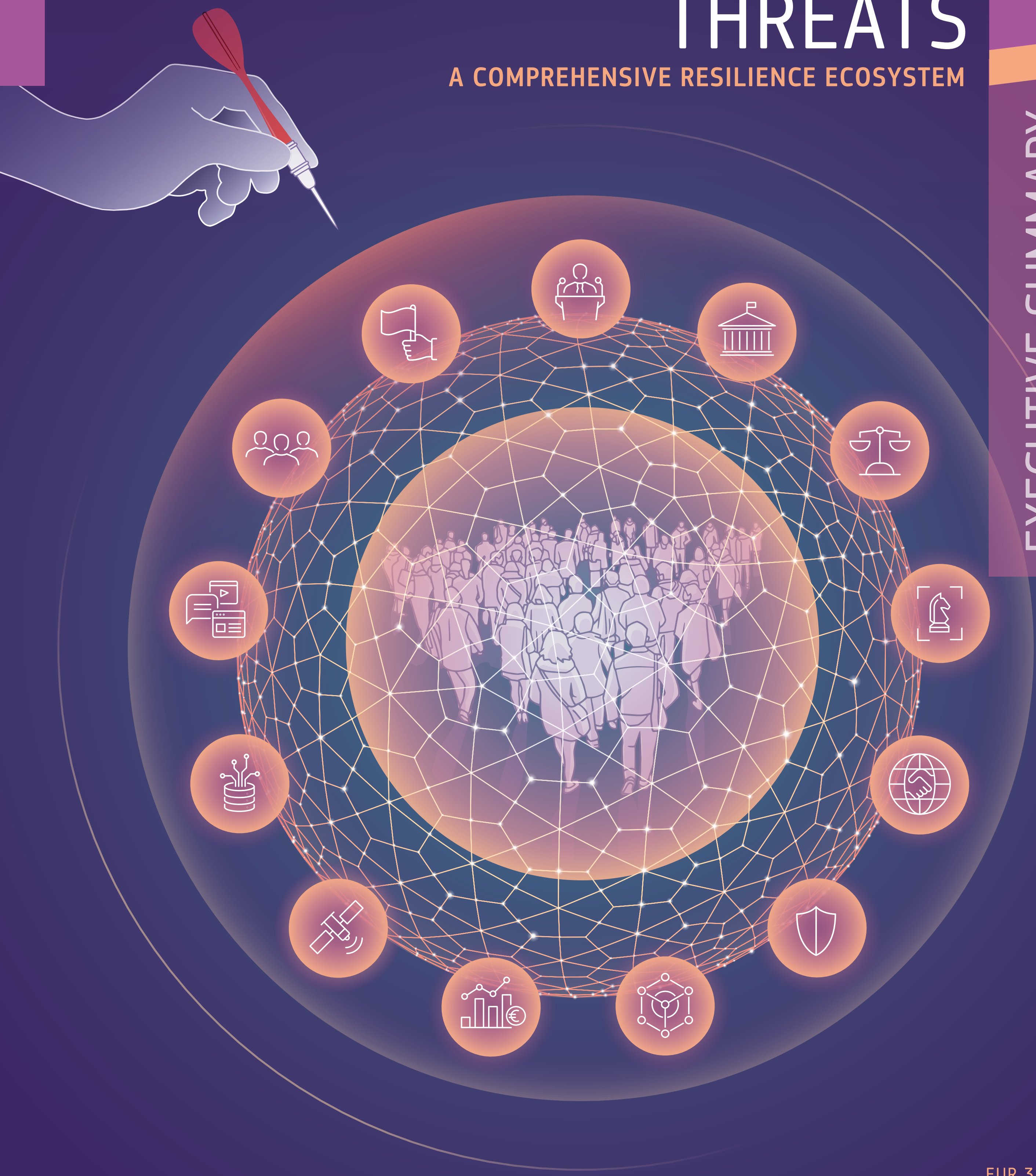
European Commission | Hybrid CoE

HYBRID THREATS

A COMPREHENSIVE RESILIENCE ECOSYSTEM

EXECUTIVE SUMMARY



EUR 31104 EN

Hybrid threats: a comprehensive resilience ecosystem

Resilience is one key component to counter hybrid threats. Resilience against hybrid threats can take advantage of the resilience measures of different domains. It needs to be thoroughly designed and implemented. Developing resilience against hybrid threats requires not only looking at resilience in each area but how to build it systemically, considering dependencies and interdependencies between the different parts of society. This report examines what is particular about resilience against hybrid threats. In this report, the comprehensive resilience ecosystem (CORE) model, which is a system-thinking representation of the society as a whole is proposed.

Manuscript completed in March 2023

This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service, prepared together with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). It is part of the series Facts4EUFuture, a stream of reports for the future of Europe. It aims to provide evidence-based scientific support to the European policymaking process.

The scientific output expressed does not imply a policy position of the European Commission nor Hybrid CoE. Neither the European Commission nor any person acting on behalf of the Commission or Hybrid CoE is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material do not imply the expression of any opinion whatsoever on the part of the European Union or the Member States.

CONTACT INFORMATION
European Commission, Joint Research Centre (JRC)
Directorate E – Space, Security and Migration
JRC.E.2 – Technologies for Space, Security and Connectivity
Contact: Rainer Jungwirth
E-mail: *JRC-E2@ec.europa.eu*

EU Science Hub
https://joint-research-centre.ec.europa.eu

Hybrid CoE website
https://www.hybridcoe.fi

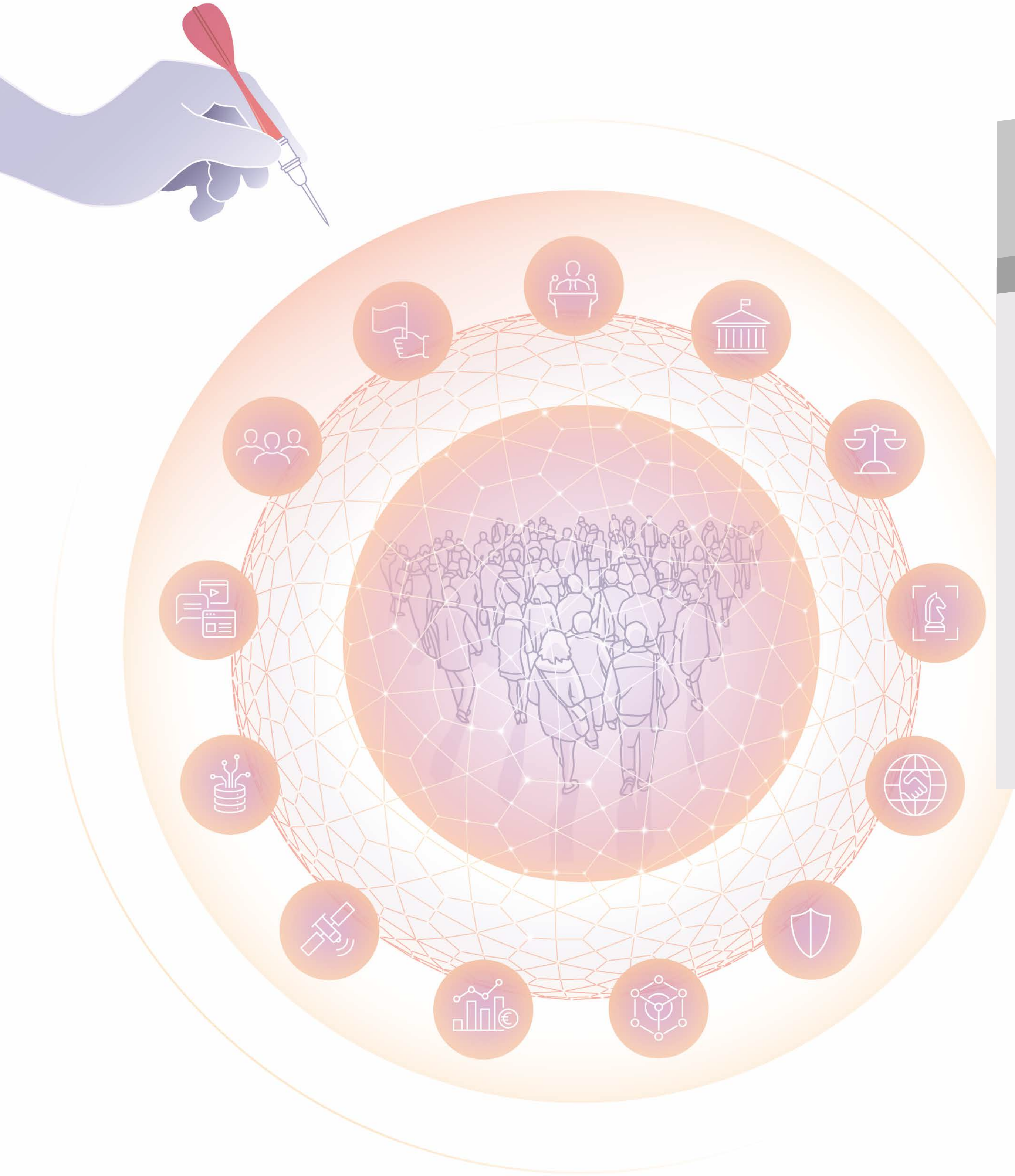
JRC129019
EUR 31104 EN

Print	ISBN 978-92-76-53496-9	ISSN 1018-5593	doi:10.2760/382543	KJ-1A-31-104-EN-C
PDF	ISBN 978-92-76-53301-6	ISSN 1831-9424	doi:10.2760/113791	KJ-1A-31-104-EN-N
EPUB	ISBN 978-92-76-53300-9	ISSN 1831-9424	doi:10.2760/486664	KJ-1A-31-104-EN-E

Luxembourg: Publications Office of the European Union, 2023

All content © European Union, 2022, except for the following images: cover graphic elaboration includes © Raman Maisei - stock.adobe.com; © funnydrew - stock.adobe.com; © rob z - stock.adobe.com; p. 15 © Olivier Le Moal - stock.adobe.com; p. 16 © Óscar MT - stock.adobe.com; p. 26 © enanuchit - stock.adobe.com; © gonin - stock.adobe.com; © dimazel - stock.adobe.com; p. 28 elaboration from © jozefmicic- stock.adobe.com; p. 30 © Konstantin L - stock.adobe.com; p. 32 © oatawa - stock.adobe.com; p. 36 elaboration from © Astibuag - stock.adobe.com; p. 43 © InsideCreativeHouse - stock.adobe.com; © vallejo123 - stock.adobe.com; © uzkiland - stock.adobe.com; © renatados - stock.adobe.com; © Monkey Business - stock.adobe.com; © Michal Kowalski - stock.adobe.com; p. 44 Brian Jackson - stock.adobe.com; © Filip - stock.adobe.com; © paulaphoto - stock.adobe.com; © Sergey Ryzhov - stock.adobe.com; p. 45 Berlin85 - stock.adobe.com; © Семен Саливанчук - stock.adobe.com; © razihusin - stock.adobe.com; © andrej pol - stock.adobe.com; © chungking - stock.adobe.com; © Negro Elkha - stock.adobe.com; p. 46 © lazyllama - stock.adobe.com; © Depe - stock.adobe.com; © Mike Dot - stock.adobe.com; © doganmesut - stock.adobe.com; © Leonid Andronov - stock.adobe.com; © kmiragaya - stock.adobe.com; p. 47 © enanuchit - stock.adobe.com; © Ravil Sayfullin - stock.adobe.com; © Tierney - stock.adobe.com; p. 48 © Looker_Studio - stock.adobe.com; p. 54 © fotograupner - stock.adobe.com; p. 58 © JackF - stock.adobe.com; p. 60 © Jacob Lund - stock.adobe.com; p. 64 © agcreativelab - stock.adobe.com; p. 66 Monkey Business - stock.adobe.com; p. 69 © guillaume - stock.adobe.com; p. 75 © pogonici - stock.adobe.com; p. 76 © Yingyaipumi - stock.adobe.com; p. 81 © vpanteon - stock.adobe.com; p. 82 © rawpixel.com - stock.adobe.com; p. 85 © Siam - stock.adobe.com; p. 86 elaboration from © babaroga - stock.adobe.com; © funnydrew - stock.adobe.com.

How to cite this report: Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., *Hybrid threats: a comprehensive resilience ecosystem – Executive summary*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019.



EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Hybrid threats constitute a combination of different types of tools, some expected and known, some unexpected and clandestine, applied to achieve an undeclared strategic objective, and without officially admitting to doing so. The common denominator for hybrid threat actors is their desire to undermine or harm democratically established governments, countries or alliances. By their very nature, hybrid threats constitute a risk to European values, governments, countries and individuals. Their overarching aim is to constrain the freedom of manoeuvre of democracies in order to discredit its model compared to authoritarian regimes or gain other advantages over democracies.

In particular, hybrid threat actors may be characterised by their wish to:

- **undermine and harm the integrity and functioning of democracies** by targeting vulnerabilities of different domains, creating new vulnerabilities through interference activity, exploiting potential weaknesses, creating ambiguity and undermining the trust of citizens in democratic institutions;
- **manipulate established decision-making processes** by blurring situational awareness, exploiting gaps in information flows, intimidating individuals and creating fear factors in target societies; and
- **maximise impact by creating cascading effects,** notably by tailoring attacks, combining elements from specific domains to overload even the best prepared systems, with unpredictable, negative consequences. These domains were outlined in a conceptual model which we, the European Commission's Joint Research Centre and the Helsinki-based European Centre of Excellence for Countering Hybrid Threats, published in 2020.

Today, Europe is facing growing and increasingly complex security challenges. Hybrid threats have become integral part of our security concerns; war has returned to Europe; instability is increasing in Europe's neighbourhood regions; there are attempts to manipulate election outcomes; and democracies increasingly are portrayed as weak governance systems. The possibility to spread disinformation rapidly and with great outreach via social media further exacerbates the potential impact of hybrid threats. Moreover, our increasing dependency on IT tools for our daily work, banking, health management as well as for elections and governance, means that every European, Member State and company is at some risk of being impacted by hybrid threats. We should also be aware that the impact of hybrid threats is not simply restricted to the security domain but also links to defence. As seen in the Communication 'Commission contribution to European defence, it urgently calls for a major boost to European resilience and defence.

Hybrid threats have become increasingly common over the past 10-15 years, and we can fully expect them to grow both in frequency and impact in future. The problem of hybrid threats is however not one that can be solved just at national and/or regional level: a concerted effort across Europe, involving all relevant partners, is crucial. For this reason we already proposed in 2020 a conceptual model that has proven a useful tool for policymakers when addressing hybrid threats.

As outlined in recent EU policy initiatives such as the 'Communication on the EU Security Union Strategy'[1] and 'A Strategic Compass for Security and Defence'[2] we are seeing fast-moving developments and an increased level of sophistication in hybrid threats. Resilience against hybrid threats therefore needs to be designed and implemented at all levels, and has to consider resilience measures, not only from multiple domains' perspective but as a comprehensive ecosystem approach. In other words, developing resilience against hybrid threats necessitates looking beyond resilience in individual areas, building it systemically while considering dependencies and interdependencies between the different parts of society.

To address these issues, we in this report for the first time apply a *systems-thinking approach* to

[1] COM(2020) 605

[2] *https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf*

> "…for the first time a systems-thinking approach to hybrid threats, with representation of society as a whole."

hybrid threats, with representation of society as a whole. Throughout the elaboration of the report and the underpinning scientific work, we have been in dialogue with Member States, notably via the Horizontal Working Party on Building Resilience and Countering Hybrid Threats of the Council of the European Union, as well as other key stakeholders. In concrete terms, we in this report propose a comprehensive resilience ecosystem (CORE) model to facilitate decision-making for policymakers.

The novelty of the CORE model is how it allows policymakers to estimate how adversaries employ hybrid threats in order to alter democratic decision-making capabilities. It shows how the hybrid threat activity bit by bit challenges democratic systems by introducing different types of stress. It also allows monitoring the dependencies and possible cascading effects. This is important for the detection of hybrid threats. Foresight plays a crucial role in this process.

The CORE model is based on the following elements, as also visualised in the following page:

1. **Seven foundations of democratic systems** lie at the heart of the ecosystem. The foundations are the ultimate goals that hybrid threat actors aim to undermine, while scoring some of their own strategic interests.

2. The **domains from the conceptual model** also are an integral part of the ecosystem. If resilience is well developed in the domains, they can act as shields against malicious activities. On the other hand, a lack of resilience in the domains can open entry points for hostile actors.

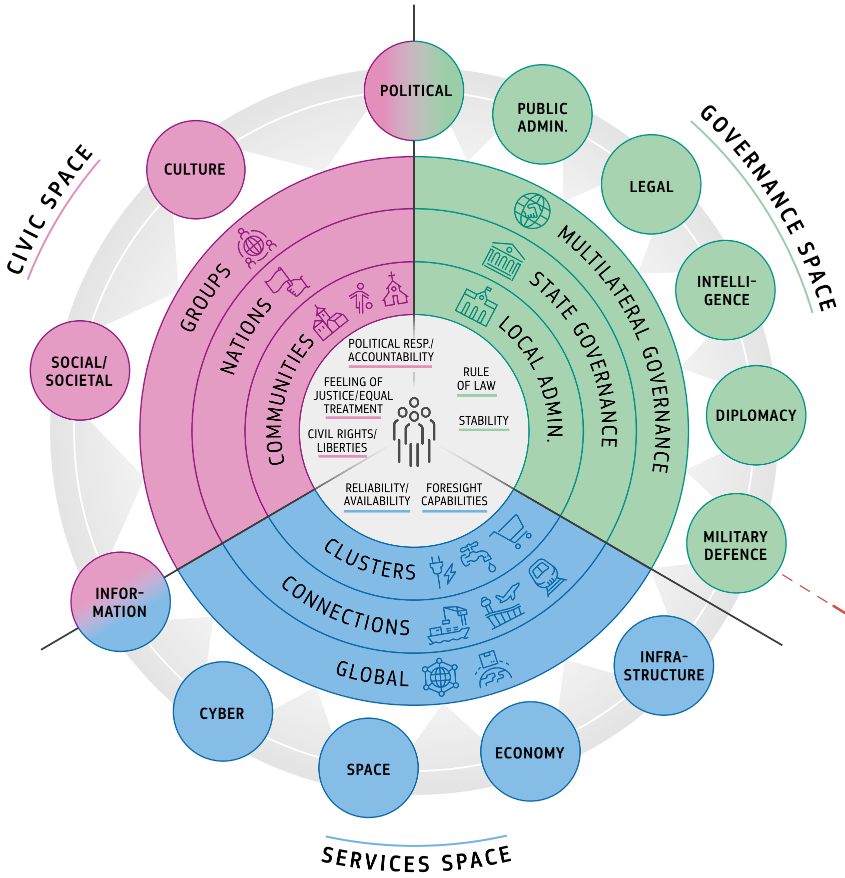
3. The ecosystem consists of **three spaces** – Civic, Governance and Services – which represent the three sectors of society.

4. **The layers of the ecosystem represent the different 'levels' that exist in society** – from the more local levels to international levels.

The connections between the four types of elements represent the whole-of-society approach. Since elements are interconnected, resilience-building measures for one element will affect other elements, positively or negatively. Actors behind hybrid threats aim to exploit the various elements and their interconnectedness to maximise their impact. Therefore, policymakers need to understand the interdependencies between the various elements, in order to build resilience against hybrid threats and for early detection of malign activity.

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.



CORE MODEL — STRUCTURE

7 FOUNDATIONS OF DEMOCRATIC SOCIETIES

Hybrid threat actors aim to undermine them to achieve their goals. Resilience requires strong foundations, supported by trust.

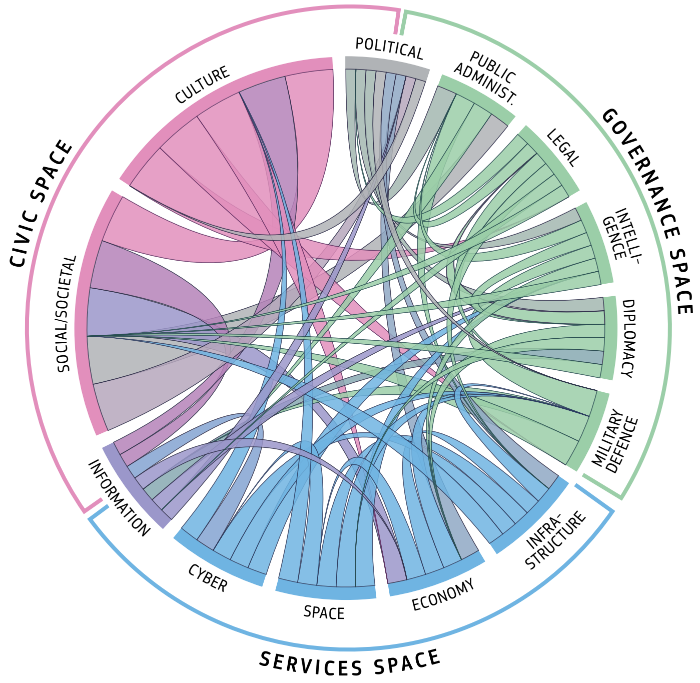
C G S
1. Local
2. National
3. Internat.

3 SPACES + 3 LAYERS

The spaces (Civic, Governance, Services) and layers represent the sectors and levels of society.

13 DOMAINS

Domains can act as shields against malicious activities or entry points for attacks.



RESILIENCE AND INTERCONNECTIONS BETWEEN DOMAINS

Resilience is key to counter hybrid threats and needs to be designed systemically.

Building resilience in domains individually is not optimal, since hybrid threats aim to create cascading effects and exploit interconnections.

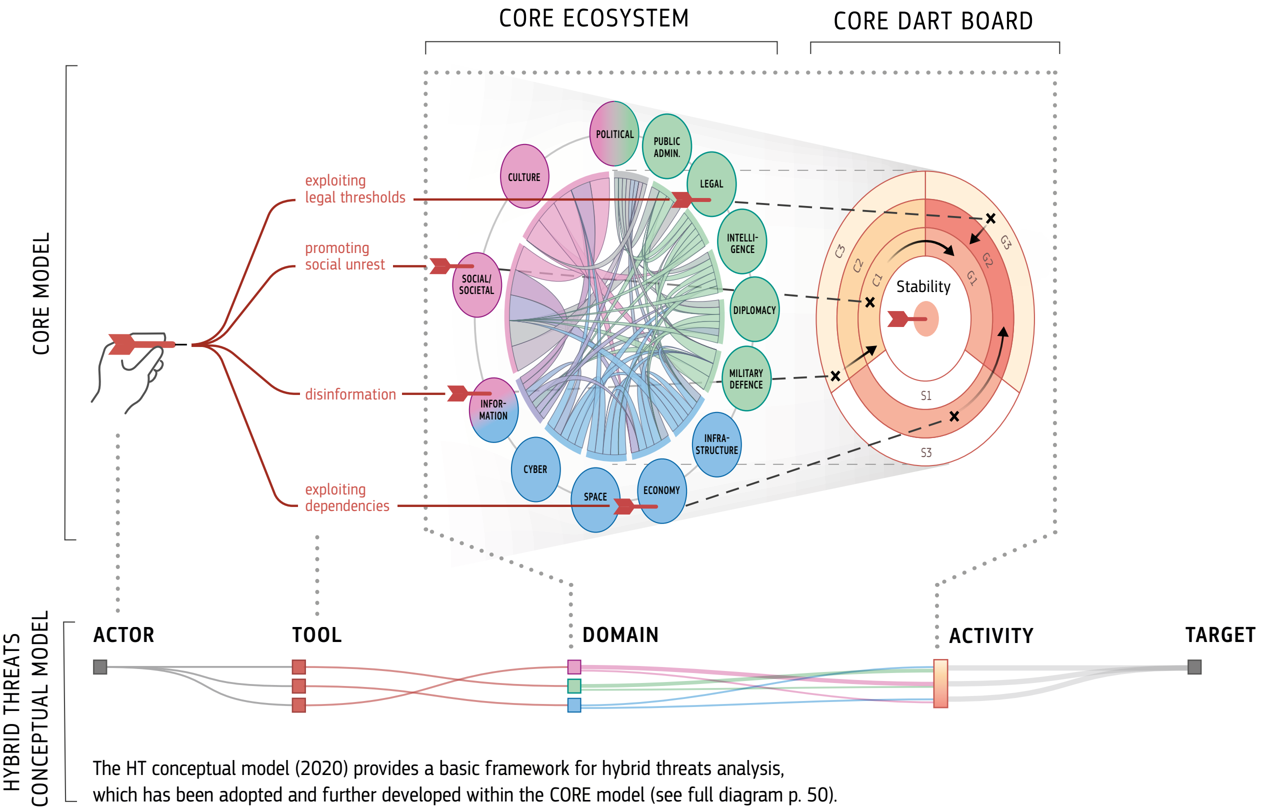
A **systemic approach** is necessary, **considering existing dependencies and interdependencies** in society.

Trust in the democratic process makes dependencies and interdependencies strong and healthy and supports the foundations of democratic systems. Hybrid threat actors seek to erode this trust.

REPRESENTING THE IMPACT OF HYBRID THREATS

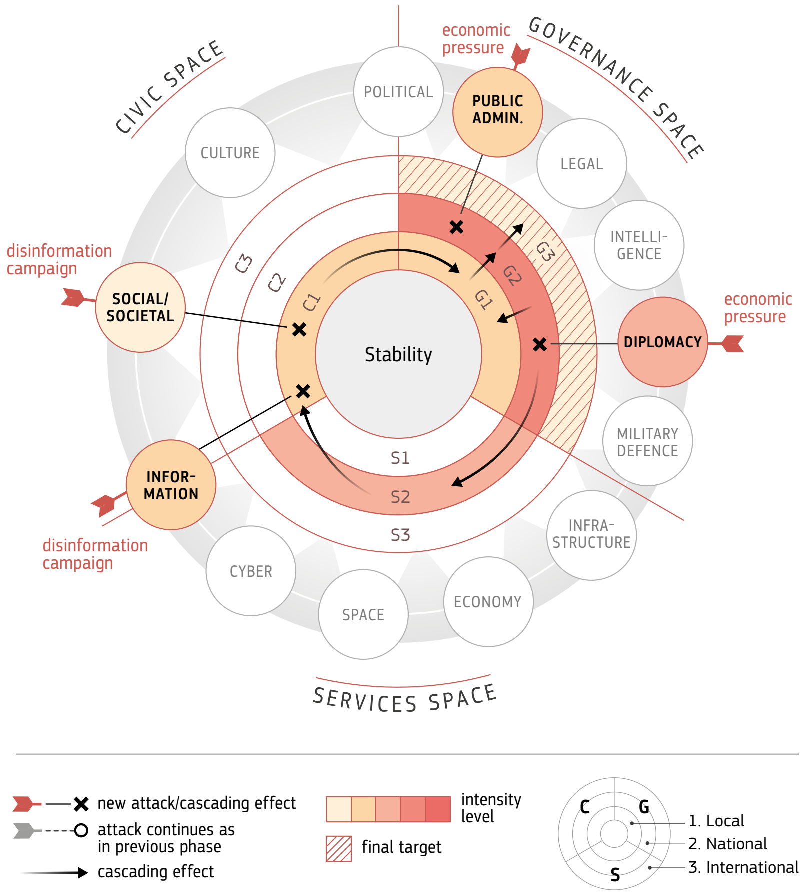
CORE can be used as a 'dart board' to map how actors use specific tools to attack different domains and create cascading effects to different spaces and layers.

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).

CORE AS A STRATEGIC DESIGN BOARD



This ecosystem approach helps to spot early signals, support their analysis and identify potential response trajectories.

It can be used to:

- **design the right measures** to counter the primary and higher-order effects in all spaces and layers of the ecosystem
- build a cross-sectoral, **whole-of-society approach to resilience**
- serve as the **conceptual foundation to support policymaking** against hybrid threats

In essence, it helps decision-makers select which resources, tools and measures to mobilise at EU, Member State and operational levels.

This ecosystem model supports anticipation and foresight work in imagining developments, assessing the scale of risks and disruptions, and representing worst case scenarios. Used as a strategic design board, the CORE model can help identify the right measures to counter the effects of hybrid threats in all spaces and layers of the ecosystem. It can help to implement a holistic approach against hybrid threats and serve as a foundation for the creation of the EU Hybrid toolbox which was announced in 'A Strategic Compass for Security and Defence'.

The seven case studies presented in this report demonstrate the extent to which hybrid threat activity can undermine and weaken the foundations of a well-functioning democratic ecosystem.

Written in response to the above-mentioned EU policy initiatives, this report may therefore be considered a strategic manual for Member States and EU institutions on how to anticipate hybrid threats, evaluate their potential impact, and identify how to pre-empt or minimise their negative impact. Of particular value are the various case studies, the timeline outlining how hybrid threats have developed, and the cultural/linguistic comparisons. All of these contribute to a broad, multi-cultural perspective that lead to a deeper understanding of what hybrid threats constitute in this day and age, while offering tangible guidance on building resilience and preparing for future challenges.

Looking ahead, the Russian invasion of Ukraine in particular highlights the need for further research on the following points:

- The Conceptual Model on hybrid threats can be further optimised by taking into account experiences from the ongoing war including the increasing role of disinformation by Russia, and how this to a large extent has been countered, not least by the Ukrainian president who has communicated well and continuously with his people and the rest of the world, being visible and transparent in showing what is going on, addressing fellow democracies to ask for support, and creating positive reactions to his country and people, successfully making Ukraine's cause the entire democratic world's cause.

- The particular case of countries in an ongoing democratisation process could be explored further, as they already have the systemic vulnerabilities of democracies but not all the protection of established institutions, traditions, and processes of democracy.

- Seeing how Russia escalated from priming and destabilizing to actual coercion, crossing the threshold from hybrid threats to conventional war, it is essential to develop a better understand of the influence of culture, mind-set and values of hostile actors, to understand their thinking. That way we will be in a better position to understand, interpret and anticipate their strategic goals, and, crucially, to pre-empt of minimise their impact.

GETTING IN TOUCH WITH THE EU

IN PERSON

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you online ***(european-union.europa.eu/contact-eu/meet-us_en).***

ON THE PHONE OR IN WRITING

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: **00 800 6 7 8 9 10 11** (certain operators may charge for these calls),
- at the following standard number: **+32 22999696**
- via the following form: ***european-union.europa.eu/contact-eu/write-us_en.***

FINDING INFORMATION ABOUT THE EU

ONLINE

Information about the European Union in all the official languages of the EU is available on the Europa website ***(europa.eu).***

EU PUBLICATIONS

You can view or order EU publications at ***op.europa.eu/en/publications.***
Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre ***(european-union.europa.eu/contact-eu/meet-us_en).***

EU LAW AND RELATED DOCUMENTS

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex ***(eur-lex.europa.eu).***

OPEN DATA FROM THE EU

The portal (***data.europa.eu***) provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Publications Office
of the European Union