politically/economically over the project. **G3/S3→G2** Uncertainty indirectly affected state level governance in various Member States, challenged public administration/legal domains at national level (G2).

Creating confusion or contradictory narratives: Spread of the narrative that Nord Stream is a non-political, purely economic project at the national level (C2). **C2→C1→G2/G1** The narrative encouraged support of local communities for the project in Germany (C1), and sparked discussions that influenced policy in state and local governance.

References

Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J. (2021) The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-56943-5, doi:10.2760/419776, JRC123305

Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue (2018). Addressing hybrid threats. Bromma: Swedish Defence University. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023) Hybrid Threats: A Comprehensive Resilience Ecosystem, EUR 31104 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-53292-7 (main), doi:10.2760/37899 (main), JRC129019.

NATO (2022). NATO 2022 Strategic Concept, adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Rubén Arcos (URJC)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Cognitive and information warfare

1.1.4

10.5281/zenodo.10063896

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.

Universidad Rey Juan Carlos

L-Università ta' Malta

NEW STRATEGY CENTER


DOMINOES
digital resilience to disinformation
Cognitive warfare
02:39

During the last years, in the face of alleged unacknowledged interference activities against Western democracies by authoritarian actors, the term information warfare has been used in the sense of weaponization of symbolic content (Arcos 2023). Digitalization and new technologies have created immense opportunities for adversaries to conduct hostile activities in the information environment and organize attacks against the cognitive domain through disinformation and information manipulations (Ibid).

The basic underlying idea behind the term cognitive warfare is that in our digital information age the battlefield is not always and solely kinetic, a physical violent clash between armies, but involves wagging war at the cognitive level (Underwood 2017). Speaking at the U.S. Department of Defense Intelligence Information System 2017 Worldwide Conference, Lt. Gen. Vincent R. Stewart remarked:

"Fifth-Generation Warfare. It will be cognitive warfare. In the 21st Century, warfare is about winning the information the decision space, either before or during a conflict. This is the deciding factor […] Robbing our enemies of the decision space and the ability to think and act […] A huge part of it is about information and how we collect, process, disseminate and protect that information and the systems that contain and deliver it" (Lt. Gen. Stewart https://youtu.be/Nm-lVjRjLD4).

General Stewart used the illegal annexation of Crimea by the Russian Federation, as an example:

"What they actually did, as they shape the information environment proclaiming that they would defend ethnic Russians, was to sent the unidentified unidentifiable little green men to seize key location and used information warfare and cyber-attacks to communication channels and media outlets. By the time they held a referendum on Crimea annexation, Ukraine's decision space was gone. Russia already had control of the peninsula all without far many shots. Sun Tzu said to fight and conquer in all our battles is not supreme excellence. Supreme excellence consists in breaking the enemy's resistance without fighting". (Ibid.)

Bernard Claverie and Francois Du Cluzel have pointed out that the cognitive domain is a domain of modern warfare, together with land, maritime, air, space and more recently with the cyber domain,

"It operates on a global stage since humankind as a whole is now digitally connected. It uses information technology and the tools, machines, networks, and systems that come with it. Its target is clear: our individual intelligences, to be considered both individually and as a group. Attacks are defined, structured, and organized to alter or mislead the thoughts of leaders and operators, of members of entire social or professional classes, of the men and women in an army, or on a larger scale, of an entire population in a given region, country or group of countries". (Claverie and Du Cluzel 2022: 2-1).

References

- **Arcos, Rubén (2023).** “Intelligence and awareness,” In Routledge Handbook of the Future of Warfare, edited by Artur Gruszczak and Sebastian Kaempf, S. (Routledge): 272-283. DOI: 10.4324/9781003299011-29

- **Claverie, Bernard and François Du Cluzel (2022).** “Cognitive Warfare”: The Advent of the Concept of “Cognitics” in the Field of Warfare,” In Cognitive Warfare: The Future of Cognitive Dominance, First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021, edited by B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel (Bordeaux: NATO-STO Collaboration Support Office): 2-1 – 2-8.

- **Stewart, Lt. Gen. Vincent R. (2017).** Remarks at the U.S. Department of Defense Intelligence Information System 2017 Worldwide Conference, https://youtu.be/Nm-lVjRjLD4

- **Underwood, Kimberly (2017)** “Cognitive Warfare Will Be Deciding Factor in Battle,” Signal, 15 August 2017. https://www.afcea.org/signal-media/cyber/cognitive-warfare-will-be-deciding-factor-battle

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Rubén Arcos (URJC)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

1.2

Legitimate and illegitimate use of information and persuasion in the information environment: disinformation, foreign information manipulation and interference (FIMI), cyber information operations

Aitana Radu | Univeristy of Malta

doi.org/10.5281/zenodo.10063918

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

DOMINOES
digital resilience to disinformation

Erasmus+

LEGITIMATE AND ILLEGITIMATE USE OF INFORMATION AND PERSUASION IN THE INFORMATION ENVIRONMENT

This module provides an introduction into the topic of disinformation and its use in contemporary societies. The module is divided into three subsections: Disinformation, Foreign Information Manipulation and Interference (FIMI) and Cyber information operations. The overall aim is to assist students in correctly identifying and distinguishing between forms of disinformation, FIMI and cyber information operations, as well as providing them with a basic knowledge of existing tools available to counter them.

UNIT OBJECTIVES

- Differentiate between disinformation, misinformation and mal-information.
- Identify the markers of fake news.
- Demonstrate the application of debunking and prebunking strategies in different contexts.
- Distinguish foreign information manipulation interference from cyber intelligence operations.
- List some of the mechanisms and/or tools available to counter disinformation and FIMI

Disinformation: definition & typology

Disinformation - verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public.

Disinformation includes:

- Fake news
- Hoaxes
- Lies
- Half-truths
- Artificially inflated engagement based on automated accounts, trolls, bots, and/or fake profiles.

DOMINOES
digital resilience to disinformation

Typology of information disorder

Disinformation

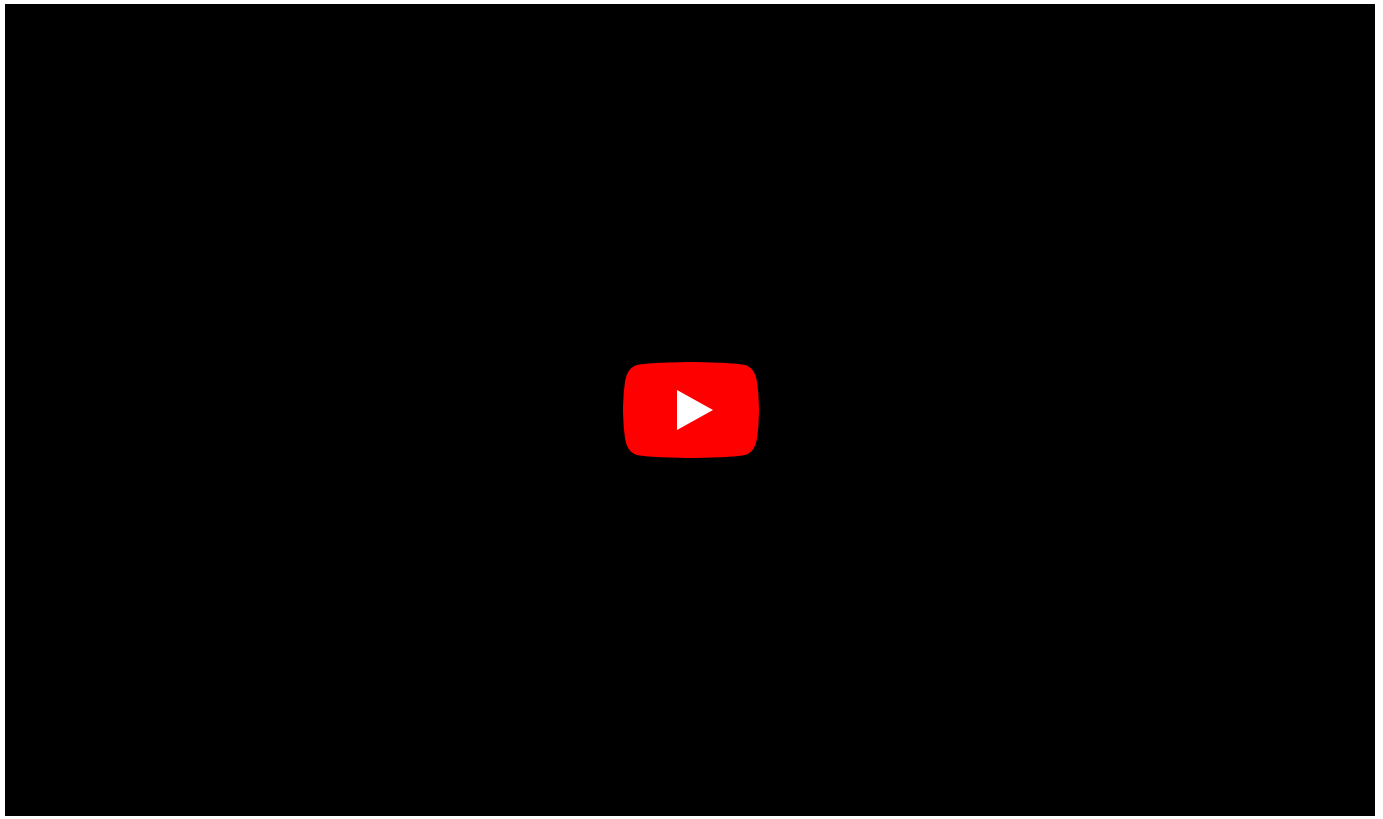
Misinformation

Malinformation

Types of disinformation & misinformation:

- Manipulated content
- Fabricated content
- Impostor content
- Misleading content (misleading use of information, such as presenting opinion as fact)
- False context of connection (factually accurate content that is shared with false contextual information)
  Satire and parody (humorous but false stories presented as being true).

Malinformation is information that is based on reality but is used to inflict harm on a person, organisation or country.



Disinformation is information that is false, and the person who is disseminating it knows it is false. “It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors”.

Misinformation is information that is false, but the person who is disseminating it believes that it is true

DOMINOES
digital resilience to disinformation

Fake news: definition and typology

Fake news is **false** or **misleading information** presented as real news.

Characteristics of fake news:

- can take the appearance of real news;
- deliberately fabricated to deceive and fool readers or to become viral on the Internet

Warning signs that help us spot fake news:

- the source: fake news come from websites that use clickbait titles or stories;
- the language: poor grammar;
- the format: words all in CAPS.
- the effect: great emotional appeal.

Fabricated journalism

Fabricated journalism: news stories that are completely made up (including fabricated quotes and sources, etc.).

Clickbait

Clickbait is a story, often sensational or featuring a sensational headline, geared toward getting “clicks” (to generate ad revenue)

newseumed.org

Sponsored content

Sponsored content is a story that is made to appear as independent journalism when in fact it is public relations or advertising;

edu.gcfglobal

DOMINOES
digital resilience to disinformation

Addressing fake news

Step 1- Asking the right questions

Step 2 – Move away from your comfort zone

- Break out of your information bubble
- Use different search engines
- Seek news from a variety of sources

Step 3 – Take your time

- Give breaking news time to develop
- Analyse information critically
- Question language, social conventions, and taboos being used to define issues and problems;
- Be aware that fake news exist;
- Try to verify information from other sources (e.g. factchecking websites/tools).

Filter Bubbles & Confirmation Bias

Filter Bubbles & Confirmation Bias

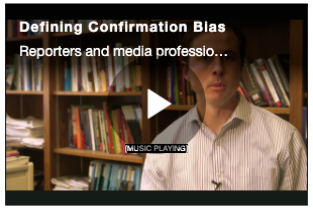
Filter Bubbles

Online services like Google, Instagram, and TikTok use computer programming algorithms to determine what information to deliver to you. Your "filter bubble" (a term coined by internet activist Eli Pariser) refers to the idea that this automated personalization, though helpful in some ways, can isolate you from other information. Sometimes referred to as an "echo chamber," the filter bubble created by your online activity can limit your exposure to different points of view and weaken your ability to avoid fake news and bias.

In this now-famous TED Talk, Pariser discusses the effects of algorithms and warns us about the dangers of online filter bubbles.

Confirmation Bias

What makes it so easy to believe fake news? As explained in the video *Defining Confirmation Bias*, people have a tendency "to accept information unquestioningly when it reinforces some existing belief or attitude," even when presented with contradicting proof.



According to *Psychology Today*, "confirmation bias occurs from the direct influence of desire on beliefs. When people would like a certain idea/concept to be true, they end up believing it to be true. ... We pick out those bits of data that make us feel good because they confirm our prejudices. Thus, we may become prisoners of our assumptions."

In this blog post on confirmation bias, author David McRaney reminds us that "there's always someone out there willing to sell eyeballs to advertisers by offering a

Bubbles & Bias: What Can We Do?

You can never get rid of all of your biases, but you can actively seek out other points of view. You can't get rid of your filter bubble either, but you can take steps to manipulate it. Here are some suggestions:

- AllSides
  is a website that presents news articles from the left, center, and right of each issue.
- Blue Feed, Red Feed
  by *The Wall Street Journal* presents side-by-side liberal and conservative Facebook posts on selected topics (but warns that posts are not edited or verified).
- DuckDuckGo
  is an internet search engine that pledges not to track your searches or save any data about you. The less data collected about your online behavior, the less chance of your filter bubble affecting your search results. Other privacy-focused search engines include Qwant, StartPage, and Swisscows.
- EscapeYourBubble
  is a Chrome extension that sends curated articles from across the aisle to your email or Facebook feed.
- How To Pop Your Filter Bubble

Source: Miami Dade College

Currency: The timeliness of the information.

- When was the information published or posted?
- Has the information been revised or updated?
- Does your topic require current information, or will older sources work as well?
- Are the links functional?

Relevance: The importance of the information for your needs.

- Does the information relate to your topic or answer your question?
- Who is the intended audience?
- Is the information at an appropriate level (i.e. not too elementary or advanced for your needs)?
- Have you looked at a variety of sources before determining this is one you will use?
- Would you be comfortable citing this source in your research paper?

Authority: The source of the information.

- Who is the author/publisher/source/sponsor?
- What are the author's credentials or organizational affiliations?
- Is the author qualified to write on the topic?
- Is there contact information, such as a publisher or email address?
- Does the URL reveal anything about the author or source?
- examples: .com .edu .gov .org .net

Accuracy: The reliability, truthfulness and correctness of the content.

- Where does the information come from?
- Is the information supported by evidence?
- Has the information been reviewed or refereed?
- Can you verify any of the information in another source or from personal knowledge?
- Does the language or tone seem unbiased and free of emotion?
- Are there spelling, grammar or typographical errors?

Purpose: The reason the information exists.

- What is the purpose of the information? Is it to inform, teach, sell, entertain or persuade?
- Do the authors/sponsors make their intentions or purpose clear?
- Is the information fact, opinion or propaganda?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional or personal biases?

Currency: The timeliness of the information.

- When was the information published or posted?
- Has the information been revised or updated?
- Does your topic require current information, or will older sources work as well?
- Are the links functional?

Relevance: The importance of the information for your needs.

- Does the informati on relate to your topic or answer your question?
- Who is the intended audience?
- Is the information at an appropriate level (i.e. not too elementary or advanced for your needs)?
- Have you looked at a variety of sources before determining this is one you will use?
- Would you be comfortable citing this source in your research paper?

Authority: The source of the information.

- Who is the author/publisher/source/sponsor?
- What are the author's credentials or organizational affiliations?
- Is the author qualified to write on the topic?
- Is there contact information, such as a publisher or email address?
- Does the URL reveal anything about the author or source?
- examples: .com .edu .gov .org .net

Accuracy: The reliability, truthfulness and correctness of the content.

- Where does the information come from?
- Is the information supported by evidence?
- Has the information been reviewed or refereed?
- Can you verify any of the information in another source or from personal knowledge?
- Does the language or tone seem unbiased and free of emotion?
- Are there spelling, grammar or typographical errors?

Purpose: The reason the information exists.

- What is the purpose of the information? Is it to inform, teach, sell, entertain or persuade?
- Do the authors/sponsors make their intentions or purpose clear?
- Is the information fact, opinion or propaganda?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional or personal biases?

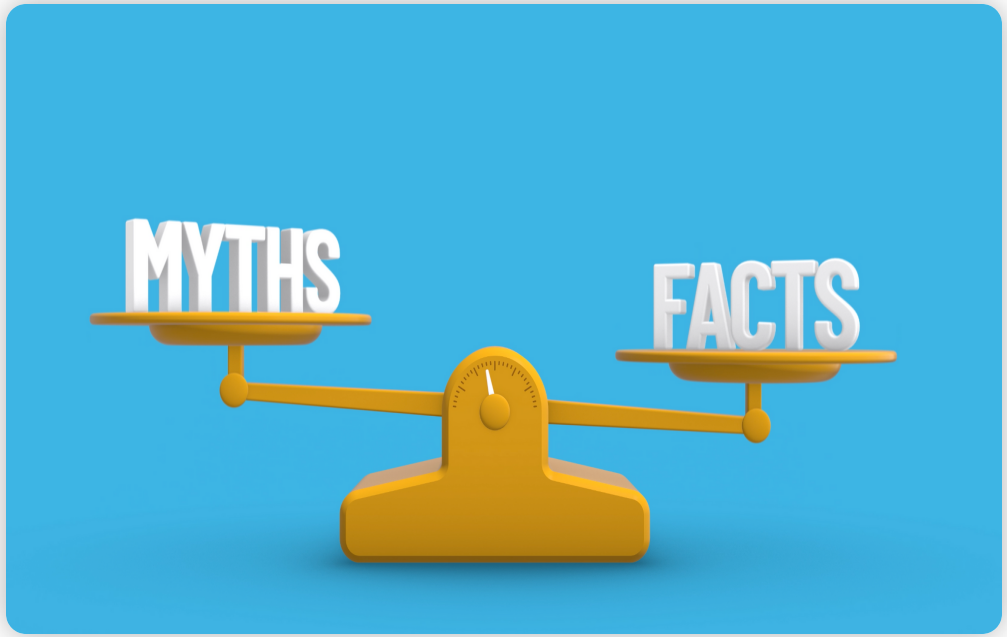
Additional Readings/References:

UNESCO (2018), Journalism, fake news & disinformation: handbook for journalism education and training

Debunking & pre-bunking

What is debunking?

What is pre-bunking?



Discussion

Debunking

- Occurs after false information has appeared;
- Aim is to correct false information and to prevent others from believing what is verifiably false information;
- Employ fact-checking strategies.

Pre-bunking

- A process where people are warned in advance that they are about to be the target of false information;
- Provide individuals with factual and some in-depth information on a particular subject beforehand
- Tell people in advance what kinds of disinformation they can expect.

Firstdraftnews.org

Pre-bunking & debunking strategies

Prebunking

- Warn people early on that conspiracy theories exist
- **Encourage rational thinking**, questioning and fact-checking
- Alert people about the **arguments behind the most common conspiracy theories** and the key traits of conspiratorial thinking.

Debunking

- **Focus on the facts** you want to communicate, not the myth you want to debunk;
- **Choose your target** – the author, source or logic behind the conspiracy theory;
- State clearly that the information is wrong, before quoting a conspiracy theory;
- Provide a fact-based alternative explanation;
- Use **visual aids** to back your argument (if available).

DOMINOES
digital resilience to disinformation

FIMI: definition and tactics

Foreign Information Manipulation and Interference (FIMI):

- mostly non-illegal pattern of behaviour
- threatens or has the potential to negatively impact values procedures and political processes
- manipulative activity
- intentional
- coordinated
- perpetrators are both state and non-state actors.

FIM Tactics

FIMI Tactics

Dismiss: to push back against criticism, deny allegations and denigrate the source;

Distort: to change the framing and twist and change the narrative;

Distract: to turn attention to a different actor or narrative or to shift the blame;

Dismay: to threaten and scare off opponents

Divide: to create conflict and widen divisions within or between communities and groups

EU Disinfo Lab, FIMI: Towards a European redefinition of foreign interference

FIMI techniques

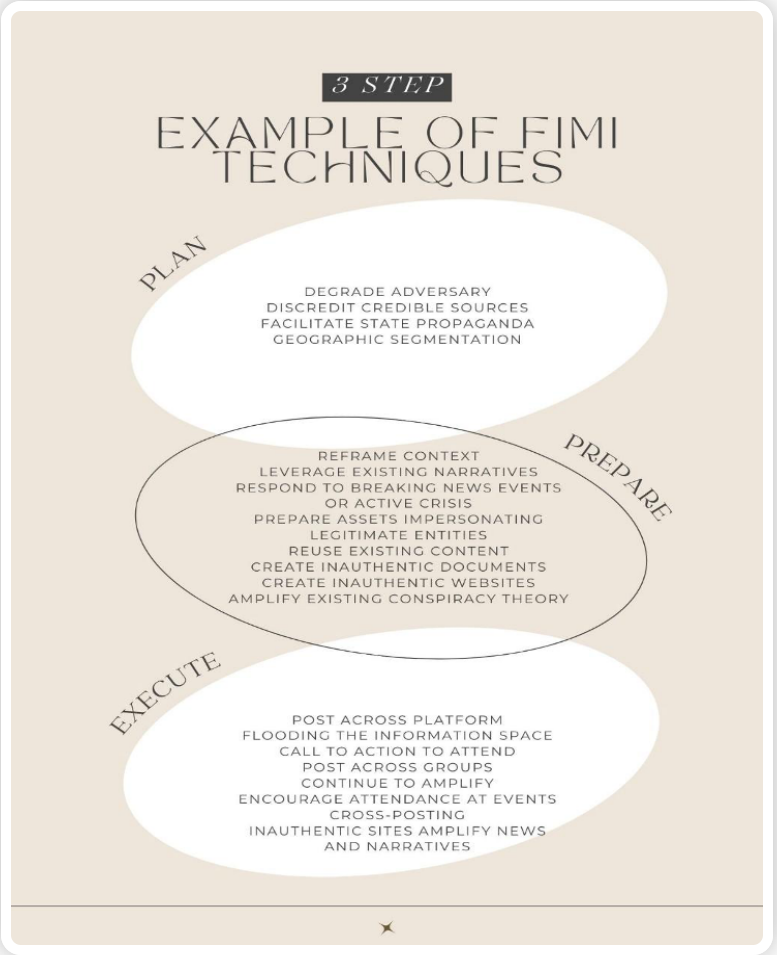
FIMI techniques:

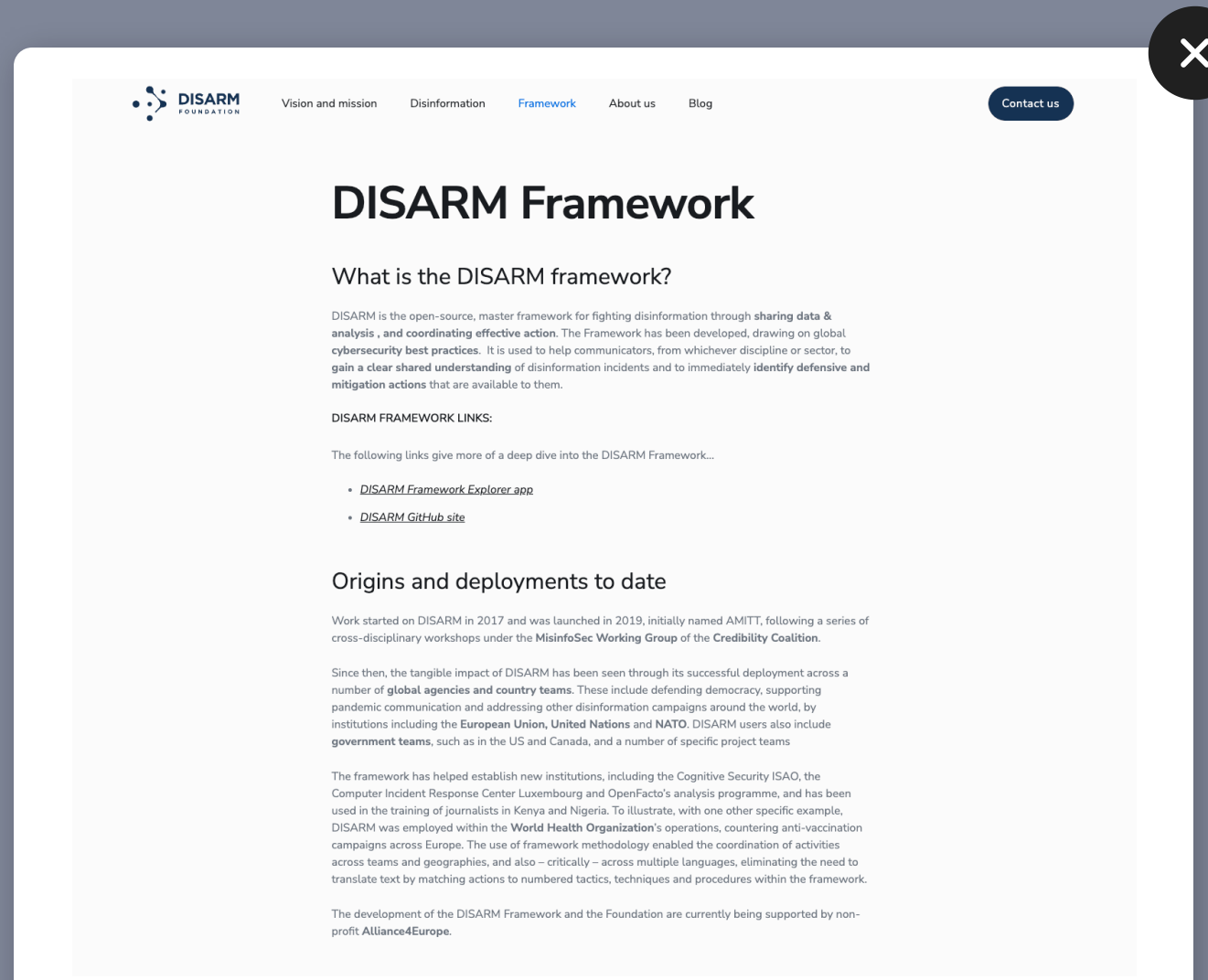
- Sorted by stage of the operation
  - i.e., plan, preparation, and execution

DISARM Framework:

- A collection of techniques
- Gain a shared understanding of disinformation incidents
- Provides a set of possible counter-actions to every hostile act, which are divided into the four typical phases of an attach:

1 Plan **2 Prepare** **3 Execute** **4 Assess**





Source: Disarm Foundation

DOMINOES
digital resilience to disinformation

Erasmus+

FIMI characteristics

Reacting to FIMI incidents

Six categories of countermeasures

- **Statement of refutal:** the targeted entity releases a statement refuting the claims of the incident
- **Debunking**: the claims of the incident are debunked and/or fact-checked
- **Content deleted:** the content is taken down in response to the incident
- **Content confined:** the content is limited in response to the incident
- **Channel limited**: the channel is limited in response to the incident
- **Channel suspended:** the channel is limited or suspended in response to the incident

The Kill-Chain Perspective

- Denying a threat actor, the completion of one step in the process would ‘kill’ the attack.

Characteristics of the Kill-Chain Perspective

- Each step requires different approaches to detection, analysis and response
- Objective analysis of the behaviour and TTPs, employed by threat actors
- Systematic development and assessment of disruptive responses, considering the potential negative side effects of each one

ABCDE framework

The ABCDE framework developed by **James Pamment** proposes to differentiate FIMI incidents in terms of actors, behabiours, content, degree and effect:

- **ACTOR**
  What kinds of actors are involved? This question can help establish, for example, whether the case involves a foreign state actor.
- **BEHAVIOUR**
  What activities are exhibited? This inquiry can help establish, for instance, evidence of coordination and intent.
- **CONTENT**
  What kinds of content are being created and distributed? This line of questioning can help establish, for example, whether the information being deployed is deceptive
- **DEGREE**
  What is the distribution of the content? Which audiences were targeted and reached?
- **EFFECT**
  What is the overall impact of the case and whom does it affect? This question can help establish the actual harms and severity of the case.

Disarm framework

The DISARM framework divides the lifecycle of an incident in four phases:

1. **Planning phase** – threat actors envision and design the desired outcome of the operation;
2. **Preparation phase** – threat actors lay the foundations to execute the plan;
3. **Executing phase** – the activities are carried out via previously established assets;
4. **Assessment phase** – the effect of the incident is assessed.

Characteristics of the DISARM framework

- **It not only defines the kill chain required to conduct FIMI incidents, but also defines tactics, techniques and procedures, which describe how the corresponding link can be accomplished;**
- **It employs a STIX (Structured Threat Information eXpression) based template for disinformation incidents;**

Name	Description
Title	Descriptive title
Summary	The TL/DR about this incident
Actor	Who was the source of the incident – threat actor identification/attribution
Timeframe	How long did the incident last
Date	Rough date this incident started
Presumed goals	What was the threat actor seeking to achieve
Method	Techniques used
Counters	Actions taken against this incident
Related incidents	Other incidents related/similar
References	Links to sources employed to complete this form

Additional Readings/References:

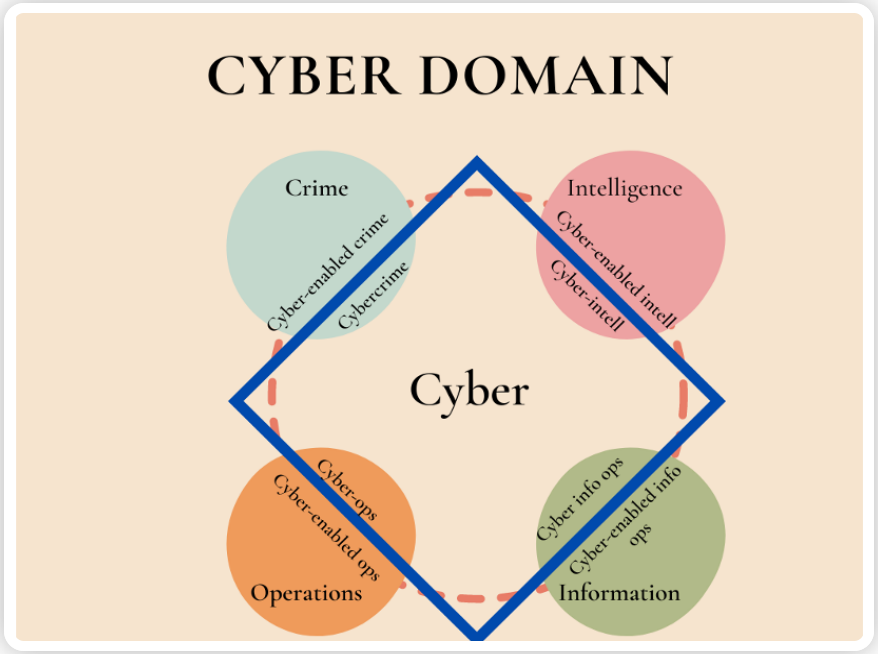
https://www.lamoncloa.gob.es/documents/constitucion_inglescorregido.pdf

Source: Disarm Foundation

Cyber information operations

Cyber information operations are:

- Content-based cyber operations
- Act undertaken clandestinely or under false pretences by a State or non-State actor
- Harnesses information in the cyber domain to influence political sentiment in a foreign State
- Falls below the threshold required to constitute a prohibited use of force and occurs outside the context of an armed conflict.



Examples of cyber information operations:

a. **Disinformation operations**: involve the spread of verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public;

b. **Malinformation operations**: which involve threatening, abusive, discriminatory, harassing or disruptive behaviour that aims to cause harm to a person, organisation or State

Additional Readi

https://www.lamc

Source: Disarm Foundation

Examples of cyber information operations:

a. **Disinformation operations**: involve the spread of verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public;

b. **Malinformation operations**: which involve threatening, abusive, discriminatory, harassing or disruptive behaviour that aims to cause harm to a person, organisation or State

DOMINOES
digital resilience to disinformation

Cybersecurity and FIMI

Role of cybersecurity in FIMI/disinformation:

- **Establishing attribution** – often established with the assistance of cybersecurity analysis
- **Defining indicator**s – specific cyber-attack techniques can act as an indicator of a FIMI/disinformation event
- **Formulating a response** – established cybersecurity practices can help the counter of FIMI/disinformation

Distinction between information/cyber incidents and FIMI/disinformation operations

- Single incidents vs. Operations
- Difficulties in establishing the duration of events
- Different analytical frameworks
- Difficulties in identifying the target
- Critical vs. non-critical targets

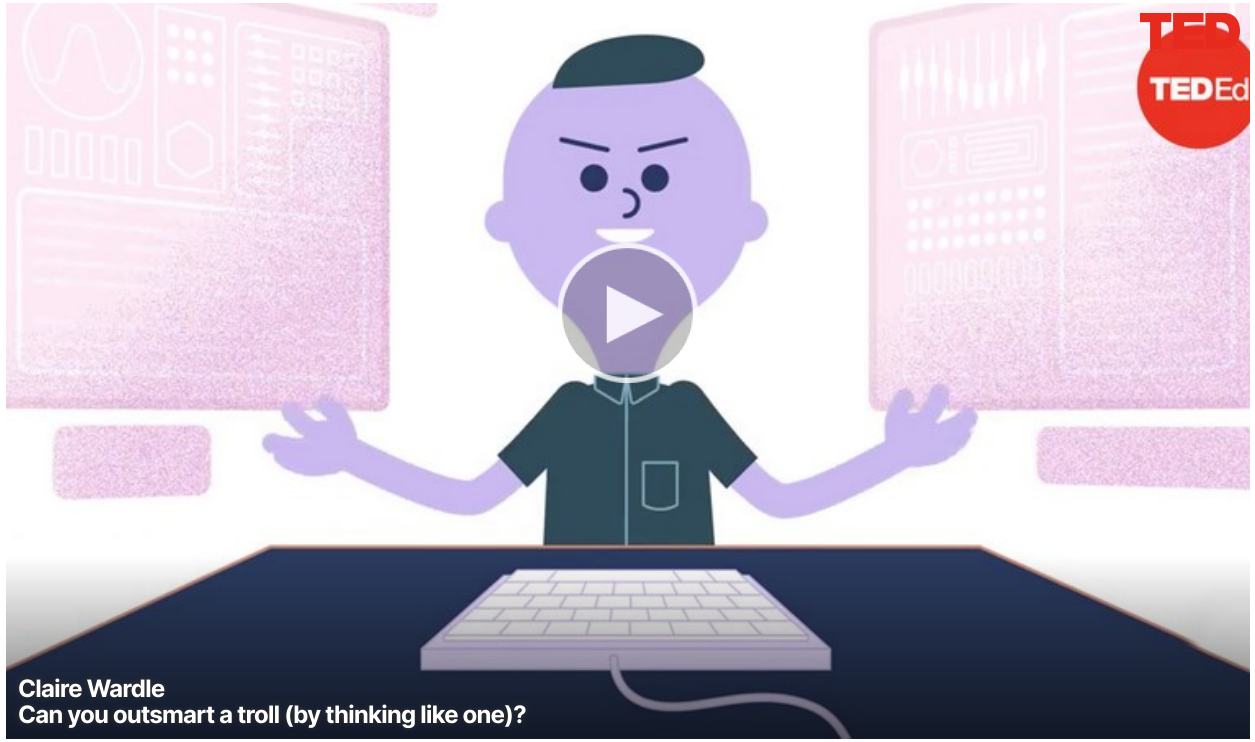
DOMINOES
digital resilience to disinformation

Democratic vulnerabilities

Democracies are targets of cyber information operations.

Features most affected:

- **Public participation** – e.g. election interference
- **Pluralism** – e.g. exploitation of social fissures and foment polarisation
- **Enlightened understanding**



Exercise:

Your town is holding a mayoral election and the stakes have never been higher. You suspect one of the candidates will begin pushing false information to swing the election. In the video, Claire Wardle explores the tactics of disinformation campaigns. Use that information & everything you have learned so far to create a 1 page strategy for a counter-campaign employing both debunking and pre-bunking strategies.

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Aitana Radu (UoM)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Disinformation, Fake news, Debunking and pre-bunking

1.2.1

doi.org/10.5281/zenodo.10063936

Co-funded by the European Union

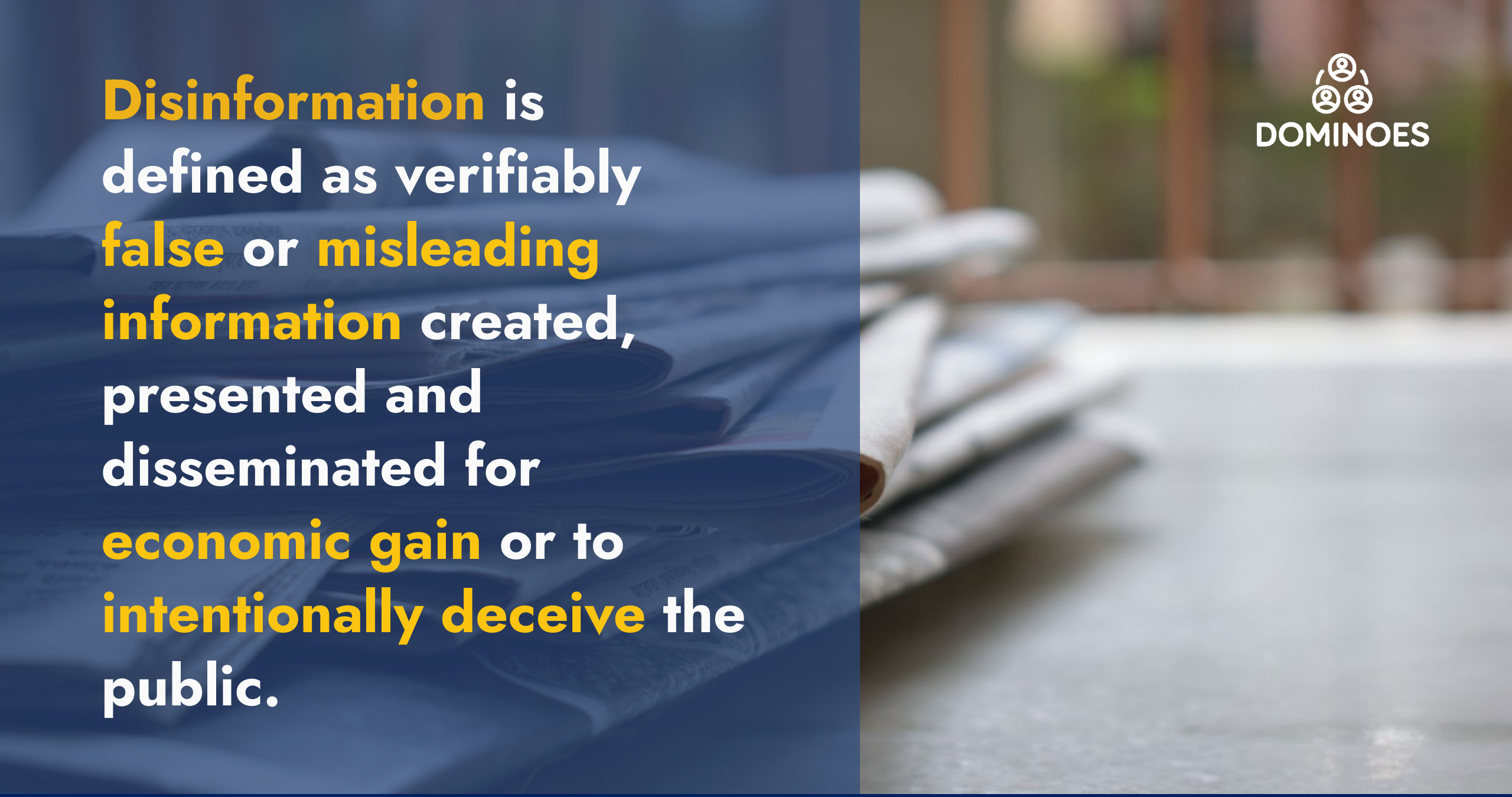
2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.

Universidad Rey Juan Carlos

L-Università ta' Malta

NEW STRATEGY CENTER



Disinformation is defined as verifiably **false** or **misleading information** created, presented and disseminated for **economic gain** or to **intentionally deceive** the public.

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Disinformation

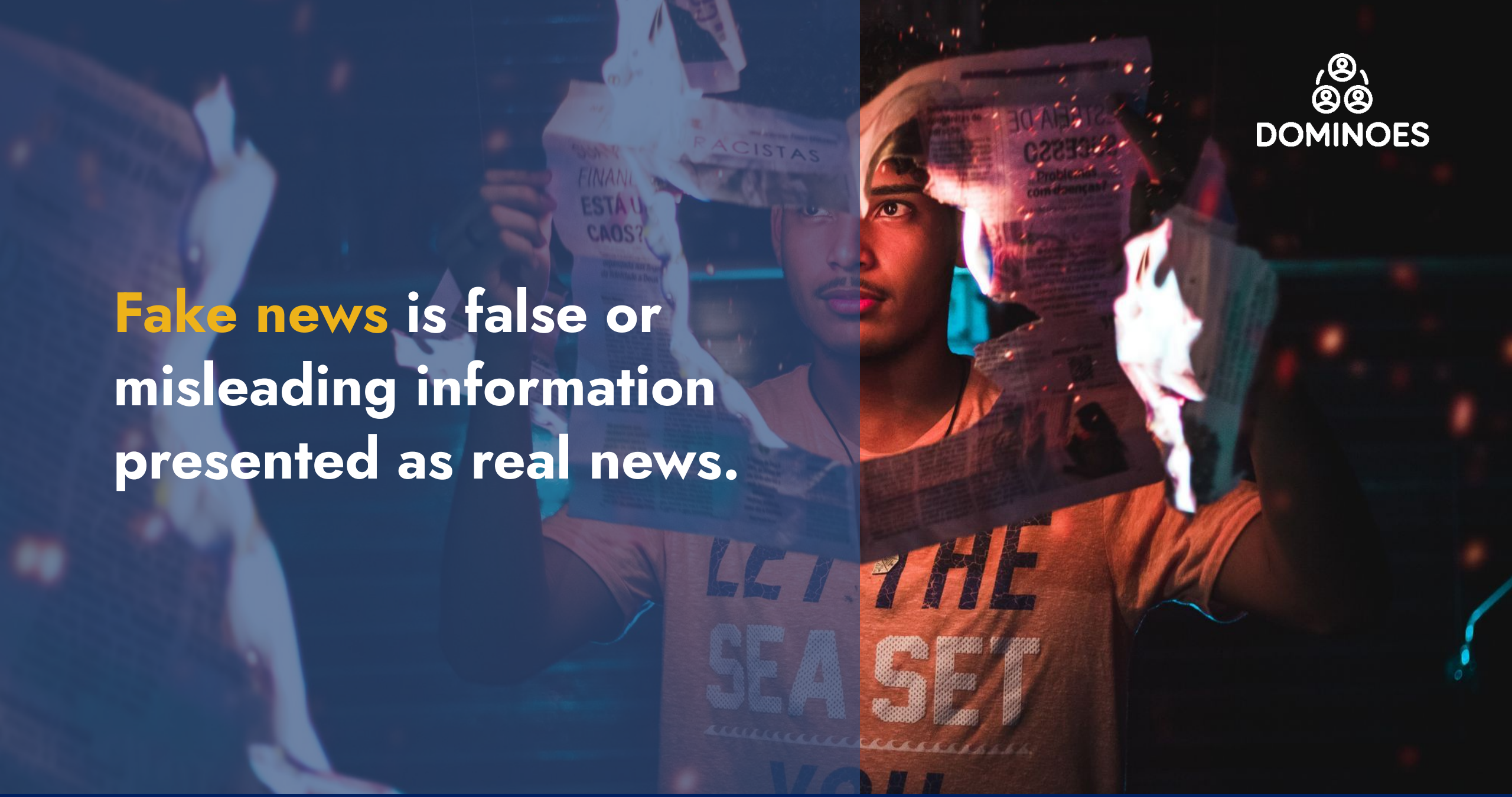
DOMINOES

1. Disinformation
2. Forms of information disorder
3. Types of disinformation & misinformation

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

Disinformation

DOMINOES



DOMINOES

Fake news is false or misleading information presented as real news.

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Fake news

DOMINOES

1 Characteristics

2 Warning signs

3 Types

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

What can we do?

DOMINOES

1. Look for...
2. Break out of your information bubble
3. Give breaking news time to develop
4. Analyse information critically

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Fake news


1.2.1_Disinformation, Fake news, Debunking and pre-bunking_2
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:12
vimeo

Debunking happens after the fact, so **after false information has appeared.** The aim is to **correct false information** and to **prevent others from believing what is verifiably false information**. Those reading or seeing the information 'see through' what is being presented as fact and/or truth. **Fact-checking strategies** can be used to debunk misinformation and disinformation.

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Pre-bunking is a **process where people are warned in advance that they are about to be the target of false information.** It builds on the reasoning that 'an ounce of prevention is worth a pound of cure'. Pre-bunking can be achieved by **providing individuals with factual and some in-depth information on a particular subject** beforehand, and then introducing the existing disinformation about the same subject. They can also be **told in advance what kinds of disinformation they can expect.**

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

What to do?

DOMINOES

1. Prebunking
2. Debunking

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

Debunking, pre-bunking

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158

Author of contents: **Aitana Radu (UoM)**
Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Foreign information manipulation and interference (FIMI)

1.2.2

doi.org/10.5281/zenodo.10063946

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.

Universidad Rey Juan Carlos

L-Università ta' Malta

NEW STRATEGY CENTER

DOMINOES

Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

FIMI Tactics, Techniques and Procedures

DOMINOES

1 Tactics

2 Techniques

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DOMINOES


1.2.2_Foreign information manipulation and interference_video 1
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:19
vimeo

Characteristics of FIMI

DOMINOES

1. State or non-state actors
2. State-controlled media
3. Domestication of influence operations
4. Use of impersonation techniques
5. FIMI is multilingual

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Characteristics of FIMI

DOMINOES

6 Diplomatic channels

7 Two main FIMI actors

8 Russian modus operandi

9 Chinese modus operandi

10 Instances of collusion between FIMI actors

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Characteristics of FIMI

DOMINOES

11 FIMI content is mostly image and video based

12 Gender differences

13 Different types of targets

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DOMINOES


1.2.2_Foreign information manipulation and interference_video 2
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:15
vimeo

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

Courses of Action to FIMI incidents. Categories of countermeasures:

DOMINOES

1. Statement of refutal
2. Debunking
3. Content deleted
4. Content confined
5. Channel limited
6. Channel suspended

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

The **Kill Chain approach** to FIMI, based on cybersecurity best practices, focuses on understanding a threat actor's behaviour as a process ranging from planning, preparing and executing. **Denying a threat actor, the completion of one step in the process would 'kill' the attack**, hence its name 'kill-chain'.

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Characteristics of the Kill-Chain Perspective:

DOMINOES

- It starts with an **objective analysis of the behaviour and TTPs, employed by threat actors**, in order to understand the vulnerabilities which are exploited

- It requires a **systematic development and assessment of disruptive responses**, considering the potential negative side effects of each one.

DOMINOES


1.2.2_Foreign information manipulation and interference _video 3
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:15
vimeo

Framework for FIMI Analysis

DOMINOES

1. Strategic Monitoring
2. Prioritisation and Triage
3. Incident Analysis and Evidence Collection
4. Knowledge Pooling and Sharing
5. Situation Awareness

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

DOMINOES

Two main frameworks

1. ABCDE framework
2. DISARM framework

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DOMINOES


1.2.2_Foreign information manipulation and interference _video 4
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:21
vimeo

DISARM is an open-source, master framework for fighting disinformation through sharing data and analysis. The Framework has been developed, drawing on global cybersecurity best practices. It is used to help communicators, from whichever discipline or sector, to gain a clear shared understanding of disinformation incidents and to immediately identify defensive and mitigation actions that are available to them.

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DISARM framework

DOMINOES

The DISARM framework divides the lifecycle of an incident in four phases:

1. Planning phase
2. Preparation phase
3. Executing phase
4. Assessment phase

In each stage of the process, threat actors can select between multiple TTPs to construct the attack. Attackers are likely to reuse certain TTPs combinations that have a good cost-benefit ratio, which can assist in attribution.

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Characteristics of the DISARM framework

DOMINOES

- It not only defines the kill chain required to conduct FIMI incidents, but also defines tactics, techniques and procedures, which describe how the corresponding link can be accomplished;

- It employs a STIX (Structured Threat Information eXpression) based template for disinformation incidents;

Example of STIX (Structured Threat Information eXpression)

Name	Description
Title	Descriptive title
Summary	The TL/DR about this incident
Actor	Who was the source of the incident – threat actor identification/attribution
Timeframe	How long did the incident last
Date	Rough date this incident started
Presumed goals	What was the threat actor seeking to achieve
Method	Techniques used
Counters	Actions taken against this incident
Related incidents	Other incidents related/similar
References	Links to sources employed to complete this form

DOMINOES

DOMINOES


1.2.2_Foreign information manipulation and interference_video 5
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:07
vimeo

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Aitana Radu (UoM)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Cyber information operations

1.2.4

doi.org/10.5281/zenodo.10063956

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.

Universidad Rey Juan Carlos

L-Università ta' Malta

NEW STRATEGY CENTER

Cyber information operations are content-based cyber operations, encompassing any act undertaken clandestinely or under false pretences by a State or non-State actor whose conduct is attributable to a State under international law that harnesses information in the cyber domain to **influence political sentiment** in a foreign State, which **falls below the threshold required to constitute a prohibited** use of **force** and occurs outside the context of an armed conflict.

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Examples of cyber information operations:

DOMINOES

1. Disinformation operations
2. Malinformation operations

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158

A growing concern in national and international security is the systematic use of disinformation within mass influence operations as an element of **hybrid warfare.** Hybrid warfare relates to the **blended use of conventional and nonconventional methods**, such as cyber warfare, disinformation, and propaganda, as part of a co-ordinated multi-domain warfighting approach to disrupt and disable an opponent's actions.The **targets of information operations** are the **perceptions of an adversary** which reside in the cognitive dimension of the information ecosystem.

DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

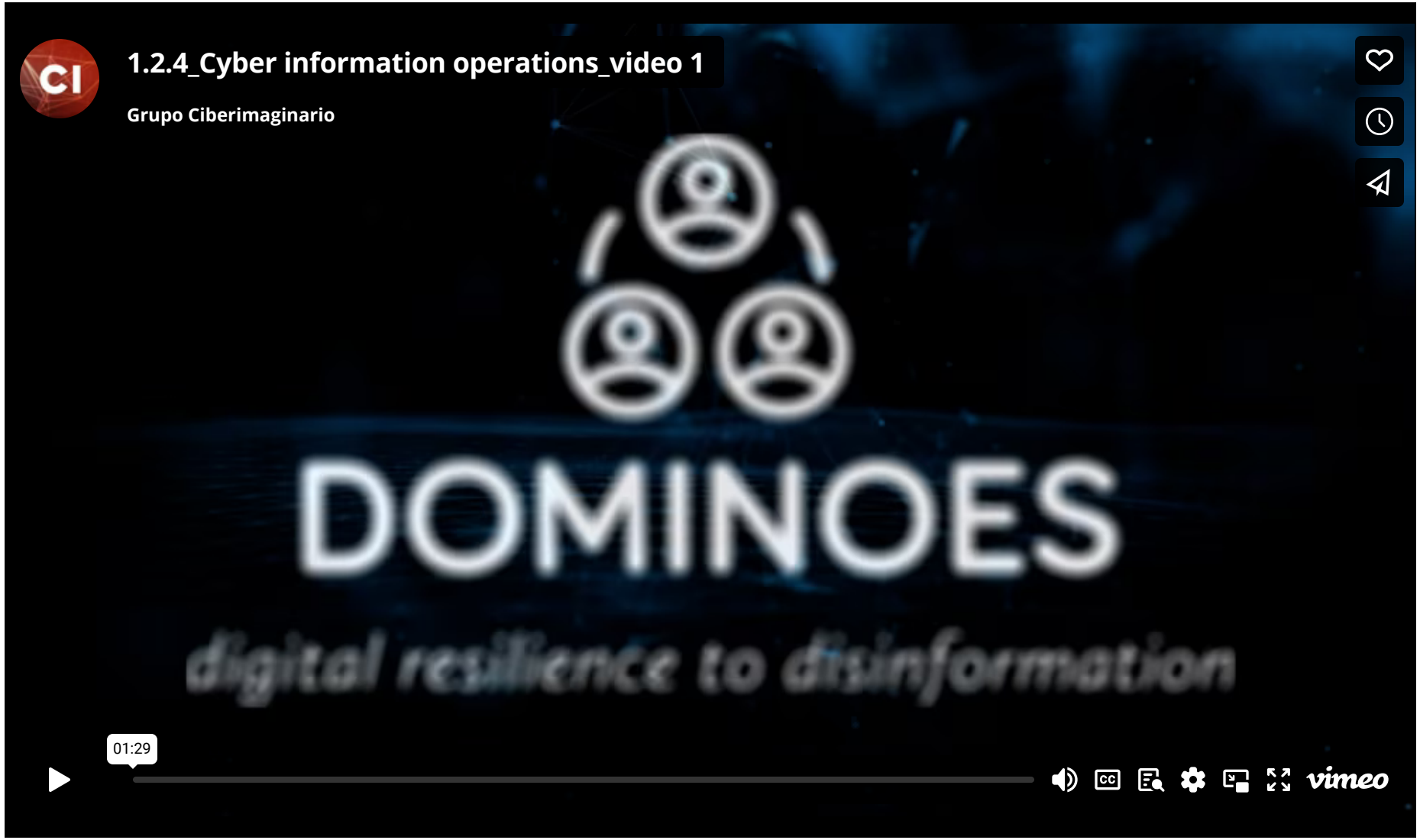
Role of cybersecurity in FIMI/disinformation

DOMINOES

1. Establishing attribution
2. Malinformation operations
3. Formulating a response

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

DOMINOES


1.2.4_Cyber information operations_video 1
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:29
vimeo

Distinction between information/cyber incidents and FIMI/disinformation operations

DOMINOES

1. Single incidents vs. Operations
2. Difficulties in establishing the duration of events
3. Different analytical frameworks
4. Difficulties in identifying the target
5. Critical vs. non-critical targets

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

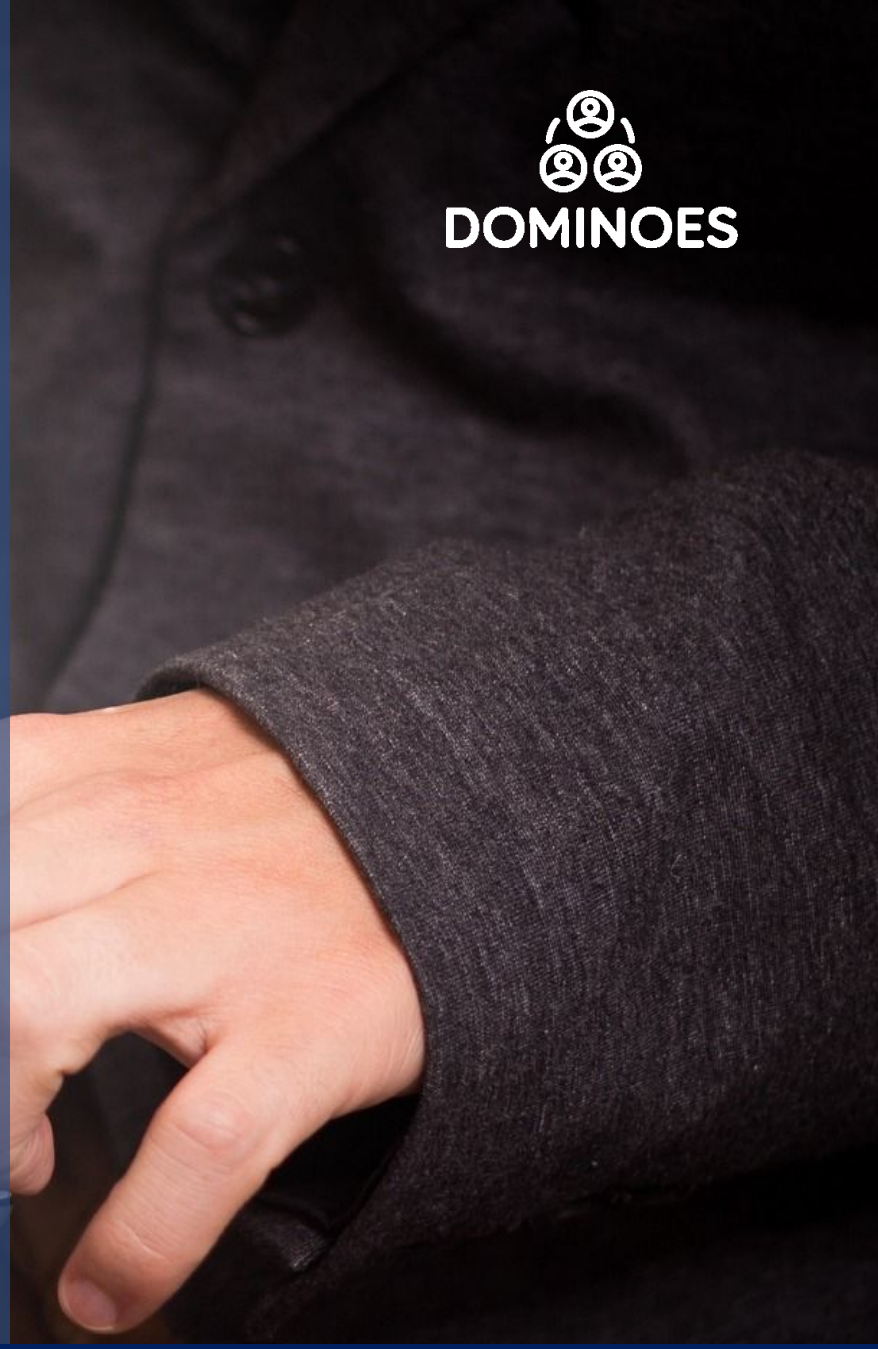

1.2.4_Cyber information operations_video2
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:36
vimeo

DOMINOES

Social bots and their use in cyber information operations

DOMINOES

Social bots are online personas or entities run or managed by technical means that are automated to act like real people using social media accounts.



Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Use of social bots for malicious purposes:

DOMINOES

1

2

3

4

5

6

How to track social bots:

DOMINOES

- Using social media trackers;
- Primitive social bots can be detected with automated tools based on their behaviour profiles: their ratio of posting messages and response times.

Features of social bots:

DOMINOES

1. Scalability
2. Target content
3. Give the appearance of diversity
4. Mobilize citizens

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem


1.2.4_Cyber information operations_video 3
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
01:24
vimeo

DOMINOES

Role of cybersecurity in FIMI/disinformation

DOMINOES

- Democracies are targets of cyber information operations, especially as the freedoms they protect make them inherently vulnerable to such incidents. The functioning of liberal democracies relies on the free circulation of information: participation, pluralism and enlightened understanding – core values which are both substantively and ideologically threated by information operations.

1. Public participation
2. Pluralism
3. Enlightened understanding

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Aitana Radu (UoM)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

1.3

Case studies of conspiracy theories and hostile narratives by authoritarian state and non-state actors

Irena Chiru | ANIMV

doi.org/10.5281/zenodo.10063931

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

CASE STUDIES OF CONSPIRACY THEORIES AND HOSTILE NARRATIVES BY AUTHORITARIAN STATE AND NON-STATE ACTORS

Section 1.3. will illustrate the current challenge that disinformation raises by looking at two examples:

1. Conspiracy theories, and
2. Hostile narratives.

This section includes both theoretical content and real case studies selected for their relevancy and explanatory potential.

UNIT OBJECTIVES

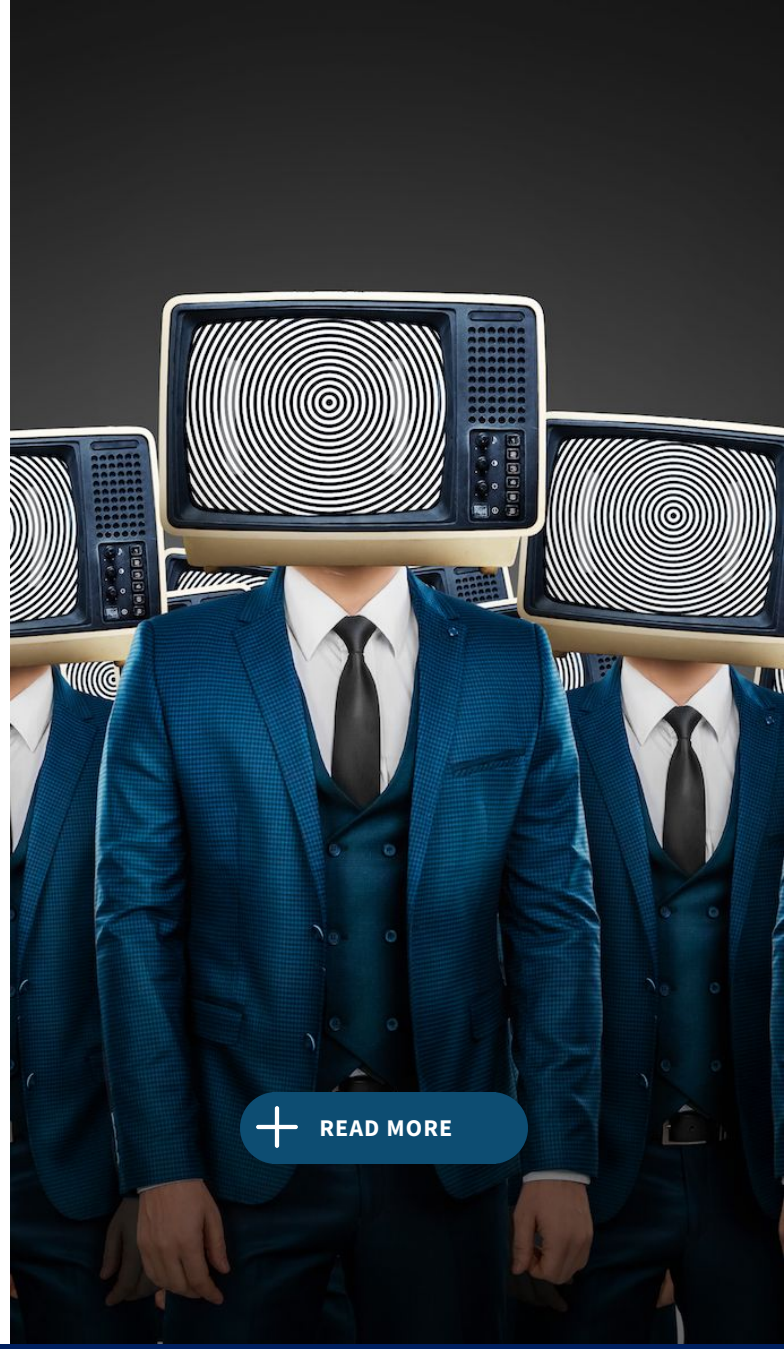
- To define and explain conspiracy theories and thus help students help students integrate and synthesize key ideas about conspiracy theories as speculative but highly circulated explanatory narratives.
- To illustrate the nature, structure and impact of conspiracy theories.
- To define and explain hostile narratives and thus help students help students integrate and synthesize key ideas about them as speculative but highly circulated explanatory narratives.
- To demonstrate the impact of hostile narratives by looking at manner in which they target feeling and emotions while using current circumstances-driven vulnerabilities (in this case the influx of refugees from Ukraine in Europe)

DOMINOES
digital resilience to disinformation

Understanding conspiracy theories

- Artificially inflated engagement based on automated accounts, trolls, bots, and/or fake profiles. explanatory causal-based, ideologically laden narratives which depict significant social events or crises as perpetrated by a group of powerful secret actors who solely follow their own nefarious interests, irrespective of the good of the masses.
- Always existed in societies, however, at present, they have gained momentum due to their easy spread and appeal in social media.
- They have begun to corrupt people's understanding of the world and their willingness to listen to experts and authorities in times of crisis and not only

- Threatening not only the further development of societies but also the very health and security of the communities they live in.



Understanding and countering the **negative effects that conspiracy theories have** on contemporary democratic societies means that first and foremost, it must become clearer what conspiracy theories are and how they can be distinguished from actual conspiracies that have and will continue to exist in society. Hence, what is a conspiracy theory? what are the characteristics of conspiracy theories? why are conspiracy theories attractive? and how do conspiracy theories affect the common understanding of events?

Conspiracy theories are explanatory causal-based, ideologically laden narratives which depict significant social events or crises as perpetrated by a group of powerful secret actors who solely follow their own nefarious interests, irrespective of the good of the masses. They have always existed in societies, however, at present, they have gained momentum due to their easy spread and appeal in social media. Moreover, they have begun to corrupt people's understanding of the world and their willingness to listen to experts and authorities in times of crisis and not only, thus threatening not only the further development of societies but also the very health and security of the communities they live in.

The works examining the determinants of belief in conspiracy theories identified as relevant several psychological and cognitive factors.

DOMINOES
digital resilience to disinformation

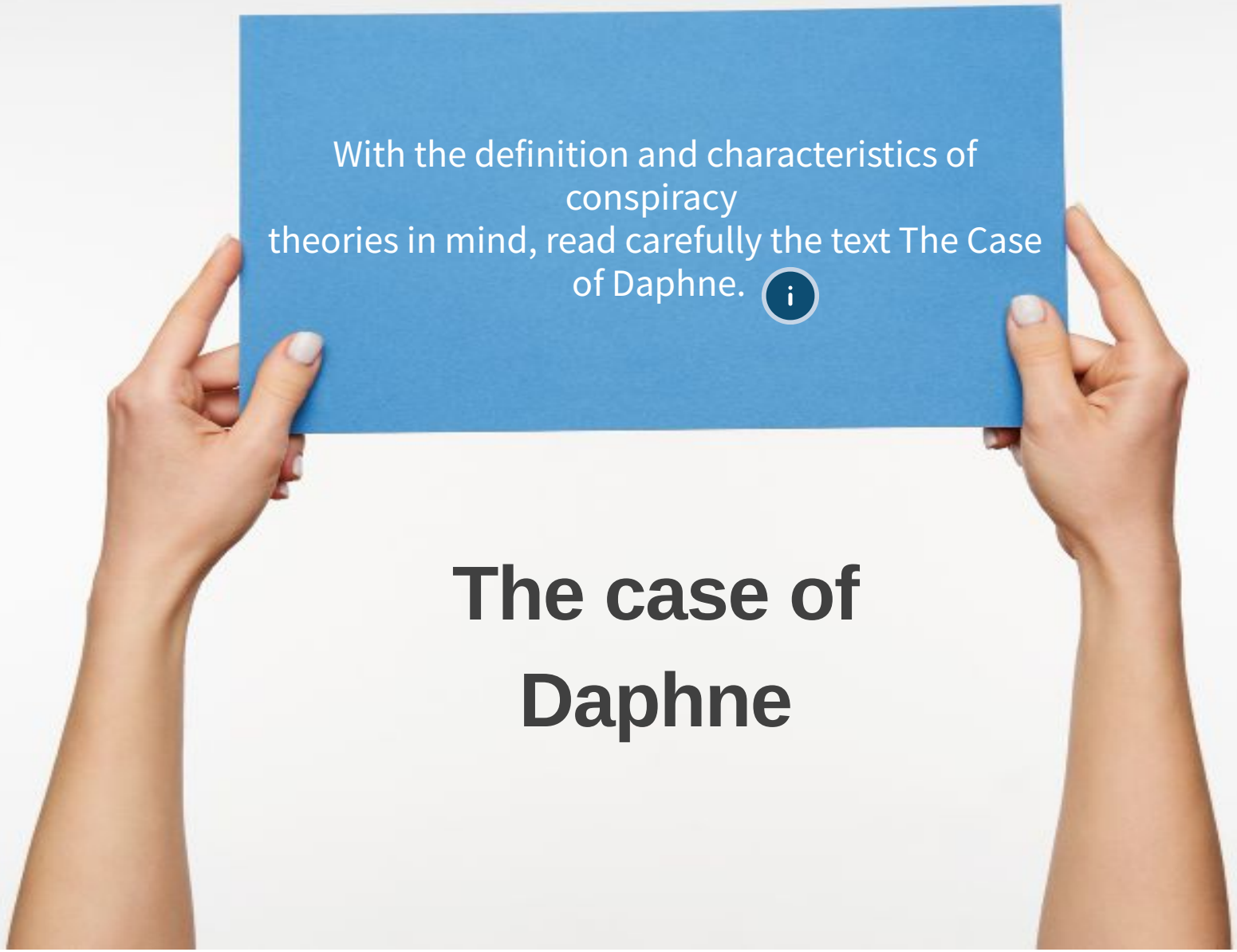
Characteristics of conspiracy theories

+ READ MORE

- **Speculative** - based on conjecture rather than knowledge, educated (or not so educated) guesswork rather than solid evidence
- **Contrarian** - they run counter to the official narrative or view, to the obvious, plausible and acceptable explanations of events
- **Premodern** - they attempt to impose order in a random, complex, uncontrollable world in which events, crises are seen to occur as a result of evil machinations not as a result of a conjunction of numerous factors
- **Amateurish**
- **Self-sealing and self-sustaining** which make them unfalsifiable
- Very **nuanced and complex** - they account for everything, for randomness and coincidence and it provide an all-encompassing explanation
- **Unknowable to and untraceable** by the larger public
- Form a **monological belief system** - each belief supports every other belief, and the more conspiracies a monological thinker believes, the more likely they are to believe new ones as well, regardless of their topic
- Purport that **people** are not merely kept in the dark, they are being actively **fooled by the authorities**

According to the existing literature, conspiracy theories share a set of common characteristics. Generally speaking, conspiracy theories :

- **Are speculative** - based on conjecture rather than knowledge, educated (or not so educated) guesswork rather than solid evidence
- **Are contrarian** - they run counter to the official narrative or view, to the obvious, plausible and acceptable explanations of events
- **Are premodern** - they attempt to impose order in a random, complex, uncontrollable world in which events, crises are seen to occur as a result of evil machinations not as a result of a conjunction of numerous factors
- **Are amateurish**
- **Are self-sealing and self-sustaining** which make them unfalsifiable
    - are very nuanced and complex - they account for everything, for randomness and coincidence and it provide an all-encompassing explanation
    - unknowable to and untraceable by the larger public
- Form a **monological belief system** - each belief supports every other belief, and the more conspiracies a monological thinker believes, the more likely they are to believe new ones as well, regardless of their topic
- Purport that people are not merely kept in the dark, they are being actively fooled by the **authorities**.



The case of Daphne

The case of Daphne

Now, with the definition and characteristics of conspiracy theories in mind, read carefully the text The Case of Daphne.

The case of Daphne [1/2]

Daphne Caruana Galizia was a very well-known Maltese reporter, editor, columnist and blogger. Her blog Running Commentary had a very high reach, comparable to the main media houses in Malta. Her continuous challenging of political power structures through her reporting on corruption, sleaze and crime, made her both liked and disliked by many. Throughout her career, Daphne Caruana Galizia received threats and was the target of several forms of harassment because of her journalism. **On 16 October 2017 Daphne was assassinated** by the triggering of an explosive device planted under her car seat outside her home in Bidnija, Malta. The investigation of her assassination further **exposed the corruption of the government** and institutions who were accused in a public inquiry of having created an atmosphere of impunity.

One such controversy is the conspiracy theory developed by Simon Mercieca, an Associate Professor at the University of Malta who employs his blog Simon Mercieca's FreePress to share a number of **fake news and conspiracy theories** on a wide variety of subjects, ranging from Maltese politics to COVID-19. According to him, Yorgen Fenech is innocent, while Daphne's assassination was organised by her husband (Peter Caruana Galizia) and her son (Matthew Caruana Galizia). According to his theory, the Caruana Galizia family is "hampering the investigation process and the court's operations so that the whole truth behind Daphne Caruana Galizia's murder will never be known. To achieve this scope, main witnesses of the prosecution, including Matthew Caruana Galizia are using the media and giving interviews to siphon issues to fit their agenda and condition the public.

A Maltese businessman, Yorgen Fenech was charged with having been the mastermind behind her assassination, but the trial is still ongoing. Three other people, Alfred and George Degiorgio and Vince Muscat were convicted of making, planting and detonating the car bomb that killed the journalist. In spite of the fact that the Police Commissioner has declared that all suspects in the case have been arrested and many of them have already been convicted, the case is still causing many controversies.

The case of Daphne [2/2]

Mercieca claims that Daphne's son, Matthew, decided to take the law into his hands and destroy potential key evidence, albeit there was never any official information to support this claim. **The key word in this theory is potential**. Mercieca's theory relies on conclusions which are drawn based on circumstantial evidence, offering an explanation that is different from the official media reports and from the evidence presented in court. This leads to the **second conspiracy theory characteristic** – it is contrarian. Mercieca capitalises on the fact that the Maltese public is still divided on the subject of Daphne's assassination, with some groups arguing that the investigation and prosecution have not been carried out in the most transparent and efficient manner. However, instead of aligning himself with those who sought justice for the journalist's assassination and her family, his conspiracy theory argues the opposite that while justice has not been served the victim has been the Maltese businessman accused of murdering Daphne Caruana Galizia, namely Yorgen Fenech.

He claims that Daphne's family have intentionally hindered the investigation and sought to gain money from the investigation, by putting the blame on a well-known Maltese businessman. Moreover, he argues that Daphne's family didn't put pressure on the authorities to bring Yorgen Fenech to justice, in the hope that as more time passes they will be able to build the case on false information and hide traces that could lead back to them.
This argument goes against official information and ignores existence evidence gathered in the case and presented during the criminal trial, including the testimonies of the people convicted for making, planting and detonating the car bomb that killed the journalist. Instead, the theory develops a scenario of demonization, whereby the real "malevolent forces" involved in the case are Daphne's family, who not only harmed Daphne but are now harming Yorgen Fenech and the Maltese society in general.

This conspiracy theory is built around self-sealing conclusions, built on information taken out of context, which makes it hard to refute. Moreover, the conspiracy theories are built one upon another, as in Mercieca uses the idea of "malevolent forces" seeking to discredit him (e.g. they would say that, wouldn't they?) as an argument against all criticism received in relation to the other ideas promoted. This can also be seen as an indicator that he does not have any other counter-arguments/evidence that he can bring in support of his theories.

DOMINOES
digital resilience to disinformation

Based on your reading of the Case of Dephne, answer the following questions:

Erasmus+

We can define conspiracy theories as being:

You can select more than one answer

- Narratives aiming to do harm
- Narratives about powerful secret actors secretly acting
- Narratives about the others
- Narratives which depict significant social events or crises

SEND

In this section, we learnt that conspiracy theories are speculative. This means that:

You can select more than one answer

- They are based on intriguing explanations
- They are based on a guess and not on information
- They are pure fictional
- They are not based on information

SEND

DOMINOES
digital resilience to disinformation

Based on your reading of the Case of Dephne, answer the following questions:

Erasmus+

Why does Mercieca's theory meet the characteristics of a conspiracy theory?

- Because it is speculative
- Because it is based on and promotes a simplistic view assigning intentionality to Daphne's family to harm the whole society
- Because it is contrarian
- Because it involves media representatives

SEND

DOMINOES
digital resilience to disinformation

Erasmus+

Understanding hostile narratives

READ MORE

As mentioned in the opening of this section, understanding and countering the negative effects of disinformation on contemporary democratic societies means that first and foremost, it must become clearer what forms and shape disinformation take. Similar to the discussion we had about conspiracy theories, in the following minutes, we will look at hostile narratives:

- What are hostile narratives?
- What are their characteristics?
- How do they relate on particular national vulnerabilities?
- What emotions do they engage?

DOMINOES
digital resilience to disinformation

How to identify hostile narratives?

- Are made of true and false information, while the narration of facts counts more than the facts themselves
- Link ardent topics such as migration to other existing insecurities, depicting it as a threat to three partly-overlapping areas:
  - Health (migrants as violent criminals, terrorists or carriers of disease), wealth (migrants as social benefits cheats or unfair competition for jobs)
  - Identity (migrants as a hostile invasion force, threatening to replace white, Christian Europeans and their traditions). For example, the narrative ‘The European Union is Bad, Russia’s Customs Union is What You Need’ widely used in Republic of Moldova apparently tackles with economics, but actually the arguments used are often based on ideological conservatism and used to create fear. In the same way, the narrative ‘Romania and NATO are a Threat to Peace’, raises people’s sense of insecurity.

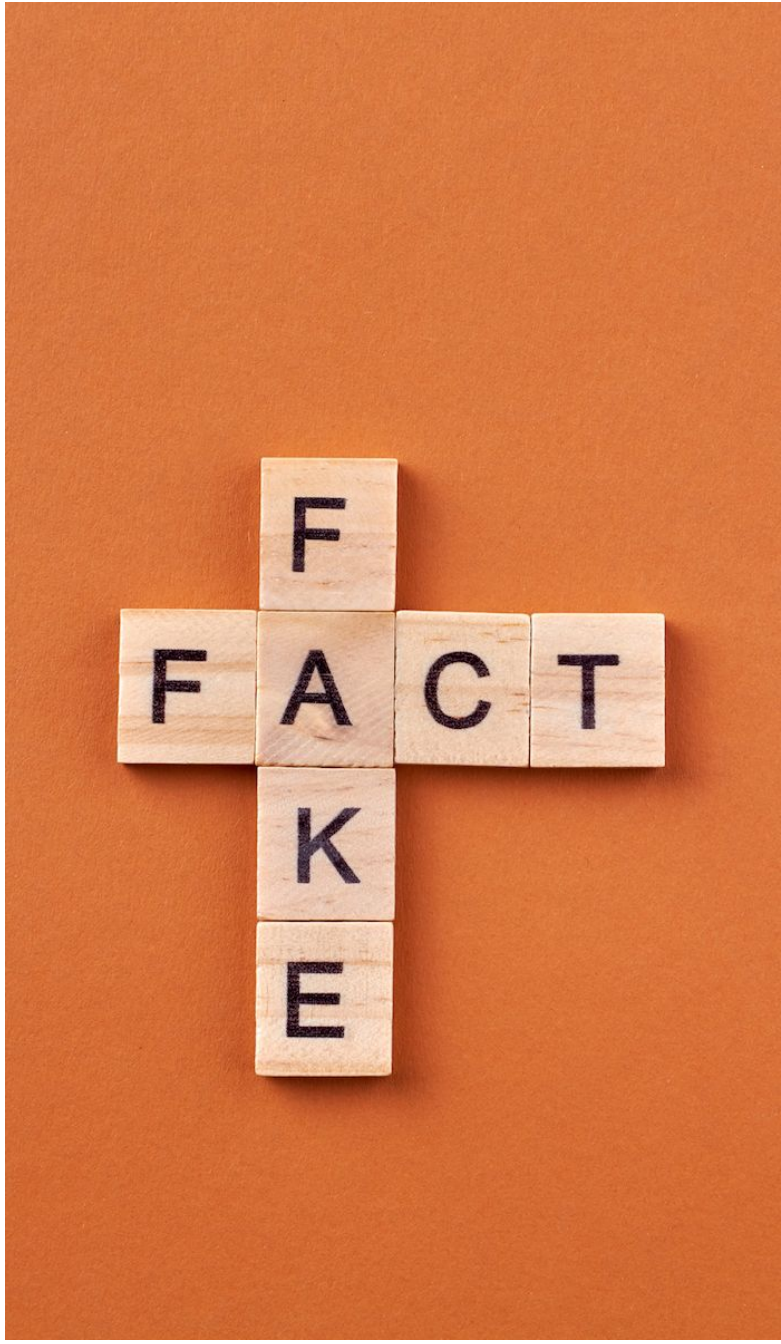
They are made of true and false information, while the narration of facts counts more than the facts themselves. Hostile narratives link ardent topics such as migration to other existing insecurities, depicting it as a threat to three partly-overlapping areas: **health** (migrants as violent criminals, terrorists or carriers of disease), wealth (migrants as social benefits cheats or unfair competition for jobs) and **identity** (migrants as a hostile invasion force, threatening to replace white, Christian Europeans and their traditions). For example, the narrative 'The European Union is Bad, Russia's Customs Union is What You Need' widely used in Republic of Moldova apparently tackles with economics, but actually the arguments used are often based on ideological conservatism and used to create fear. In the same way, the narrative 'Romania and NATO are a Threat to Peace', raises people's sense of insecurity.

Food for thought

Think about the impact of:

Mass media

Artificial inteligence



In some cases (Republic of Moldova), the effect is augmented by the mechanisms of the news landscape - where media control lies in the hands of pro-Kremlin politicians or oligarchs.

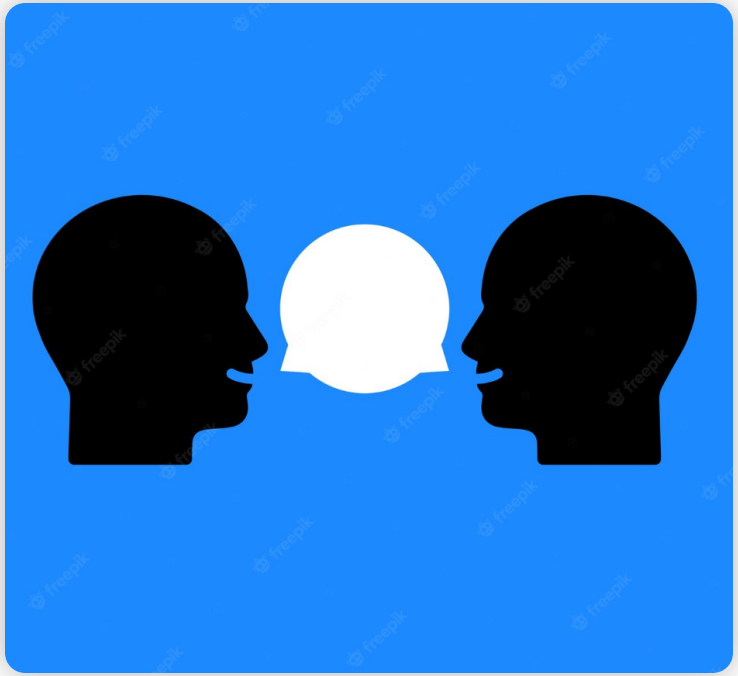
Or, based on shared interpretations of national sovereignty and self-determination, by the potential political gain of political parties expressing their commitment to conservative Christian values against ‘rampant Western decadence’ (Farber, 2014). Far-right, Euro-skeptic parties (e.g. the Hungarian Jobbik populist party, Communist Party of Portugal, The Communist Party of Greece, French “National Assembly”).

The role of AI in this matter is central.

Whether using Deep fakes, content dissemination through bots or chatbots, or selection of content according to its prediction of viralization, AI can play an ambivalent character, supporting the generation of content that serves hostile actors, while also having an essential role in combating disinformation and its effects, detecting content, as well as potentially malicious social media accounts.

Debate time

+ INFO



Q1 - The receptivity to hostile narratives depends on our capacity to be self-aware of our values and emotions. Which values, beliefs and emotions do you think make us more vulnerable in accepting and sharing hostile narratives?

A Manichean ideas of dualism - tending to look at things as having two sides that are opposed

B Anger and fear

C Rational self-defense and self-survival instincts

D Lack of trust in institutions

DOMINOES
digital resilience to disinformation

Erasmus+

Debate time

+ INFO

Q2 - In many European countries, the ”demonisation” of the Ukrainian migrants has been instrumentalized by political parties and widely disseminated in social media. How do you think this should be tackled?

- **A** By developing a EU migration diplomacy addressing the structural factors facilitating the instrumentalisation of migration by third countries
- **B** By investing in raising public awareness of this political instrumentalization
- **C** By exposing the vested interests behind such an instrumentalization
- **D** By widely disseminating such demonisation narratives

DOMINOES
digital resilience to disinformation

Erasmus+

Debate time

+ INFO

Q3 - One of the narratives broadly used to gain public support for the intervention in Ukraine is based on the assumption that ”The Ukrainian government is not self-sufficient and is just following the instructions of Western leaders”. Which arguments can we use in order to counter the legitimacy of using this assumption in forging the war in Ukraine?

A Historical Agency: Ukraine's pursuit of independence and self-determination has a long history. The country has a distinct culture, language, and identity, and Ukrainians have consistently fought for their autonomy throughout history.

B Democratic Processes: Ukraine has a functioning democratic system with elected representatives who are accountable to their constituents. The country has held multiple elections since gaining independence in 1991, including presidential, parliamentary, and local elections.

C International Recognition: Ukraine is a sovereign nation recognized by the international community. It holds a seat in the United Nations and maintains diplomatic relations with numerous countries worldwide.

D Domestic Accountability: The Ukrainian government is accountable to its citizens through democratic processes and institutions. Elected officials are responsible for making decisions that reflect the will and interests of the Ukrainian people.

DOMINOES
digital resilience to disinformation

Debate time

+ INFO

Q4 Hostile narratives as so effective because:

A They deceive ordinary citizens as “unwitting agents”

B They are amplified by platforms’ algorithms which quickly propagate false stories on an unprecedented scale

C They are based on false beliefs which persist and even spread to communities where everyone is deeply committed to collect and share factual information

D They can be instrumentalized by groups which have always had interest in influencing public beliefs

DOMINOES
digital resilience to disinformation

Case Study of Hostile Narratives Eroding Support for Ukraine

Case1: Case Study of Hostile Narratives Eroding Support for Ukraine

Since the beginning of the war in Ukraine the propaganda campaign has aimed to stoke fear and **divisions** among Ukraine's critical European allies. **One of its main topics was the influx of refugees from Ukraine**. And while Europeans remain overwhelmingly supportive of fleeing Ukrainians, there are signs that Russian efforts to weaponize the issue may be finding their mark: lies about Ukrainian refugees have been widely used to capitalize on Europeans' fears, and to polarize the public discourse.

The proportion of information that is hostile toward Ukrainian refugees "is increasing and generating greater engagement on social media" (Neidhardt, 2022). Several examples can be provided here.

In Poland on Telegram posts depicted Ukrainian refugees as aggressive and a threat to Polish peace and stability. They made unsubstantiated claims about Ukrainian refugees being treated better than Polish citizens. Some Telegram messages discouraged Polish families from hosting 'dangerous' refugees. Others circulated old videos purporting to show the violent behavior of Ukrainians in other European countries, although these had been previously debunked (Givi & Ponce de Leon, 2022).

Case1: Case Study of Hostile Narratives Eroding Support for Ukraine

In **Romania**, one of the main narrative attempted to induce the idea that Ukrainian **refugees coming to Romania are extremely rich**, and therefore need no support:
”The hospitality with which the Ukrainian refugees were received gave rise to some confusion (…) We can say that they feel almost at home in our city, prioritizing their own comfort, at the expense of following the rules. This fact is perfectly illustrated by the images captured on the land behind the Microreservation, near the Dolphinarium, where a Maserati with Ukrainian numbers was parked on the green space. The Mercedes of a compatriot kept him company (…). We note that there are parking spaces a few meters away, but they seem to prefer the unpaved area. Of course, the empathy that law enforcement feels for those driven by war prevents them from intervening. The “poor” Ukrainian refugees have the right to park wherever they want, even where it is not allowed…” (March 2023).

In other countries, such as in **Czech Republic**, the topic has been rapidly included in the extremist political discourse. For example, for Czech citizens the prevailing sentiment suggests that basic help for refugees is supported but not if it is at their own expense. Towards the end of 2022, refugees became used more as a proxy topic to criticize the government and potentially gain some advantages in the presidential elections. In **Slovakia** too, prominent narratives targeting the government’s policy on refugees portrayed it as an “extremist liberal” agenda being pushed by President Čaputová. Additional narratives attempted to present the refugees as puppets and victims of a war of aggression in-cited by NATO or the West in general. Among the V4 countries, Slovaks bear the biggest aversion toward Ukrainian refugees (52%).

Likewise, in **Germany** the demonization of Ukrainian refugees was perpetuated via social media hoaxes and bogus news stories. The campaign against Ukrainian refugees presented them as a threat to Europeans’ health and wealth with the anti-refugee messaging being fueled by a sprawling, coordinated, Russia-based network of fake news websites, Telegram channels, YouTube and Instagram channels.

Time for practice

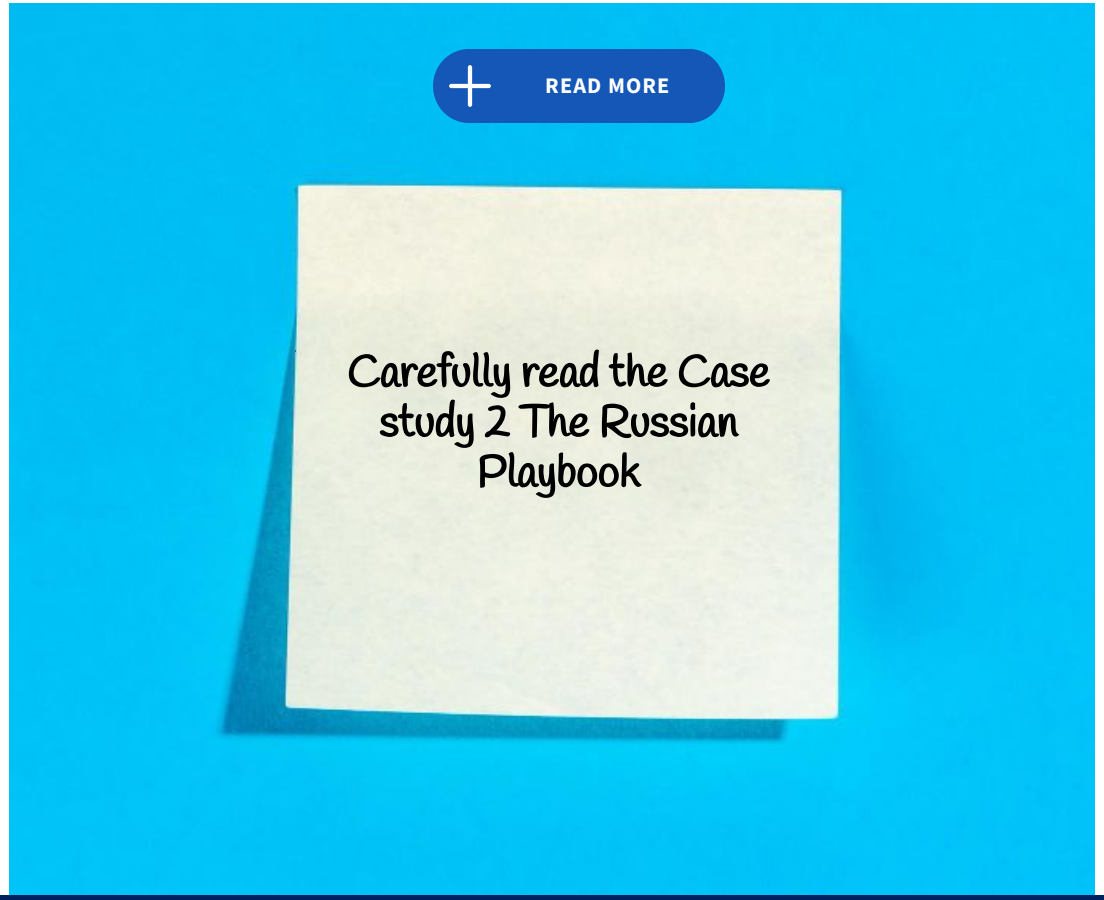
Whereas past waves of disinformation targeting Middle Eastern refugees portrayed them as a “cultural” threat to Europeans, the campaign against Ukrainian refugees presents them as a threat to Europeans’ health and wealth. This particular narrative can be considered hostile because:

You can select more than one answer

- It targets Europeans' sense of identity
- It is pro-Russian
- It targets migrants
- It plays with existing local fears

SEND

Case Study of Hostile Narratives Eroding Support for Ukraine



Case Study of Hostile Narratives Eroding Support for Ukraine [1/6]

A comprehensive timeline of the Russian war against Ukraine shows a telling **pattern of the fake narratives used in the information war**. At the beginning of the aggression, mid-February 2022, the Russian propaganda machine advanced the idea that there is a Ukrainian crisis caused by the disregard of the West towards the “neo-Nazi crimes” of the Ukrainian government associated forces.

Later on, EU and NATO were made responsible for the support of the Neo-Nazi movement, allegedly having organized a coup d’état to create a militarized Nazi state in Ukraine and install what was labeled as illegitimate government. Poland and Romania were accused of attempting to occupy part of Ukraine, while the Ukrainian military “was denounced” to be behind the actual Russian inflicted attacks (Kramatorsk station) or crimes (Bucha, Irpin etc.). In April 2022, US was already accused of operating biolabs to develop toxins that target the Slavic genotype while Ukraine was repeatedly accused of preparing attacks with biological, nuclear, or dirty bombs etc.

The pattern shows a sequence of narrative that attempt to **persuade audience by denying facts and blaming the opponent for own deeds**: Russia did not attack and does not wage war, the Ukrainian population is decimated by its own government forces, attacks are inflicted by third parties and imagined enemies aspire to conquer Ukrainian territories. Denying the own crimes and justifying war through the existence of imaginary enemies seems to have been a preferred narrative theme used to confuse, detour attention or simply create as much as possible plausible deniability. By the end of 2022, Russian propaganda and disinformation seem to have focused on two main areas:

1. to control domestic audiences, maintain support and persuade that the Russian government is waging a just war against an imminent threat against Russian borders and identity and
2. to undermine support for Ukraine in European countries and the US.

Case Study of Hostile Narratives Eroding Support for Ukraine [2/6]

The key narratives used to systematically mock and devaluate Ukraine since 1991 have been also researched in a series of articles published by Inna Polianska, and listed below:

Narrative #1: 'Ukraine is a failed state which never existed before the USSR's creation.'

Narrative #2: 'Ukraine is not a sovereign state, but an "anti-Russia project" financed by the West to destabilise Russia.'

Narrative #3: 'The Ukrainian language is an artificially created dialect of Russian with Polish influences.'

Narrative #4: 'Ukraine is one of the most corrupt states in the world so it will never be ready for EU membership. Even Western weapons are stolen and sold to Russia.'

Narrative #5: 'The Ukrainian government is not self-sufficient and is just following the instructions of Western leaders.'

Narrative #6: 'Ukraine must be de-Nazified for infringing the rights of the Russian-speaking population and then integrated into Russia'.

Case Study of Hostile Narratives Eroding Support for Ukraine [3/6]

A closer look at these narratives also shows that they can equally be flagged all across the ex-Soviet bloc, evidence from media content in e.g. Belarus, Moldova, Georgia, the Baltic countries or Romania showing similar opportunistic use of the 6 narratives every time the social and political context allowed it and if the historical background matched the potential use.

This leads to the conclusion that what we face is rather a set of templates populated with updated content and used repetitively to create feelings of inferiority, distrust, confusion, fear.

In a similar vein, larger, more complex narratives have been employed to **attack the liberal world and Europe in particular**.

Another EU vs. Disinfo article references the following adjacent storytelling frameworks:

- The elites vs. the people, a populist frame for numerous conspirational theories dedicated to Big Corporations, Jews, Muslims, Financial elite etc.
- Threatened values (and traditions o.n.) - a framework often used against minorities
- Lost sovereignty or threatened national identity
- Imminent collapse (of Europe)
- The hahaganda narrative (using sarcasm to annihilate evidenced accusations in e.g. the Skripal case).

□Case Study of Hostile Narratives Eroding Support for Ukraine [4/6]□

Let's take one example and a closer look at the one of the most promoted myths about Russia's invasion of Ukraine - the situation in Ukraine is the one that triggered the conflict.

This is part of an extended list of dangerous myths — some of them outright lies — illustrating the Kremlin's attempt to spread disinformation and manipulate information in order to justify its military aggression against Ukraine. The myths were extensively documented by the EUvsDisinfo.

Myth: "The situation in Ukraine triggered this conflict. There is proof that Ukraine is committing atrocities against its Russian-speaking population in the country's east. Russia has to intervene, not least because Ukraine and Russia are 'one nation.' Ukraine simply belongs to Russia's "privileged sphere of influence".

To galvanize domestic support for Russia's military aggression, Russian state-controlled media have tirelessly sought to vilify Ukraine, falsely accusing it of genocide in eastern Ukraine, drawing groundless parallels with Nazism and World War Two, and fabricating stories aimed at striking a negative emotional chord with audiences.

Case Study of Hostile Narratives Eroding Support for Ukraine [5/6]

There are **many instances of such fabricated stories**, best illustrated by the famous example of a Russian television report accusing Ukrainian forces of crucifying a young boy in eastern Ukraine in the beginning of the conflict.

For example:

On July 12, 2014, state-owned Channel One (Pervy Kanal) showed an interview with a woman calling herself Galina Pyshniak. Pretending to be an eye-witness, she described a heart-breaking story about a three-year-old child being crucified by Ukrainian nationalists in front of his mother's eyes in the city of Slovyansk. The unconscious mother was then tied to a tank and driven around the square. The story was one of the peaks of the Kremlin-orchestred campaign targeted at inciting hatred against Ukrainians.

Journalists from Novaya Gazeta debunked (opens in a new tab) the story within 24 hours, and other testimonies disproving the Channel One's lie appeared, among them one from Ukrainian Stopfake.

Sadly, none of the stories that proved that the story was a fake could have reached such a massive audience as a TV channel with supposedly 250 million viewers worldwide. Fact-checkers were quick to prove that the story was entirely made up. But similar stories have continued to be produced.

In reality, there is no evidence that Russian-speaking or ethnic Russian residents in eastern Ukraine face persecution – let alone genocide — at the hands of Ukrainian authorities. This has been confirmed in reports published by the Council of Europe, the UN High Commissioner for Human Rights, and the OSCE

Case Study of Hostile Narratives Eroding Support for Ukraine [6/6]

The often-used claim that **Ukraine and Russia are "one nation" is one of the oldest and most deeply ingrained myths used against Ukraine**. Even from a long-term historic perspective, this argument does not hold. While they have common roots dating back to Kievan Rus, which existed from the ninth century to the mid-13th century, it is just not true to argue that Ukrainians and Russians are one nation 800 years later. Despite long periods of foreign rule, Ukraine has a strong national culture and identity, and is a sovereign country.

The notion of an "all-Russian nation" with no political borders is an ideological construct dating back to imperial times and has been used as an instrument to undermine Ukrainian sovereignty and national identity.

Since 2014, **the Russian government has cultivated this myth** with renewed vigour in an attempt to rationalise and justify its military aggression against Ukraine.

Notions of "spheres of influence" have no place in the 21st century. Like all sovereign states, Ukraine is free to determine its own path, its foreign and security policies and alliances, and its participation in international organisations and military alliances.

To advance the idea that Ukraine belongs to Russia's "sphere of influence," Russian authorities and state-controlled media frequently claim that Ukraine is not a "real" state. State-sponsored Russian propaganda tries to misrepresent history in order to legitimize the idea that Ukraine belongs to Russia's natural sphere of interests.

DOMINOES
digital resilience to disinformation

Time to practice

Erasmus+

What we can take from “The Russian playbook” is that when information is taken out of context:

You can select more than one answer

- We need to see if reading and checking on it worth our time
- We need to find other coverage and other sources
- We need to see if expert sources agree on with the information
- We need to trace claims and understand the original context

SEND

References

- Alberto-Horst Neidhardt (2022). Disinformation on refugees from Ukraine: Boosting Europe's resilience after Russia's invasion, ISSUE PAPER EUROPEAN MIGRATION AND DIVERSITY PROGRAMME, available at https://www.epc.eu/content/PDF/2022/Disinformation_IP_v3.pdf

- Gigitashvili, Givi and Esteban Ponce de León "Polish-language Telegram channels spread anti-refugee narratives", Digital Forensic Research Lab - Atlantic Council, 31 May 2022.

- Tétrault-Farber, G. Far-Right Europe Has a Crush on Moscow. The Moscow Times, 25 November 2014. Available at: http://www.themoscowtimes.com/news/article/far-right-europe-has-a-crush-on-moscow/511827.html (Accessed on 11 January 2015).

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Irena Chiru (MVNIA)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Understanding conspiracy theories

1.3.1

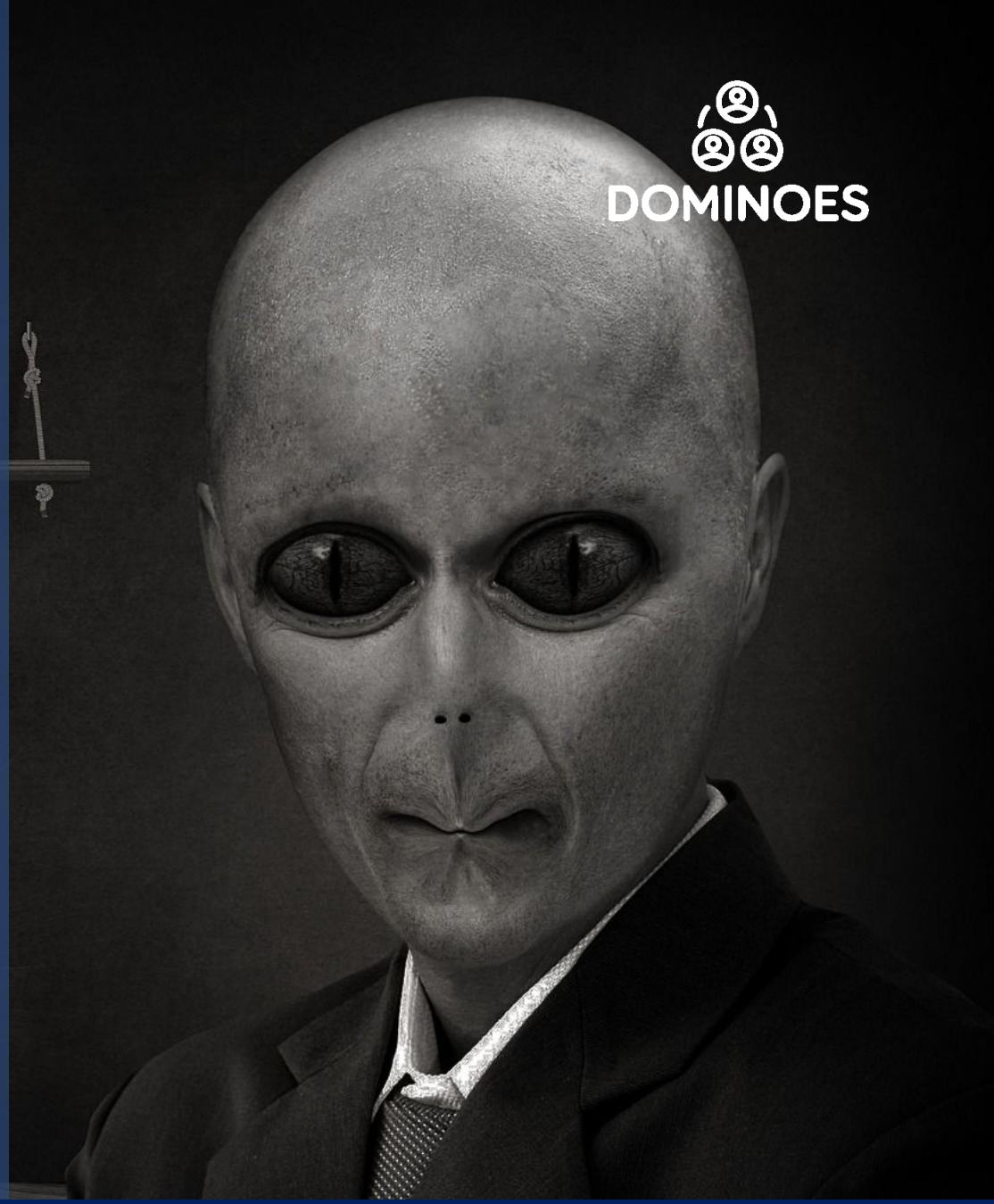
doi.org/10.5281/zenodo.10063982

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Conspiracy theories are explanatory causal-based, ideologically laden narratives which depict **significant social events or crises** as perpetrated by a group of powerful secret actors who solely follow their own nefarious interests, irrespective of the good of the masses. They have always existed in societies, however, at present, they have gained momentum due to their easy spread and appeal in social media. Moreover, they have begun to **corrupt people's understanding of the world** and their willingness to listen to experts and authorities in times of crisis and not only, thus threatening not only the further development of societies but also the very health and security of the communities they live in.



DOMINOES

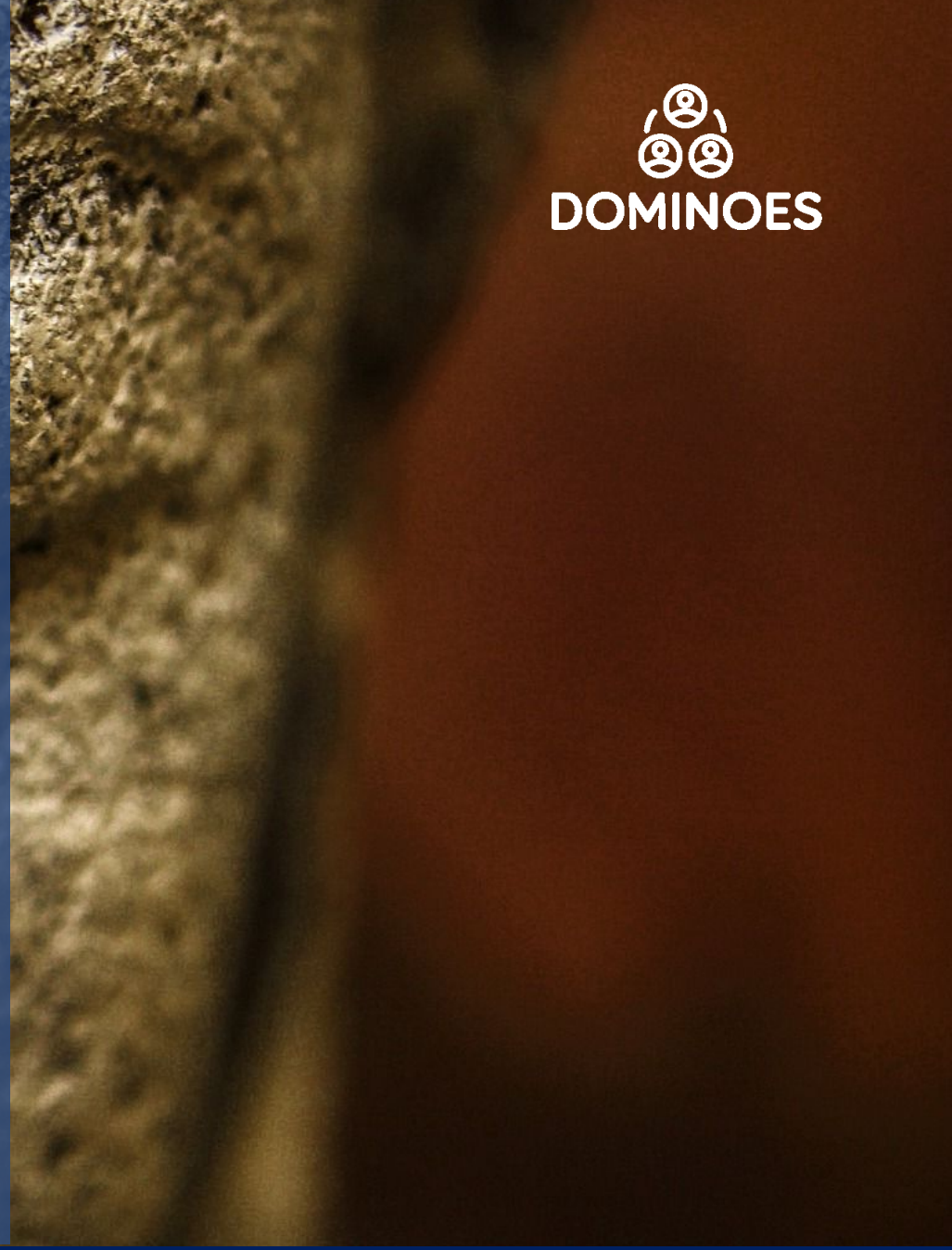
Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Psychological factors

- Paranoia and suspiciousness
- Low self-efficacy
- Higher levels of anxiety
- Low self-esteem
- Insecurity about elements of the environment
- Dissatisfaction with life
- Distrust of others



DOMINOES

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Cognitive factors

- Difficulty of handling complex and incomprehensible situations
- Creating and working with causal relationships without conscious control
- Understanding what others are thinking and/or doing not solely based on our own actions
- Jumping to conclusions
- The tendency to overestimate the importance of the dispositional explanations of behavior (based on personality features which make conspiracy theories much more attractive explanations than non-conspiratorial ones

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

Characteristics of conspiracy theories

DOMINOES

1. Speculative
2. Contrarian
3. Premodern
4. Amateurish
5. Self-sealing and self-sustaining
6. Very nuanced and complex
7. Unknowable to and untraceable
8. Monological belief system
9. Authorities

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Irena Chiru (MVNIA)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Case studies of hostile narratives and conspiracy theories by authoritarian state and non-state actors

1.3.2

doi.org/10.5281/zenodo.10063999

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER


1.3.2_The case of Daphe
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
04:53
vimeo

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Irena Chiru (MVNIA)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Understanding hostile narratives

1.3.4

doi.org/10.5281/zenodo.10064015

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.

Universidad Rey Juan Carlos

L-Università ta' Malta

NEW STRATEGY CENTER

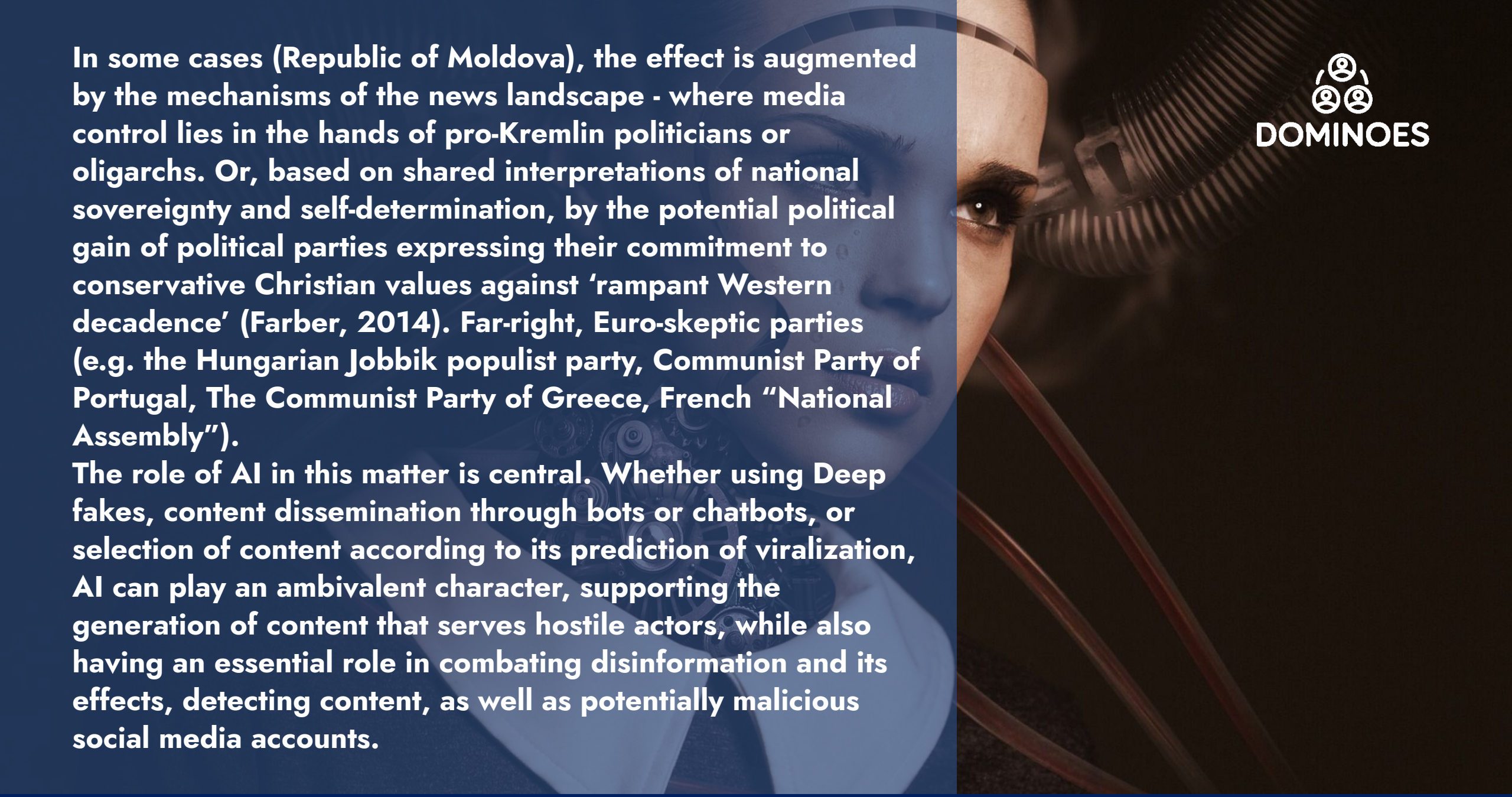
Hostile narratives rely on negatively charged emotions, like fear or anger. They specifically target feelings and emotions – such as the sense of belonging, the sense of self- determination, a sense of economic security, and a sense of physical security. Each narrative touches upon particular national vulnerabilities, but no matter the country, the tactics behind them can be recognized in other, similar narratives promoted by Vladimir Putin's Kremlin. Hostile narratives in countries along the Russian border share many similarities with a mix of residual memories, political failures, and regional conflicts or using historical iconic images.

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem

By using and promoting negative feelings and by touching upon specific social vulnerabilities, they aim to order lower the means of rational self-defence and trigger self-survival instincts, creating a psychological condition that makes the brain respond positively rather than negatively to bigoted statements and divisive rhetoric (Flore, 2020).
They are made of true and false information, while the narration of facts counts more than the facts themselves. Hostile narratives link ardent topics such as migration to other existing insecurities, depicting it as a threat to three partly-overlapping areas: health (migrants as violent criminals, terrorists or carriers of disease), wealth (migrants as social benefits cheats or unfair competition for jobs) and identity (migrants as a hostile invasion force, threatening to replace white, Christian Europeans and their traditions). For example, the narrative 'The European Union is Bad, Russia's Customs Union is What You Need' widely used in Republic of Moldova apparently tackles with economics, but actually the arguments used are often based on ideological conservatism and used to create fear. In the same way, the narrative 'Romania and NATO are a Threat to Peace', raises people's sense of insecurity.

DOMINOES

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem



In some cases (Republic of Moldova), the effect is augmented by the mechanisms of the news landscape - where media control lies in the hands of pro-Kremlin politicians or oligarchs. Or, based on shared interpretations of national sovereignty and self-determination, by the potential political gain of political parties expressing their commitment to conservative Christian values against 'rampant Western decadence' (Farber, 2014). Far-right, Euro-skeptic parties (e.g. the Hungarian Jobbik populist party, Communist Party of Portugal, The Communist Party of Greece, French "National Assembly").

The role of AI in this matter is central. Whether using Deep fakes, content dissemination through bots or chatbots, or selection of content according to its prediction of viralization, AI can play an ambivalent character, supporting the generation of content that serves hostile actors, while also having an essential role in combating disinformation and its effects, detecting content, as well as potentially malicious social media accounts.

DOMINOES

Exercise 1

DOMINOES

The receptivity to hostile narratives depends on our capacity to be self-aware of our values and emotions. Which values, beliefs and emotions do you think make us more vulnerable in accepting and sharing hostile narratives?

You can select more than one answer

- Lack of trust in institutions
- Manichean ideas of dualism - tending to look at things as having two sides that are opposed
- Rational self-defense and self-survival instincts

SEND

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Exercise 2

DOMINOES

In many European countries, the ”demonisation” of the Ukrainian migrants has been instrumentalized by political parties and widely disseminated in social media. How do you think this should be tackled?

You can select more than one answer

- By exposing the vested interests behind such an instrumentalization
- By widely disseminating such demonisation narratives
- By developing a EU migration diplomacy addressing the structural factors facilitating the instrumentalisation of migration by third countries

SEND

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Exercise 3

DOMINOES

One of the narratives broadly used to gain public support for the intervention in Ukraine is based on the assumption that ”The Ukrainian government is not self-sufficient and is just following the instructions of Western leaders”. Which arguments can we use in order to counter the legitimacy of using this assumption in forging the war in Ukraine?

You can select more than one answer

Historical Agency: Ukraine's pursuit of independence and self-determination has a long history. The country has a distinct culture, language, and identity, and Ukrainians have consistently fought for their autonomy throughout history.

Democratic Processes: Ukraine has a functioning democratic system with elected representatives who are accountable to their constituents. The country has held multiple elections since gaining independence in 1991, including presidential, parliamentary, and local elections.

SEND

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

Exercise 4

DOMINOES

Hostile narratives as so effective because:

You can select more than one answer

- They deceive ordinary citizens as “unwitting agents”
- They are amplified by platforms’ algorithms which quickly propagate false stories on an unprecedented scale
- They can be instrumentalized by groups which have always had interest in influencing public beliefs
- They are based on false beliefs which persist and even spread to communities where everyone is deeply committed to collect and share factual information

SEND

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158
Digital cOMpetences INformatiOn EcoSystem


1.3.4_Case1: Case Study of Hostile Narratives Eroding Support for Ukraine
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
03:26
vimeo

DOMINOES

Exercise

DOMINOES

Whereas past waves of disinformation targeting Middle Eastern refugees portrayed them as a “cultural” threat to Europeans, the campaign against Ukrainian refugees presents them as a threat to Europeans’ health and wealth. This particular narrative can be considered hostile because:

You can select more than one answer

- It targets migrants
- It is pro-Russian
- It targets Europeans' sense of identity

SEND

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Digital cOMpetences INformatiOn EcoSystem

DOMINOES


1.3.4_Case study 2: The Russian Playbook
Grupo Ciberimaginario
DOMINOES
digital resilience to disinformation
08:52
vimeo

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union

2021-1-RO01-KA220-HED-000031158

Author of contents: **Irena Chiru (MVNIA)**

Audiovisual and multimedia production: CIBERIMAGINARIO

DOMINOES
digital resilience to disinformation

Evaluation 1.4

S1. The information environment

10.5281/zenodo.10063871

Co-funded by
the European Union

2021-1-RO01-KA220-HED-000031158

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Exercise in Groups

Running time:
40 minutes

Participants split into **6 Groups of 5 members**

Each group should appoint **1 representative** for taking notes (in addition to engage in discussion) and present the results

- 2 Groups dealing with:
  - Malta
- 2 Groups dealing with
  - Romania
- 2 Groups dealing with
  - Spain

Method

Participants will engage in a structured discussion around the following questions:

- **How do you characterize the security environment?**
  - What are the main trends and drivers shaping potential scenarios for the region (Southern Europe and the Mediterranean)?
- **What are the main players** (state and non-state) **in the region from a political and security perspective?**
- **What are threats and most important challenges** (perspective of implications for Malta or Romania or Spain?)

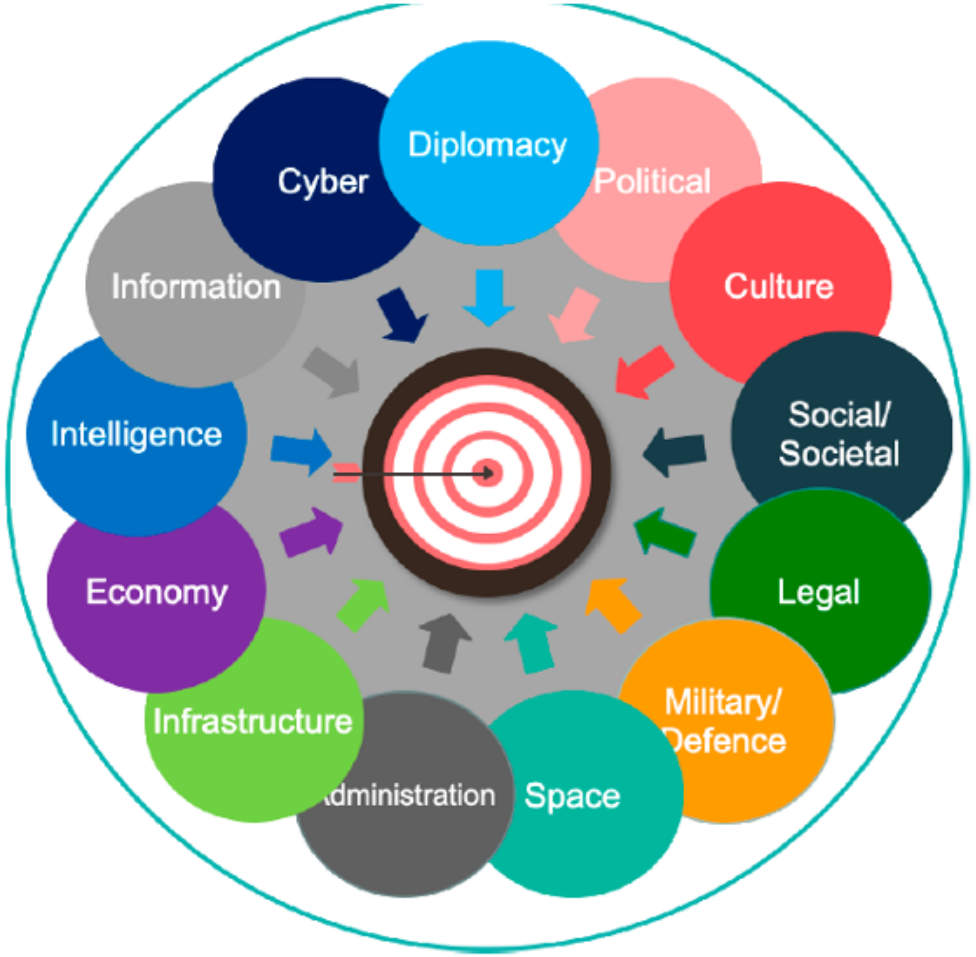
Method

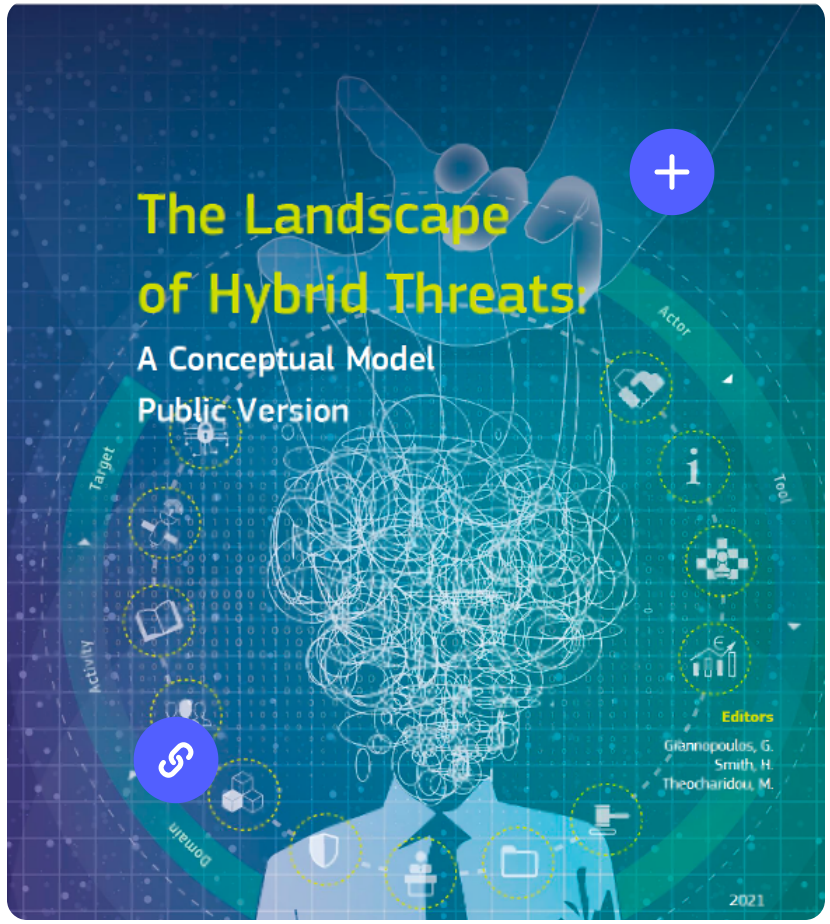
Participants will engage in a structured discussion around the following questions:

- **What vulnerabilities** (13 domains) **and opportunities** (local, national, transnational) **could be exploited by hostile actors through information manipulations and disinformation?**
- **What potential measures/initiatives could strengthen Malta/Romania/Spain's capability and competence to deal with those threats and with their potential manipulative activities in the information environment?**
    - (Consider not only government actors but also civil society)

Method

Use the **13 domains of hybrid threat activity of the JRC/Hybrid CoE conceptual framwework** when discussing on vulnerabilities and potential mitigation measures/initiatives



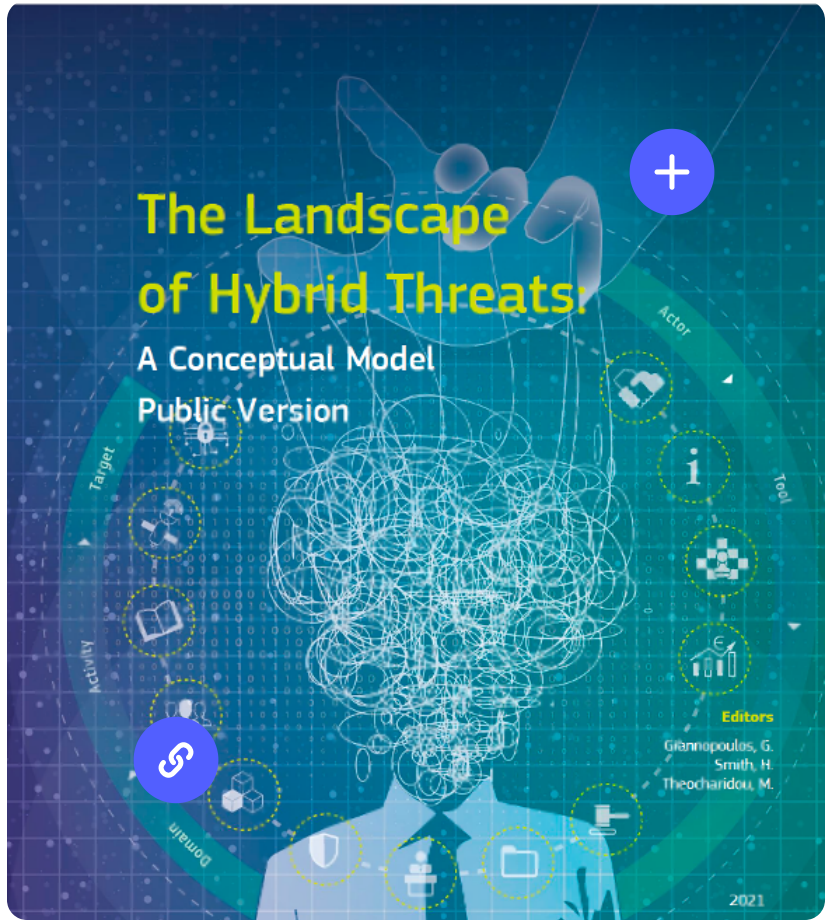


Lorem ipsum dolor

Method

1. **Discuss the results** of **your in-group discussion** with the other group that was assigned the same country.
2. **Agree on key points** to be presented to the whole classroom.
3. **Presentations** (5 minutes per country).

NOTE: You can use post-its and flipcharts to organize the inputs in your in-group discussion



Lorem ipsum dolor

DOMINOES
digital resilience to disinformation

Digital cOMpetences INformatiOn EcoSystem

ANIMV DARE. LEARN. INNOVATE.
Universidad Rey Juan Carlos
L-Università ta' Malta
NEW STRATEGY CENTER

Co-funded by the European Union
2021-1-RO01-KA220-HED-000031158

Author of contents: **Rubén Arcos & Manuel Gertrudix (URJC)**
Audiovisual and multimedia production: CIBERIMAGINARIO