European Commission

Hybrid CoE

HYBRID THREATS

A COMPREHENSIVE RESILIENCE ECOSYSTEM

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.

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

JRC129019

Print	ISBN 978-92-76-53293-4	ISSN 1018-5593	doi:10.2760/867072	KJ-NA-31-104-EN-C
PDF	ISBN 978-92-76-53292-7	ISSN 1831-9424	doi:10.2760/37899	KJ-NA-31-104-EN-N
EPUB	ISBN 978-92-76-53290-3	ISSN 1831-9424	doi:10.2760/436951	KJ-NA-31-104-EN-E

Luxembourg: Publications Office of the European Union, 2023

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*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.

HYBRID THREATS

A COMPREHENSIVE RESILIENCE ECOSYSTEM

FOREWORD

MARGARITIS SCHINAS
EUROPEAN COMMISSION
VICE-PRESIDENT
FOR PROMOTING OUR
EUROPEAN WAY OF LIFE

We are living in a time of historic turmoil, in which the security of Europe is being challenged at many different levels. Russia's unprovoked and unjustified invasion of Ukraine since February 2022 has resurrected the prevalence of new methods of warfare in the 21st Century.

Hybrid attacks, combining the use of various tools to achieve ambiguous strategic objectives, are among the new emerging risks to the security landscape. Hybrid threats may be of a military but also of a non-military nature, such as cyberattacks, damage to critical infrastructure, disinformation campaigns, radicalisation of the political narrative or the instrumentalisation of migration, which are becoming more and more sophisticated and commonly used to exploit the vulnerabilities of the European Union. They represent a particular danger to Europe and its neighbourhood, because they specifically target democratic systems and countries in the process of modernisation.

Addressing innovative and complex security threats in an efficient manner requires a holistic approach. This is why the EU works to forge a genuine boost to EU security and stability, bringing internal and external but also digital and physical security to the same level. This approach is spelled out in recent EU policy initiatives, particularly the 'EU Security Union Strategy of 2020'[1] and 'A Strategic Compass for Security and Defence of 2022'[2].

The Joint Research Centre (JRC), with its anticipatory capabilities and long-standing expertise in security matters, is a key actor in developing the necessary common understanding on hybrid threats and incubating a reinforced security ecosystem. The conceptual model presented in 2020 by the JRC, in partnership with the Helsinki-based European Centre of Excellence for Countering Hybrid Threats, is now widely used by policy-makers across Europe and is a key step in this direction.

Next is to design a resilience framework against hybrid threats in the EU. This is the purpose of this report, which puts forward a whole-of-society approach that can serve as a strategic manual for Member States and EU institutions to anticipate hybrid threats, assess their impact and guide a response. I warmly welcome this important and very timely work, which will help build further resilience across the entire European continent against hybrid threats and prepare for future challenges.

1 COM(2020)605

2 A Strategic Compass for Security and Defence, 2022, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

FOREWORD

MARIYA GABRIEL
EUROPEAN COMMISSIONER
FOR INNOVATION,
RESEARCH, CULTURE,
EDUCATION AND YOUTH

Hybrid threats are a growing concern to our societies, which depend on the well-functioning and robustness of our critical infrastructures.

As the report points out, these types of threats have become increasingly common over the past 10-15 years, and we can expect them to remain an important source of risk to our European strategic autonomy.

We need to make all efforts to understand it from their motivation, organisation, and technological perspectives. Research plays a key role in developing a deep, cross-cutting understanding that support all stake-holders, societal and economic, to improve their readiness. Research can support policy makers to have access to reliable background to take informed decisions.

Almost two years ago the European Commission's Joint Research Centre and the Helsinki-based European Centre of Excellence for Countering Hybrid Threats published 'The Landscape of Hybrid Threats: A Conceptual Model'. It has since then become the de-facto standard in the EU when speaking about hybrid threats.

The model was only a first step towards systematically addressing the issue. Events since then have highlighted the need for further research. For instance, the Russian, unprovoked and unjustified, act of aggression against Ukraine has demonstrated the importance of building resilience for the security and prosperity of the EU in a changing security environment.

I am happy to introduce this report as a new component of the Commission's efforts to counter hybrid threats. It builds on the conceptual model for hybrid threats, outlining in detail how democratic societies can effectively build resilience against hybrid threats.

It will support the assessment of the sectoral hybrid resilience and proposes a hybrid threat toolbox to give policymakers a clear overview of potential threats and associated options. It is an essential step forward in our joint efforts, recalling us that by identifying the gaps in addressing hybrid threats we will be able to develop robust and targeted resilience strategies.

Let me congratulate the Joint Research Centre and the Centre of Excellence for the important work done presenting a Comprehensive Resilience Ecosystem for the benefit of the whole of society.

TABLE OF CONTENTS

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'[3] and 'A Strategic Compass for Security and Defence'[4] 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 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:

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

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.

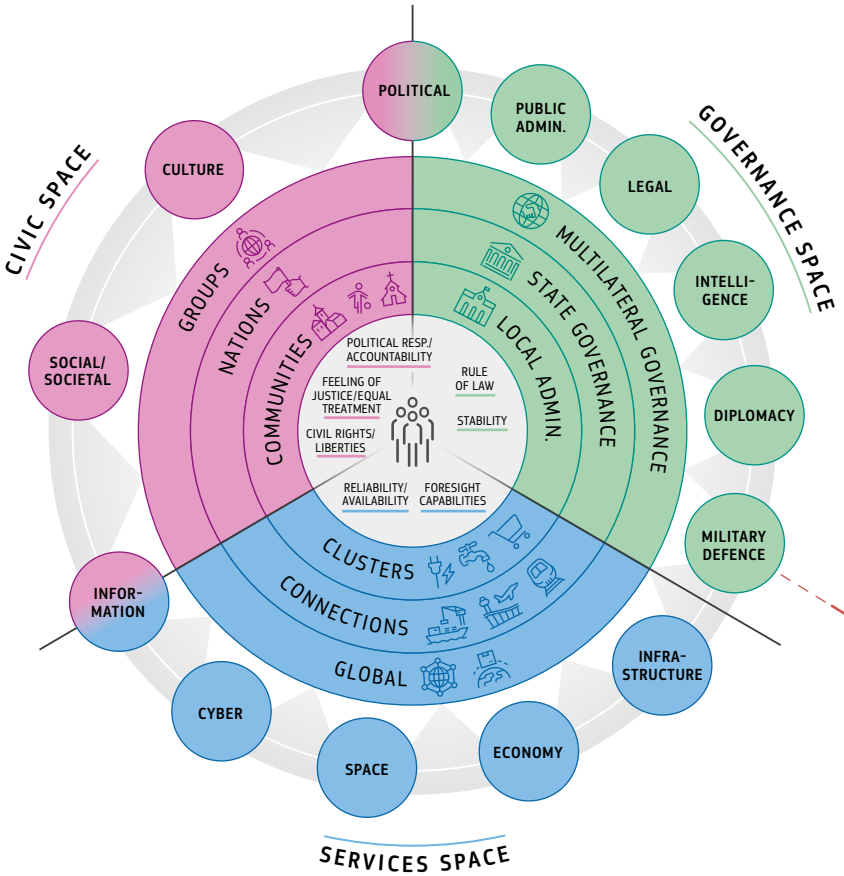
3 COM(2020) 605

4 *https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf*

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.

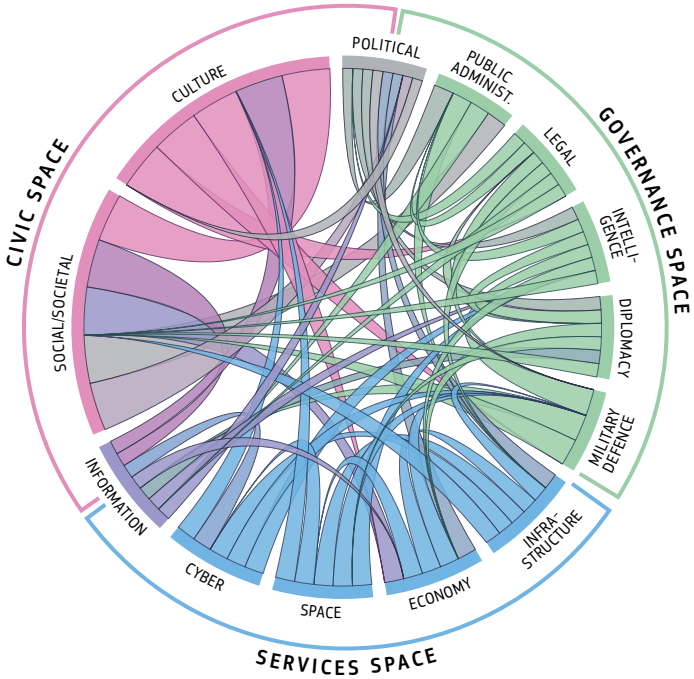
3 SPACES + 3 LAYERS

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.

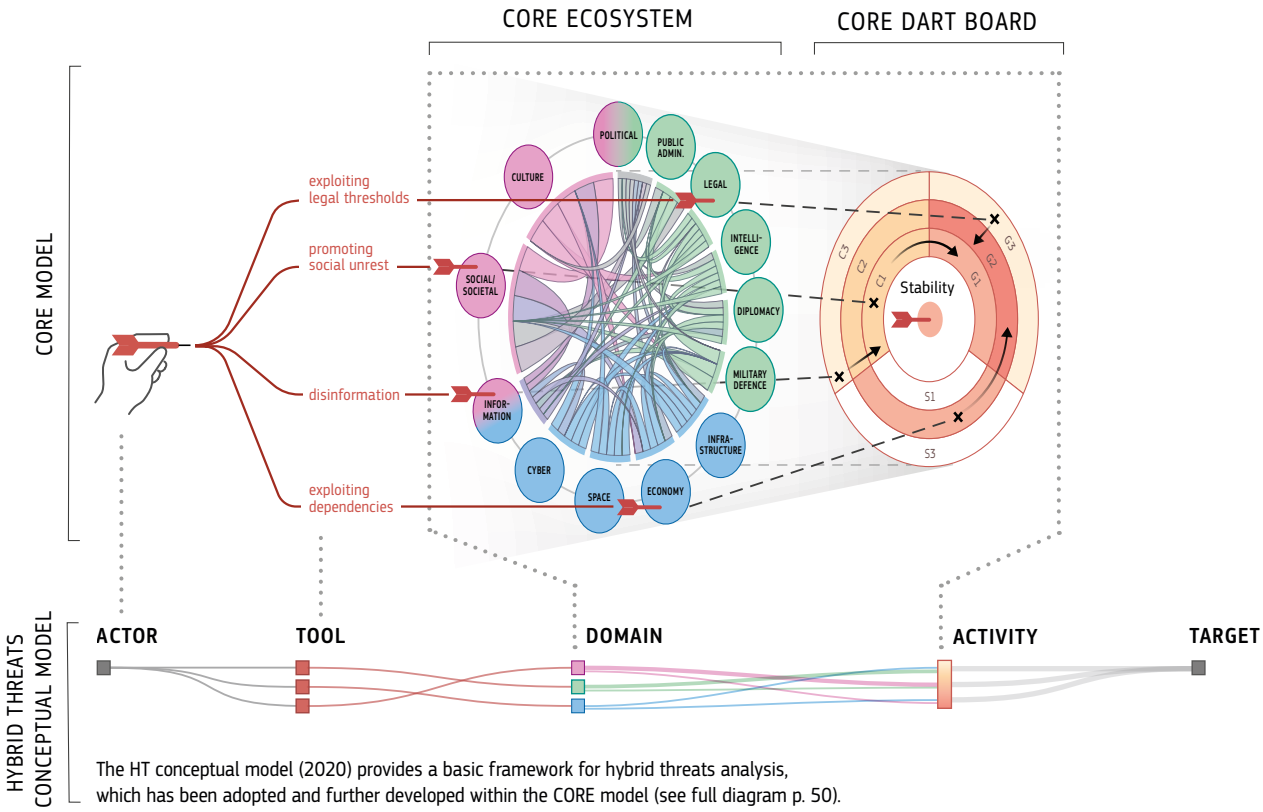
A **systemic approach** is necessary, **considering existing dependencies and interdependencies** in society.

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.

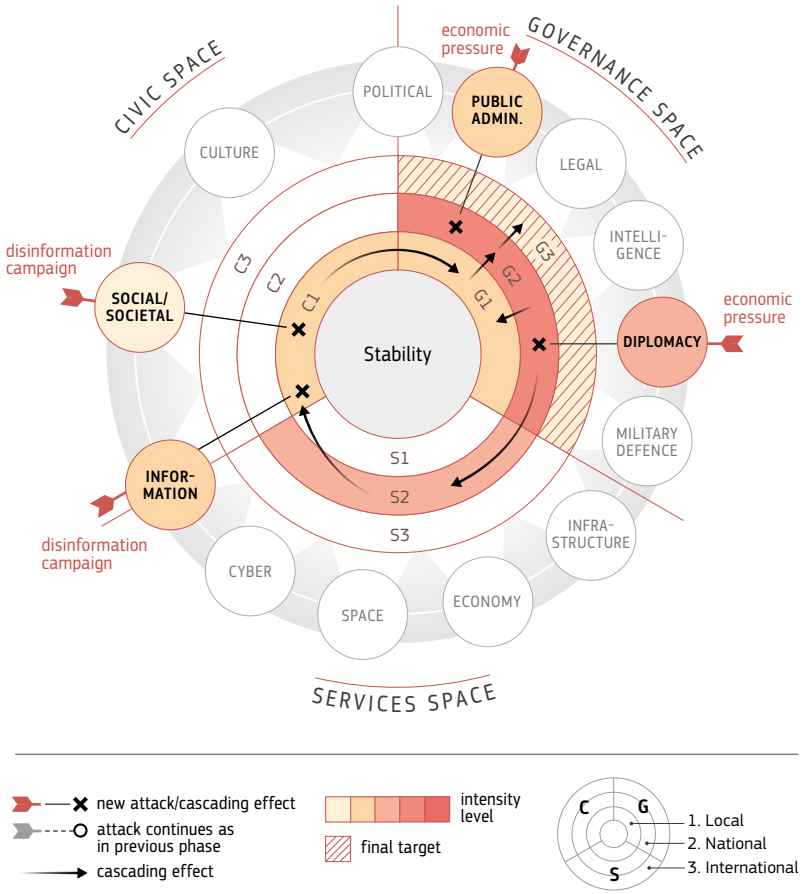
REPRESENTING THE IMPACT OF HYBRID THREATS

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.

INTRODUCTION

For several years the European Union has realised the importance of resilience in order to cope with the fast-evolving security environment across different *domains* (social, political, legal, cyber etc.), *layers* (local, national, international) and *spaces* (civic, governance and services). Today more than ever we are surrounded by complex security challenges. We are facing strategic competition; war has returned to Europe and sources of instability are increasing in our neighbourhood and beyond. This all also means that we need to be prepared for hybrid threats to grow both in frequency and impact.

The Russian war in Ukraine shows a possible outcome if we fail to counter hybrid threats. Hybrid threat activity targets specifically democratic systems and those in the democratisation process.[5] Those, as Ukraine, who are in an ongoing democratisation process are in the most vulnerable position. They already have the systemic vulnerabilities of democracies but not all the protection of established institutions, traditions, and processes of democracy. For decades, Russia exercised hybrid threat activity in Ukraine prior to the start of the war. Its activity escalated from priming to destabilising to the coercion phase. While apparently Ukraine was not able to fully counter the hybrid activities, it was able to deny the strategic aims of Russia. This combination has shown that a hybrid threat actor could potentially escalate activity if it does not reach its goals and ultimately the situation crosses the threshold from the landscape of hybrid threats to conventional war. This also shows that understanding the underlying causes of the hybrid threat activity and the exploitable vulnerabilities in our societies are a prerequisite in order to build resilience against hybrid threats.

To foster resilience against hybrid threats a comprehensive ecosystem model is presented in this report. This builds strongly upon prior work on hybrid threats carried out jointly by The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and the JRC, who developed a conceptual framework for hybrid threats and provided the technical characteristics of their domains. It is intended that this ecosystem approach will be the foundation of a toolkit for policymakers in making the EU and our societies more resistant to hybrid threats.

First, the starting point is the reasons behind the hybrid threat activity – the strategic competition that has emerged between authoritarian and democratic states/actors. We are therefore talking about man-made activity, and events caused directly by conscious decisions that aim to harm and undermine democratic societies. This presents us with a challenge relating to foresight, actor analysis and response planning.

Secondly, we need to be able to deny and respond to activity that uses complex synchronised and coordinated methods. Authoritarian actors have a linear power structure and complex network-like methods, while in democratic states the power structures are complex, but our processes are linear and sectoral. This presents us with a challenge relating to detection, decision-making and preparedness.

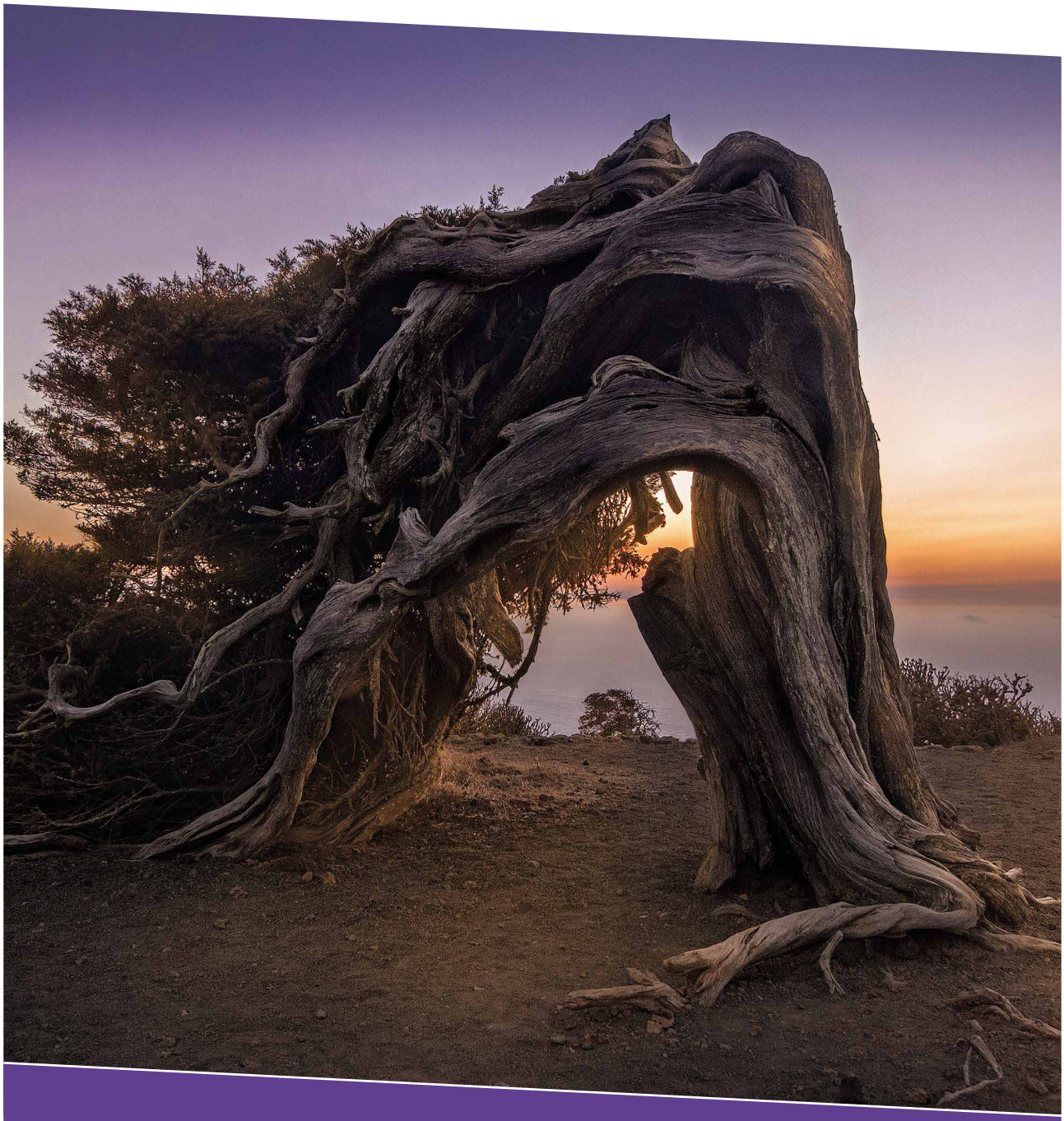
5 Hybrid threats refer to specific types of interference and influence methods by authoritarian state or non-state actors targeting democratic systems and those in the process of democratisation. Democratic states use different types of method, while an authoritarian state acting against another authoritarian state uses yet different methods. There are similarities, such as using multiple means, but here, when talking about hybrid threats we refer to authoritarian states and non-state actors targeting specifically systemic vulnerabilities in democracies. See Cullen et al. (2021) for a more detailed definition of hybrid threats.

> “...we need to be able to deny and respond to activity that uses complex synchronised and coordinated methods.”

Third, hybrid threats are creative and evolve continuously, so resilience building needs to have a similar nature. Sectoral resilience alone does not guarantee optimal resilience, since hybrid threats aim to create cascading as well as force-multiplier effects (the impact is greater than the sum of activity).

To fully comprehend what is needed for effective and holistic resilience-building against hybrid threats we need a strategically designed board.

To that end this report proposes a **Comprehensive Resilience Ecosystem** (CORE) to counter hybrid threats. Three different spaces – civic, governance and service – are explored in this report and highlight the complexity and interdependence of the environment in which we live today. The report will show dependencies between civic groups, local level administration and system connections, between nation, state and clusters as well as multilateral, communities and global layers.



HIGHLIGHTS

The term ‘resilience’ is used in many different fields and definitions vary by discipline. Nevertheless, the literature on resilience has shifted over time from a static approach, which is about controlling shocks by resisting them and returning to equilibrium, to a dynamic approach, which is about overcoming shocks by adapting and moving towards a new stable equilibrium that is close to the original one. This change has been accompanied by a growing interest and increase in scientific publications in all fields on the topic of resilience, but especially in the area of social sciences and policymaking.

It is important to understand whether and how the term resilience is used in other cultures. An analysis of the term in Russian, Chinese and Arabic literature shows that there are parallels but also differences in resilience thinking. However, a common element is that ‘resilience’ in all three languages has the meaning of flexibility, agility and innovation.

FRAMING RESILIENCE

1.1. Introduction

This section examines some of the literature on resilience to help frame our understanding of resilience in terms of hybrid threats. In English, the term resilience has been used in several disciplines for at least eighty years and applied to multiple research entities. Consequently, although applied in many disciplines, there is no universally shared definition of resilience. In Russian, Chinese and Arabic languages the term 'resilience' has historical roots, but even if similarities with English language exist, there are significant differences. To strengthen our understanding of resilience in the hybrid threat context both the English language literature and an understanding of resilience in different languages are important. Only then can we see our own strengths and weaknesses. We can also learn more about the ways actors behind the hybrid threat activity think and thus see where they want to hit us.

> Understanding the concept of resilience in a variety of cultures helps to strengthen our understanding of it in relation to hybrid threats.

1.2. The concept of resilience

Generally, resilience refers to the ability of an entity to overcome adversity, with two main perspectives underpinning understanding of resilience: reactive and proactive. Researchers in the field of psychology, ecology and materials sciences have typically understood resilience from a **reactive perspective**, considering resilience as 'an inherent property of a person, object, or other entity that allows it to recover from a disturbance' (Jackson & Ferris, 2015). In the field of engineering, researchers have understood resilience from a **proactive perspective**,[6] including also 'how the object anticipates and plans for the disturbance and how the object might avoid or reduce the effect of the disturbance' (Ibid.).

Throughout time, the literature on resilience shifted from a static approach of controlling shocks by resisting and returning to the equilibrium, to a dynamic approach of overcoming shocks by adapting and moving toward a new stable equilibrium close to the original one. Thus, the evolution of the concept of resilience led to Holling's concepts of adaptive cycle (Holling, 1986; 2001) and panarchy (Holling, 2001; Gunderson, 2002) to assess where complex systems stand in terms of resilience, considering how they evolve internally and interact with other complex systems.

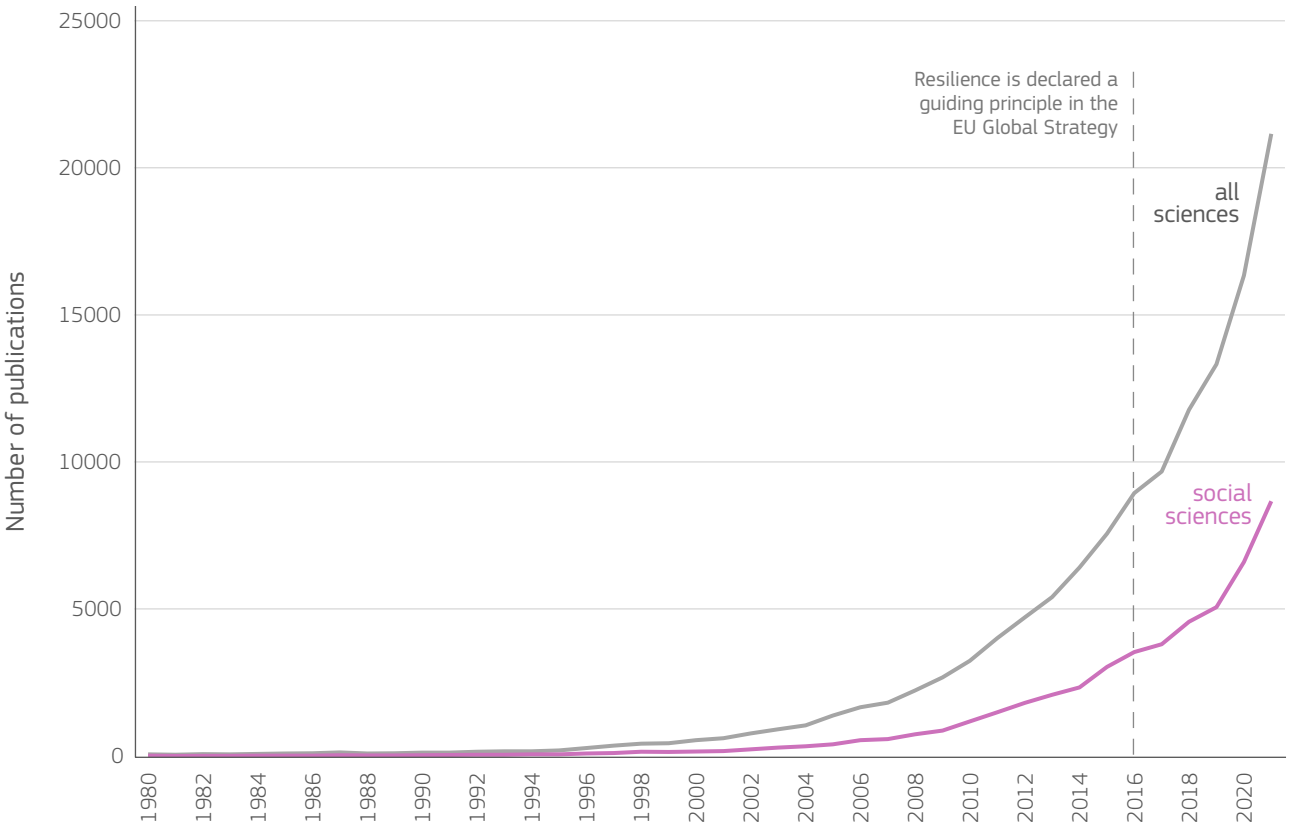
6 The concept of 'transition' that is stressed in EU policies like the digital and green transition and that also plays a major role in the 2020 Strategic Foresight Report (see European Commission (2020)) can also be regarded as 'proactive resilience'.

Since its use in the 1940s, the concept of resilience has been embraced by a variety of disciplines, often taking a sectoral approach. Applying the lens of hybrid threats to resilience analysis shows that technology-related domains such as infrastructure, cyber, space, economy, etc. have in the past often taken a different approach, compared to non-technology domains such as culture, intelligence, politics, and legal. It is very important to understand this gap, since it is also one basis on which to argue for a comprehensive approach of resilience to counter hybrid threats. Since the 2010s, a growing interest can be observed in academic publications with a significant increase after 2016, when resilience was declared in the EU Global Strategy (EUGS) (2017) as one of the five guiding principles for the EU's role in the world.

The aim of policymakers was to extend the concept of resilience from the traditional areas of foreign policy – diplomacy, defence, and development – to the external dimension of all other policy areas, from research and infrastructure to energy, climate, and trade (Tocci, 2020). Accordingly, there has been a noticeable increase in publications that address or discuss resilience in the context of the EU's external or internal policy approach, in the technical domains (cyber, infrastructure, and economy), as well as in the non-technical domains (information, social/societal, military/defence, and political).

Nevertheless, other domains, such as legal, public administration, culture, space, and intelligence, remain comparatively under-researched. This indicates that resilience still means different things to researchers in diverse domains. The lack of clarity in resilience-related literature is one of the reasons that political implementation of the concept has been hampered.

FIG 1. Overview of the number of publications (Scopus search, performed by the JRC)



1.3. The concept of resilience in other cultures

Words resonate differently from one country, one collective, one people, to the next. So when we translate, this is not a process between languages only, but between cultures. This is especially true if we are trying to translate complex semantic terms, such as resilience, into another language[7].

Our own understanding forms the basis for our strategies and actions. When trying to build resilience against hybrid threats it is an advantage to understand how others think too. This will help us to get a more comprehensive picture of resilience thinking. *Table 1* provides a useful summary of the variety of interpretations of resilience in Russian, Chinese and Arabic. It shows similarities but also differences in their literature on resilience thinking, as well as differences to Western resilience analysis. In all three languages, resilience has connotations of flexibility, agility and innovation. All of those elements should be part of resilience against hybrid threats.

Conclusion from the Russian literature review

There is no consensus about the translation of 'resilience' in Russian so far. Political elites are quite indifferent to this term (in the speeches of President Putin translators use 'resilience' as a translation for '*ustoichivost*' – which means not resilience but rather robustness). A plausible explanation would be that Russian official discourse is centred around the term of stability, portraying it as the *absence* of shocks and crises, while resilience particularly describes reaction to shocks. There is also a strong element (from different contexts) that views resilience as an ability to develop – despite or even due to external pressures. The main cultural dimension of the internal resilience discourse in contemporary Russia, which is closely intertwined with the political dimension, is now becoming a value-based discourse of resilience,

> "In all three languages, resilience has connotations of flexibility, agility and innovation."

promoted through the media and think-tanks close to the authorities and is put in the context of anti-Westernisim and sanctions.

Conclusion from the Chinese literature review

Chinese conceptualisations of resilience are inconsistent. In part, this may be attributed to different understandings of resilience in the classical philosophy. Various discourses of resilience, in any case, appear to centre around either adaptability or toughness. In other instances, these are used synonymously.

Concurrently, in a societal context, resilience is conceptualised as both adaptability of the weak, as well as development through adversity. In political discourse, shaped by the Communist Party of China (CPC), expressions of resilience centre on the idea of 100 years of humiliation. Thus, expressions of resilience are used to build legitimacy for the CPC and thus applied to justify regime preservation. Moreover, influenced by the cultural classics, resilience is often used in Chinese policy discourse to legitimise the CPC approach to governance and national economy, and to discredit Western democracies.

A particular form of expression of resilience – calls for strengthening Chinese cultural confidence – can

7 Three background papers commissioned to support this part of the report were produced by external collaborators. Summaries of the papers are presented here.

be seen as a threat response to foreign influence. Interestingly, the approach seems to combine different elements of classical philosophy; it gives the appearance of weakness and emphasises the (national) character-building quality of resilience, while bringing to the fore the toughness and self-renewal capability of Chinese culture.

All in all, in contrast to many Western conceptualisations of resilience, in the Chinese context cultural and philosophical classics emphasise flexibility and longevity in facing challenges. This could be understood as resilience of the 'weak' (China) against resilience of the 'strong' (West).

Conclusion from the Arabic literature review

In Arabic language discussions, three major, different words are used to mean 'resilience': *muruuna* (قنورم), *sumud* (دومص) and *salaaba* (قبالص). Importantly, the Arabic terms for resilience can have the connotation of flexibility and agility as well as perseverance and steadfastness or even being or becoming hard and rigid. Therefore, resilience in Arabic language literature has a wide spectrum of meanings.

Context is also of high importance. Even the same term can have different connotations depending on the cultural and socio-political context in a specific time and location. For example, in the context of the COVID-19 pandemic, economic adaptation is highlighted, while in the context of the Palestinian struggle against occupation, resistance and steadfastness are more prominent.

TABLE 1. Summary of the variety of interpretations of the word 'resilience' in Russian, Chinese, and Arabic.

CIVIC SPACE (Cultural/Social policy – understanding/usage of resilience)

RUSSIAN

vynoslivost' = physical resilience. The ability to adapt to various conditions, both environmental and social.

zhiznesposobnost' = viability. The ability as individual human to manage one's own resources.

gotovnost' k ispytaniâm = to be up for a challenge. The ability to be ready for challenges. Has a connotation of courageous behaviour.

Resilience understood as a term to describe pensioners surviving on a pension that is below the living wage or young students travelling around the world on a tight budget. Manifestation of heroic behaviour and durability of individuals. Moreover, resilience is used to describe the negative attitude towards the 'westernisation' of Russian values and culture.

CHINESE

fengyu dili, chuxin ru pan; jiexu fendou, jiajin chongci; qiannian suyuan, yuanmeng jinzhao = adversary, as in wind and rain, hardens the soul but with continued struggle the spirit is elevated and long-held dreams are achieved. The ability in times of difficulties to build personal capabilities and, thus, resilience.

gourixin ri ri xin you rixin = if you can renew yourself in one day, do so daily; then there will be daily renewal. The ability for self-reflection and innovation to strengthen and develop its abilities.

erjin maibu congtou yue = with firm strides, we can cross the summit once again. The ability to use challenges as a path for development

Resilience derived from quotations from classical texts or from famous politicians and used in the contemporary propaganda of the Chinese state media. In particular, it aims to stimulate and build the resilience of each individual citizen and of society as a whole by promoting a specific resilience against foreign influences, rooted in Chinese culture.

ARABIC

al-muruuna al-ijtimaa'iyya = societal resilience. The ability of society to cope and adapt to pressures such as social or economic change.

al-qadra 'ala al-sumud = the ability to withstand, resist, oppose. The ability to overcome difficulties by active resistance.

Resilience understood as a certain flexibility or a capability by a society to adapt fast to new challenges and political measures imposed from those in power. Moreover, it is understood as the resilience of a society or population that actively resists oppression.

GOVERNANCE SPACE (Domestic/Foreign policy – understanding/usage of resilience)

RUSSIAN

stressoustoichovost' = stress resistance, or stress tolerance. The ability to resist external pressure.

Resilience understood as the ability of countries to be resistant to hostile foreign policy interference.

CHINESE

renxing yuan yu minzhong guangfan zhichi = toughness of the political regime. The ability to provide stability.

zhengzi mianyili = political immunity. The ability to resist foreign influences.

wenhua zixin = cultural confidence. The ability to be resilient against the spread of Western values and political influence.

bu zhan er sheng = winning without fighting. The ability to defeat the opponent without a fight by having enough resilience.

fan bingjia zhi fa yao zai yingbian = military strategies must be adaptable. The ability to engage with the opponent and build specific resilience.

With regard to domestic policy, resilience is used to describe the stability of one's own system and generate legitimacy. With regard to foreign policy, resilience is used to refer to the ability to resist foreign influences. From a strategic/military perspective, resilience is used to describe a high defensive capacity that prevents attacks.

ARABIC

muruuna al-dawla = resilience of the state. The ability of the state to withstand and respond to challenges.

muruuna al-siyaasiyya = political flexibility. The ability to be flexible to respond to unexpected and challenging changes.

Resilience used to refer to the ability of a state or a region to deal with problems such as poverty, corruption, or poor governance. Moreover, it refers also to the ability to resist foreign sanctions.

SERVICES SPACE (Economic/Financial policy – understanding/usage of resilience)

RUSSIAN

ustoichivost' = durability, stability. The ability to resist, to withstand blows, to survive and recover.

shokoustoichivost' = shock resistance. The ability to adequately respond to external disturbing influences.

Resilience understood as the ability of a (regional) system to withstand economic and financial shocks, including the ability to anticipate, prevent, resist, absorb, react, adapt, and recover.

CHINESE

tanxing = flexibility. The ability to overcome economic hardships.

renxing = toughness. The ability to cope with a changing global and domestic economic situation.

Resilience used to refer to the strength and adaptability of the Chinese economy in the context of a perceived hostile US economic policy.

ARABIC

salaaba = becoming hard, firm, solid, stiff, or rigid. The ability of being able to withstand economic hardship.

Resilience used to refer to the ability to recover economically from the negative effects of the COVID-19 pandemic.

1.4. Conclusion

When mapping the concept of resilience in English, Russian, Chinese and Arabic, the understanding of resilience in the respective cultures has similarities but also noteworthy differences. In this way the concept of resilience becomes more comprehensive, including ideas that resilience is support of the people, maintenance of lifestyle, adaptation to various conditions, cultural confidence and the ability to stand your own ground and manage resources.

This report, starting from the established concepts of resilience, will expand the understanding of resilience into the hybrid threat framework – which, as will be shown, differs from traditional thinking on resilience.

HIGHLIGHTS

The concept of resilience has become increasingly relevant in both EU and NATO discourse over the last twenty years. Moreover, over the last five years, the EU and NATO have increasingly linked resilience to the fight against hybrid threats and approached the concept from a more holistic perspective. At the same time, hybrid threats have played an increasingly important role in EU policy over the last decade, as the security environment of the European Union has changed dramatically and the Union has to adapt accordingly. The new EU and NATO core documents therefore describe resilience as a crucial element in preventing and protecting against hybrid threats.

The approach of this report is to combine resilience and hybrid threats in one new systemic approach. To increase resilience to hybrid threats, the EU must be understood as a comprehensive yet complex system in which multiple interconnected adaptive systems (spaces, layers and domains) interact synchronously.

RESILIENCE IN THE CONTEXT OF HYBRID THREATS

EU AND NATO PERSPECTIVE

The concept of resilience has been increasingly present in both EU and NATO discourses over the last twenty years. In the EU context, resilience was initially applied during 2000s to technical systems, critical infrastructure protection, and crisis management.[8] It was mainstreamed into policy making in 2017 with the European Union Global strategy 'Shared Vision, Common Action: A Stronger Europe' (EEAS, 2017). Especially since the outbreak of the COVID-19 pandemic, resilience has become a key element in the EU's recovery plans (European Commission 2020b; 2020c). It became a new compass for EU policymaking (European Commission 2020a; 2021), in the different strategic goals of the EU Security Union Strategy (European Commission, 2020d), and in the Strategic Compass (Council of the European Union, 2022).

> To build resilience against hybrid threats, the EU should be understood as a comprehensive yet complex system. Resilience measures taken in one area can have effects in another.

Since its inception in 1949, NATO has considered resilience as a core element for 'maintain[ing] and develop[ing] their individual and collective capacity to resist armed attack' (NATO, 2021a), and has believed resilience to be 'NATO's first line of defence' (NATO, 2020) but 'first and foremost a national responsibility' (NATO, 2021a). In response to the pandemic, NATO has strengthened its commitment to enhance national and collective resilience from a broad approach and highlighted the importance of civil-military engagement and

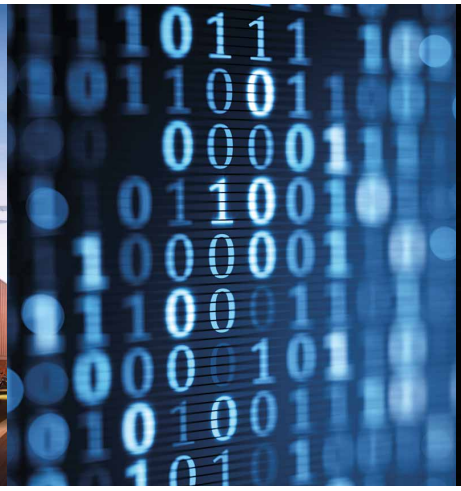
8 With the EC COM(2004) 702 (see European Commission (2004)), the EC Green Paper (see European Commission (2005)), the EPCIP Communication (see European Commission (2006)), the ECI Directive (see Council of the European Union (2008)) and the Revised ECIP 2013 (see European Commission (2013)).

cooperation (NATO, 2021b). In addition, over the last five years the EU and NATO have increasingly linked resilience with countering hybrid threats, approaching the concept from a more holistic perspective.

TABLE 2. References to hybrid threats since 2010 at EU and NATO levels.

	DOCUMENT	TITLE	RELEVANCE OF THE DOCUMENT AS WRITTEN IN THE TEXT
2010	NATO' Strategic Concept **NATO**		'Vigilance, prevention, resilience and commitment to our fundamental values' were argued to be the best response in the fight against terrorism
2015	Consilium 8971/15	**Council Conclusions on Common Security and Defence Policy (CSDP)**	Called for a 'joint framework with actionable proposals to help counter hybrid threats and foster the resilience of the EU and Member States, as well as partners'.
2016	JOIN(2016)18 final	**Joint Framework on countering hybrid threats**	Bringing hybrid threats to the focus of policymaking, and proposing 22 actions to counter hybrid threats, most of which recognised resilience as a key element.
	Warsaw Summit **NATO**		Heads of State and Government committed to enhance their resilience against 'the full spectrum of threats, including hybrid threats, from any direction'.
	Warsaw Summit **NATO**	**Commitment to achieve seven baseline requirements (7BLR) for civil preparedness**	These stressed the relevance of ensuring the 'continuity of government, essential services, and civil support to the military', and were designed in an interconnected way, reflecting that if one area was impacted, others could be impacted as a result.
		Shared Vision, Common Action: A Stronger Europe — European Global Strategy	Mainstreamed the concept into policy making.
2018	JOIN/2018/16 final	**Increasing resilience and bolstering capabilities to address hybrid threats**	Importance of building resilience to counter hybrid threats was reiterated and expanded to sectors such as CBRN and cyber threats.
2019	Council Conclusions, 14972/19	**Complementary efforts to enhance resilience and counter hybrid threats**	The Council '(expressed) its continued commitment to strengthening the Union's and its Member States' resilience to multi-faceted and ever-evolving hybrid threats and enhancing cooperation to detect, prevent and counter them.
2020	COM/2020/456 final	**Europe's moment: Repair and Prepare for the Next Generation**	Must guide and build a more sustainable, resilient and fairer Europe for the next generation.
	JOIN(2020) 8 final	**Tackling COVID-19 disinformation - Getting the facts right**	Proposed among others things a 'calibrated response (...) from all parts of society' and to build resilience of citizens against disinformation.

	DOCUMENT	TITLE	RELEVANCE OF THE DOCUMENT AS WRITTEN IN THE TEXT
	Council Conclusions, 8910/20	**Council Conclusions on Security and Defence**	'The EU is facing an already challenging international environment in which the unprecedented COVID-19 pandemic risks are amplifying existing global fragilities and tensions. This calls for more European unity, solidarity and resilience [...]'. Furthermore, in relation to hybrid threats, the Council called for 'stepping up efforts at national level and regarding EU policies and legislative initiatives to counter hybrid threats, [...] [and] for improving the EU's preparedness and its autonomous analysis capacity to deal with hybrid threats and to help increase partners' resilience', and encouraged the 'EU institutions, together with the Member States, to further work (...) to enhance the resilience and the security culture of the EU against cyber and hybrid threats'.
	SWD (2020) 152 final	**Joint Staff Working Document Mapping of measures related to enhancing resilience and countering hybrid threats**	Almost 200 measures were mapped, reflecting the relevance and interconnection between the two fields, resilience and hybrid threats, and the effort taken by EU institutions to reinforce them during the last years.
	COM(2020) 605 final	**EU Security Union Strategy**	'[F]ocuses on building capabilities and capacities to secure a future-proof security environment [...] and sets out a whole-of-society approach to security that can effectively respond to a rapidly-changing threat landscape in a coordinated manner'.
2020		**2020 Strategic Foresight Report**	Resilience as new Compass for EU policies.
2021		**The landscape of hybrid threats: A conceptual model**	The proposed conceptual model provides a narrative with a respective visual representation and depicts the main concepts and variables and more importantly their relationships. More specifically, the conceptual model is developed around 4 main pillars: Actors (and their strategic objectives), domains, tools, and phases.
2022	Joint SWD(2022)21 final	**'Joint Staff Working Document: Identification of sectorial hybrid resilience baselines'**	'The 2020 EU Security Union Strategy underlines the need to build resilience to prevent and protect the EU against hybrid threats and the importance to systematically track and objectively measure progress in this area: "Building resilience is central to preventing and protecting against hybrid threats. It is therefore crucial to systematically track and objectively measure progress in this area. A first step will be to identify sectoral hybrid resilience baselines for both Member States and EU institutions and bodies.' The objective of this Joint Staff Working document is to contribute to this task by listing existing and proposed sectoral EU-legislation and policy documents, which contain elements of hybrid resilience baselines at EU level.'
	7371/22	**A Strategic Compass for Security and Defence**	'The Compass gives the European Union an ambitious plan of action for strengthening the EU's security and defence policy by 2030. The more hostile security environment requires us to make a quantum leap forward and increase our capacity and willingness to act, strengthen our resilience, and invest more and better in our defence capabilities.'


Hybrid threats start to figure in EU policies over the last decade, prompted by dramatic changes in the European Union's security environment and the need for the Union to adapt accordingly. The 2015 Council Conclusions on Common Security and Defence Policy (CSDP) called for a 'joint framework with actionable proposals to help counter hybrid threats and foster the resilience of the EU and Member States, as well as partners' (Council of the European Union, 2015, p.3). The 'Joint Framework on countering hybrid threats' (European Commission, 2016) was published a year later, bringing hybrid threats to the focus of policymaking, and proposing 22 actions to counter hybrid threats, most of which recognised resilience[9] as a key element. This framework was followed by the communication on 'Increasing resilience and bolstering capabilities to address hybrid threats' in which the importance of building resilience to counter hybrid threats was reiterated and expanded to sectors such as CBRN[10] and cyber threats (European Commission, 2016).

Following a 2019 Council conclusion (Council of the European Union, 2019), almost 200 measures were mapped in the 'Joint Staff Working Document Mapping of measures related to enhancing resilience and countering hybrid threats' which was published in 2020 (European Commission, 2020e). These measures reflected the relevance and interconnection between the two fields – resilience and hybrid threats – and the efforts made by EU institutions to reinforce them during the last years.

However, the mapping of these measures highlighted what has already been noted, namely that sectors such as infrastructure, cyber, and space had received the highest attention to the detriment of others such as culture, political, and intelligence. It also indicated that while resilience had gained a strategic role in the EU agenda, it was still primarily thought of from a sectoral perspective.[11]

In the interim, given its mandate, NATO's approach to resilience had been primarily linked to the military/defence domain. Ensuring resilience against an attack or disruption to communication, transport and transit routes were highlighted in 2010. NATO's Strategic Concept (NATO, 2010): 'vigilance, prevention, resilience and commitment to our fundamental values' were argued to be the best response in the fight against terrorism (NATO, 2011; 2012); and the internal cohesion and resilience of the Alliance were highlighted in the

9 In the JOIN (2016)18 final (European Commission, 2016), resilience is understood as 'the capacity to withstand stress and recover, strengthened from challenges' (p.5).

10 Taking into account targeted attacks on civilians inside the EU using CBRN (chemical, biological, radiological and nuclear) agents, such as the poisoning of Sergei and Yulia Skripal with a Russian chemical warfare agent.

11 Which to a certain extent also reflects the different competences of the EU vs. the competences of the Member States.

light of the Russian annexation of Crimea in 2014 (NATO, 2014). At the 2016 Warsaw Summit, Heads of State and Government committed to enhance their resilience against '*the full spectrum of threats, including hybrid threats, from any direction*' (NATO, 2016).

Furthermore, they agreed on seven baseline requirements (7BLR) for national resilience against which Member States could measure their level of preparedness. These stressed the relevance of ensuring the continuity of government, essential services, and civil support to the military (NATO, 2021a), and were designed in an interconnected way, reflecting that, if one area was impacted, other(s) could be impacted as a result.

In early 2020, the COVID-19 crisis, the unprecedented disruptions that the pandemic directly inflicted on societies, and the opportunistic exploitation of both by hybrid threat actors **brought the concepts of resilience and hybrid threats into the centre of policymaking**. The pandemic exposed existing vulnerabilities and enabled Member States, the EU and NATO to assess their levels of resilience and reaction capabilities in different sectors. Accordingly, both the EU and NATO applied the lessons learned to their policies.

Resilience plays a key role in the EU's measures, such as the EU recovery plan. In addition, Member States welcomed the reviews of existing Directives, such as the Critical Infrastructure Directive of 2008 and the Network and Information Security (NIS2) Directive, to accommodate the resilience of critical entities to evolving challenges, such as hybrid threats. The European Commissions Strategic Foresight Report saw resilience 'as the new compass for EU policies' (European Commission 2020a). It defines resilience as the 'ability not only to withstand and cope with challenges but also to undergo transitions in a sustainable, fair, and democratic manner.' This definition is close to the **proactive understanding** of resilience described above: a society proactively undergoes transition in order to be more resilient in the future. Here, transition must be coupled to strategic foresight for the transition to occur in the right direction.

> "It defines resilience as the ability not only to withstand and cope with challenges but also to undergo transitions in a sustainable, fair, and democratic manner."

To this end, the Commission came up with a generic conceptualisation of resilience and with the corresponding dashboard of measures in order to support resilience-building (European Commission 2020a; 2021a). This dashboard – which gives indicators for the social and economic, green, digital, and geopolitical dimensions – has been thoroughly considered in the present work. Nevertheless, in the case of hybrid threats, building resilience requires some specific attributes. This report has also taken as a starting point systemic thinking and the holistic approach. However, a tailor-made approach is proposed, which addresses the specificities of hybrid threats and the respective challenges for building resilience.

The need for building resilience was also highlighted in the Council Conclusions on Security and Defence (8910/20) (Council of the European Union, 2020) which called for 'more European unity, solidarity and resilience' (p.2). On 21 March 2022,

the Council approved the **'Strategic Compass'** (Council of the European Union, 2022), a new approach designed to strengthen European security and defence policy.

Resilience was also highlighted as a crucial element for the security of Member States and the EU in the **EU Security Union Strategy**. In order to develop a better response to hybrid threats, the EU Security Union Strategy proposed to 'mainstream hybrid considerations into policy making' and remarked the central role of resilience in preventing and protecting against hybrid threats. To this end, it encouraged the identification of sectoral hybrid resilience baselines for both Member States and EU institutions and bodies.

A staff working document contributing to this task was released on 26 January 2022,[12] and already included the domains approach of the JRC/Hybrid CoE Conceptual framework. It lists existing and proposed sectoral EU-legislation and policy documents, which contain elements of hybrid resilience baselines at EU level. 53 resilience baseline elements have been identified for enhancing resilience and countering hybrid threats. This identification complements the mapping of measures related to enhancing resilience and countering hybrid threats (European Commission, 2020e).

The impact of the COVID-19 pandemic was also reflected in NATO's approach to resilience. The pandemic tested resilience in NATO and its allies, who continuously worked to 'enhance preparedness across the whole of government, especially in the health sector' (NATO, 2021a) and kept monitoring and assessing the impact of the crisis on an ongoing basis, facilitating the exchange of

12 Joint SWD (2022)21 final 'Joint Staff Working Document: Identification of sectorial hybrid resilience baselines' (internal document — not publicly accessible).

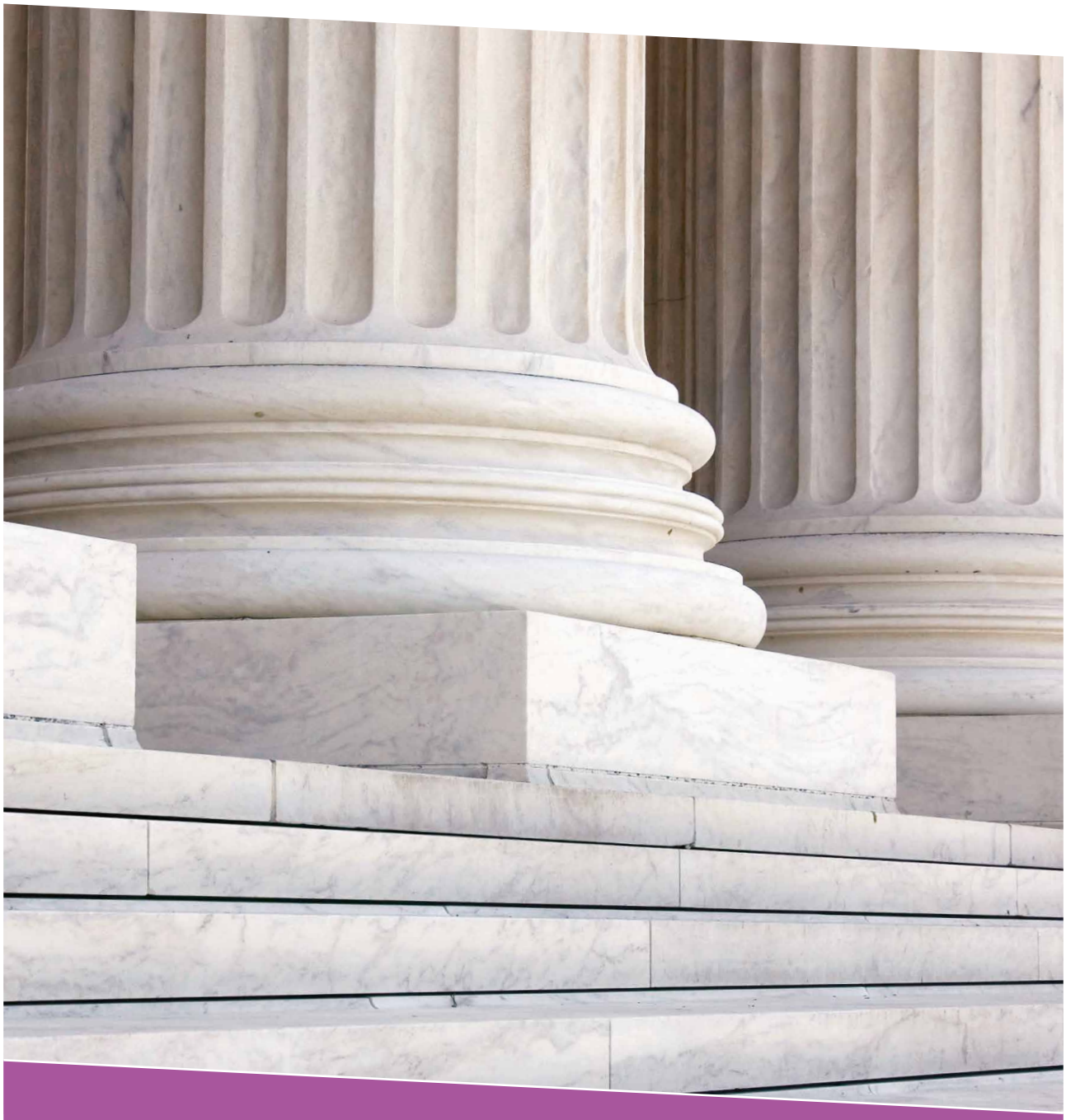
> “In order to build resilience against hybrid threats, the EU should be understood as a comprehensive yet complex system, in which several interconnected systems must be considered.”

information and best practices among allies. In 2020, the seven baseline requirements (7BLR) were updated to reflect the implications of the pandemic, as well as the challenges posed by emerging communication technologies. In addition, the commitment to resilience was strengthened at the 2021 Brussels Summit, where the Allies agreed a ‘Strengthened Resilience Commitment’ that set out future steps, and addressed resilience from a broad approach, including ‘work across the whole of government, with the private and non-governmental sectors, with programmes and centres of expertise on resilience established by Allies, and with our societies and populations, to strengthen the resilience of our nations and societies’ (NATO, 2021b).

2.1 Conclusion: Resilience and hybrid threats – a new approach

Resilience effectively functions as a mechanism that helps emphasise strengths instead of problems and challenges. In the hybrid threat context, this means considering the other side of the coin – in addition to looking for vulnerabilities, which needs to precede resilience-building, resilience as a concept leads us to think about our own abilities and strengths, and how these can be harnessed to counter hybrid threat activities in an innovative and creative way. Simply put, just as a hybrid threat can target one sector and have a negative effect on another (e.g., a cyber-attack can have a negative effect in the society domain), resilience measures taken in one area can have a positive effect in another.

We therefore argue that **in order to build resilience against hybrid threats, the EU should be understood as a comprehensive yet complex system, in which several interconnected adaptive systems (spaces, layers and domains) and which interact synchronically, must be considered.** The paradigm shift on security undergone by the EU and NATO in order to respond to continuously evolving hybrid threats is also reflected in the way we build resilience against such threats.



HIGHLIGHTS

Hybrid threats always aim to damage and undermine democratic systems by destroying the foundations on which they are based. These foundations, in turn, are the prerequisite for resilience and democracies needed to strengthen them in order to protect themselves against hybrid threats. At the heart of all foundations is trust, which is essentially the glue that makes dependencies and connections strong and healthy in democracies and supports the foundations of democratic systems.

The seven foundations introduced in this report that are essential for building trust are (1) feeling of justice and equal treatment, (2) civil rights and liberties, (3) political responsibility and accountability, (4) rule of law, (5) stability, (6) reliability / availability, and (7) foresight capabilities. These seven foundations are the basis of very resilient, democratic society and are essential in building resilience against hybrid threats.

FOUNDATIONS OF THE DEMOCRATIC SYSTEM

3.1. Introduction

Hybrid threat activity always aims to harm and undermine democratic systems. This means that when thinking about resilience in the context of hybrid threats, we need to be able to identify the core foundations that are targeted by hybrid threat actors. In this report seven core foundations are introduced. These foundations are based on the values, norms and expectations of democratic societies.

Strong foundations are a prerequisite to resilience against hybrid threats. This is one more aspect that distinguishes conventional resilience from resilience against hybrid threats. While conventional resilience emphasises technical capabilities and recovery – the ability to survive shocks – resilience against hybrid threats also safeguards democratic processes.

> Trust makes dependencies and connections strong and healthy and supports the foundations of democratic systems whereas hybrid threat actors seek to erode trust in the democratic process.

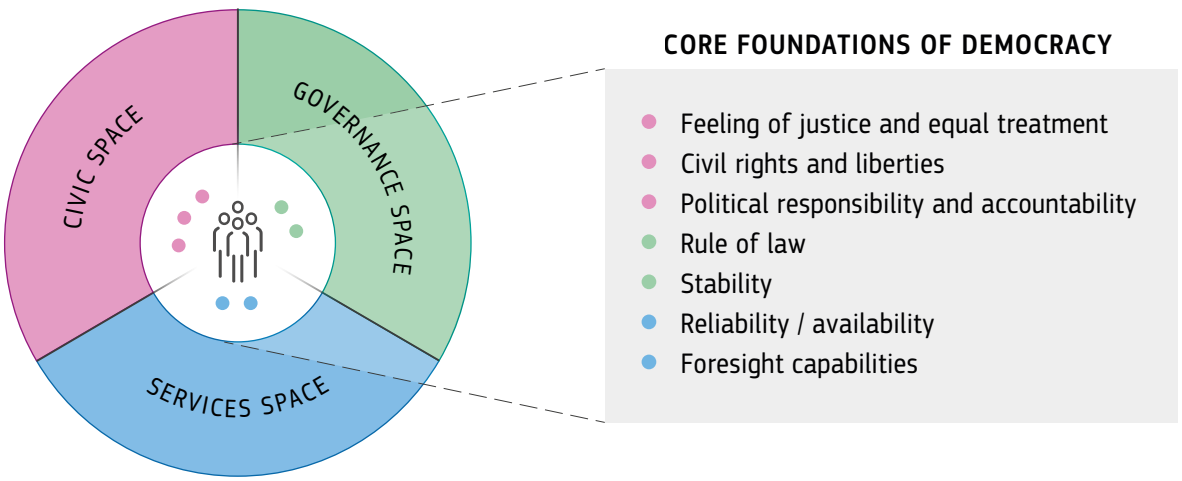
Safeguarding democratic processes has become ever more important. The past two decades have witnessed a slow erosion of some of the key foundations of democracies (O'Donnell, 1995). Erosion of the foundations of democracy can lead to autocratisation effects. Since 1994, 70% of cases of autocratisation were as a result of democratic erosion rather than quick takeovers of power (Lührmann & Lindberg, 2019). This gives us an indication that we have first and foremost to understand our own societies, their weaknesses and strengths, if we are to be able to protect our democratic systems.

To safeguard democratic processes effectively, we need to consider trust as the force that binds societies together. Francis Fukuyama has argued that societies with high levels of trust thrive contrary to low trust societies. There are three main reasons why trust is essential for resilience (Chesley & Amitrano, 2015). First, trust brings greater predictability. For the civic space this

> “To safeguard democratic processes effectively, we need to consider trust as the force that binds societies together.”

means that government will do what it is expected to do. Secondly, trust is essential for the reactive and transformative parts of resilience since during times of change citizens are more willing to follow trusted leaders and hence implement change. Thirdly, trust affects how people communicate and how people assess the honesty and validity of what is being communicated. Trust is therefore essentially the glue that makes dependencies and connections strong and healthy in democracies as well as supports the foundations of democratic system. It is precisely this that hybrid threat actors seek – to turn dependencies into vulnerabilities and use connections to weaken the foundations of democratic societies. This lack of trust affects a society’s capacity to absorb shocks, recover quickly, adapt, innovate and develop further, which in turn will erode the foundations of the democratic system. The seven foundations essential to trust building are presented below.

FIG 2. The seven foundations of democratic societies



3.2. The seven foundations

Feeling of justice and equal treatment – Civic life in liberal democracies is based on the citizens' trust that their rights, identity and property will be protected against abuse by political, social, economic or military power.[13] A feeling of justice and equal treatment goes beyond but is intimately linked to the rule of law and legality. It also entails unwritten rules for interaction and creates a community of trust and belonging in society. The feeling of justice and equal treatment is much more subjective than objective. The civic space is especially prone to passions and emotions which increase the subjective nature of these building blocks. However, without the feeling of justice in the civic space, it is hard to maintain stable and resilient societies. This foundation is connected to the rule of law.

Civil rights and liberties – Civic life in democracies relies on the twin bedrocks of civil rights and liberties.[14] Civil rights include the right to vote, the right to a fair trial, the right to government services, the right to a public education, and the right to use public facilities etc. Civil rights are a central component of democracy. If individuals are being denied opportunities to participate in political society, they are being denied their civil rights (Britannica, 2022).

Liberties are those freedoms that allow the citizenry to exist as a sovereign in the public space: freedom of assembly, freedom of expression, freedom of movement, freedom of thought, freedom of religion etc. Freedoms relate to the capacity of citizens to organise and have a voice in the political system. Individual freedoms safeguard the rights of individual citizens in the public and private spheres. Civil rights and liberties are interdependent.

Political responsibility and accountability – The civic life of democracies revolves around a system of political responsibility and accountability of political leaders (Rosanvallon, 2020). The people / citizenry is sovereign, and it delegates its sovereignty to representatives by the means and institutions of election. Representation is at the heart of liberal democracy: free and fair elections allow a debate of ideas over the direction of the civic space. Elections constitute a mandate for a given representative parliament and government to deliberate and take decisions for the greater interest of the citizenry in the name of the people's sovereignty. Political responsibility and accountability is an essential building block of resilience in the civic space because it gives a clear mechanism to correct courses. Here the election processes play a key role.

Rule of law – In its simplicity rule of law is that all political power must be based on law. In a liberal democracy, governance institutions – especially

"The civic life of democracies revolves around a system of political responsibility and accountability of political leaders."

13 Democracies have committed themselves to a set of values that protects their citizens' rights against abuse. The Lisbon Treaty (adopted in 2007) that sets the current form of the European Union and its functioning, commits to defend 'Rights of a human person, freedom, democracy, equality and the rule of law,' (Lisbon treaty art. 1 of the Preamble) as well as 'Human dignity, freedom, democracy, equality and respect of human rights, pluralism, non-discrimination, tolerance, justice, solidarity and equality between men and women' (Lisbon treaty art. 1 of the General Provisions) (European Union, 2010).

14 Liberalism is above all a doctrine that aims at limiting the power of the state as a safeguard to civil rights and liberties (Raynaud, 2008).

the executive, legislative and judiciary powers, as well as law-enforcement and defence institutions – execute their mandates, stemming from national sovereignty with clear constrains as to their functions and the extent of their possibility to act. The limitation of power through its division among diverse balancing entities is the essence of liberal democratic governance, so that no single entity can abuse its power. A clear framework of separation of powers, checks and balances and accountability are key to the legality – meaning regulation by law – of public and private life. Annual Reports on the State of Democracy, Rule of Law and Human Rights by the Secretary General of the Council of Europe remind us of the criticality of the rule of law, its participative character and inclusivity for reaching a more perfect democracy. Deepening divides that relate to the rule of law or, for instance, cases of corruption, are efficient ways of undermining the perception that liberal democracies are governed by the rule of law (Council of Europe, 2021).

Stability – An essential function of governance in a liberal democracy is to provide for the stability of public and private life. Stability is the quality that stems from the fairness, transparency, and predictability of the work of governance institutions and how they relate to the civic space actors by maintaining a virtuous trust relationship. Stability is an essential expectation under the social contract whereby individuals accept to delegate their powers and limit their immediate freedoms in society (Thrasher & Vallier, 2013). Theories of the social contract insist on the delegation of freedom from individuals to the state in order for the latter to preserve the necessary stability for every individual to enjoy their individual freedoms, also private property rights and public freedoms. Stability is essential for the private sector (subsequently "Service space") with regard to private property, safety of investments, the business environment and common market rules. The perception that governance actors are providing stability is a key foundation that can be relatively easily targeted by hybrid threat activity.

Reliability / availability – This factor encompasses the connection between public and private sectors in the democratic system. Without reliable services trust between the civic space and governance space is difficult. Here, the role of the service space

is key. A complex logistical system maintains the constant distribution of goods and services. All these systems are also interlinked. A disruption of one system can lead to cascading effects that halt the delivery of essential services (Greenberg, 2018). It is not just immediate supply of goods and services that matter. The vitality of the economy has a longer impact on a society's prospects. The more trade potential, the more investment, the more activity, the better foundation for collection of taxes, the better development of the public sector. Positive prospects increase trust and vice versa. In the field of hybrid threats, adversarial interests often benefit from fading trust in the targeted societies, which can be undermined by a perception of unavailability / unreliability of systems. Undermining the services space portrays the image of a failed governance and inability to provide reliability, thus generating further vulnerabilities to hybrid threats (Cullen et al., 2021).

The consequences of the COVID-19 crisis management have underlined the criticality of supply and value chains for the smooth functioning of society. Global interdependencies have put a stress on the efficiency of goods and services delivery, which has impacted on the perception of reliability and stability, while raising questions as to why governance institutions failed to anticipate disruptions in goods and services provision on such a scale. The reliability and availability of goods and services have a tremendous impact on people's perception that their governance institutions ensure stability and predictability.

Foresight capabilities – Vital systems supporting livelihood were often established by states or other public sector actors. In the contemporary economy, they are mostly privately owned companies, and no longer under public sector control. Globalisation has further led to a deregulation of global markets and disintermediation of finance, with a growing pre-eminence of private entities. The ability to foresee disruptions, and therefore prepare in time, is a key foundation because of the criticality of delivery of goods and services for the regular functioning of society. Foresight capabilities must be considered essential to keep up with trends, innovate and to avoid disruptions and cascading effects of shortages or unreliability. Foresight in the context of an interconnected world requires intense public-private cooperation at multiple layers of responsibilities.

3.3. Conclusion

The **seven foundations** presented above are also the basis of very resilient, democratic societies and are essential in building resilience against hybrid threats. Only by understanding that the aim of hybrid threat activity is to undermine democracy by eroding trust can progress be made.

These seven foundations introduced here thus represent the key focal points of a more strategic approach to resilience building. In the following chapter, the seven foundations are placed at the core of the ecosystem model.

HIGHLIGHTS

The aim of a hostile actor by utilising hybrid threats is to undermine and harm the integrity and functioning of democracies, to change decision-making processes, and to create cascading effects. This report presents a comprehensive resilience ecosystem (CORE) to better understand and mitigate against the actions and objectives of hostile actors. CORE enables us to model the entire society, thus creating a better understanding of the whole-of-society concept in the context of hybrid threats and enabling us to track the impact of hybrid threats on the entire society as well as to derive targeted resilience-building measures.

The ecosystem approach represents the interaction dynamics linking the 13 domains from the conceptual framework with three spaces (civic, governance, services) and their layers (local, national, international). We suggest it as a practical device to enhance understanding of the effects of hybrid threats and offer guidance on how to build resilience against them.

THINKING RESILIENCE TO HYBRID THREATS

A COMPREHENSIVE RESILIENCE ECOSYSTEM (CORE)

4.1. Introduction

The aim of hybrid threat activity is to constrain the freedom of manoeuvre of democracies in order to discredit its model compared to authoritarian regimes. Therefore, the aim and intent of the hostile actor is to:

- **undermine and harm the integrity and functioning of democracies**, by targeting vulnerabilities of different domains, creating new vulnerabilities through interference activity, exploiting any seams, creating maximum ambiguity and undermining trust of citizens in democratic institutions;

- **change the decision-making processes**, by blurring situational awareness, exploiting gaps in information flows, intimidating individuals and creating fear factors in target societies;

- **create cascading effects** by using a tailor-made combination from the 13 domains of the conceptual model to challenge and overload even the best-prepared systems. This can result in unpredicted consequences.

Resilience to hybrid threats should be thought of from the outset as resilience against the aims and intents of the hostile actor, notably the three aims outlined above. Essentially, it is a 'whole of society' resilience, which safeguards the seven foundations presented in the previous chapter. The methodology that we will present in the following will:

> To build resilience against hybrid threats a systems-thinking approach to the EU ecosystem is needed which must also include anticipation of an adversary's strategic goals.

- introduce a method that will allow the whole of society to be modelled;

- create a better understanding of the concept of whole of society in the context of hybrid threats;

- show a method that allows the tracking of effects of hybrid threat activities throughout society;

- ultimately, facilitate targeted resilience-building measures.

4.1.1. Why we need the ecosystem

Resilience against hybrid threats can take advantage of the resilience measures of different domains. But this is insufficient, since the character of hybrid threats is ambiguous, creative, uses decoys, blurs the situational awareness, targets a wide range of domains, and continues to seek and create new vulnerabilities to exploit. In the conceptual model 13 domains were explored to highlight the tools that hostile actors can use and how those tools can be combined. This showed how, in the hybrid threat security environment, there are multiple domains that the hostile actor is using, with a very comprehensive approach.

> “The comprehensive resilience ecosystem can promote cross-sectoral, whole-of-society effort by taking stock of the crucial interlinkages between issues often addressed separately within different spaces.”

The comprehensive resilience ecosystem can promote cross-sectoral, whole-of-society effort by taking stock of the crucial interlinkages between issues often addressed separately within different spaces. It provides a methodology to achieve a better understanding of the behaviour between complex systems, institutions and societal factors and improves the assessment of the cascading effects of hybrid threats and effects of policy interventions. Building on the 13 domains of the conceptual model, the comprehensive resilience ecosystem will facilitate the development of an effective hybrid toolbox.

The **ecosystem** approach represents the interaction dynamics that connect **domains** with three **spaces** and their **layers**. Domains are considered as the entry points and through them attacks can spread to different spaces and their respective layers.

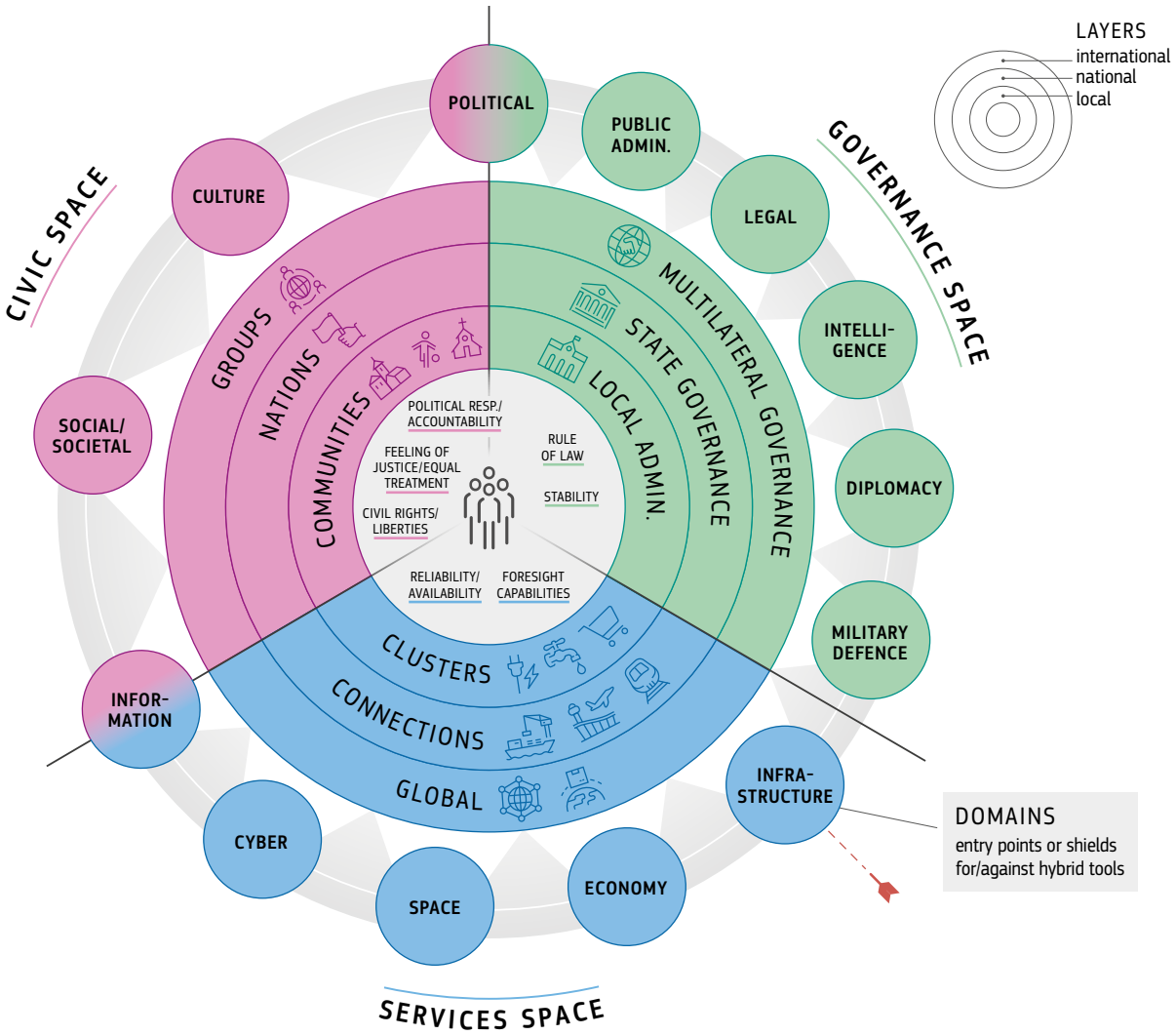
Hence, building resilience against hybrid threats means taking into account the following key elements:

5. **Capability of the adversary to alter our decision-making to align our goals with their strategic goals** – it is therefore necessary to know the strategic goals of the enemy as well as to know ourselves and to clarify our strategic goals. Foresight can play a crucial role in this process.

6. **Undermine the democratic foundations** – hybrid threat actors ultimately want to challenge the foundations of democratic societies, i.e. the values, norms and expectations of democratic societies. These must be especially protected, as a democratic society can regrow from them, even after a severe crisis.

7. **Synchronised use of different tools** – this can lead to a situation in which the different parts of the EU and/or MS are under constant stress. There is a possibility that the ecosystem has to continuously absorb negative impacts and

FIG 3. The comprehensive resilience ecosystem



to respond to their effects without the chance to recover and to (better) prepare for the next event – both of which are an integral part of resilience-building. If focus is only on the domains that are initially targeted, recovery in one domain might leave other domains vulnerable.

8. **Cascading effects that might occur across domains, spaces and layers** – resilience against hybrid threats is not (only) resilience against a single tool, or resilience against the effect of one tool in one domain, but also resilience against the effects spreading across domains.

4.2. Foundations of the ecosystem

As described above, the **seven foundations** are the core and strength of the democratic system:

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

In this CORE model, the foundations are in the centre and are surrounded by the different layers

> “When we re-think building resilience as a cross-domain issue, it becomes clear that the resilience of the entire EU or MS ecosystem is more than the sum of the domain-specific resilience.”

of society as well as by the domains, which can act as shields against – as well as entry points for – hybrid threat activities.

4.3. Role of domains in the ecosystem

The interconnections, dependencies and links of the various domains which constitute the fabric of our society need to be considered. When we re-think building resilience as a cross-domain issue, it becomes clear that the resilience of the entire EU or MS ecosystem is more than the sum of the domain-specific resilience. It is possible that building resilience in one part of the EU or MS ecosystem might (positively or negatively) influence the resilience of other parts of the ecosystem. The sum of domain-specific resilience is not equal to the resilience of the whole ecosystem nor is it the weakest link. In the best case, by increasing resilience in one part of the ecosystem, resilience is increased over the whole system. In the worst case, it is decreased.

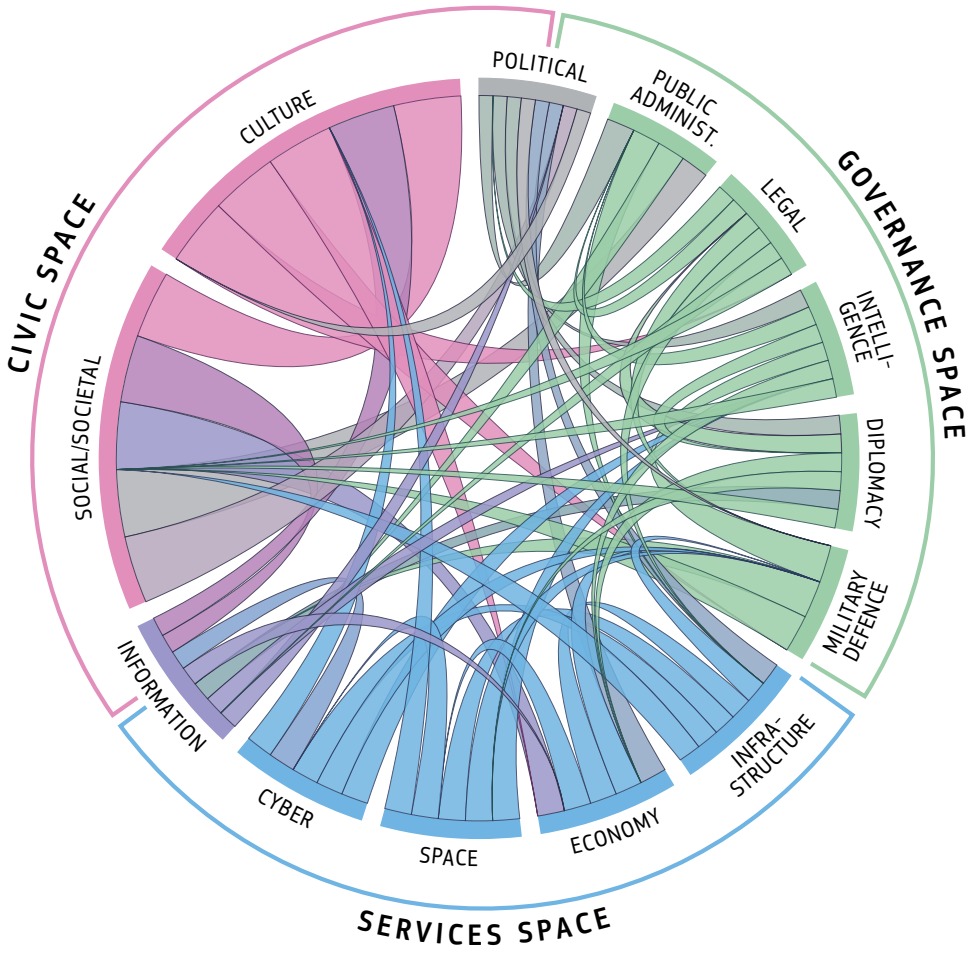
Furthermore, the interconnections between domains are crucial in building resilience against hybrid threats. As the effects of hybrid threats may spread across domains it is necessary to interrupt the spread and to contain the effects – much like building a ‘firewall’. This does not mean that domains should be disconnected but that the connections themselves need to become resilient. An obvious prerequisite is to be aware of these connections, as illustrated in *Figure 4.*

Without solid resilience in the different domains the ecosystem lacks an effective ‘shield’. In terms of resilience awareness and maturity, several domains are more advanced than others, with ‘infrastructure’ and ‘cyber’ recognised as having high resilience awareness and high maturity[15] Based on answers received from the Member States during the second iteration of the Hybrid Risk Survey (awareness) and on a semi-quantitative literature review (maturity) the domains *infrastructure* or *cyber* can be regarded as having high resilience awareness and high maturity. In contrast, domains like *culture* or *legal* have lower awareness and maturity. Given the complex interactions and connectivity between the domains, those which are less resilient can be the entry point for systemic failures and large-scale cascade effects.

A prerequisite for this holistic approach is an in-depth understanding of the level of maturity and preparedness with respect to resilience measures, practices and tools and awareness by authorities of the importance of building resilience in a specific domain for countering hybrid threats. Overall, to build resilience against hybrid threats

15 Based on answers received from the Member States during the second iteration of the Hybrid Risk Survey (awareness) and on a semi-quantitative literature review (maturity).

FIG 4. The connections between domains



a systems-thinking approach to the domains and interconnections of the ecosystem is needed, which must also include anticipation of the adversaries' strategic goals.

Further to our analysis of their maturity and vulnerability, the results for each domain are presented in the Annex to this report.

4.4. The three spaces of the ecosystem

The ecosystem that we propose consists of three spaces – civic, governance and services – which represent the three sectors of society. The domains are connected to the three spaces according to their relevance. Furthermore, the foundations of the ecosystem are also connected to specific spaces. In short, the ecosystem as well as each space can be imagined as consisting of domains, the connections between the domains as well as the relevant foundations. Together with the *layers*, which will be introduced below, this represents the whole-of-society approach.

4.4.1. The civic space

The civic space comprises those interactions that constitute the public life of societies – the collective and individual rights, duties, and liberties of citizens. Public life relates to three different layers: groups, nations and communities. The domains that are included in this space are notably the societal, cultural and, to some extent, also information and political domains. The civic space in

democracies rests on three foundations: justice and equal treatment; civil rights and liberties; political responsibility and accountability. The role of the governance space is, in turn, to enhance the resilience of the civic space by protecting the processes and institutions of democracy. Civic space resilience reduces the risk of outside interference. Social cohesion, efficient democratic deliberation, equal treatment and a culture of trust and discussion are key markers of a resilient civic space. The link between trust and increased level of resilience in the civic space can be identified. Trust is key in the feeling of security, the sense of predictability, and the maintenance of social cohesion. It marks confidence in society as a whole.

4.4.2. The governance space

The governance space is where public institutions exercise their mandates, regulate public and private life, take political decisions and are accountable to the body politic. The layers that are part of the governance space are local governance, state-level governance and multilateral governance. The relevant domains here are administration, diplomacy, legal, political, intelligence and military underpinned by the foundations of the rule of law, and stability. Resilience in governance space can be interpreted as maintaining the state of autonomy and freedom of action as a prerequisite. On the one hand, the governance space acts as an enabler of resilience for other spaces, as it plays a central role in the drafting of preparedness legislation, steering and development as well as in the implementation of preparedness measures and crisis management. On the other hand, resilience of governance itself is an objective, which ultimately translates into continuity of government, institutions and their operations at local, state and multilateral layers, in times of disturbance or crisis.

4.4.3. The services space

This space consists of systems, infrastructure, supply, logistics and value chains that are dependent on the private sector, while being essential to societal security. This space's three layers are *connections*, *clusters* and *global*. The domains that belong to the services space are *cyber*, *space*, *infrastructure*, *economy* and *information*. The foundations for this space are *reliability* (goods and services availability) and *foresight capability* (trends, future developments and possible disruptions). Resilience in the services space supports the good functioning of society by taming the effects of hybrid threat activity and lowering their disruptive potential. It can be achieved by stockpiling of essential goods, maintaining diversified and open markets, consultation, co-operation and coordination between the public and private sectors, a harmonising and coordinating regulative framework within a single market area, and systematic exchange of information.

4.5. Layers of the ecosystem

The layers of the ecosystem represent the different 'levels' that exist in the organisation of society, from local to international. Such a layering can be observed in all three spaces. The distinction is important, as the impact as well as the *modus operandi* of hybrid threat activity is different in the respective layers.

> "The layers of the ecosystem represent the different 'levels' that exist in the organisation of society, from local to international."

4.5.1. Local layers

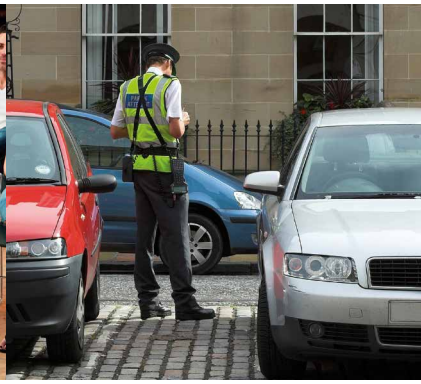
COMMUNITIES — Communities are made of individuals with objective or subjective affinities in politics, social, economic, cultural or other domains. Communities can be constituted over sectorial interests (economic and social), identity questions (religious, ethnic, gender, generational), ideological (protection of animals, environmental, gun-rights activists) or leisure related topics (e.g., hunting, swimming, or baking). They can also be entities that have a feeling of unity or belonging like villages, schools, neighbourhood. The communities are micro-level entities which are always very local. They are part of a nation and can have connection with communities that cross borders.



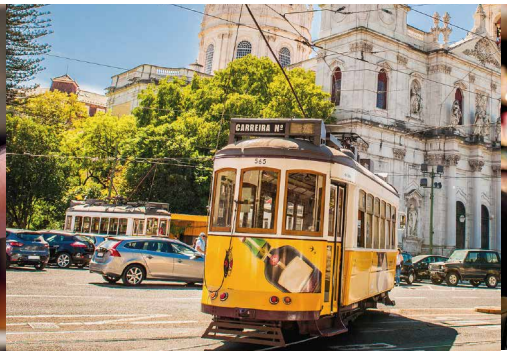
LOCAL ADMINISTRATION — A considerable proportion of the political decisions that affect people's everyday lives are made by municipal boards and councils as the local administration is often in charge of social services, health care and education for example. The role of the local level in the landscape of hybrid threats is increased further by the global trend towards urbanisation. It is also local government that has to respond to various disturbances, which might be caused by an outside actor (or not). Local government also interacts on a daily basis with all three layers of the civic space.

Today, more than half of the world's population lives in urban areas (UN News, 2014). Challenges to sustainable development, such as climate change, economic and social policy, integration and migration issues, are largely solved at the city level (UN Habitat, 2016). Cities are also focal points for social tension, while individual places within them may gain an enormous symbolic status in social movements. This means that, increasingly, cities may be targets of hybrid threats.





CLUSTERS — Clusters are the final link in supply chains for goods and services where they meet individual consumer demand. They can be heavily impacted by the connections and global layers of the services space, since supply and logistical chains are heavily dependent on global trends, disruptions in the world economy, as well as on disruptions in the 'connections' layer. Disruptions in both layers could leave the Clusters isolated and thrown back on their own capacities. For certain critical services and goods, this layer is also influenced by the governance space (for example, transportation networks are built and maintained by the state). The right balance of influence from the governance space has a direct influence on the resilience of the Clusters (for example, reaching strategic autonomy could be a defined goal). Through the Connections and Global levels, parallel Clusters will also influence each other (e.g., transportation of goods from one Cluster to another through global supply chains).

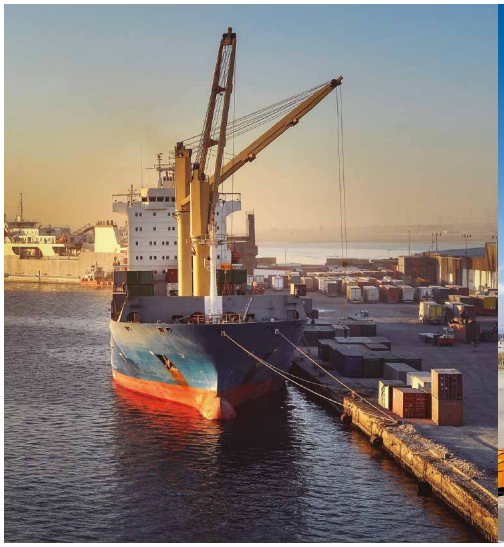


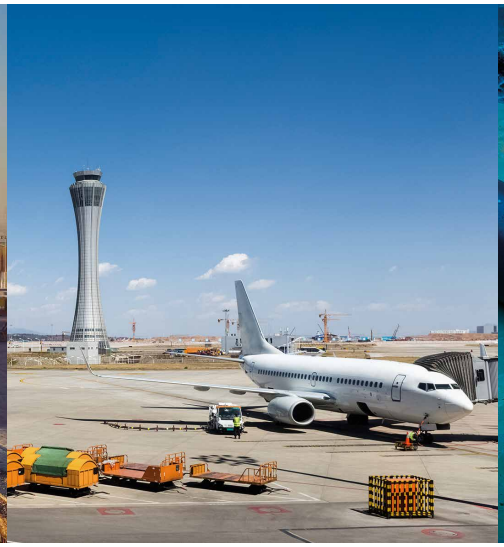
4.5.2. National layers

NATION — The concept of nation is understood differently in Eastern and Western cultures. The Eastern understanding is that the nation makes the state and the Western understanding is that the state makes the nation. Although a simplification, from the hybrid threat perspective, this is a very important difference. If the Eastern understanding is that the state is made by the nation, then this is also what needs to be broken before a state can be weakened. The concept of nation is also seen as a political or social construct, but a central source of unity. Nation is often seen to have a common narrative about its origin, the historical national continuity, language, territory, and traditions etc. – things that unite. Nation-building is connected to state-building and state-building to nation-building. It is this connection that has become even more important in today's world and merits further analysis. If an outside actor manages to break the link between nation and state, it has already managed to harm and undermine the state and its democratic system. This becomes even more complex when we are looking at the international level.

STATE LEVEL GOVERNANCE — A state is a sovereign legal entity which also has defined territory. The core state institutions (parliament, state administration, courts, army), are there to execute their legally defined functions and to maintain lawfulness, functioning and predictability in the state. Institutions must be resilient against all challenges that derive from outside the lawful, democratic decision-making process. This is especially important in the case of the judiciary, as only the courts can give the final, compelling interpretation of the law. In some recent challenges, institutions (especially courts) have been seen to successfully stabilise a process, where a society was potentially drifting towards a constitutional crisis (Brexit and the 2021 protests after the Presidential election in the United States).

CONNECTIONS — *Connections* are the nodes of goods and services supply chains where the global supply chains are in contact with the more local *clusters.* In this sense, the 'connection' layer can be seen as the literal connection between the global level and the cluster level in the services space. Disruptions in this layer can cut off the clusters from the global level, leaving the clusters isolated and thrown back on their own capacities. Disruptions in this layer can also negatively influence global supply chains if a cluster that is the sole provider of a certain good or service is cut off from the global level. Examples of this layer could be port facilities of strategic value as well as certain critical transport ways (like the Suez Canal).



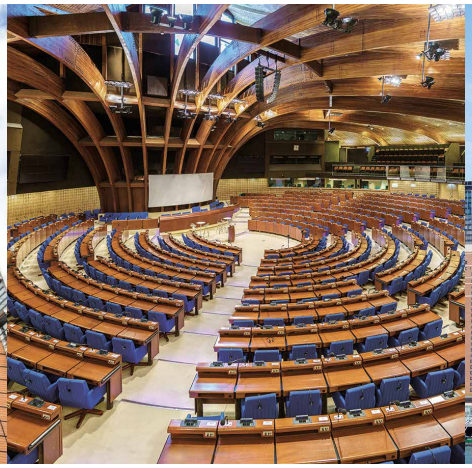
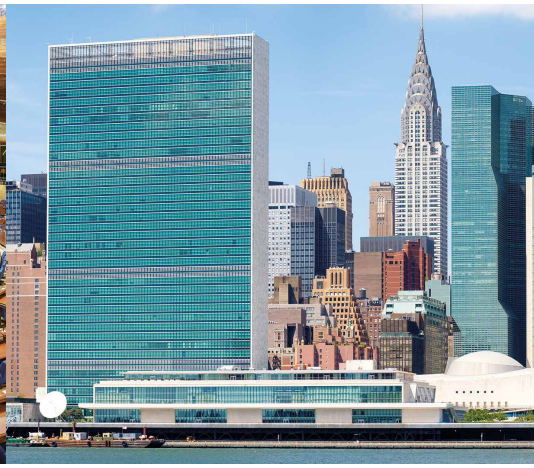


4.5.3. International layers

GROUPS — The groups in the civic space transcend the state boundaries and form transnational networks of affinities among different groups in every nation. Groups and networks are at the basis of a transnational civic space which for a series of political, economic and social issues are extremely active, such as in addressing climate change. The group layer is especially relevant for identifying the subjective and objective feelings that connect various groups across national boundaries.



MULTILATERAL LEVEL GOVERNANCE — Multilateral level governance is the international layer within which states and supra-national institutions interact within the framework of state diplomacy or within the framework of regional or global integration. The multilateral layer concentrates the interactions of mandates, delegated competences and shared competences especially in the EU context that determine the conduct of interstate relations in Europe. The EU multilateral context makes national institutions relate and cooperate with institutions of other states through various arrangements. States are usually very hesitant to give away such core executive powers as policing, national defence, taxation and competence to legislate. Nevertheless, such multilateral arrangements exist, where some institutional power has been delegated to supranational organs (international tribunals, UN Security Council, some parts of the EU, etc.).

GLOBAL — The global layer designates the environment of macro-economic-level dependencies between markets as well as global supply and value chains. The global level interacts with the clusters (immediate contact with and perception from individuals) and the connections (nodes of goods and services providers) and together with them forms the landscape of global interdependencies. This level is often perceived as having direct impact on the lives of individuals while it is also perceived as being beyond the individual's control and beyond the control of local and state level governance (e.g., pricing of certain goods depends on a global market, certain multinational companies seem 'mightier' than states etc.)



4.6. Conclusion – suggesting the ecosystem as a practical device

The comprehensive resilience ecosystem (CORE) is a representation of the system within which the use of hybrid threat activities leads to an erosion of democracy, blurred decision-making and cascading effects. Despite knowing this, even the best prepared countries can be put under significant stress.

The CORE model can be used to enhance understanding of the effects of hybrid threats and offer guidance on how to build resilience against them. The ecosystem functions can be represented as a **dart board,** depicting the main dependencies, spaces and layers affected by a given hybrid threat activity. It can be used in foresight work, to picture 'what ifs' and worst-case scenarios; it can also be used during a crisis caused by a hybrid threat activity in order to have a clear perception of the scale of risk. The CORE model can also help when thinking about the type of resilience we need, where we need it, where the gaps are and what could be the way to calibrate the response to hybrid threat activity.

The next chapter will show that a well-functioning, resilient ecosystem that is able to deny hybrid threat activity and its impacts, as well as the strategic goals of the hostile actor, has the following elements:

- There is comprehensive, multidisciplinary, and agile approach to decision-making
- Interaction and interdependencies between different domains, spaces and layers are observed and acknowledged
- Information flows are horizontal as well as vertical
- The foundations of a democratic system are protected, and act as a strength against hybrid threat activity
- Sectoral resilience is in place. While domains are entry points into the ecosystem, they can also act as shields.

HIGHLIGHTS

The impact of hybrid threats on the ecosystem is depicted using a dartboard. It shows the spaces and layers affected by hybrid threats and their dependencies. A test case study and seven real case studies are used to show how the strategic design board works, what different forms of hybrid threats exist, and how they are utilised over different timeframes by different actors. The essence of using the ecosystem is to detect early signals, help analysis of hybrid threats, and identify potential response trajectories, which in the best case are implemented in a timely manner.

The case studies confirm the validity of the ecosystem approach in identifying connections, effects, and needs for resilience. Moreover, they showed that through using the ecosystem approach, it was possible to represent events, disruptions, and effects along the three spaces of the ecosystem and according to their respective layers, while also picturing timelines and phases. Hence, the ecosystem can form a comprehensive basis for a monitoring and information-sharing mechanism.

REPRESENTING THE IMPACT OF HYBRID THREATS

THE ECOSYSTEM AS A DART BOARD

5.1. Introduction

This chapter goes through a series of case studies[16] that are analysed within the ecosystem framework. The ecosystem represents a **dart board** — it shows the spaces and layers affected by hybrid threats and their dependencies. Chapter 6 will delve into the use of the ecosystem as a **strategic design board** to calibrate the response to hybrid threat activity, by representing where key countermeasures could stem from, and their own impact.

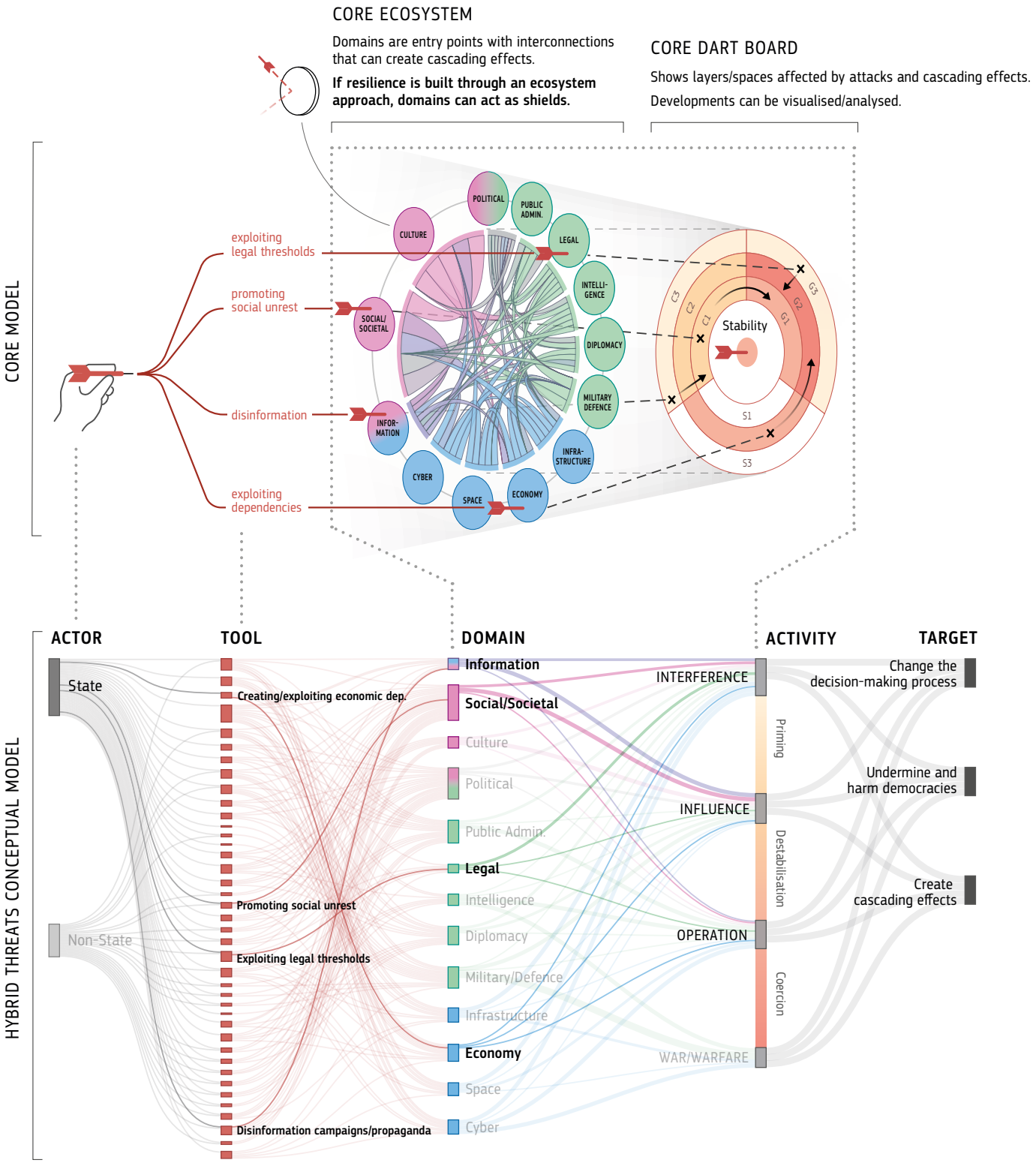
> Using the ecosystem approach helps to spot early signals of hybrid threats, support their analysis and identify potential response trajectories.

The purpose of the case studies is also to show the heuristic value of the ecosystem as an analytical framework. The case studies correspond to three categories: thematic, regional, and state-focused. The case studies demonstrate the diversified nature of both state and non-state actors' activities and depict combinations of different domains and tools, consolidating and expanding the list presented in the conceptual model.

The three different spaces of the ecosystem and their respective layers underline the complexity of the current strategic environment. The case studies depict the state of the ecosystem during distinct phases, enabling it to be illustrated over a defined period. Depicting ecosystems in different timeframes makes it possible to visualise and trace certain developments in the past or to infer further developments for foresight. The nature of hybrid threats implies that they are difficult to anticipate. Early warning usually means finding the known unknowns. Albeit important, early warning also requires the discovery of surprising activities. The phenomena of unknown unknowns can be key to identifying potential hostile hybrid threat activity and building resilience to it. Using the ecosystem precisely fosters decision-makers' ability to identify unknown unknowns. In the context of hybrid threats, connecting the dots is extremely difficult, due to threshold manipulation, deception, and distraction elements. The essence of using the ecosystem is to detect early signals, help analysis of hybrid threats, and identify potential response trajectories.

16 The case studies presented here are summaries of a longer version of the respective case studies written by experts for the JRC.

FIG 5. The strategic design board

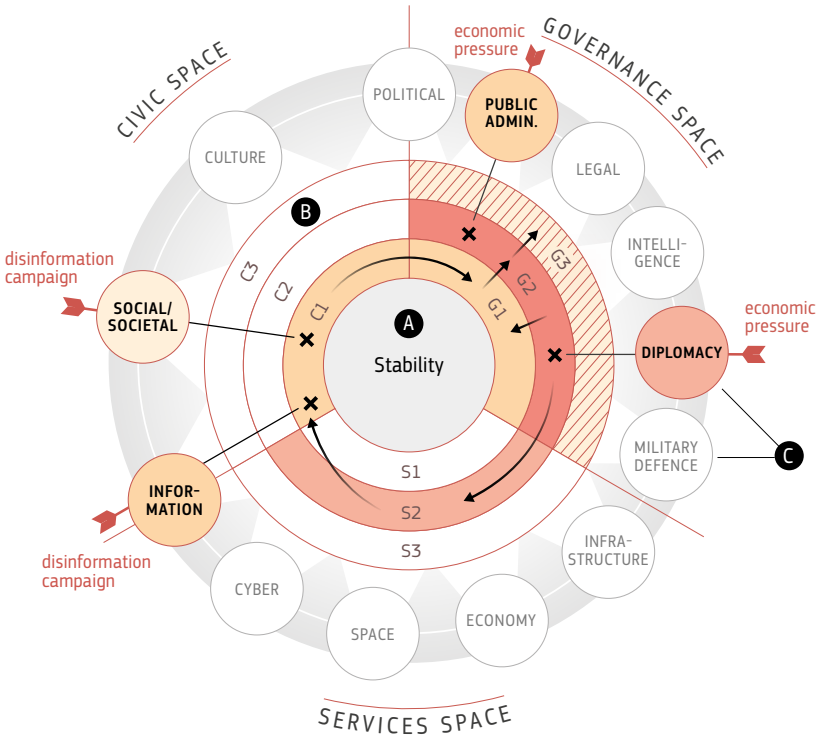


The HT conceptual model defines the process of **Actors** employing **Tools** to target **Domains** to reach **Strategic Goals**.
Activities can escalate through phases: **Priming→Destabilization→Coercion**.

5.2. How to interpret and use the comprehensive ecosystem

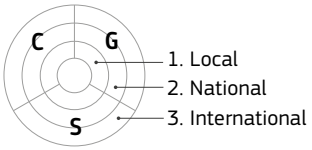
5.2.1. Components

FIG 6. Example case



A FOUNDATIONS: Core elements of democracy that hybrid threat actors aim to compromise and must be protected.

B SPACES AND LAYERS: The ecosystem is composed of three spaces with three layers. Each layer is represented by the capital letter of the space (C,G,S) plus a number corresponding to its "location" (1,2,3).



CIVIC SPACE	GOVERNANCE SPACE	SERVICES SPACE
C1–Civil Communities	G1–Local Administration	C1–Services Clusters
C2–Civic Nations	G2–State Governance	C2–Services Connections
C3–Civic Groups	G3–Multilateral Governance	C3–Services Global

C DOMAINS: Placed around the ecosystem according to the space they have the strongest ties with.

ARROWS

- New attack on the ecosystem that has not occurred before.
- Attack that has already occurred in a previous phase and continues to occur.
- Cascading effects between compromised spaces/layers. It may happen within one space (G1→G2), between spaces (C1→G1), and between spaces and layers (S2→C1).

COLOUR

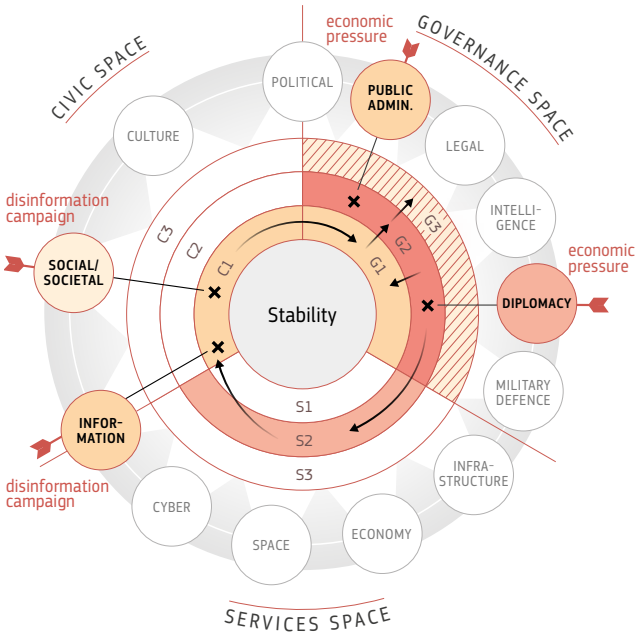
Intensity of compromise (qualitative assessment)

- low
- medium
- medium-high
- high
- very high

Ultimate space/layer that the hybrid threat actor aims to compromise.

In some cases, the space/layer compromised with higher intensity is not the final aim but a distraction element.

5.2.2. How to use the ecosystem (hypothetical scenario)



The comprehensive ecosystem depicts the state of the system at a given instance in time. Hence, it is possible to illustrate the ecosystem and its changes over a certain period of time through several graphics. As the case studies will show, the depiction of ecosystems in different time instances serves, among other things, to visualise and trace certain developments in the past or to help anticipate certain developments in the future. From outside to inside:

1. It reflects the domains that have been compromised with their respective intensity (depicted with colours) by the use of hybrid threat related tools.

2. The effect of the compromised domains is reflected in the spaces/layers. For instance, a hybrid threat actor applies economic pressure against a country and launches a disinformation campaign targeting its citizens:

   - On the one hand, diplomacy and public administration domains are impacted by the **economic pressure**, compromising the Governance level primarily at the State (G2) layer, having an effect on national companies, represented in the Services (S2) Clusters layer.

   - Meanwhile, a **disinformation campaign** impacts the Information and Social domains, and is addressed to extremist groups in the country (e.g., both far right and far left groups) aiming to increase unrest, having a direct effect in Civic space in the Groups (C1) layer. As a result of the disinformation campaign (in which the narrative of the sanctions is used) and the effects in S2 by the **economic pressure**, protests arise throughout the country, having an impact on the Governance space at the Local (G1) and Nation (G2) layers. This instability also impacts the Multilateralism (G3) layer, as the polarisation suffered within the state is picked up by international organisations.

3. As a result, the foundation *Stability* (depicted at the centre of the ecosystem) is compromised.

Meanwhile, even though the segments compromised with a higher intensity were at the local and national levels, an analysis of the strategic objectives of the hybrid threat actor may show that its 'ultimate objective' is to increase instability within the Multilateralism (G3) layer (depicted with a thicker border). In this way, by aiming to impact the National (G2) and Groups (C1) segments, the 'ultimate objective' can be achieved, hindering attribution by using a distraction element.

> "The ecosystem can form a comprehensive basis for a monitoring and information-sharing mechanism."

5.3. NORD STREAM CASE STUDY

Compromised foundations: stability, reliability and availability, foresight

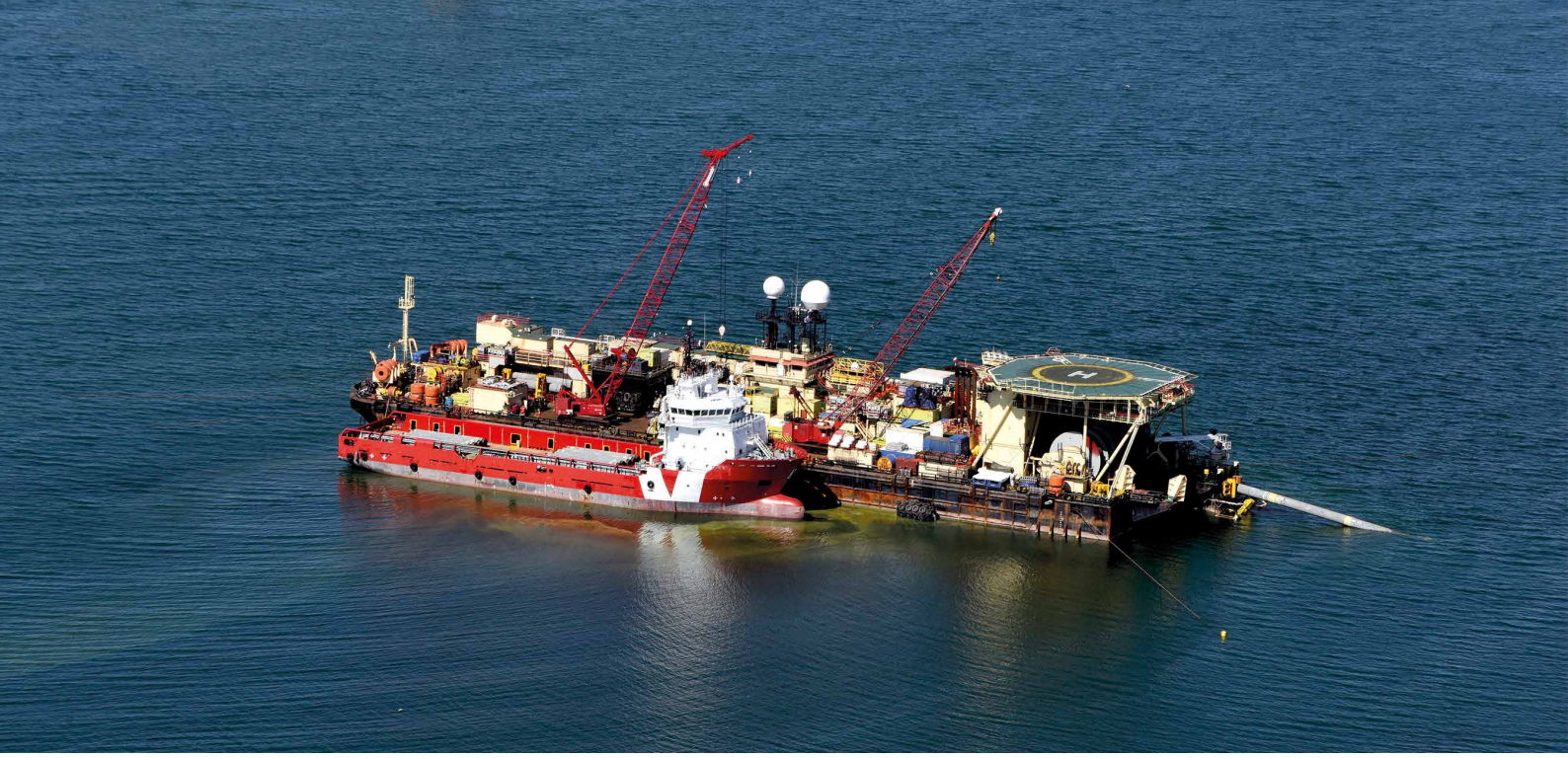
Following the Russian invasion of Ukraine in February 2022, Nord Stream 2 was stopped. This case study analyses the situation up to the end of 2021 and hence does not directly take into account more recent events. It is not the intention of the case study to depict the influence of a war on an infrastructure 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.

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.



Nord Stream 2 shows the risk of adopting a strictly sectoral approach to enhancing energy security if it disregards the interdependencies between the governance and services spaces. It overlooks the fact that the concept of private sector autonomy does not exist in authoritarian regimes. The sectoral and business logic of the project has been instrumentalised by the Russian side to aggregate elements of political and diplomatic interference, weakening Germany's stance within the EU (creating divisions among EU MS) and towards the US (sanctions against the project).

Analysing the Nord Stream 2 case through the ecosystem lenses shows that overlooking the implications and dependencies in a sectoral endeavour may ultimately diminish resilience elsewhere by creating crevices in other spaces of the ecosystem. Measures taken in the international layer of the governance space cascaded through the governance layers. The tensions spread from the national to the international layer, amplifying the cleavage between Member States and returning to the national layer, with interference attempts in the latest German elections. The long path dependency of the decision slowly eroded trust and increased the polarisation potential of the civic space. In the German federal election in 2021, Russia targeted and discredited certain politicians in the context of the debate on the construction of the Nord Stream 2 gas pipeline. The effects of Nord Stream 2 on the European security environment are an example of how sectoral resilience-building can have negative implications throughout decades-long processes. It is key to understand the linkages within the ecosystem and the need to build resilience through better foresight calculations and dependency-mapping.

This case study can be represented to have compromised the following ecosystem foundations:

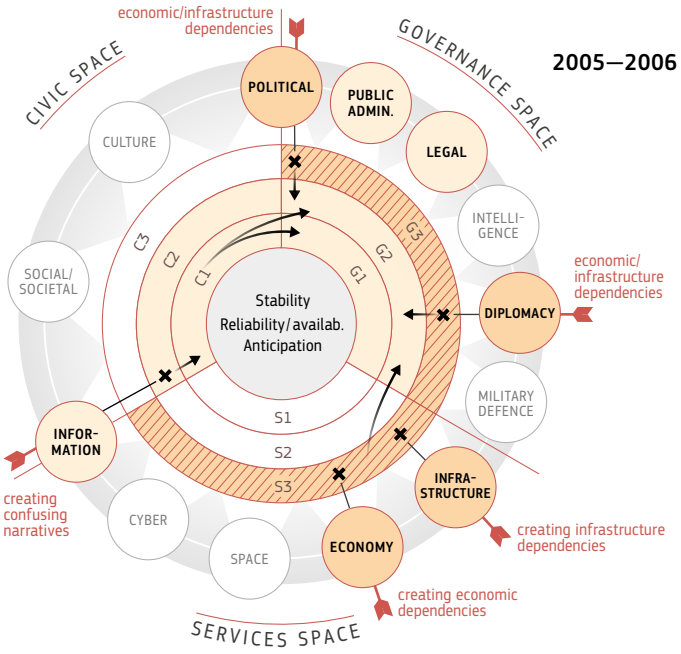
- **Stability:** the various divisions and debates within the EU, and especially between countries on the receiving end of the project and countries feeling bypassed by the project in a deteriorating geopolitical environment.

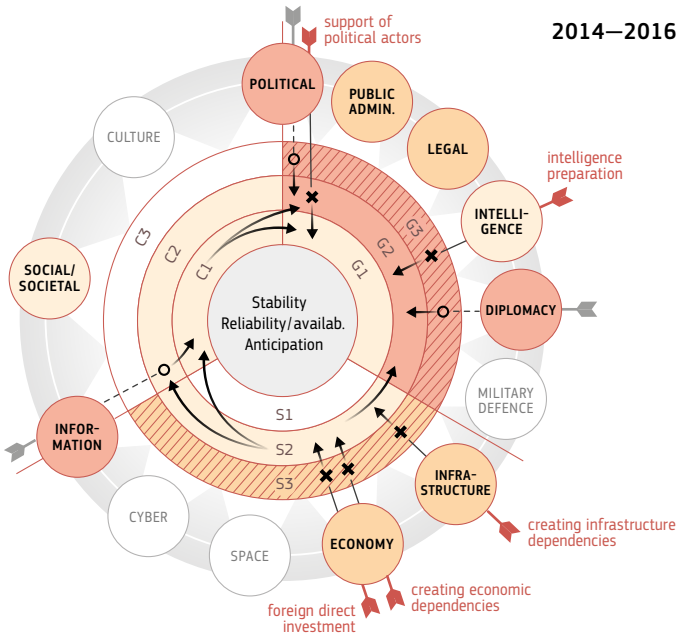
- **Reliability and availability:** the deteriorating security situation on the continent may prevent the business logic and the project from moving forward, therefore not delivering on the energy provision. The lack of reliability and availability should the project not succeed can be instrumentalised by Russia in target societies.

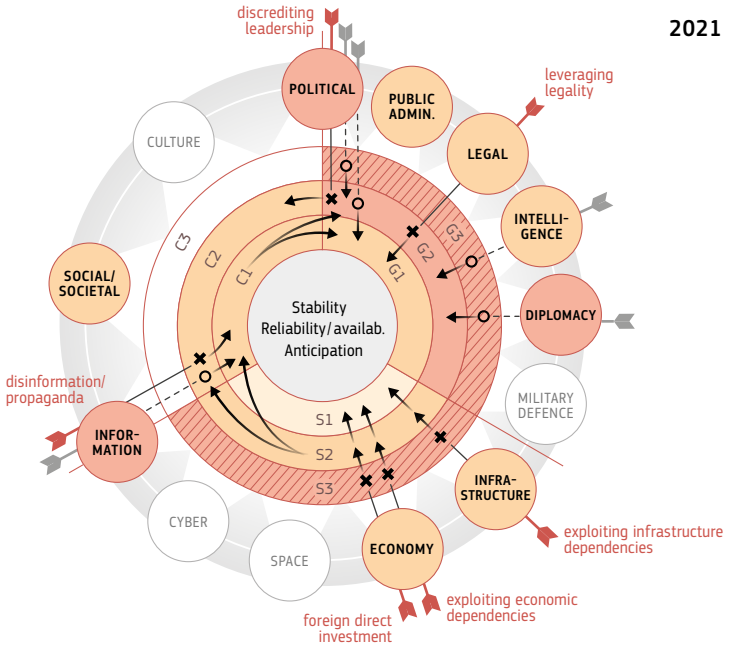
- **Foresight:** the web of interconnection of business interests within a tense security environment has only rendered more complex the vulnerability surface that hybrid threat actors could exploit to undermine target states and societies.

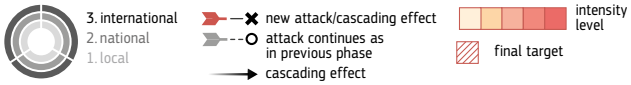
FIG 7. Nord Stream — CORE analysis

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









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.

INTERFERENCE/INFLUENCE

- **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.

INFLUENCE/CAMPAIGN

- **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.

5.4. CATALONIA CASE STUDY

Compromised foundations: stability, rule of law, political responsibility and accountability

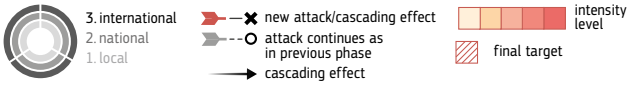
The events in Catalonia stemmed from a severe erosion of trust due to structural weakening of the feeling of justice and equal treatment experienced by Catalan separatists. The crippling effects of the economic crisis that started in 2008 created a series of gaps in trust between the federal state, the Catalan authorities, and parts of the population. The unconstitutional secession referendum of 2017 was symptomatic of the exhaustion of the foundation of political responsibility in finding a negotiated compromise out of the dispute. Calling a referendum in a highly volatile and tense political environment was a further polarising action. Meanwhile, although Russia did not create the issue, it exploited it for its own benefit, by attempting to influence perceptions, attitudes, and decisions of target audiences. The aim of the Kremlin in this case was not an independent Catalonia, but 'a very deep and long internal instability of Spain', a country member of the EU and NATO, which would ultimately influence 'all Western countries' (Warsaw Institute, 2017).

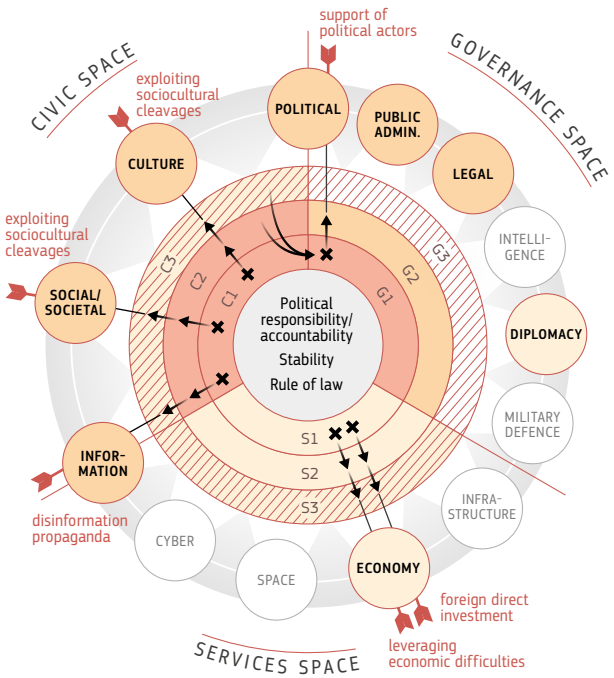
The dispute in Catalonia stems from deep historical roots that subjects it to multiple tensions. Over the course of the 2000s, the economic crisis and a trend of distrust toward the State and the traditional Catalan political elites, made Catalonia become a fertile scenario for several actors to sow seeds of hostility and increase polarisation. Catalan separatists intensified their activities, simultaneously targeting the three spaces and culminating in a referendum – in defiance of the constitution – and the unilateral declaration of independence in 2017, in response to which the Spanish government temporarily imposed direct rule and jail sentences for nine Catalan separatist leaders (The Economist, 2021). In addition, in order to advance their agenda of establishing their own state, Catalan separatists aimed to create their own structures, separated from their Spanish equivalents, in the banking, telecommunications, and energy sectors, seeking external support and funding, as well as constantly relying on different platforms to spread disinformation campaigns and propaganda.

The Catalan dispute was instrumentalised by Russia in an attempt to undermine and harm the integrity and functionality of democracy, create cascading effects in other MS, and influencing decision-making processes. Former Catalan independence movement leaders were linked with Russian intelligence operatives and organised crime figures. European police and intelligence reports quoted go as far as establishing links between destabilisation attempts in Catalonia with those Russian connections (The New York Times, 2021). Although the activities to influence and destabilise society occurred primarily on the local layer of the ecosystem, Russia's targets were the national and international layers, as its aim was not an independent Catalonia but a very deep and long internal instability of Spain and the EU. To this end, among others, Russia relied on tools such as supporting political actors and the use of proxies, polarising society and exploiting societal cleavages, promoting contradictive narratives, financing cultural groups and think tanks, discrediting leadership, cyber operations, and foreign direct investment.

FIG 8. Catalonia — CORE analysis

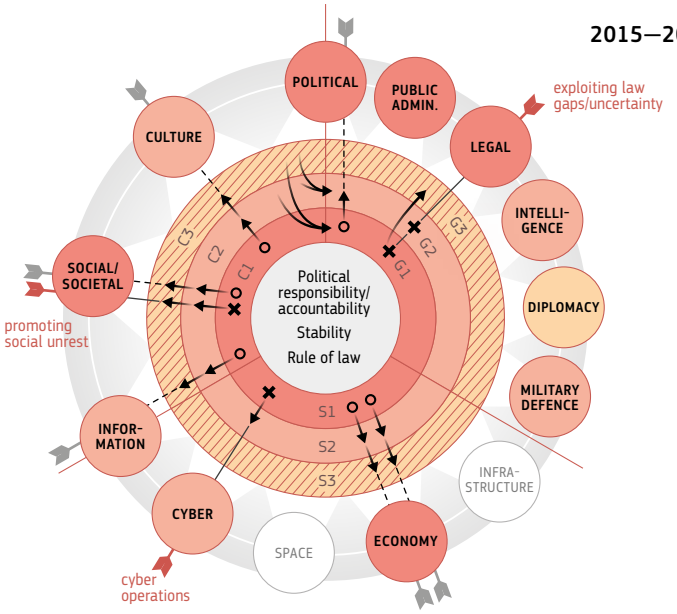
Although activities take place at the local level, the end target of the hybrid threat actor is the international layer.





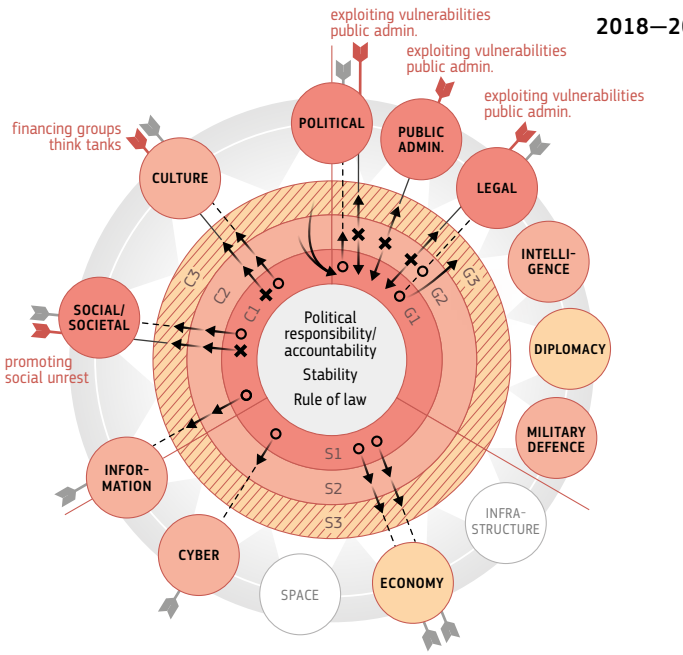
INTERFERENCE/INFLUENCE

- **Exploitation of sociocultural cleavages** in part of the Catalonian society (C1).
  C1→C2/C3→G1 It became an issue for Spanish society and at international level (C2/C3), indirectly influenced local Catalan politics and diplomacy (G1).
- **Support of political actors** by Russia who supported separatist politics (G1).
  G1→G2 Became an issue of national politics and affected public administration and the legal system, as support for separatists came from dubious/illegal sources (G2).
- **Leveraging economic difficulties. Foreign direct investments** Tools used by Russia to exploit economic difficulties in Catalonia and support separatists (S1).
  S1→S2/S3 Had implications for Spanish economy and beyond.
- **Disinformation campaigns and propaganda** by Russia were aimed at further promoting the Catalan separatist movement and polarising society (C1).
  C1→C2/C3 This form of propaganda spread all over Spain and internationally (C2/C3).



CAMPAIGN/OPERATION

- **Promoting social unrest** by Russia to escalate the situation in Catalan society (C1).
  C1→C2/C3→G1/G2 This created stark polarisation in Spanish society and beyond (C2/C3), leading to the involvement of Spanish military, intelligence, and diplomacy in the conflict (G1/G2).
- **Exploiting thresholds, non-attribution, gaps and uncertainty in the law:** Russia provided financial and logistical support for the illegal referendum held by the separatists (G2/G1).
  G2/G1→G3 The illegal referendum held became an international issue, affecting the public administration and political domain (G3).
- **Cyber operations** by Russia to destabilise the situation i n Catalonia (S1).
  S1→S2 This had an impact on cybersecurity at the state level (S2).



INFLUENCE/CAMPAIGN

- **Exploiting vulnerabilities in public administration** by supporters of the separatists and political parties, some of whom now bear political responsibility at the national level (G2).
  G2→G1/G3 This influenced politics at the local level in Catalonia and at the international level, and indirectly affected the diplomacy domain (G1/G3).
- **Financing cultural groups and think tanks**, as well as influencing the education curricula, by separatists in power, to further promote their ideology through cultural means (C1).
  C1→C2/C3 This had an impact on Spanish society and beyond (C2/C3).

The vulnerability that Russia exploited by priming the two extremes of the political spectrum involved in the Catalonia issue was hardly understood and not considered from a resilience point of view. The Catalonian case illustrates how social divisions are exploited by local and foreign state actors seeking to destabilise either an EU Member State or the EU itself. In the absence of a holistic approach to resilience, the tailor-made combination of tools and domains can result in unpredicted consequences. A comprehensive approach to identify the connections between all spaces and layers of the resilience ecosystem and to understand the criticality of the nodes could have denied the cascading effects back in 2017 and could help anticipate what could come in the near future.

The hybrid threat activities in Catalonia compromised the following foundations of the ecosystem:

- **Stability:** the use and amplification of existing vulnerabilities of the society led to unpredictability of governance and a potentially serious breach of the social contract.
- **Rule of law:** Spanish constitutional order and territorial integrity were challenged by domestic political actors deliberately standing outside of the law, supported by Russian operative figures in the years after the turmoil, nurturing a potential for continuation.
- **Political responsibility and accountability:** secessionist populism offers a wide vulnerability surface in leveraging political polarisation, leading to abuse of power and excess of mandate while undermining democratic processes.

5.5. COVID-19 CASE STUDY

Compromised foundations: stability, rule of law, reliability, political responsibility and accountability

Hybrid threat actors in the context of the fight against the Covid 19 pandemic sought to weaken the credibility of democratic systems by stressing the many ways in which services were made unreliable and disrupted. Hybrid threat actors also attempted to demonstrate how democratic leaders would be structurally incapable of maintaining stability. They also leveraged a growing feeling of injustice and differentiated treatment among citizens, as well as highlighting the rule of law and civil rights and liberties suspended by democratic systems themselves. Authoritarian regimes need to discredit the governance of democratic systems regarding their ability to provide stability for a well-functioning society. They need to spin the democratic social contract and open societies as fragile and weak, especially in crises.

The Covid-19 pandemic management measures displayed how hybrid threat actors can instrumentalise a multi-faceted crisis with the aim of promoting authoritarian regimes, altering global governance, and discrediting Western states by destabilising cohesion and undermining the trust basis of societies. The hybrid threat activities by China and Russia in the context of Covid-19 have included many essential characteristics of hybrid threats, such as exploiting the seams of democratic societies, use of multiple, synchronised tools, as well as distraction elements.

Exploitation of ongoing crisis and existing institutional stress:

- Use of complex interdependencies between civic-governance- and services spaces
- Discrediting the open society
- Lack of foresight of known unknowns and unknown unknowns.

On the other hand, positive findings from a resilience point of view include:

- Joint action and pooling
- Crisis improvisation that results in advances to act more strategically.

China and Russia have exploited the pandemic in two ways: targeting Covid-19-related vulnerabilities, such as the lack of masks, medical equipment, and vaccines; using COVID-19 as a distraction element to advance their strategic agenda in different regions as well as domestically, by trying to show that authoritarian systems are better than democratic systems at bringing beneficial policy outcomes.

The pandemic demonstrated the complex interdependencies between civic, governance and services spaces. This paved the way for widespread cascading effects. In the case of Covid-19, it was an exogenous shock, which ended up having wide negative externalities in every space and layer of the ecosystem. Working along a principle of efficiency with little redundancy, the services space's inability to absorb the scale of disturbance undermined governance and civic spaces as well. Hybrid threat actors took advantage of the effects of a

natural shock and undermined and harmed the integrity and functioning of democratic processes, values, and institutions. The Covid-19 pandemic and related hybrid threat activities stressed the essential role of the services space for the good functioning of society. Hybrid threat actors exploited the window of opportunity and the lack of reliability / availability in the services space and shaped perceptions of the ability of democratic governance to ensure stability and predictability.

Both actors have exploited Covid-19 related vulnerabilities in different manners, albeit sharing the main objectives and several similar tools. One of the most exploited vulnerabilities has been the vaccine vacuum and a perceived failure of the West to provide vaccines to the world. This has allowed China and Russia to target low- and middle-income countries especially and depict themselves as the global providers of vaccines. In both cases the activities directly targeted four foundations of democratic societies:

- **Stability:** the hybrid threat activities sought to undermine the principles and performance of democracies as providers of stability in times of crisis, by attempting to portray authoritarian regimes as more efficient in pandemic management and vaccine production.

- **Rule of law:** the hybrid activities were also specifically aimed at undermining people's trust in the rule of law by exploiting a growing sense of injustice.

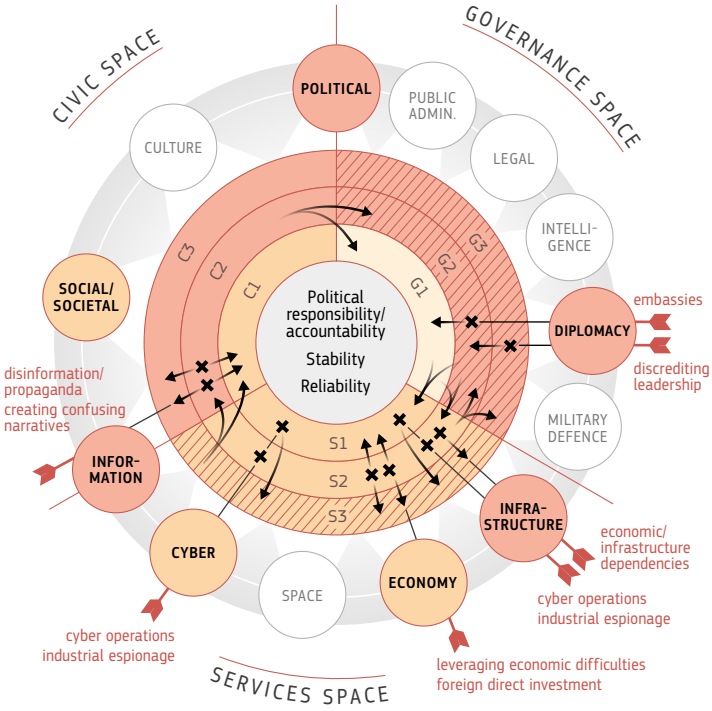
- **Reliability:** the ability of democratic systems to deliver in times of crisis was undermined by exploiting the flaws in global supply chains, dependencies, and just-in-time logistics with comparative promotion of authoritarian regimes and governance.

- **Political responsibility and accountability:** COVID-19 was a window of opportunity to undermine the democratic model of decision-making in crisis times, compared to a perceived efficacy of authoritarian types of crisis management.

FIG 9. Covid-19 — CORE analysis

Vulnerabilities in a society in an emergency situation such as the Covid-19 pandemic can be exploited by actors in different ways.

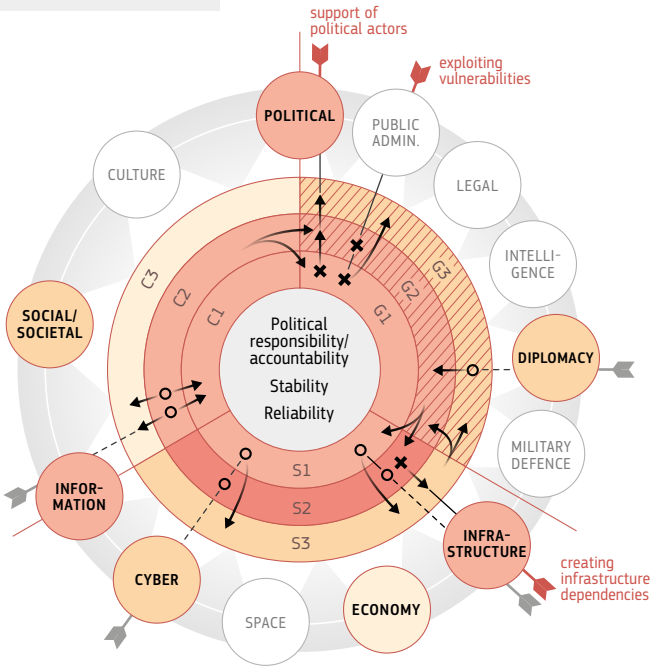
CHINA (CAMPAIGN)



2020—2021

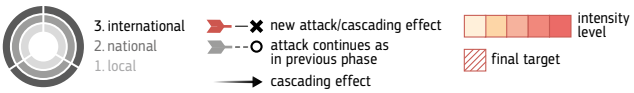
- **Creating and exploiting infrastructure and economic dependencies** by providing medical equipment or vaccines, especially to countries of the southern hemisphere (S2).
  S2→S3→G2/G3 Increased fundamental dependence on China in certain world regions and value chains (S3) and its political leverage over those countries/regions (G2/G3).
- **Foreign direct investment. Leveraging economic difficulties** Tools used to take advantage of the emergency to expand national economic influence (S2).
  S2→S3/S1→G2/G3 Strengthened China's global and local economic influence (S3/S1) and its political leverage over countries/regions (G2/G3).
- **Cyber operations and industrial espionage** were applied in the context of the aid given to countries (S2/S1).
  S2/S1→S3 China's role in global cyberspace is strengthened.
- **Disinformation campaigns and propaganda. Creating confusion or contradictory narratives** Tools aimed to promote authoritarian models of government, by spreading the idea in societies that they are more effective in crisis-management than democracies (C2).
- **Discrediting leadership and/or candidates** of other countries during the pandemic (G3).
  G3→G2→S2/S1 Influenced politics in the respective countries (G2), spilling down indirectly to national and local levels through disinformation (S2/S1).
- Through the **use of embassies**, China's diplomacy helped undermine state authority by offering questionable assistance (G2).
  G2→G1→S2/S1 This activity extended to the local level and was spread indirectly through disinformation on the national and local level (S2/S1).

RUSSIA (CAMPAIGN)



2020—2021

- **Creating infrastructure dependencies** by providing medical equipment or Covid-19 vaccines to national governments (S2).
- **S2→S3→G2/G3** Increased fundamental dependence on Russia in certain world regions and value chains (S3) and its political leverage over those countries/regions (G2/G3).
- **Exploitation of vulnerabilities in public administration** by arranging the supply and production of vaccines at national or regional level (G2/G1).
  G2/G1→G3 Led to diplomatic disarray at international level (G3).
- **Support of political actors** who spoke out in favour of Russian aid and Russian vaccine (G1).
  G1→G2/G3 Impacted national politics causing diplomatic disarray at international level (G2/ G3).



5.6. WESTERN BALKANS CASE STUDY

Compromised foundations: rule of law, political responsibility and accountability, reliability and availability, stability

In the Western Balkans a strategic competition between different actors can be observed. Its centre of gravity is the credibility of the EU in regional integration. Russia and China position their economic actors to control the reliability and availability of a growing share of the market supply chains and key nodes. To prevent EU enlargement to the region, Russia has an interest in undermining improvements in democracy, good governance, and the rule of law. Keeping the prospect of the Western Balkans joining the EU at bay is a strategic interest for Russia, thus targeting the foundations of the rule of law, justice, and equal treatment, as well as civil rights and liberties. It sustains networks of corruption related to business deals, for instance, as a crippling impediment to good governance.

The Western Balkans are increasingly the area of competition between various foreign actors. On one side, the EU is enhancing peace, democracy, and the rule of law in the region and fostering reforms towards solidifying human rights, democracy, and the rule of law. On the other side, authoritarian states have the opposite approach. In particular, Russia has long had a strong presence in the region and its influencing and destabilising activities are depicted by wide-ranging efforts to:

- position itself in key economic sectors as an indispensable actor
- discredit the promotion of human rights, democracy, and the rule of law
- influence the regional balance of power
- project cultural attractiveness through a narrative of historic, linguistic, and religious bonds
- engage in public diplomacy and domestic crisis and support nationalist or anti-Western networks in the region

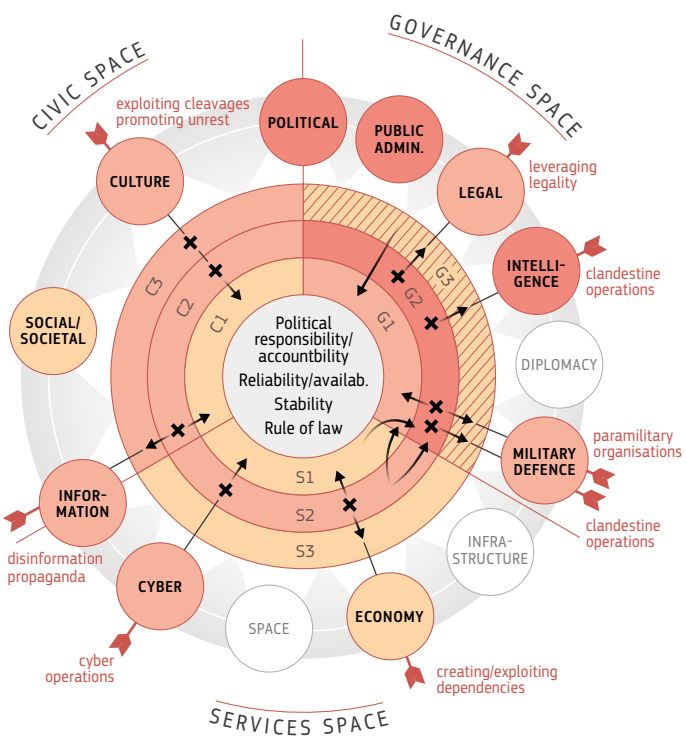
Those efforts are part of a strategic intention to hamper the consolidation of democratic states and civil society, and weaken the countries' EU aspirations. Russia even offers alternatives, with potentially lower adoption and reform costs. In the services space, the conditions imposed on local or national layers of the ecosystem aim to override respective EU standards and exert influence, dependency, and leverage. Russia's goal of establishing a strong economic footprint in the Western Balkan economies through authoritarian practices brings many risks, lowering the reliability and foresight elements of the services space.

Russia has also exploited the seams between governance and services spaces as business deals are mostly negotiated with political and economic elites. The inflow of financing from Russia to Western Balkan countries lacks transparency and proper checks and balances, and runs the risk of exacerbating corruption and elite capture. Strategic corruption obstructs stability and undermines the rule of law. Thus, influence on local and national layers cascades to the international layer and affects the abilities of Western Balkan countries to meet EU standards on the rule of law.

FIG 10. Western Balkans — CORE analysis

Russia's hybrid threat activities in Western Balkan countries.

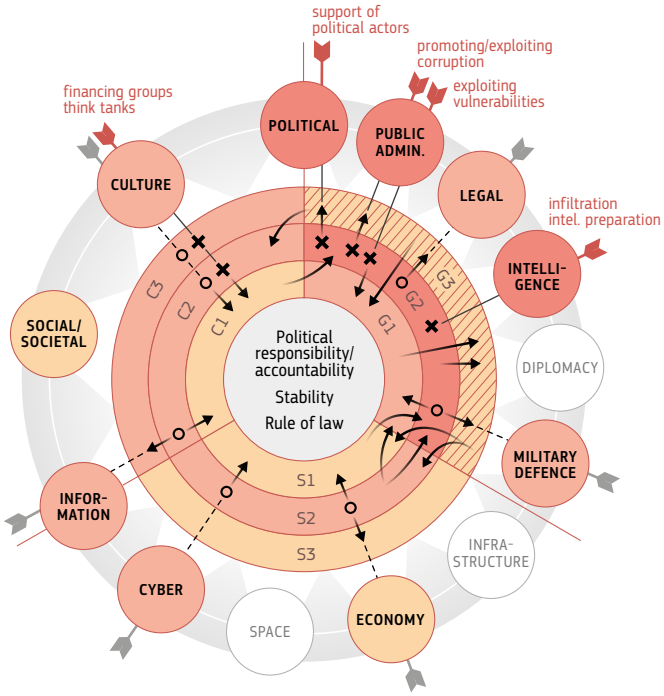
RUSSIA IN WESTERN BALKANS (DESTABILISATION)



2015—2017

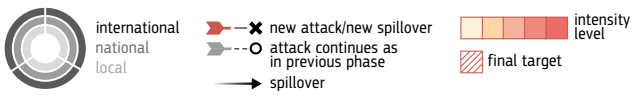
- **Creating and exploiting economic dependencies** by Russian actors.
  S2→S1/S3→G1/G2 Russian economic influence spilled to local and international levels (S1/S3), granting political influence at the local and national levels (G1/G2).
- **Exploiting sociocultural cleavages and promoting social unrest** Russia aimed to invoke historical, linguistic, and cultural bonds and use them as a tool in the event of a crisis.
  C3/C2→C1 This unrest impacted societies at the local level (C1).
- **Leveraging legal rules, processes, and institutions** by Russian actors aimed to undermine the rule of law and development of democracy.
  G2→G3→G1 This impacted the entire region (G3) and indirectly affected local public administrations and political actors (G1).
- **Cyber operations** by Russia aimed to destabilise the country.
  S2→S1→G2 This impacted local level services (S1), interfering with national public administration (G2).
- **Disinformation campaigns and propaganda** established an anti-Western narrative.
  C2→C1/C3 This affected societies locally and throughout the region.
- **Clandestine operations** aimed at sabotaging the functioning of democracy.
  G2→G3 This impacted the region and obstructed the functioning of public administrations (G3).
- **Paramilitary organisations (proxies)** aimed at undermining the stability of state authorities (G2).
  G2→G1/G3 Local/regional political stability was negatively affected.

RUSSIA IN WESTERN BALKANS (INFLUENCE)



2018—2021

- **Financing cultural groups and think tanks** to spread Russophile views and culture.
  C2/C3→C1→G2 Influenced cultural sensibilities at local level (C1) and societies and public administration at national level (G2).
- **Promoting and exploiting corruption** aimed to undermine the development.
  G2→G3→S1/S2 It had a negative impact on the entire region (G3), harming local and national economic development (S1/S2).
- **Exploiting vulnerabilities in public administration** to undermine its efficiency.
  G2→G1→G3 Poor governance led to discontent at the local level (G1), which affected the entire region (G3).
- **Support of political actors** who represent pro-Russia views.
  G2→G3→C2 Affected Russia's influence in the region (G3) and polarised societies (C2).
- **Infiltration and intelligence preparation** by Russian services.
  G2→G3 Covert expansion of military influence affected the entire region (G3).



The coordinated use of multiple hybrid threat tools has implications beyond the governance and services spaces. In the civic space, Russia aims to prevent and reverse political aspirations to EU membership. Alternative standards are being sown by using multiple tools and domains, seeking to prevent adherence to principles and processes essential to democracy. This is implemented by promoting a narrative centred around the credibility and effectiveness of authoritarian regimes.

The foundations that are being compromised in the Western Balkans are:

- **Rule of law:** Russian actions which cause confrontation, polarization, and support for existing corrupt state institutions, impedes good and transparent governance which deepens distrust towards governments.

- **Political responsibility and accountability:** the bargain between local politicians and authoritarian state elites trading national interest for personal gains, diminishes accountability and threatens the development of a robust political culture in ways that may be detrimental to the democratic prospects of the Western Balkans.

- **Reliability:** the poor state of national economies means that economic state actors within authoritarian regimes become attractive alternatives, as they provide quick and easy investments with no immediate strings attached.

- **Stability:** the polarisation of societies and instability in the region are highly prone to outside influence, with external actors exploiting these instability factors to further their own agenda in the region. The mutual distrust and negative sentiments between states and different nationalities have been used by outside actors.

5.7. EDUCATION CASE STUDY

Compromised foundations: stability, political responsibility and accountability, justice and equal treatment

Influencing education opens the possibility for hybrid threat actors to durably undermine the foundations of the civic space. Gaps in regulations for schools, especially in terms of religious teachings and secularism, may render it possible for external actors to fund, influence and control otherwise legal educational entities. Universities can also be an environment of hybrid threat influence, especially in terms of intellectual property, international exchanges, and sources of funding. The area of education touches the key foundations of the feeling of attachment to liberalism and democracy.

Education is key to societal resilience. It fosters equal opportunities, improving social trust and integration of society. Education in the context of hybrid threats has particularly focused on building the resilience of societies to disinformation (European Parliament, 2021). Education systems as targets of hybrid threat actors' attempts to influence school and higher education has received less attention, yet hybrid threat actors have attempted to influence school and higher education.

Influencing education has long-term impacts. It may undermine democratic values, disrupt social trust in the target state, deepen cleavages within society, or even lead to transfer of intellectual property (Cullen et al., 2021). For hybrid threat actors, influencing education can sway individuals' long term belief systems, thus undermining the core of the ecosystem. Education has a twofold importance: not only does it set the conditions for building resilience to a wide range of hybrid threats, but it also contains considerable cascading potential.

Specifically:

1. States may not supervise all institutions providing education. Salafi networks have exploited gaps in public education planning and provision as they embarked upon a business-based approach for their influencing campaigns within the educational sector.

2. The secular character of most EU Member States is a challenge in terms of regulating religious education. Fringe educational institutions can gain ground within a state, outside of the public education system.

3. Education can become an international battleground around values. The Russian national security strategy of 2021 defines some 'informational-psychological' sources as a threat, such as liberal values in education.

4. University funding and dependency on students from a single country can create influence channels that can be exploited. Student exchange programmes, grant applications and international cooperation may pave the way for interference practices.

As with most influencing activities, instrumentalising the education system for hybrid threat activities is often legal, taking advantage of freedom of religion, thought and expression, which makes it a challenging task for national authorities

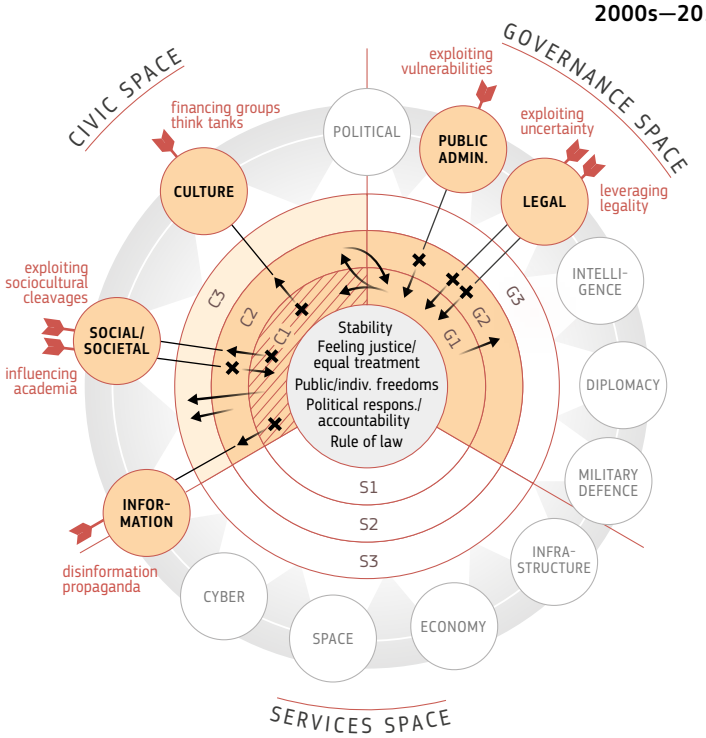
to respond to appropriately. Vulnerabilities can also emerge from education systems themselves. The process should involve foresight work to take stock of potential future developments and worst-case scenarios and consider by whom, with what funding, and how the education is provided.

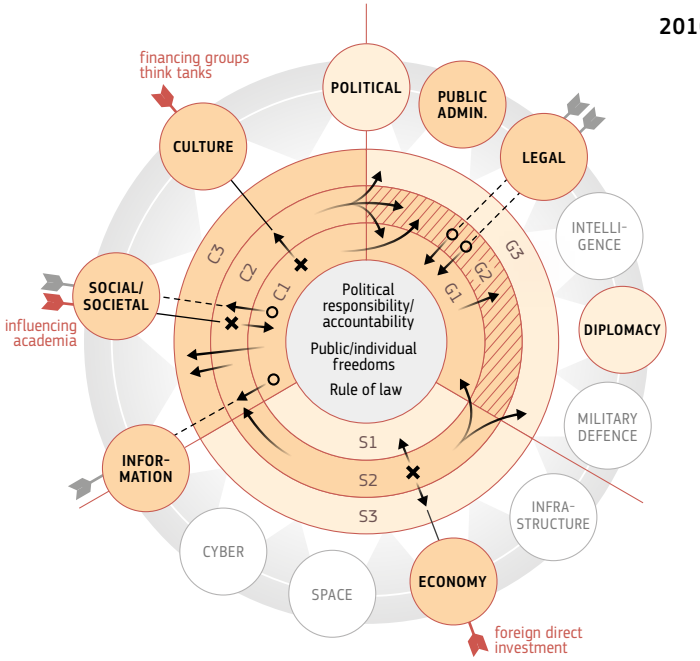
This case study shows that the following foundations can be undermined by hybrid threat activity:

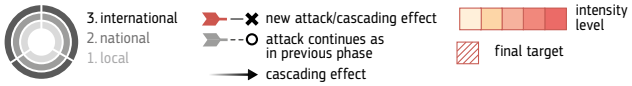
- **Stability:** the disruptive potential of teachings and perceptions over the long term can undermine the solidity of trust towards the state and within society itself, producing a danger of societal disaggregation.
- **Political responsibility and accountability:** the principle of representative democracy and participation in democratic life requires citizens to have a strong attachment to the form of the political regime, which can also be undermined by influencing long-term perceptions.
- **Justice and equal treatment:** since the existence of alternative or even disruptive education systems, alongside public education, undermines the principle of unity of education and equal opportunities.

FIG 11. Education — CORE analysis

Hybrid threat activities to change a person's belief system in the long term can undermine the core of the ecosystem.







SALAFIS (INTERFERENCE)

- **Influencing curricula and academia** in schools.
  C2→C1→C3 It affected the local civic level (C1) and indirectly promoted the movement and its culture internationally (C3).
- **Exploiting vulnerabilities in public administration** to establish their own education model.
  G2→G1→C1/C2 Spilled down to local governance (G1) and then indirectly affected society and culture at local/national level (C1/C2).
- **Financing cultural groups and think tanks** to spread the ideology and undermine democracy.
  C1→C2→G1 Impacted on culture at national level (C2) and indirectly affected local public administration (G1).
- **Exploitation of sociocultural cleavages** widened by ideology.
  C1→C2→C3 Impacted society at national level (C2) and indirectly affected the cultural domain at international level (C3).
- **Disinformation campaigns and propaganda** spread divisive ideas and fake news.
  C1→C2→C3 National impact (C2) that indirectly affected the cultural domain internationally (C3).
- **Leveraging legal rules, processes, institutions and arguments. Exploiting thresholds, non-attribution, gaps and uncertainty in the law.** Tools that aimed to exploit the legal ambiguities regarding religious education in some secular states.
  G2→G1→G1/G2 This had an impact on education at the local level (G1) and indirectly affected local/national public administration (G1/G2).

RUSSIA (INTERFERENCE/INFLUENCE)

- **Influencing curricula and academia** in schools and universities.
  C2→C1→C3/G2 had an impact at local level (C1) and indirectly promoted Russian government's views internationally in the culture domain (C3) and on a national level in the political domain (G2).
- **Financing cultural groups and think tanks** to spread Russian government's world views, protect Russian version of historical truth and strengthen the position of the Russian language.
  C1→C2→G1/G2/G3 Had an impact on culture at national level (C2) and indirectly affected the local public administration (G1), national politics (G2), and international diplomacy (G3).
- **Foreign direct investment** by Russia to strengthen the position of Russian companies in global competition as well as forming a favourable image of Russia abroad through educational programmes.
  S2→S1/S3→C2/G1/G3 First impacts the economy on the local and international levels (C2) before spreading beyond and indirectly affecting the society at the national level (C2), the public administration at the local level (G1), and the diplomacy domain at the international level (G3).

FORESIGHT–IDENTIFYING FUTURE CHALLENGES

5.8. FRANCE CASE STUDY

Compromised foundations: stability, rule of law, reliability

The 2017 French presidential campaign shows how non-state actors and individuals bound by a common transnational ideology attempted to undermine trust during a crucial election cycle. This transnational network of actors plugged into existing polarisation and French political figures to discredit a candidate. The fabricated allegations, hacks, and leaks sought to induce the idea that the candidate would not be bound by the rule of law and would be corrupt, as that would undermine the foundations of justice and equal treatment, as well as trust in the class of politicians in general.

'MacronGate' and the 'MacronLeaks' in 2017 and the Russian media coverage of the Yellow Vests movement of 2018-2019 were a series of information manipulations. MacronGate and MacronLeaks refer to information manipulations using hack and leak tools to discredit a candidate in a key electoral race. MacronGate consisted of fabrication and diffusion of documents suggesting Emmanuel Macron possessed an offshore bank account. The fabricated information was primarily relayed on Twitter by American alt-right profiles. MacronLeaks refers to the hacking and leaking of candidate Macron's campaign data. In both cases, the events were the work of a fluid galaxy of French and international alt-right supports and pro-Kremlin profiles on mostly informal discussion platforms.

Some of the strongest hybrid threat activities in the information domain are rooted in what is, or at least appears to be factual. They often rely on existing social tensions in the target audience by leveraging and amplifying divisive content. The coverage of the Yellow Vests movements corresponded to a long-standing agenda of Russian media outlets (RT France and Sputnik) to instrumentalise any division in western societies to counter the liberal criticism of the Russian regime. Coverage did not rely on disinformation or fabricated content because of resilience measures in place, but instead on biased and intensely politicised narratives. The case-study illustrates:

1. Attempts to use the election cycles as key vulnerability moments to interfere into democratic processes

2. Outside interference is enabled by existing polarisation to undermine the trust basis in the society.

3. Manipulation of a narrative of unbiased news coverage, to discredit the 'mainstream media'.

The 2017 hacks and leaks, and the 'non-biased' coverage of the Yellow Vests violent protests suggest a proximity of Russian influence policies with the European and American far right. Activities mostly targeted national and local levels of the civic and governance spaces, but were supported and amplified by activities and transnational communities in the international layer of civic space. In the civic and governance spaces, those activities aimed to undermine democratic processes and institutions and leverage the political polarisation to undermine the foundations of trust in the society. The multifaceted nature of the challenge implies that resilience to such information

disorders also goes well beyond the information or cyber domains and covers many aspects of the civic space, governance and citizens and must be placed within a framework of resilience to other societal and democratic challenges.

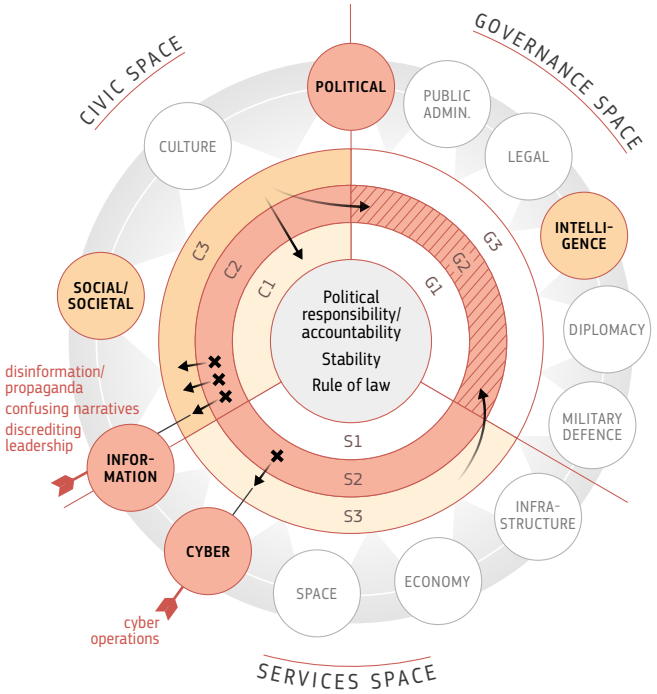
This case study shows that the following ecosystem foundations have been impacted:

- **Stability:** the tense societal and political moments within which those information manipulation attempts took place (election cycle and national social conflict) were particularly critical for the channels of peaceful diffusion of tensions.
- **Rule of law:** the purpose of the hack and leak attempts was to suggest that forefront politicians would be corrupted tax-evaders or that they would break electoral and political campaigning laws.
- **Reliability:** the narrative on 'non-biased' coverage by RT and Sputnik regarding the Yellow Vest protests suggests that media coverage would be biased and of inherently bad faith.

FIG 12. France — CORE analysis

State and non-state actors exploit vulnerabilities in a country by different means and on different occasions to unbalance social and political peace.

MACRONGATE/LEAKS (INFLUENCE)



2017

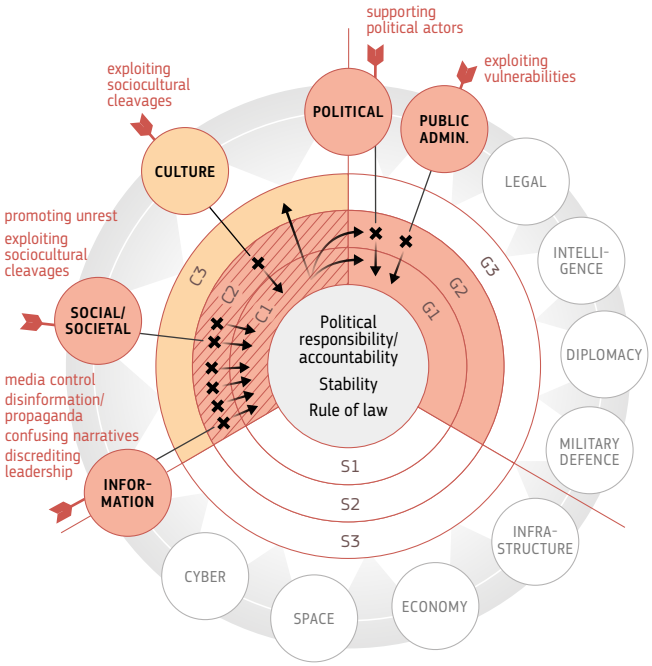
- **Cyber operations:** hacking and creating fake information against the campaign team of then-presidential candidate E. Macron.

  S2→S3→G2 International alt-right activists became active and participated in the creation and spread of fake information (S3), which affected the election campaign in France alerting intelligence services about possible Russian involvement (G2).

- **Creating confusion or contradicting narratives. Discrediting leadership or candidates. Disinformation campaigns, propaganda**
  Tools all aimed at using leaked and false information created to damage Macron's reputation in society (C2).

  C2→C3→C1/G2 The leak was picked up and disseminated by right-wing groups internationally (C3), spreading the issue in France at local level (C1) and influencing the election campaign (G2).

YELLOW VESTS (CAMPAIGN)



2018

- **Creating confusion or contradicting narratives. Discrediting leadership or candidates. Disinformation campaigns and propaganda. Media control and interference**
  Tools used to further inflame French society through false information spread by Russian media outlets (C2).

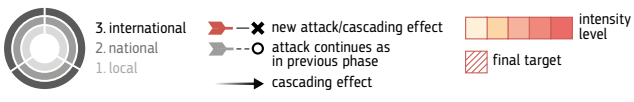
  C2→C1→C3/G2/G1 This affected local-level protests (C1), before having an international impact and influencing national and regional politics in France (C3/G2/G1).

- **Exploiting sociocultural cleavages. Promoting social unrest**
  Tools used to radicalise the protest movement and aggravate the domestic situation and national tension in society (C2).

  C2→C1→G2/G1 It then spilled over to the local level (C1) with implications for national and regional policy (G2/G1).

- **Exploiting vulnerabilities in public administration. Support of political actors:** Influenced public administration by targeting and supporting politicians who favoured the protests.

  G2→G1 This situation at national level then spilled down to local level and regional politicians became involved (G1).



5.9. CHINA'S STATE PROXIES CASE STUDY

Compromised foundations: civil rights and liberties, political responsibility and accountability, foresight

The use of non-state proxies by China shows a systemic merging of public and private actors, in the form of weaponising individuals, groups or businesses and associations. The practice of penetration over time into the influential circles of given countries could lead to decreasing trust in the integrity of governance actors. It also increases the fragility of the ecosystem since it opens opportunities for them to be leveraged in interfering patterns. This could especially undermine civil right and liberties as well as the rule of law.

The patterns of China's use of non-state actors (NSAs) as state proxies in different phases of hybrid threats are derived from several case-studies.

The use of NSAs in hybrid threat activities is not a phenomenon unique to China. Although not all Chinese NSAs act as state proxies, Chinese networks are notable for their significant level of organisation and outreach. Similar networks with almost identical peer organisations have been observed in several countries. NSAs offer China power to exert influence through interference, create change without clear affiliation. NSAs in diverse types of hybrid threat activities offer deniable escalation potential.

The distinctive feature of China's NSAs-related hybrid threat activities is that they are primarily conducted through the United Front system – a vast network of party and state associations responsible for influencing groups outside the CPC. The United Front Work Department (UFWD), under the direction of the Central Committee of the CPC is the organizational centre of the system. The associations, either directly or indirectly part of the network, are typically not illegal, highlighting the problematic nature of United Front work. The activities are managed through an easily deniable, yet constant presence within legal frameworks.

In the priming phase, the scope and intensity of China's NSA activities differ significantly, extending within a large spectrum from more legal forms of influence to attempt to change the way societies work. This creeping process is incremental and has potential to alter decision-making processes. Various associations, with strong links to the United Front system are active in EU Member States in several domains.

1. The NSA networks operate especially on the national and local layers of the civic, governance and services spaces, since they leverage their good integration into target societies.

2. In the civic space, United Front-related actors seek to establish civil organisations as a cover to avoid drawing attention. Student, scholar, and science associations have been explicitly defined as a major target groups of United Front work.

3. In the governance space, intelligence gathering, perception management and other efforts to deepen connections with major political parties, or placing individuals in key political positions that are prime candidates for future and opportunistic influence. The networks of the International Liaison Department of the CPC are a case in point.

4. Operating between governance, civic and services spaces, various business associations and Chinese state-owned enterprises (SOEs) establish economic connections at different layers of the ecosystem.

Non-government organisations (NGOs) with close ties to CPC or Chinese SOEs actively promote China's overseas economic interests and undermine various international norms (diplomacy, political, legal, economy, information, cultural, intelligence). In a destabilisation phase, the activities of China's NSAs become more visible and aggressive in the form of hybrid operations. China has applied NSAs in hybrid operations in Taiwan, and against its opponents in the South and East China Seas. As the intensity increases the use of SOEs becomes less covert. Offshore drilling companies have faced accusations of working together with the People's Liberation Army (PLA) to intimidate neighbouring countries. China's para-military maritime militia is an integral part of China's hybrid threat efforts towards its territorial claims. The maritime militia offers China deniability, executing its maritime hybrid threat operations and creates ambiguity and exploits the seams between governance and services spaces. China's use of NSAs further suggests patterns of destabilisation activity entailing vigorous narrative promotions, disinformation, and propaganda, as well as cyber-attacks. NSAs have been used in activities suppressing independence movements, undermining local identity, and seeking support for China's political system.

China's United Front Strategy takes advantage of a broad variety of NSAs as state proxies to create an effect that harms and undermines the decision-making algorithm and liberal democratic system of the target state. Despite the uncoordinated use of NSAs, the hybrid threat activities in one domain, space, or layer, supplement the objectives elsewhere. Given the complex network of China's NSAs and often covert nature of their activities, China seeks to mask its activities and strategic goals through concealment and deception. For this reason, it is paramount to understand the interaction dynamics between the components of the ecosystem and apply a comprehensive and more strategic approach to resilience building.

China's NSA leveraging undermines the following foundations:

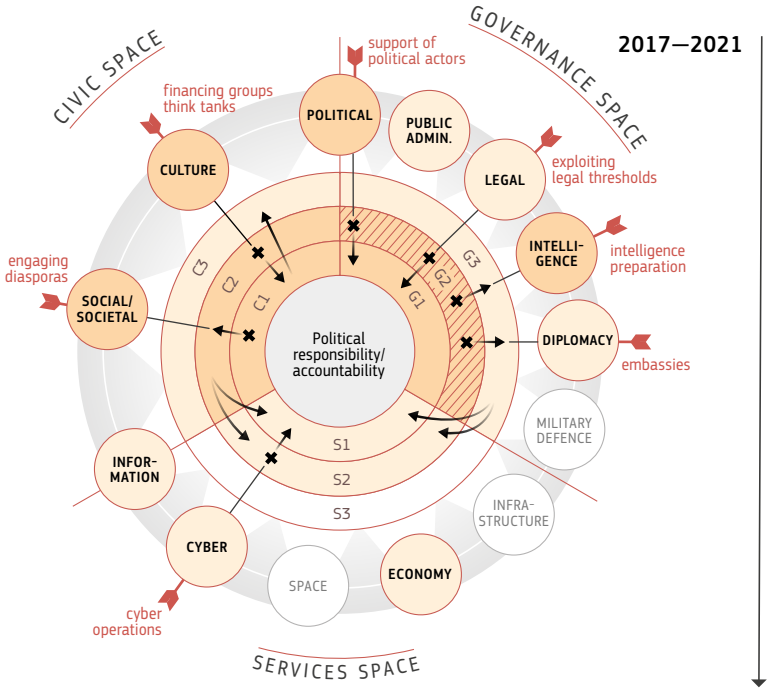
- **Civil rights and liberties:** especially freedom of expression, if criticism of the Chinese actions and regime gradually tends to be discouraged or subject to a chilling effect in multiple ways.

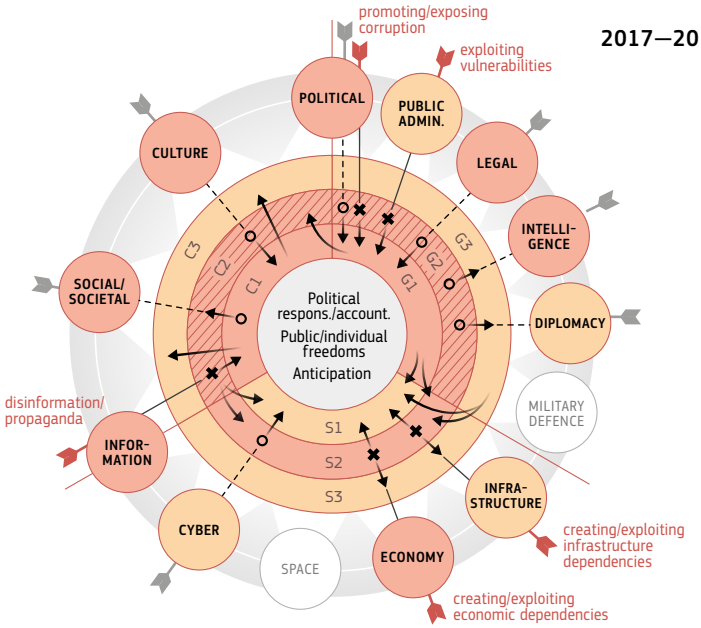
- **Political responsibility and accountability:** public and private decision-makers may be influenced or won-over by the work of non-state actors, state owned enterprises or other civil networks.

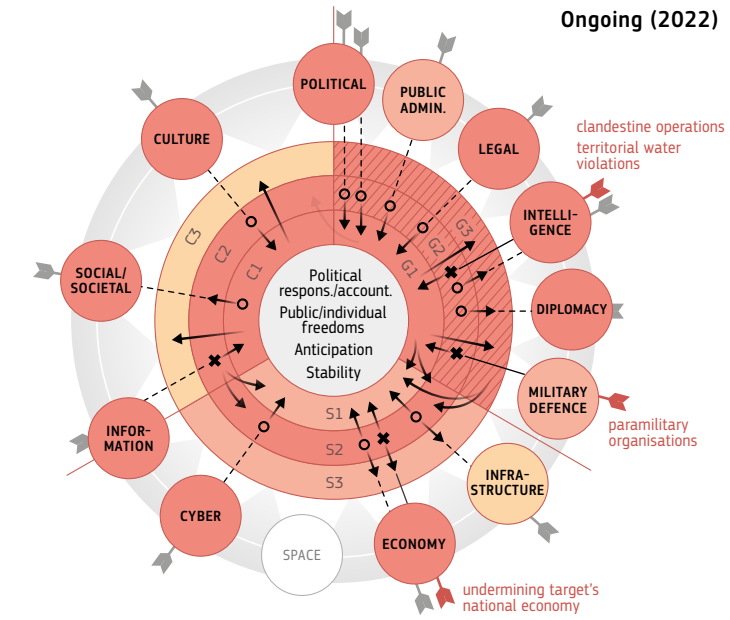
- **Foresight:** the blurring between business logic and international security interests makes it more complex to predict the behaviour of non-state actors.

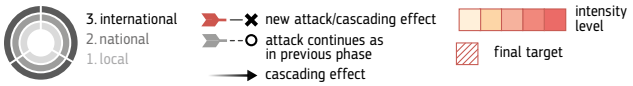
FIG 13. China's state proxies — CORE analysis

China engages in hybrid threat activities through proxy-none-state actors in several countries with varying intensity to gain influence.









FINLAND (INTERFERENCE)

- **Engaging diasporas to influence them** to establish societal and cultural links.
  C1→C2→S1/S2 Cascading to national level (C2). The networks built effected indirectly national and local economy (S1/S2).
- **Financing cultural groups and think tanks** to spread pro-Chinese views.
  C2→C1→C3 Affected the local level (C1) and indirectly influenced society and the information domain at the international level (C3).
- **Support of political actors** who took a pro-China stance.
  G2→G1 Had influence on local politics (G1) and thus indirectly on local public administration (G1).
- **Intelligence preparation** by Chinese proxies.
  G2→G3→S1/S2 Had an impact on the knowledge of Chinese intelligence services at the international level and indirectly on their access to the local and national Finnish economy (S1/S2).
- **Cyber operations** by Chinese proxies.
  S2→S1 Impacted cyberspace also at local level (S1).
- **Exploiting legal thresholds** to establish Chinese presence in Finland.
  G2→G1 Affected legal basis down to local level (G1).
- **Use of embassies** to provide shelter to non-state actors.
  G2→G3 Affected international diplomacy (G3).

AUSTRALIA (INFLUENCE)

- **Creating and exploiting economic and infrastructure dependencies** to gain leverage.
  S2→S1/S3 Had impact on economy and infrastructure on the local (S1) and international level (S3).
- **Disinformation and propaganda** to spread Chinese narratives.
  C2→C1→C3 Cascading effect to local level (C1) before indirectly affecting politics and society internationally (C3).
- **Promoting and exploiting corruption** in politics through Chinese bribery.
  G2→G1→C2/S2/S1 Impacted local politics (G1) and indirectly influenced society at national level (C2), as well as the economy at local and national level (S2/S1).
- **Exploiting vulnerabilities in public administration** through covert actions.
  G2→G1 Spills down to the local level of public administration (G1).

TAIWAN (CAMPAIGN/OPERATION)

- **Proxies: paramilitary organisations** prepare for military crisis/emergency.
  G2→G1→G3 Has impact at local level (G1) and indirectly affects Chinese intelligence globally (G3).
- **Clandestine operations** to increase preparedness.
  G2→G1→G3 Has impact down to the local level (G1) and indirectly affects the military domain on a global level (G3).
- **Territorial water violations** to gather information and test boundaries.
  G2→G1→G3 Has impact down to the local level (G1) and indirectly affects the legal domain internationally (G3).
- **Undermining the target's national economy** through economic influence.
  S2→S1/S3 Has impact on the economy at local and international level (S1/S3).

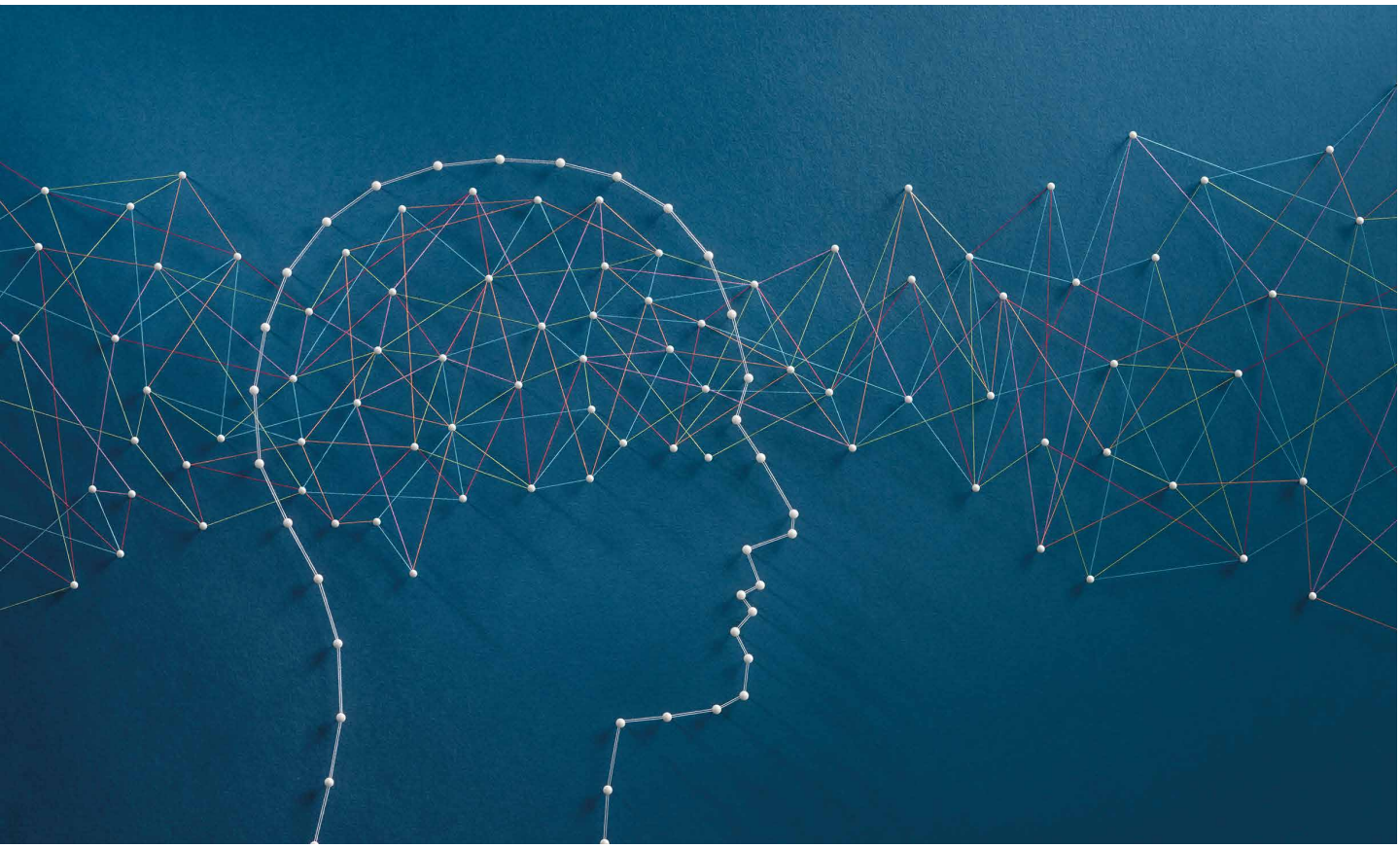
5.10. Conclusion: framing situational awareness

These case studies demonstrate the gaps between the governance, services, and civic spaces. Economic and business actors are aware of the inherent global integration of systems and inter-dependent processes and flows, but they are not always connected to the governance space and therefore they might not share governance side threat assessments. 'Civic' shows there is a lot to be done to connect the civic space to service and governance spaces. It also shows, based on the case-studies, that the civic space is a vital part of resilience-building, while the culture, social and political domains need much more attention and innovative ideas for building resilience against hybrid threats. The gaps between the three spaces explain parts of the crisis of trust in democracies and the rise of diverse types of illiberal populism within democracies. It is a key vulnerability, which has been used extensively by hybrid threat actors. This was evident in the Catalonia, Covid-19 and France cases.

> "The ecosystem dart board can facilitate foresight and situational awareness, as well as indicating where responses should originate and from which jurisdictions."

The case studies confirm the validity of the ecosystem approach in identifying connections, effects, and needs for resilience. The list of vul-nerabilities exploited or created can provide an agenda for building resilience in domains and spaces. The case studies indicate in several ways in which the ecosystem's foundations have been weakened, showing the main types of vulner-abilities that could undermine the EU's and its Member States' resilience. A strategic approach to resilience against hybrid threats must be guided by the dangers against the foundations of the ecosystem as those are the key choke points that hybrid threat actors seek to undermine and harm. Hybrid threats deploy through multiple spaces and layers with domain-based tools. Activity detected in a particular space and layer can provide early signals as to where more action can be expected. The case studies also suggest that decisions taken in response to perceived threats can directly undermine the ecosystem's foundations. Therefore, decision-making in countering hybrid threats needs to strike a delicate balance between action, propor-tion, and patience.

The ecosystem can form a comprehensive basis for a monitoring and information-sharing mechanism. The case studies, analysed through the prism of the ecosystem, showed that it was possible to represent events, disruptions, and effects along the three spaces of the ecosys-tem and according to their respective layers, while also picturing timelines and phases. Representing the ecosystem as a dart board can frame and support situational awareness at various levels among EU Member States as well as within EU Member States, by bringing a common frame of reference and terminology. Representing the ecosystem as a dart board can also help to build common situational awareness and improve the relevance of information exchanges between



European partners. It might also help in information sharing.

The case studies presented diverse types of activity from interference to destabilisation with different degrees of intensity and timeframes. The escalation potential of hybrid threat activity indicates a need to differentiate short, medium, and long-term resilience-building. The ecosystem dart board can facilitate foresight and situational awareness, as well as indicating where responses should originate and from which jurisdictions. The following chapter will expand on the use of the ecosystem as a strategic design board of response options to support policy coordination against hybrid threats.

HIGHLIGHTS

The ecosystem perspective is a blueprint for adaptive thinking and understanding the ways in which the EU and its Member States can individually and collectively foster resilience and enhance their margin of manoeuvre in countering hybrid threats. The domains can act as shields to protect the ecosystem and/or limit the impact of the domain-based tools but – if not well protected – they can also be the entry points to our ecosystem. The seven case studies presented in this report demonstrated the extent to which hybrid threat activity can undermine and weaken the foundations of our ecosystem, the foundation of a well-functioning democratic system.

The CORE model, used as a strategic design board, can help to design the right measures to counter the primary and higher-order effects of hybrid threats in all spaces and layers of the ecosystem, to implement a holistic approach for countering hybrid threats and serve as the conceptual foundation for the EU Hybrid Toolbox.

BUILDING RESILIENCE TO HYBRID THREATS

THE COMPREHENSIVE RESILIENCE ECOSYSTEM (CORE) AS A STRATEGIC DESIGN BOARD

6.1. Introduction: the added value of the CORE model

Resilience to hybrid threats acts to safeguard the way of life in democratic states, as well as processes connected to the democratic state system.

The CORE model brings new elements to the conceptual model, which is central when thinking of resilience against hybrid threat activity (Cullen et al, 2021). One of the characteristics of hybrid threats discussed in the conceptual model was that they take advantage of the seams in democratic societies. Practically, the proposed structure of the CORE model – with the three spaces and three layers in each space – aims, among other things, to provide an answer to this characteristic of hybrid threats. Hostile actors will try to take advantage of different spaces, hoping that these will not communicate with each other. In so doing it also takes advantage of local, national and international layers, which are also often somewhat disconnected. Furthermore, the domain-based tools used can vary depending on the layer. Without this consideration, resilience-building in the national layer can be undermined by low resilience in local or international layers. An approach that takes the spaces and layers into account enables the hostile actor to remain below the threshold of detection for quite some time, to blur the aim of the activity and create ambiguity. It may create cascading effects and surprises: for example, a local-level event that starts to challenge the whole state and even the EU. This type of activity challenges our legislative processes, our way of structuring administration, detection abilities, and foresight capabilities.

> The CORE model can support the development of an EU hybrid toolbox by structuring different measures through the spaces, layers and domains.

In the centre of the model stand the individuals, whose role in building resilience is essential. The foundations of the ecosystem are to protect the individuals in the democratic system. However,

individuals can also help to maintain the strength of the foundations and therefore also strengthen resilience by recognising, respecting and supporting the EU values recognised by various treaties. It is important to maintain the social contract between the civic, governance and service spaces, as well as individual buy-in in resilience building. The role of the service space (private sector) has also become a key factor in building resilience against hybrid threats, as well as developing response capability.

In practical terms, **the CORE model can serve as a strategic design board** for deciding which resources, tools and measures to mobilise in the face of hybrid threat activities at EU and MS levels, as well as at more operational levels, in order to support activities such as hybrid threat scenario exercises.

> “It is important to maintain the social contract between the civic, governance and service spaces, as well as individual buy-in in resilience building.”

6.2. Overarching themes for resilience against hybrid threats: response capability building

6.2.1. Legislative processes

The legislative processes in the EU and in the MS can become an essential element for countering hybrid threats. A functioning rule of law also builds trust in society and respect of norms. However, laws can also be seen as a systemic vulnerability, in so far as certain rules or features of a legal system, – such as gaps and uncertainties in the law – may lend themselves to exploitation by hostile actors (Sari, 2021). The potential risks that may arise from an ambiguous legal environment on the one hand, and, on the other, a lack of adequate collaboration between internal and external security, constitute new challenges for state authorities in the era of hybrid threats (Ferm, 2017). The legislative processes touches upon most of the 13 domains in all the spaces and layers of the ecosystem. Legislative processes are therefore a key component of democratic states when building resilience against hybrid threat activity.

In principle, the legislation-making process in the EU has a strong sectoral component – and rightly so. The inclusion of considerations and notions from hybrid threats will enable the ecosystem approach to be implemented in the EU and MS legislative process. While, in principle, a legislative act is focused on a specific space, layer and respective domain, the inclusion of hybrid threat considerations will lead to legislative acts that are more holistic and comprehensive, such as taking into account the links and dependencies with other spaces, layers and domains. Recent legislative acts such as the Network and Information Security (NIS2) Directive and Resilience of Critical Entities Directive are examples of how legislation at EU level can take a more holistic approach, considering several domains and the complete resilience cycle from mitigation of vulnerabilities to reporting and enhancing of governance structures. Regarding Member States’ legislative processes, a good example is the way in which Finland adapted new amendments to the legislation concerning the Territorial Surveillance Act and the Criminal Code in Finland, which entered into force on 15 July 2017.

The powers of the territorial surveillance authorities were reinforced so that they would better cover situations where Finland's territorial integrity is violated by a military group without insignia.

6.2.2. Paradigm shift in the security culture

Developing the necessary security culture within the EU and within each MS in order to build resilience against hybrid threats will require a paradigm shift in the culture of the organisations and officers working in this area. The mainstream security culture in many cases restricts information flow between the various levels (local, national and international), leading to a linear, silo approach. Building trust and connecting silos requires considerable investment, time and a horizontal approach.

Experience has shown that there is a good interagency cooperation model in the field of internal security. For example, police, customs and border guards have various platforms where they can exchange information and even plan joint operations. However, sharing of information, best practice and lessons learned – apart from their organisational, cultural aspects – also requires the necessary regulatory environment.

Building this security culture also requires a better understanding of multidisciplinary topics. For example, highly skilled cyber security officers need to be trained in areas related to communication and vice versa. Staff working in one of the three spaces (civic, governance, and services) need to have a good understanding of what is happening in other spaces as well.

6.2.3. Detection

Detecting hybrid threat activity in its early stages (priming) can help enhance resilience. In order to have effective detection capabilities specifically designed to identify hybrid threats, a networked 'points of contacts' (POC) approach in all domains, layers and spaces is recommended. POCs can be identified and defined in all of the EU's fields of shared and exclusive competences. The same applies to the national networks of Member States.

Technology can play a central role in improving detection capabilities and the ability to 'connect the dots'. This does not apply to all domains in the same way, but does touch upon all the CORE model spaces and layers, through different domains. The collection of mass datasets and their analysis inevitably invites discussion of the role of AI and how it can be leveraged in security-related datasets. This is a very good example of how technical capability needs to be connected to multidisciplinary analysis abilities, and how technology can be of help to security analysts.

Another important factor in detection capabilities is the identification of the true actors behind the hybrid threat activity, since these are deliberately concealed. The use of undisputable facts to identify the actors is a central element of resilience against hybrid threats. Responses to state and non-state actors need to be different, however, as there is no one-size-fits-all approach. Furthermore, an activity that looks like a foreign hybrid threat might not be so.

Detection of threat actors is the remit of the MS Intelligence services, which have specific tools and mechanisms in place. This capability should be strengthened, with Open-Source Intelligence (OSINT) across national administrations. This has proven its value during hybrid activities, both in the priming phase but also during full escalation phases (as is the case in Ukraine in 2022). The intelligence community should situate itself as an enabler of this interagency cooperation, thus strengthening resilience against external hybrid threats. While the community of intelligence analysts has taken steps to integrate the various policy perspectives – see, for example, the role of the Office of the Director of National Intelligence (ODNI) in the United States or the Intelligence and

Situation Centre (SIAC) in the EU – the challenge also applies to intelligence as a target domain for hostile activity.

6.2.4. Ability to innovate, develop and adapt

An important part of classical resilience-building is the ability to recover and 'bounce back' or 'bounce forward'. However, when countering hybrid threats, recovery, 'bouncing back', or 'bouncing forward' might in fact be the goal of a hostile actor. When refer to 'bouncing forward' we must always take into account the possibility that we are unknowingly being 'pushed forward' in the direction the hostile actors want us to go. So, when talking about hybrid threat-related activities and their goals, more attention is needed to avoid the trap of *reflexive control* by a hostile actor. Focus must be on the ability to truly innovate, develop and adapt, as well as the capacity to *define* what innovation, development and adaption entail.

The ability to innovate, develop and adapt are key elements of the economic growth, well-being and dynamic nature of a state. For democracy to endure and support innovation, it needs a culture that stems not only from structure, but also from the principles of an open society, where actors agree to disagree, respect the rights of the opposition to participate and contest (when they are in power), and trust in the possibility of future change (when they are in opposition) (Pepinsky, 2020). The concept of 'authoritarian innovation' describes governance practices designed to shrink spaces for meaningful public participation (ibid., p.1902). If a hybrid threat actor manages to shrink our space for meaningful public participation and limit or guide the decision-making process, it will manage to harm and undermine a strength in democratic societies. In this respect we should enhance our own capabilities for 'democratic innovations' that would support our abilities to innovate, develop and adapt to new challenges.

6.2.5. Foresight

As hybrid threats evolve, new tools are used, new opportunities created and priming constantly carried out. **Strong resilience against hybrid threats is very much a matter of developing capabilities to look ahead and anticipate**, even to define the agenda. Foresight is therefore the essence of the utility of the CORE Model. All the spaces and their layers should be considered from a forward-looking perspective. The case studies in this report provide a good starting point – how to use knowledge of what has happened to look forward and anticipate. Ecosystem thinking could serve in regular review and foresight assessments of ongoing hybrid threat activity, both in the EU and in individual Member States.

6.3. Implementing the ecosystem approach: how to enhance resilience against hybrid threats?

6.3.1. Civic space

The civic space in democracies rests on three foundations: justice and equal treatment; civil rights and liberties; political responsibility and accountability. These three foundations ensure that the democratic system brings welfare and prosperity to democracies. A well-functioning and democratic society that is resilient against harmful outside influences is able to protect the three foundations of civic space. Individuals at the centre need to be able to feel that their human rights are respected, that they are included in their societies and in the international communities to which their countries belong. They need also to be engaged in the political processes. **A resilient civic society is active in engaging in its societal developments with healthy polarisation.** The cultural and information domain play a very significant role here.

Education

Education-building and planning is a Member State competence. Schools are key institutions in

building solidarity, preparing for future security challenges and changes in our societies. The case studies showed that, for example, poor knowledge of history, being unfamiliar with the world of disinformation, or dropping out of society have been exploited by outside actors to interfere, influence and destabilise. Teachers in primary and secondary schools across the EU should be seen as a central group to be engaged with when building long-term resilience. In all spaces, resilience-building should start at the local level. Since hostile hybrid threat actors are using education as a tool we should use education in our own countering strategies. The EU can bring added value by supporting the production of new teaching materials and by supporting initiatives to strengthen media literacy. Here it should be borne in mind that different generations have different needs when it comes to media literacy.

Information

Information is the domain that is used most by hybrid threat actors to cause disruptions, especially in the civic space. The information domain amplifies the impact of other malign tools. Information-related hybrid threat activity in the civic space aims at creating cascading effects, using many different domains and different tools, depending on the layer. The manipulative information interference can then negatively impact the governance and service space. To build resilience against the harmful effects of manipulative information interference the EU and Member States should consider the following:[17]

- Foster the trust in media, media sustainability, and access to quality news;
- Foster openness, transparency, and participation in strategic communications;
- Safeguard democratic dialogue and civil society;
- Transparency – publish information on ownerships for all media (print, radio, TV, social media, internet news pages etc.). The legal status of social media platforms also plays an important role here.
- The legislation regarding 'deepfakes', use of bots and robo-journalism needs to be examined and updated both at EU and Member State levels.
- Protection of free, independent media; for example, media laws that support and protect free reporting

Participation

Societal unity is an important part of increased resilience against hybrid threats. Participation of citizens in the democratic decision-making processes can help to create a feeling of being heard, being understood and – even if one's own views are not fully represented by the

17 The following recommendation are partially based on the Hybrid CoE (2019) report.

sitting governments – the feeling of belonging to the same system. Participation in democratic processes happens primarily through general elections. Elections bring stability to democratic systems. It is therefore of utmost importance to safeguard elections at all levels against foreign manipulative interference. While the focus is often on elections at national level, local elections should be safeguarded with the same vigour.

To this end, the European Democracy Action Plan should be more widely promoted among citizens, explaining how it touches each individual within the EU (European Commission, 2020f). The Action Plan sets out measures to promote free and fair elections, strengthen media freedom and counter disinformation. The Plan aims to protect and promote the meaningful participation of citizens, empowering them to make their choices in the public space freely, without manipulation. The Plan proposes actions to increase the protection of journalists and to combat disinformation and interference, while fully protecting freedom of speech.

Another possible line of action is to create resilience against hybrid threats through solidarity between citizens of the EU Member States. A high level of cohesion and solidarity with the citizens in the distressed country will lead to a higher level of support from Member States and even the EU. In order to achieve this solidarity, connections between the spaces and layers need to be improved. This aspect should be considered while developing the hybrid toolbox.

6.3.2. Governance space

The rule of law and stability are the foundations of the governance space. Both are foundations that the hybrid threat actors would aim to undermine and harm. Resilience against hybrid threats in the governance space means institutional continuity as well as the ability to adapt, both in and outside of normal circumstances. **A resilient governance space adopts a holistic approach; its ability to create and maintain social contracts is high; it is prepared for unexpected circumstances, and its response and decision-making capabilities are fast and firm.** A number of specific measures can be put in place, but these are national responsibilities, to be designed according to the specificities of each country. The situation at the EU level is the same. The CORE model can be used to introduce the strategic element into the planning process.

Whole of governance approach in countering hybrid threats

Surprise and related institutional stress are normal working conditions for crisis decision-making. When it comes to the ability to counter the crippling effects of hybrid threats, timely decision-making is essential. One of systemic weakness in the landscape of hybrid threats for democratic states is that our political power is complex, but our practitioner level and domain-related decision-making is

often disconnected and separated. This means that the principle of protecting a whole interlinked ecosystem against hybrid threats requires a holistic and swift approach.

Governments should facilitate inter-agency and inter-ministerial approaches, where the potential of hybrid threats is handled. Sectoral jurisdictions and responsibilities must naturally be maintained, but in the organisation of joint work, a common situational awareness should be upheld. The sharing and assessment of sensitive information should take place in a timely way between all relevant trusted actors. When needed, this should lead to planning for further collection of information or operational countermeasures.

Furthermore, lowering the barriers between government actors and maintaining the possibility to start investigating weak signals that are potentially significant but not fully validated, is important for building resilience, notably during the priming phase. This can be achieved through a culture that recognises hybrid threats as an existing, albeit mainly invisible fact.

Horizontal structures at government level need to be developed further, with the capability to have access to, collect and analyse information and coordinate actions across ministries. In the case of EU Member States, the layer of multilateralism becomes particularly important, given the existing structures at EU level which need to be maintained and reinforced. Collaboration with NATO is another element of resilience in the multilateralism layer.

Social contract

Trust has been identified as an essential element for effective resilience. Trust is the glue that makes dependencies and connections in democracies strong and healthy and binds societies together. The governance space plays a key role in building trust, partly because of the responsibility of governance space actors to foster social contracts. It has been shown that social contracts enhance the viability and stability of a society. Social contracts are established through legitimacy, which stems from at least three sources: *performance* (what leaders, or the governing, do for the benefit of followers, or the governed, and what followers must do to receive benefits); *processes of exchange* (mechanisms by which leaders and followers interact); and *shared values* (identities and interests common to leaders and followers that bring them together into a consensual pact) (Magnuson et al., 2022).

Preparedness planning and response implementation

The credibility of responses to hybrid threats depends on the effectiveness of the implementation of decisions. Pooling and sharing at the operative level is one of the strong points of EU integration and inter-institutional cooperation. Mechanisms, common measures and obligations, as well as platforms can be mobilised for EU or national crises as appropriate. This is one way to increase the individual and collective margin of manoeuvre of EU Member States. The Union Civil Protection Mechanism, especially with rescEU, is an example of successful pooling and sharing. Extending the thematic scope of such a mechanism – or building a similar mechanism in the security domain –would be a key credibility-building element regarding the EU's capacity to pool resources and be more than the sum of its parts.

Throughout its various crises, the EU has adapted and created *in situ* mechanisms that have set precedents and good practices in managing surprise, emergency and stress at EU level. The Integrated Political Crisis Response (IPCR) mechanism and its different modes is a good example of that trend. Improving the IPCR could entail using the ecosystem /CORE Model in all modes for a shared situational analysis / appreciation, especially with respect to the Integrated Situational Awareness and Analysis reports produced by a lead-service in the Commission or (potentially) the European External Action Service (EEAS).

6.3.3. Services space

Resilience against hybrid threats in the service space means reliability and filtered impact of direct hybrid threat activity. Since the service space primarily protects the foundations of reliability, availability, and foresight, **resilience building against hybrid threats in the service space should consider investments, public-private cooperation and secure logistical networks** of goods and services. This is a space in which the domains are relatively well protected. A high level of resilience has already been built in the domains and sectors, but there is still a need to pay more attention to 'connecting the dots'.

Investment

The ecosystem approach aims to improve resilience against hybrid activities. By definition, this requires investment from Member States in all spaces, layers and domains. Nevertheless, the use of available resources, which obviously are not infinite, should be prioritised in order to maximise the impact of investments. This requires a careful analysis of vulnerabilities across domains and the identification of those entry points that can maximise the impact of hybrid activities. Exercises like the response to Action 1 of the Joint Communication of 2016 are essential in order to identify vulnerabilities and entry points. The prioritisation of investments in resilience should be seen in a more systemic way. Apart from the analysis of vulnerabilities within domains, attention should also be paid to connections, dependencies, and potential non-linear effects.

Public-Private partnership

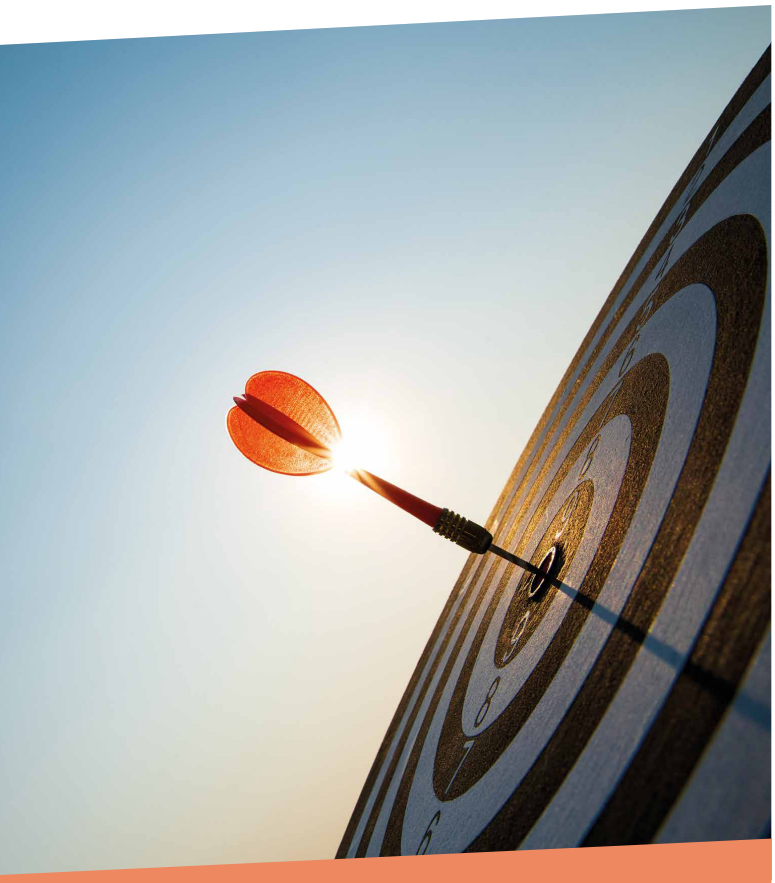
A vast majority of services are privately owned and follow a business logic. In the hybrid threat realm, the service space can be targeted by hostile state actors. Their capacity to penetrate systems and inflict damage goes beyond what the various service branches are used to handling. Governments should assess the services jointly in terms of vulnerabilities and resilience requirements. Key services should be seen as potential targets, attracting protection and situational awareness support from the agencies.

Throughout the resilience ecosystem, it is useful to prepare for the collection of valid evidence for possible attribution, if the true actors behind a hybrid threat are hidden. The private sector plays an essential role in evidence collection. Domains belonging to the service sector, like infrastructure, cyber, space and economy, are prone to be used as entry points into the ecosystem. The aim of the activity is to damage, slow down, overload or in any other way disrupt the services. Member States, together with the private sector, are encouraged to establish requirements for monitoring critical entities. This would also support the EU's and Member States' capabilities for detection, as well as foresight.

Building resilience requires raising the awareness of businesses regarding hybrid threats, including the ways in which they manifest themselves and the intentions behind them. This could improve cooperation between public and private sectors.

Resilient supply of goods and services and access to critical technologies

Disturbances in supply chains, or rapid, unexpected increases in demand for any goods, components, or materials, can have serious consequences for the services. Based on lessons learned during the pandemic, governments should pay attention to the availability of critical material during disturbances, as laid out in the updated '2020 New Industrial Strategy' (European Commission, 2021b). EU Member States should exchange experiences and best practices on how resilience can be enhanced by public and private stockpiling, and through funds, etc. At a more strategic level, the concept of strategic autonomy should be applied in a series of sectors and domains. The recent announcement about secure space connectivity shows how the EU should become more sovereign in critical technologies and critical services (European Commission,



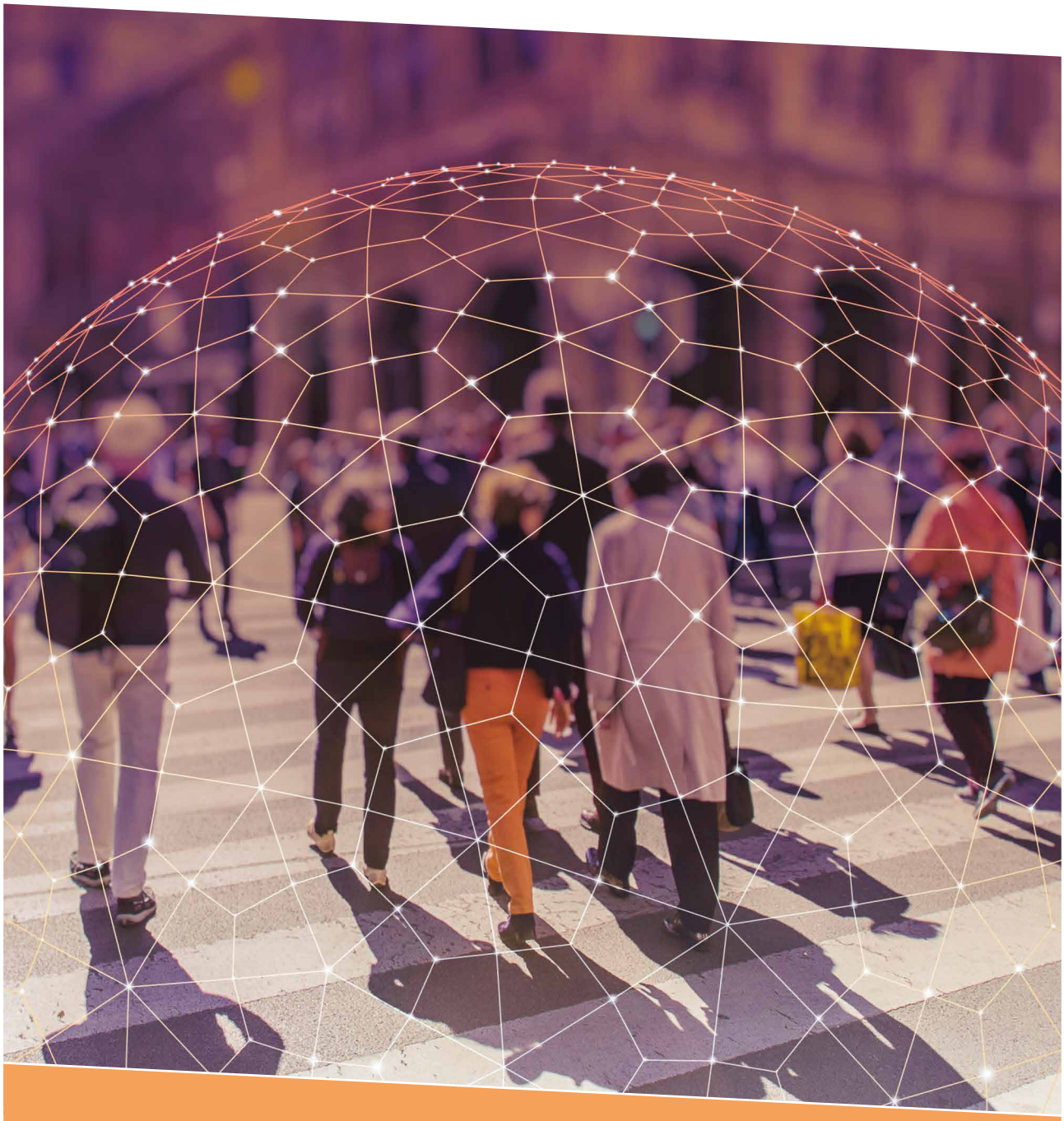
> “Responding to a crisis with measures that undermine the foundations of the ecosystem hands strategic victory to hybrid threat actors on a silver platter.”

2021e, European Commission, 2022a). This is a vast area for the EU to work upon and requires close involvement with the private sector.

6.4. Conclusion

States need to expand their analysis and awareness of a given situation in order to escape the traps embedded in a hybrid threat activity. Responding to a crisis with measures that undermine the foundations of the ecosystem hands strategic victory to hybrid threat actors on a silver platter.

To ensure that those strategic victories will not be achieved, whether small or large, the EU is working on a hybrid toolbox to enhance the EU’s resilience, including responses and baselines. The CORE model could be one of the elements to inspire the design of the hybrid toolbox and to structure various measures through spaces, layers and domains. The development of capability might consider foresight, detection and decision-making abilities. Attention should be paid to the use of legal frameworks to enhance resilience and maintain a margin for manoeuvre. The security culture needs to be updated in order to match the current security environment, while the interconnections between different spaces, layers and domains need to be explored further. Response implementation can benefit from stronger solidarity within the EU and between different Member States. Meanwhile, EU-NATO cooperation should be seen as a resilience measure. Domain-based resilience can act as a shield against hybrid threat activities, but without a stronger emphasis on the ecosystem approach, the core foundation of the ecosystem could be in danger. If we manage to strengthen the foundations, we will also build resilience against harmful hybrid threat activities.



HIGHLIGHTS

This report argued that the ultimate goal of hybrid threats is to undermine and erode democracy and that therefore a holistic and systemic approach is needed to enhance the fostering of resilience to hybrid threats. The comprehensive resilience ecosystem model (CORE) that we propose provides such a holistic and systemic approach to enhance the understanding of the effect of hybrid threats and which provides guidance on how to build resilience against them.

The ecosystem perspective is a blueprint for adaptive thinking and understanding the ways in which EU Member States can individually and collectively foster resilience and enhance their margin of manoeuvre in countering hybrid threats. The CORE model can serve as a strategic dashboard for deciding which resources, tools and measures to mobilise in the face of hybrid threat activities. Furthermore, it can provide the necessary conceptual basis for building a comprehensive whole-of-society approach to resilience.

TOWARDS MORE TRUSTED AND RESILIENT SOCIETIES AGAINST HYBRID THREATS

We have argued in this report that the **aim of hybrid threat activity is ultimately to undermine and erode democracy.** We highlight the **importance of trust** in resilience-building, as it brings greater predictability; citizens are more willing to follow trusted leaders during times of change, and it affects both how people communicate and how people assess the honesty and validity of what is being communicated. Indeed, political leaders should have high trust levels as their north star, so that the level of resilience in their countries against hybrid threats remains high.

Fostering resilience to hybrid threats therefore requires a holistic and systemic approach. To facilitate this process, we identify the key components and foundations of democratic societies and how these could be used in a systematic manner in the resilience-building process. The elements of spaces, layers and the connection with the domains transform the concept of resilience into something tangible that can be used by policymakers.

> The CORE model advocates a comprehensive, whole-of-society approach to build resilience against hybrid threats and provides practical guidance on how to achieve this.

This is essential, since resilience 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 different spaces, layers and domains. **In the realm of hybrid threats, resilience aims at addressing the key elements of such threats: 1) the synchronised use of different tools 2) the cascading effects that might occur across domains and 3) the strategic goals of the adversary.** The model proposed here aims at addressing these issues.

The concept of resilience has been embraced by a variety of disciplines, often taking a sectoral approach and is currently more developed in technology-related domains such as infrastructure, cyber, space and the economy. In non-technology domains such as culture, intelligence, politics, and law, the approach has been different, and the level of maturity does not necessarily match that in technology-related domains. This is one of the reasons that political implementation of the concept has been hampered thus far. It is also why it is essential to implement an ecosystem approach to resilience that considers connections and interdependencies among sectors.

The comprehensive resilience ecosystem model (CORE) that we propose enhances the understanding of the effect of hybrid threats and provides guidance on how to build resilience against them. The ecosystem represents the main dependencies, spaces and layers affected by a given hybrid threat activity.

Based on the case studies it is clear, for example, that that the civic space is a vital part of resilience-building, while the culture, social and political domains need much more attention and innovative ideas for building resilience against hybrid threats. Countries with high levels of resilience in the services space, for example, might face negative surprises due to a low level of resilience in the civic space. These different levels of resilience may explain parts of the crisis of trust in democracies and the rise of diverse types of illiberal populism. This is a key vulnerability, which has been used extensively by hybrid threat actors. Although challenging, democratic societies will need to identify ways to innovate in the civic and governance spaces.

In the previous chapters we refer to resilience as it is perceived in other cultures as, to date, this has not been thoroughly considered in countering hybrid threats. We need to be able to better understand the culture of others, put ourselves in their shoes and understand their thinking. In this way we will be in a better position to understand, interpret and even anticipate their strategic objectives, in particular for state actors.

Building resilience against hybrid threats also requires the ability to understand, in depth, future

> “The ecosystem perspective is a blueprint for adaptive thinking and understanding the ways in which EU Member States can individually and collectively foster resilience and enhance their margin of manoeuvre in countering hybrid threats.”

trends rather than responding to identifiable crises. It is important to develop foresight capabilities and credible scenarios as part of a shared vision of the security environment in order to strengthen the EU's resilience. This evolution from fact-based to trend-based risk management constitutes a paradigm shift in building resilience.

The ecosystem perspective is a blueprint for adaptive thinking and understanding the ways in which EU Member States can individually and collectively foster resilience and enhance their margin of manoeuvre in countering hybrid threats. At the EU level, this perspective could highlight the breadth of potential solutions, measures and tools that could be mobilised to counter hybrid threats.

While we need to take a holistic approach to resilience, countries should equally be in a position to apply a high level of granularity, in particular to detect early signals of hybrid threat activity. Therefore, decision-making in countering hybrid threats needs to strike a delicate balance between action, proportion, and patience.

On 21 March 2022, the EU published the Strategic Compass, which makes reference to building resilience against hybrid threats through the development of a hybrid toolbox. This will bring together existing and possible new instruments, including the creation of EU Hybrid Rapid Response Teams to support Member States, Common Security and Defence Policy missions and operations, and partner countries in countering hybrid threats (Council of the European Union, 2022).

The CORE model can serve as a strategic dashboard for deciding which resources, tools and measures to mobilise in the face of hybrid threat activities. It is a device to help practitioners and policymakers to be more aware of context-specific disruptive potentials, various response levers and dependencies among layers and spaces.

We are currently in an environment with increased instability, geopolitical competition and technological evolution. **The CORE model proposed here is timely, as it can provide the necessary conceptual basis for building a comprehensive whole-of-society approach to resilience. We cannot afford to do otherwise.**

REFERENCES

- Aaltola, M., Fjäder, C., Innola, E., Käpylä, J., Mikkola, H. , 'Huoltovarmuus muutoksessa: Kansallisen varautumisen haasteet kansainvälisessä toimintaympäristössä', *FIIA Report No 49*, Ulkopoliittinen instituutti, 2016, pp. 3-49. *https://www.fiia.fi/wp-content/uploads/2017/04/fiiareport49_huoltovarmuus_muutoksessa.pdf*
- Adger, W. N., 'Social and Ecological Resilience: Are They Related? Progress in Human Geography,' Vol. 24, No 3, 2000, pp.347-364. *https://doi.org/10.1191/030913200701540465*
- Britannica, 'Civil Rights.' Accessed March 8, 2022. *https://www.britannica.com/topic/civil-rights*
- Britt, T. W., & Oliver, K. K., 'Morale and cohesion as contributors to resilience' in R. R. Sinclair & T. W. Britt (Eds.), Building psychological resilience in military personnel: Theory and practice, *American Psychological Association*, 2013, pp. 47-65. *https://doi.org/10.1037/14190-003*
- Chesley, D.L. & Amitrano, M., 'Resilience: A journal of strategy and risk', *PwC*, 2015, pp. 1-6. *https://www.pwc.ch/de/publications/2016/pwc_ceo_survey_resilience_e.pdf*
- Council of Europe, 'State of Democracy, Human Rights and the Rule of Law: A Democratic Renewal for Europe', *Secretary General of the Council of Europe*, 2021, pp. 1-46. *https://rm.coe.int/annual-report-sg-2021/1680a264a2*
- Council of the European Union, 'Decision No 1364/2006/EC of the European Parliament and of the Council of 6 September 2006 laying down guidelines for trans-European energy networks and repealing Decision 96/391/EC and Decision No 1229/2003/EC, L262/1', *Official Journal of the European Union,* 2006. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006D1364&from=EN*
- Council of the European Union, 'Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection', *Official Journal of the European Union*, 2008, pp. 75–82. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=en*
- Council of the European Union, 'Council Conclusions on CSDP', Foreign Affairs Council, *8971/15*, 2015, pp. 1-16. *https://data.consilium.europa.eu/doc/document/ST-8971-2015-INIT/en/pdf*
- Council of the European Union, 'Council Conclusions on Complementary efforts to enhance resilience and counter hybrid threats', *4972/19*, 2019, pp. 1-11. *https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf*
- Council of the European Union, 'Council Conclusions on Security and Defence', 8792/20, 2020, pp. 1-11. *https://www.consilium.europa.eu/media/44521/st08910-en20.pdf*
- Council of the European Union, 'Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU, L170/69,' *Official Journal of the European Union*, 2021, pp. 66-148. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0696&from=EN*
- Council of the European Union, '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', *7371/22*, 2022, pp. 1-47. *https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf*
- Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., 'The landscape of Hybrid Threats: A Conceptual Model' (Public Version), edited by Giannopoulos, G., Smith, H. and Theocharidou, M., EUR 30585 EN, *Publications Office of the European Union*, Luxembourg, 2021, pp. 6-52. *http://dx.doi.org/10.2760/44985*

- Cutter, L. S., Barnes, L., Berry, M., Burton, C., Evans, E., Tate, E. & Webb, J., 'A Place-Based Model for Understanding Community Resilience to Natural Disasters', *Global Environmental Change*, Vol. 18, No 4, 2008, pp. 598-606. *https://doi.org/10.1016/j.gloenvcha.2008.07.013.*
- Etzold, B., Jülich, S., Keck, M., Sakdapolrak, P., Schmitt, T. & Zimmer, A., 'Doing institutions. A dialectic reading of institutions and social practices and its relevance for development geography', *Erdkunde*, Vol. 66, No 3, 2012, pp. 185-195. *https://doi.org/10.3112/erdkunde.2012.03.01*
- European Commission, 'Communication from the Commission to the Council and the European on Critical Infrastructure Protection in the Fight Against Terrorism', *COM(2004) 702 final*, 2004. *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF*
- European Commission, 'Green Paper: Damages Actions for Breach of the EC Antitrust Rules', *COM(2005) 672 final*, 2005. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0672&from=EN*
- European Commission, 'Communication from the Commission on a European Programme for Critical Infrastructure Protection', *COM(2006) 786 final*, 2006. *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF*
- European Commission, 'EU-Russia Energy Dialogue', *Direcorate-General for Energy*, 2011. *https://ec.europa.eu/energy/sites/ener/files/documents/2011_eu-russia_energy_relations.pdf*
- European Commission, 'Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure', *SWD(2013) 318 final*, 2013. *https://data.consilium.europa.eu/doc/document/ST-13280-2013-INIT/en/pdf*
- European Commission, 'Joint Communication to the European Parliament and the Council on the Joint Framework on Countering Hybrid Threats: a European Union Response', *JOIN(2016) 18 final,* 2016. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN*
- European Commission, 'Report from the Commission to the European Parliament and the Council on the implementation of the Galileo and EGNOS programmes and on the performance of the European GNSS Agency', *COM(2017) 616 final*, 2017. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0616&from=FR*
- European Commission (2020a), *2020 Strategic Foresight Report: Charting the Course Towards a More Resilient Europe*, Publications Office of the European Union, Luxembourg. *https://ec.europa.eu/info/sites/default/files/strategic_foresight_report_2020_1.pdf*
- European Commission (2020b*), Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Europe's moment: Repair and Prepare for the Next Generation*, COM(2020) 456 final. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0456&from=EN*
- European Commission (2020c), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU budget powering the recovery plan for Europe*, COM(2020) 442 final. *https://eur-lex.europa.eu/resource.html?uri=cellar:4524c01c-a0e6-11ea-9d2d-01aa75ed71a1.0003.02/DOC_1&format=PDF*
- European Commission (2020d), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy*, COM(2020) 605 final. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN*
- European Commission (2020e), *Joint Staff Working Document on Mapping of Measures Related to Enhancing Resilience and Countering Hybrid Threats*, SWD(2020) 152 final. *https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/swd/2020/0152/COM_SWD(2020)0152_EN.pdf*
- European Commission (2020f), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. On the European democracy action plan*, COM(2020) 790 final. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN*

- European Commission (2020g), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on 2020 Rule of Law Report: The rule of law situation in the European Union,* COM(2020) 580 final. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0580&from=EN*
- European Commission (2021a), *Resilience Dashboards for the Social and Economic, Green, Digital, and Geopolitical Dimensions*, Publications Office of the European Union, Luxembourg. *https://ec.europa.eu/info/sites/default/files/dashboard_report_20211129_en.pdf*
- European Commission (2021b), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery,* COM(2021) 350 final. *https://ec.europa.eu/info/sites/default/files/communication-industrial-strategy-update-2020_en.pdf*
- European Commission (2021c), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on 2021 Rule of Law Report: The rule of law situation in the European Union*, COM(2021) 700 final. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0700&from=EN*
- European Commission (2021d), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Action Plan on synergies between civil, defence and space industries*, COM(2021) 70 final. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0070&from=EN*
- European Commission (2021e), *Work to build an EU space-based global secure connectivity system to start in 2022 https://ec.europa.eu/defence-industry-space/work-build-eu-space-based-global-secure-connectivity-system-start-2022-2021-11-10-1_en*
- European Commission (2022a), *Space: EU initiates a satellite-based connectivity system and boosts action on management of space traffic for a more digital and resilient Europe, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_921*
- European External Action Service (EEAS), 'Shared Vision, Common Action: a Stronger Europe: a Global Strategy for the European Union's Foreign and Security Policy', *Publications Office of the European Union,* 2017, pp. 1-62. *https://data.europa.eu/doi/10.2871/64849*
- European Parliament, Directorate-General for External Policies of the Union, Wigell, M., Mikkola, H., Juntunen, T., 'Best practices in the whole-of-society approach in countering hybrid threats', European Parliament, 2021, *https://data.europa.eu/doi/10.2861/702047*
- European Union, 'Consolidated versions of the Treaty on European Union and the Treaty on the functioning of the European Union: Charter of Fundamental Rights of the European Union', *Publications Office of the European Union*, 2010. *https://data.europa.eu/doi/10.2860/58644*
- Ferm, T., 'Laws in the era of hybrid threats,' *Hybrid CoE*, 2017. *https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE-SA-3-Ferm.pdf*
- Fjäder, C., 'The nation-state, national security and resilience in the age of globalisation', *Resilience*, Vol. 2, No 2, 2014, pp. 114-129. *https://doi.org/10.1080/21693293.2014.914771*
- Giles, K., 'Hybrid Threats: What Can We Learn From Russia?,' *Security Policy Working Paper*, No. 16, Federal Academy for Security Policy, 2019, pp. 1-5. *https://www.baks.bund.de/sites/baks010/files/working_paper_2019_16.pdf*
- Greenberg, A. 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', Wired, August 22, 2022. *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*
- Gunderson, L. H. *Panarchy synopsis: Understanding transformations in human and natural systems*, Washington: Island Press, 2002.
- Hagelstam, A., *Resilience Inside and Out: A Finnish Perspective. In Forward Resilience: Protecting Society in an Interconnected World*, edited by Daniel S. Hamilton, Washington: Center for Transatlantic Relations, 2016, pp. 67-75.

- Helliwell, J., Huang, H. & Wang, S., *New evidence on trust and well-being,* edited by E. M. Uslaner, The Oxford Handbook of Social and Political Trust, Oxford University Press, 2018, pp. 409-446. *https://doi.org/10.1093/oxfordhb/9780190274801.001.0001*
- Hellquist, E. & Tidblad-Lundholm, K., 'National Defence and International Military Missions: The Swedish Armed Forces at home and abroad 1958–2020, FOI-R--5060—SE, 2021, pp. 2-72.
- Holling, C. S., 'Understanding the Complexity of Economic, Ecological, and Social Systems,' *Ecosystems*, Vol. 4, No 5, 2001, pp. 390–405. *http://www.jstor.org/stable/3658800*
- Holling, C. S., Malone, T. F., & Roederer, J. G., *Resilience of ecosystems: Local surprise and global change,* Cambridge: Cambridge University Press, 1985.
- Hybrid CoE, 'Countering disinformation: News media and legal resilience,' *Workshop organized by the Hybrid CoE and the Media Pool*, Finnish Emergency Supply Organization, 2019. *https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf*
- Hybrid CoE (2020a), *Tackling the bureaucratic vulnerability: an A to Z for practitioners*, Hybrid CoE Paper 3, COI Hybrid Influence. *https://www.hybridcoe.fi/wp-content/uploads/2020/07/Hybrid-CoE-Paper-3.pdf*
- Hybrid CoE (2020b), *China Power Team. "How Influential is China in the World Trade Organization?"* China Power, 2019. *https://chinapower.csis.org/china-world-trade-organization-wto/*
- Hybrid CoE (2020b), *Trends in China's Power Politics. Hybrid CoE expert pool meetings on China. https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200710_Trend-Report-5-China_Web.pdf*
- Hynes, W., Trump, B., Love, P. et al., 'Bouncing forward: a resilience approach to dealing with COVID-19 and future systemic shocks,' *Environ Syst Decis*, No 40, 2020, pp. 174–184. *https://doi.org/10.1007/s10669-020-09776-x*
- Ilmomen, K., & Jokinen, K., *Luottamus modernissa maailmassa*, Jyväskylä: SoPhi, 2002.
- Jackson, S., Cook, S., & Ferris, T. L. J., 'A Generic State-Machine Model of System Resilience,' *INSIGHT*, Vol. 18, No 1, 2015, pp. 14–18. *https://doi.org/10.1002/inst.12003*
- Schmid, J., 'Hybrid warfare in Vietnam – How to win a war despite military defeat', *ISPAIM – Monitor Strategic 2–4/2020*, B. No. 17/02.12.2020/0691, Bucuresti, 23, 2021, pp. 54–67. *https://www.hybridcoe.fi/wp-content/uploads/2021/03/210302_HW-in-Vietnam_table-of-content.pdf*
- Keck, M., & Sakdapolrak, P., 'What is social resilience? Lessons learned and ways forward,' *Erdkunde*, Vol. 67, No 1, 2013, pp. 5–19. *https://doi.org/10.3112/erdkunde.2013.01.02*
- Kotkavirta, J., *Luottamus instituutioihin ja yksilöllinen hyvinvointi,* edited by K. Ilmonen, Sosiaalinen pääoma ja luottamus, Jyväskylä: SoPhi, 2000, pp. 55-68. *https://jyx.jyu.fi/bitstream/handle/123456789/47905/SoPhi42978-951-39-6488-7.pdf?sequence=3*
- Linkov, I., & Trump, D. B., 'Applying Resilience to Hybrid Threats: Integrating Infrastructural, Digital and Social Systems,' edited by Linkov, L. Roslycky & B. D. Trump, *NATO science for Peace and Security Series D: Information and Communication Security*, Vol. 55, 2019, pp. 1-12.
- Lührmann, A., & Lindberg, S. I., 'A Third Wave of Autocratization is Here: What is New About It?,' *Democratization*, Vol. 26, No 7, 2019, pp. 1095–1113. *https://doi.org/10.1080/13510347.2019.1582029*
- Magnuson, S., Keay, M., & Metcalf, K., 'Countering Hybrid Warfare: Mapping Social Contracts to Reinforce Societal Resiliency in Estonia and Beyond,' *TNSR*, Vol. 5, No 2, 2022. *https://doi.org/10.26153/TSW/24028*
- NATO, 'Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon,' November 19, 2010. *https://www.nato.int/cps/en/natohq/official_texts_68580.htm?selectedLocale=en*
- NATO, 'Statement by the North Atlantic Council on the occasion of the 10th anniversary of the invocation of article 5 on 12 September 2001,' September 12, 2011. *https://www.nato.int/cps/en/natohq/news_77926.htm?selectedLocale=en*
- NATO, 'NATO's policy guidelines on counter-terrorism: Aware, Capable and Engaged for a Safer Future,' May 21, 2012. *https://www.nato.int/cps/en/natohq/official_texts_87905.htm?selectedLocale=en*

- NATO, 'Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales,' September 5, 2014. *https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en*
- NATO, 'Commitment to enhance resilience: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw', 2016, July 8. *https://www.nato.int/cps/en/natohq/official_texts_133180.htm*
- NATO, 'NATO Experts – How does NATO support Allies' resilience and preparedness?' November 4, 2020. [Video]. *https://www.natomultimedia.tv/app/asset/649516*
- NATO (2021a, June 11), *Resilience and Article 3*. *https://www.nato.int/cps/en/natohq/topics_132722.htm*
- NATO (2021b, June 14), *Strengthened Resilience Commitment*. *https://www.nato.int/cps/en/natohq/official_texts_185340.htm?selectedLocale=en*
- Newman, N., Fletcher, R., Schulz, A., Andi, S., Robertson, C. T., & Nielsen, R. K., 'Reuters Institute Digital News Report 2021,' *Reuters Institute for the Study of Journalism*, 2021. *https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf*
- Nimmo, B., 'The Breakout Scale: Measuring the impact of influence operations', *The Brookings Institution*, 2020. *https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf*
- O'Donnell, G. A. 'Do Economists Know Best?' *Journal of Democracy*, Vol. 6 No 1, 1995, pp. 23–28. *https://doi.org/10.1353/jod.1995.0015*
- OECD, 'Fostering economic resilience in a world of open and integrated markets: Risk, vulnerabilities and areas for policy action,' *Report prepared for the 2021 UK presidency of the G7*, 2021, pp. 2-118. *https://www.oecd.org/newsroom/OECD-G7-Report-Fostering-Economic-Resilience-in-a-World-of-Open-and-Integrated-Markets.pdf*
- Pepinsky, T., 'Authoritarian innovations: theoretical foundations and practical implications', Democratization, Vol. 27, No 6, 2020, pp. 1092-1101. *https://doi.org/10.1080/13510347.2020.1775589*
- Raynaud, P., *Libéralisme*, edited by Raynaud P., Rials S., Dictionnaire de philosophie politique, Quadrige Dicos Poche, Presses Universitaires de France, Paris, 2008.
- Roepke, D. W., Thankey, H., 'Resilience: the first line of defence,' *NATO Review*, February 27, 2019. *https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html*
- Rosanvallon, P., *Le siècle du populisme: histoire, théorie et critique*, Les livres du nouveau monde, Seuil, Paris, 2020.
- Rothstein B. & Stolle D., *Social Capital, Impartiality and the Welfare State: An Institutional Approach*, edited by Hooghe M., Stolle D., Generating Social Capital. Palgrave Macmillan, New York, 2003, pp. 191-209. *https://doi.org/10.1057/9781403979544_10*
- Sari, A., 'Hybrid threats and the law: Building legal resilience,' Hybrid CoE Research Report 3, 2021. *https://www.hybridcoe.fi/wpcontent/uploads/2021/10/20211104_Hybrid_CoE_Research_Report_3_Hybrid_threats_and_the_law_WEB.pdf*
- Schmid, J., 'Hybrid Warfare – a very short introduction,' *COI S&D Conception Paper*, Helsinki, 2019.
- Schmid, J., 'Hybrid warfare in Vietnam – How to win a war despite military defeat,' *ISPAIM – Monitor Strategic 2–4/2020,* B. Nr. 17/02.12.2020/0691, Bucuresti, No 23, 2021, pp. 54–67. *https://www.hybridcoe.fi/wp-content/uploads/2021/03/210302_HW-in-Vietnam_table-of-content.pdf*
- Schomaker, R., & Bauer, M., 'What Drives Successful Administrative Performance During Crises? Lessons from Refugee Migration and the Covid-19 Pandemic,' *Public Administration Review*, Vol. 80, No 5, 2020. *https://doi.org/10.1111/puar.13280*
- Smith, S., & Baylis, J., *The globalization of world politics: An introduction to international relations*, Oxford: Oxford University Press, 2001.
- The Economist, 'Talks about the Catalan conflict are about to start,' September 11, 2021. *https://www.economist.com/europe/2021/09/09/talks-about-the-catalan-conflict-are-about-to-start*
- The New York Times, 'Married kremlin spies, a shadowy Mission to Moscow and Unrest in Catalonia,' September 23, 2021. *https://www.nytimes.com/2021/09/03/world/europe/spain-catalonia-russia.html*

- The Security Committee , 'The Security Strategy for Society,' *Government Resolution / 2.11*, 2017. *https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf*
- Thrasher, J., & Vallier, K., 'The Fragility of Consensus: Public Reason, Diversity and Stability,' *The European Journal of Philosophy*, Vol. 23, No 4, 2013, pp. 933-954. *https://doi.org/10.1111/ejop.12020*
- Tocci, N., 'Resilience and the role of the European Union in the world', *Contemporary Security Policy*, Vol. 41, No 2, 2020, pp. 176-194. *https://doi.org/10.1080/13523260.2019.1640342*
- Treverton, F. G., Thvedt, A., Chen, R. A., Lee, K., McCue, M., 'Addressing Hybrid Threats,' 2018. *https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf*
- Turcotte, J., York, C., Irving, J., Scholl, R., Pingree, R., 'News Recommendations from Social Media Opinion Leaders: Effects on Media Trust and Information Seeking', *Journal of Computer-Mediated Communication*, Vol. 20, No 5, 2015, pp. 520–535. *https://doi.org/10.1111/jcc4.12127*
- UN Habitat, 'Urbanization and development: Emerging futures, World cities report,' 2016. *https://unhabitat.org/sites/default/files/download-manager-files/WCR-2016-WEB.pdf*
- UN News, 'More than half of world's population now living in urban areas', *UN survey finds*, July 10, 2014. *https://news.un.org/en/story/2014/07/472752-more-half-worlds-population-now-living-urban-areas-un-survey-finds*
- Warsaw Institute, 'Catalonia referendum: What does Russia want?,' October 5, 2017. *https://warsawinstitute.org/catalonia-referendum-russia-want/*
- Watkins, P., 'Resilience and deterrence,' *Resilience First*, January 29, 2020. *https://www.resiliencefirst.org/news/resilience-and-deterrence*

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
CBRN	Chemical, Biological, Radiological and Nuclear
CI	Critical Infrastructure
CORE	Comprehensive Resilience Ecosystem
COVID-19	Coronavirus Disease 2019
CPC	Communist Party of China
CSDP	Common Security and Defence Policy
EC	European Commission
ECI	European Citizens' Initiative
ECIP	European Customs Information Portal
EEAS	European External Action Service
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
EUGS	EU Global Strategy
GDP	Gross Domestic Product
GNSS	Global Navigation Satellite System
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
ICT	Information and Communication Technology
IPCR	Integrated Political Crisis Response
JRC	Joint Research Centre
MS	Member State
NATO	North Atlantic Treaty Organisation
NGOs	Non-Government-Organisations
NIS	Network and Information Security
NSAs	Non-state-actors
ODNI	Organisation of Economic Co-operation and Development
OSINT	Open-Source Intelligence
PLA	People's Liberation Army
PNT	Positioning, Navigation and Timing
POC	Points of Contract
RT	Russia Today
SIAC	Intelligence and Situation Centre
SOEs	State-Owned-Enterprises
SWD	Staff Working Document

TFEU	Treaty on the Functioning of the European Union
UFWD	United Front Work Department
UN	United Nations
US	United States of America
7BLR	Seven Baseline Requirements

LIST OF FIGURES AND TABLES

ANNEX

RESILIENCE IN THE DOMAINS

In the following we take stock of the 13 domains of hybrid threats discussed in the conceptual model under the prism of resilience, in order to articulate the role of each domain within a larger approach of resilience, while identifying how domains could be an entry point for hybrid threats actors in order to maximise the impact of their campaigns. To this end, a systematic approach to identifying efforts aimed at building resilience across sectors is presented, showing which domains require additional investments and which domains are at a more advanced stage. Special focus is on the interconnection of the domains and the relative positions within the ecosystem.

CIVIC SPACE

The Civic space comprises the Social/ Societal domain and the Culture domain. The Information domain is part of the Civic as well as Services space, whereas the Political domain is part of the Civic and Governance space.

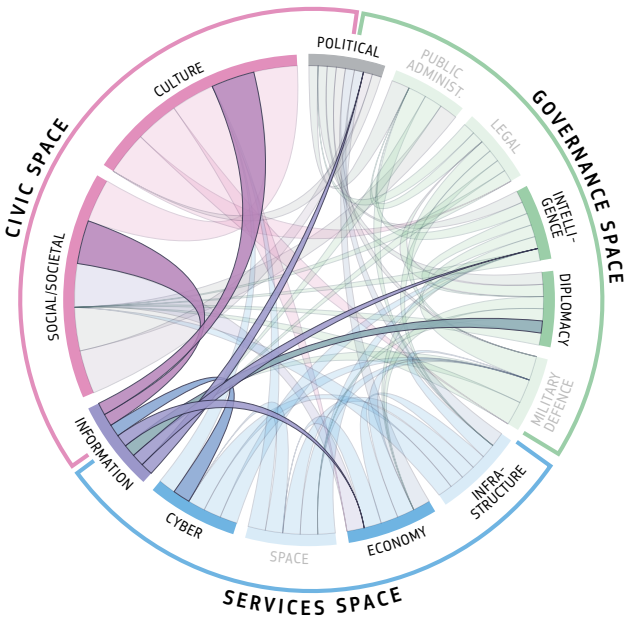
The Civic space comprises those interactions that constitute the civic life of societies. It is about the rights, obligations, liberties, and public life of the citizenry.

Information domain

Part of the Civic space as well as the Services space.

In the Information domain 'soft' factors (literally Information) as well as 'hard' factors (Information infrastructure, e.g., publishing companies, newspaper etc.) are combined. The Information domain permeates all aspects of everyday life hence it is directly or indirectly related to almost every other domain of hybrid threats. Information manipulation and interference remains the hallmark of hybrid threats and nonlinear strategies. Hence it is paramount to examine in more detail how we can foster resilience in this domain.

Connected to: Social/Societal, Culture, Political, Intelligence, Diplomacy, Cyber, and Economy.



Civic space

Trust in traditional media has declined over the past few decades amidst changes in our information market and architecture (Turcotte et al., 2015). This 'trust gap' is particularly problematic for youth and populations likely to consume news digitally, for people who do not pay for news, and in regions that lack independent public news services. Fears about false and misleading information have grown, especially about false information online, but not exclusively (Newman et al., 2021).

Services space

Our contemporary information architecture, facilitated by internet and communications technology available to both reliable and unreliable actors - presents a powerful tool for manipulation. Meanwhile, traditional media remain an important medium, due to wide penetration and authority.

Although operations in the information domain is not something entirely new, there are some notable trends. There is a growing sophistication as a response to better detection capabilities, outsourcing of campaigns as a means to achieve deniability, the spread of encrypted messaging services which are exempt from fact-checking and content moderation, and finally, artificial intelligence and machine learning in the form of deepfakes.

Governance space

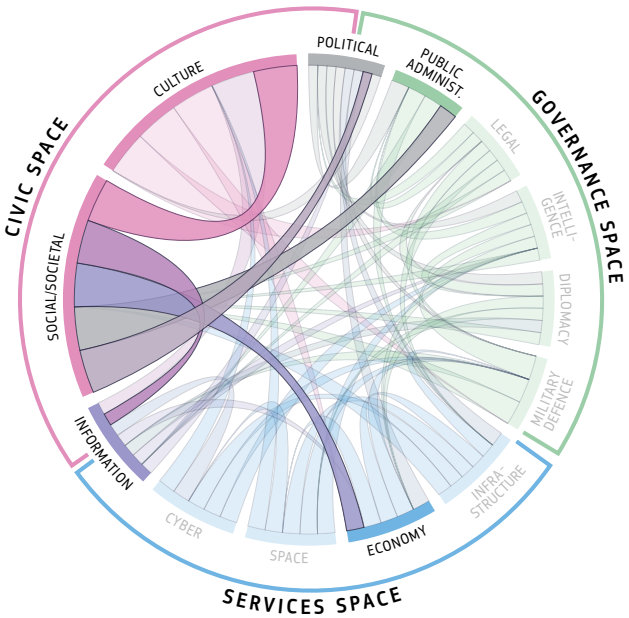
A great challenge for stakeholders is to understand the actual impact of disinformation campaigns so as to make an appropriate and proportional response. Schemes such as *The Breakout Scale:* (Nimmo, 2020) aim at providing solutions in this direction. The scale divides influence operations into six categories, based on whether they remain on one platform or traverse multiple platforms, including traditional media and policy circles, and whether or not operations reach multiple communities.

Since the Information domain is among the most targeted by hybrid threats, the topic of resilience-building in this domain will be further deepened.

Social/Societal domain

Part of the Civic Space.
Connected to: Culture, Information, Economy, Political, and Public Administration.

A resilient society is able to sustain its societal wellbeing under all circumstances, which can be interpreted as social cohesion and a culture of trust. Well-functioning institutions and public administration reduce the risk. Despite some inevitable losses following a shock, a resilient society has the ability to prioritise functions necessary to ensure the usual functionality and adapt quickly and comprehensively. If the situation becomes unbearable and a transformation is necessary, a resilient society can maintain its autonomy and decision-making capability to manage the change on its own terms.



Civic space

The link between trust and increased level of social resilience has been identified, although not widely studied (Helliwell et al., 2018). However, it can be argued that the need for trust is an inherent part of resilience in the social domain. At the societal level, trust seems to have a positive effect, through increased feelings of security, predictability, and social cohesion. It also increases confidence in the functioning of society as a whole (Ilmomen & Jokinen, 2002). Without trust, neither the institutions of society nor the economic system can function properly (Kotkavirta, 2000).

Universally implemented social public policy would be one of the best ways to build trust in society between different social classes, between individuals and between individuals and institutions. Overall, trust between citizens seems to flourish in countries where citizens perceive public institutions as fair and just, with civil society having a subordinate role in generating trust (Rothstein & Stolle, 2003). Hence, the basis of trust lies within the foundations of the Civic space: Freedom, Equality and Justice, and Political Responsibility.

Governance space

Resilience-building in the social domain should also be looked at from the governance point of view. Society contains several social entities that may differ in terms of their degree of vulnerability, socio-economic status and their access to resources – meaning that an effective and equal social public policy is often the most fruitful tool to decrease vulnerabilities that could be exploited by hybrid threat actors. It is of paramount importance to identify the social cleavages within a society in order to be able to plan preparedness and anticipate potential points of fracture in social resilience and to act accordingly.

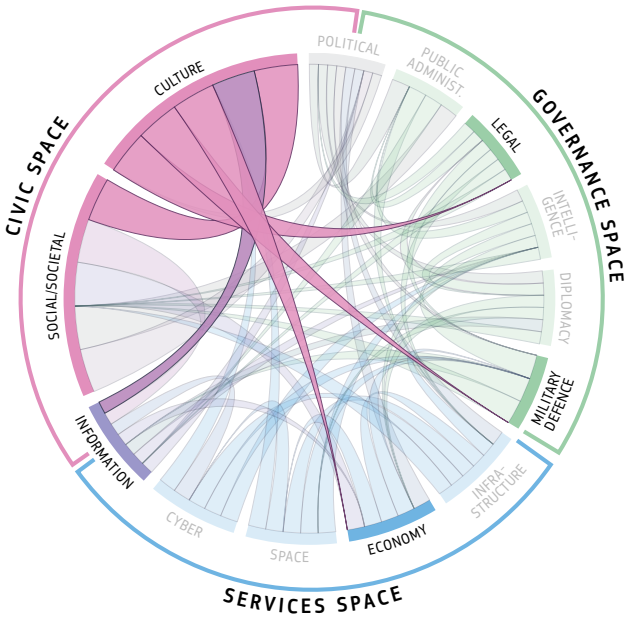
Ultimately, increasing resilience in the Social domain requires constant efforts from the Governance space to improve social welfare within vulnerable and marginalised groups (European Parliament, 2021). The aim of resilience in the Social domain is to ensure the system's ability to avoid such situations, which would imply an unfair distribution of wellbeing.

Services space

An important consideration for social resilience thinking includes the systemic view, or the ability of differing systems to affect and potentially harm other systems during various shocks and stresses (Linkov & Trump, 2019). For social considerations, a systemic shock or stress may create cascading effects that overwhelm resilience capacities. It should be accepted that not all systems and services can be protected at all times. In the case of an attack or crisis, there will be situations where some systems and services will be available. So, resilience-building requires the prioritisation of those functions critical for society to exist, and the infrastructure and systems upon which these functions rely (Hagelstam, 2016). However, during exceptional circumstances, like a state of emergency, the prioritisation may lead to a certain level of inequality. For this reason, this should be communicated to the population in order to avoid false expectations and misperceptions that may decrease social resilience (Fjäder, 2014). Simply focusing and improving one form of resilience can actually reduce another form of resilience. Hence, resilience-building should involve constant analysis of who the winners and losers are, and what are the social implications of the actions (Keck & Sakdapolrak, 2013).

Culture domain

Part of the Civic space.
Connected to: Social/Societal, Legal, Military, Information and Economy.



Culture is a highly subjective, dynamic and context-dependent concept that has been defined, understood and analysed from different perspectives throughout history. Given the large cultural diversity of the European countries, the European Union has not provided a unified definition of culture. Instead, the concept of culture is left to the discretion of the Member States and individuals to define, based on their national, local and individual sensitivities, while the EU's competences in the field of culture are to 'carry out actions to support, coordinate or supplement the actions of Member States' (Article 6, TFEU).

In the context of hybrid threats, the Culture domain 'entails the use of cultural statecraft by an aggressor to support an objective through hybrid threat activity. The scope of cultural statecraft may be internal, external or both' (p.30). Hybrid threat actors seek to exploit the root elements that foster cohesion and create an underlying division in the targeted society, promoting a positive picture of their culture and a negative one of their adversaries'. In this way, hybrid threat activities targeting the culture domain can take the shape of both short-term disruptive activities and the promotion of long-term progressive changes.

Civic space

Cultural resilience has been primarily understood as an **inherent property of society that allows the latter to recover from a disturbance and return to the status quo**. From this point of view, increasing resilience would mean to **foster internal cohesion,** for example by promoting dialogue and embracing cultural diversity. In this way, internal conflicting issues that push society apart are less likely to appear, as there is respect and recognition for different opinions and values. Here, the Culture domain is highly related to the Social/Societal domain. The emergence of social cleavages (e.g., concerning religion or ethnicity), and contentious issues such as unemployment, poverty and education, among others, have the power to polarise society, especially if the issues align.[18] This may create critical vulnerabilities which can be exploitable by hybrid threat actors. For this reason, the foundations of 'Freedom', 'Equality and Justice', and 'Political Responsibility' play a critical role in strengthening cultural resilience.

Nevertheless, in the context of hybrid threats, cultural resilience should also be understood from a proactive perspective, **considering how disturbances can be anticipated and planned in order to be avoided or to reduce their effects.** From this perspective, increasing cultural resilience would entail increased **preparedness and resistance against external disturbances,**[19] for example by promoting awareness and literacy to enable citizens to recognise potential malign

18 For example, if an ethnic minority is at the same time the poorest and less educated etc.
19 For example, promotion of extremism by foreign actors

activities promoted by hybrid threat actors. Hence, the Culture domain is also closely related to the Governance space and the Services space.

Governance space

In the Governance space, the Legal and Public administration domains are key to ensuring cultural resilience. On the one hand, they play a critical role in **setting and implementing the frameworks for fostering internal cohesion.** Cultural norms are reinforced when national and international legal frameworks back them up (e.g., the respect of human rights) and when public administration bodies are able to effectively implement the legal framework (e.g., sanctioning the violation of human rights). In this way, these two domains also set the framework for the cultural transformation to take place, as given a certain legal framework, some behaviours will be reinforced while others are rejected (as the process of the adoption of human rights as a normative framework showed). On the other hand, they play a critical role in **setting and implementing the frameworks to counter external malign activities**. By ensuring that fundamental values are respected (e.g., freedom of speech), but also regulating the exploitation of these values by malign actors (e.g., fighting against the embracement of terrorist propaganda), the Legal and Public Administration domain promotes a proactive cultural resilience, anticipating and disrupting these types of malign activities. For this reason, the foundations of the Rule of law and Stability play a critical role in strengthening cultural resilience.

Services space

Within the Services Space, it is crucial to consider the Information domain. Hybrid threat actors will likely launch disinformation campaigns promoting a positive narrative of themselves and a negative picture of their adversaries. For this reason, the foundation of 'Foresight' plays a critical role. On the one hand, **increasing media literacy** – connecting the Information Culture domains – will help society to recognise fake news and propaganda, and make it more resilient to blindly believing what is being promoted. On the other hand, **anticipating these activities will facilitate the adoption of legal frameworks that actively counter these type of malign activities**, bringing together the Services space and the Governance space through the Information, Legal and Public Administration domains – as exemplified by the Joint Communication on Tackling COVID-19 disinformation [JOIN(2020)].

GOVERNANCE SPACE

The Governance space contains the Legal, Diplomacy, Military/Defence, Intelligence and Public Administration domains. It also contains the Political domain, which is also part of the Civic space.

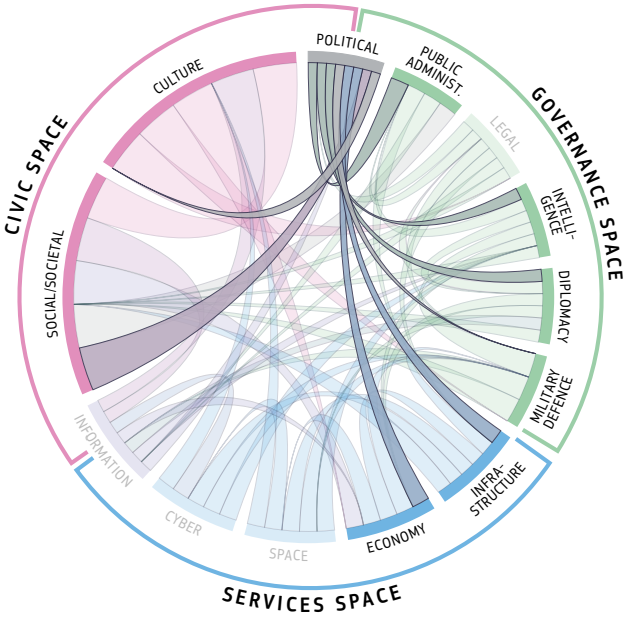
The Governance space is where public institutions exercise their mandates, regulate public and private life, take political decisions and are accountable to the body politic.

Political domain

Part of the Governance space.
Connected to: Public Administration, Intelligence, Diplomacy, Military, Infrastructure, Economy, Social/Societal, Culture

Liberal democracy presents many seams that hybrid threat actors may leverage as vulnerability surfaces. **The nature of power in democracies is unsettled**: democracy is about three kinds of

interrelated powers which make it fundamentally unstable at its core – the power of all, the power of anyone and the power of no one. It means that power can be conceptually defined as an empty place: no individual, no group, no majority can confiscate the power of the people in its entirety. The people's sovereignty is the foundation of political legitimacy but it implies the coexistence of the three kinds of interrelated powers noted above. Those three kinds of powers are destined to prevent different types of tyranny: a tyranny of the masses in which the majority imposes its will on minorities and a tyranny of an autocrat, imposing the will of a strong minority over a majority.



Governance space

Democracy's conception of power is meant to make tyranny impossible. Democracy is also based on the premise of representation. In the 19th century, the use of the notion of "representative government" prevailed over the notion of "democracy", which was negatively connotated as a synonym for chaos and unruliness. **The principle of representation** is what makes political deliberation and reflection possible. Representation allows for a democracy to debate about desirable means, ways and outcomes of policy. It is the very condition for political deliberation and channeling social conflicts in constructive ways. The principle of representation gives the people **oversight of government**. Representation and regular elections make it possible to vote governments out of office on the merit of their policy choices. Representation makes **accountability** of governments and **reversibility** of policy courses possible.

Civic space

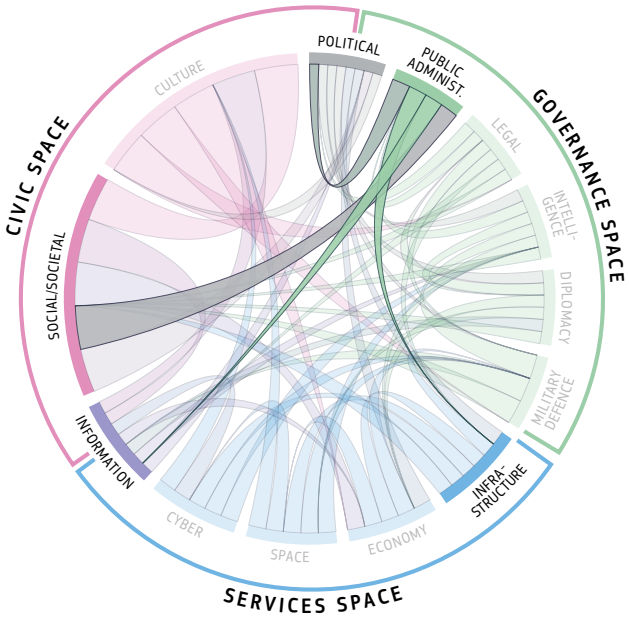
The crisis of trust and political participation in Western liberal democracies makes representation a potential wedge for hybrid threats actors to exploit. Representation as a principle reveals a gap between ideal and reality. The system of representation will always struggle to approximate the arithmetic reality of the people it must represent. Democracy is a regime intent on making the experience of representation ever more perfect. Hybrid threat actors can leverage the political domain to discredit liberal democratic governance. In particular, the politics of illiberal populism have been leveraged by hybrid threat actors to contest democracy in its essence compared to authoritarian systems.

Services space

The key argument of illiberal populism is to put the direct appeal to the people's expression above all principles and instances of representative democracy. The key danger of illiberal populism is the exhaustion of the possibilities for the people to hold their governments accountable and change policy courses if necessary: should the people decide on everything without political or governmental deliberation, then it would be the only instance responsible for errors, mistakes or counter-productive policy courses. The expression of the people would become trivial and unimportant: the value of the people's expression would become mundane if it can decide on less important policy courses. This would risk polarizing and radicalizing democracy: if legitimacy is to be limited to those leaders acclaimed by the people then this necessarily promotes authoritarian power concentration.

Public Administration domain

Part of the Governance space. It permeates all aspects of everyday life.
Connected to: Political, Infrastructure, Information, and Social/Societal.



Governance space

Institutions under public administration implementing the law and policy decisions, essentially define the socio-economic system in terms of distribution of assets (Adger, 2000). Public administration is characterised by its social impact on citizens, and institutions pertain to all social systems. So, societal resilience is perceived institutionally determined (Etzold, 2012).

Public administration can be identified in many levels, from constitutional bodies to local-level daily governance. The role of public administration in the context of societal resilience is twofold. On the one hand, public administration acts as an enabler of resilience for other domains, as it plays a central role in the drafting of preparedness legislation, steering and development, as well as in the implementation of preparedness measures and crisis management (The Security Committee, 2017). On the other hand, the resilience of public administration is itself an objective, which in the end translates into continuity of government and its operations at local as well as state level administration, in times of disturbance or crisis. Resilience in public administration can be interpreted as maintaining state autonomy and freedom of action as a prerequisite under all circumstances.

Clear, planned, and coherent communication can reinforce effective cross-government cooperation and also plays a key role in maintaining and increasing trust in public administration (Hybrid CoE, 2020a). Also, the quality of networks and agile multi-actor cooperation across different administrative bodies and actors from civil society are positive factors for robustness in public administration in times of disturbance (Schomaker & Bauer, 2020).

Civic space

It should be kept in mind that trust is not only present in the interaction between people, but also between an individual and an institution, and between institutions. Resilient institutions under public administration and with public trust in them, are especially relevant in a hybrid threat environment. In order to build trust in public administration, these institutions should be impartial, fair, universal and sufficiently effective. If citizens believe that the institutions are guided by these principles, they can trust them to meet their expectations (Rothstein & Stolle, 2003).

Services space

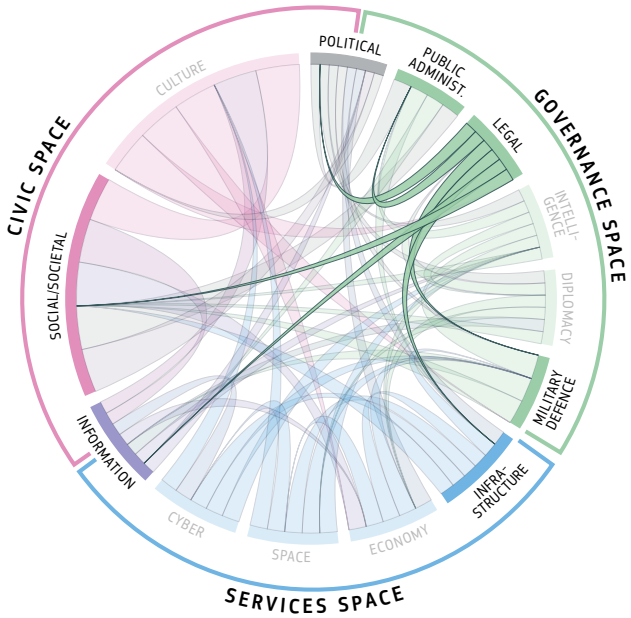
Resilience includes the adaptive process that facilitates the ability of the system to re-organise and change in response to a threat (Cutter et al., 2008). Here, the institutions under public administration have a central role, as societal resilience is seen as influenced by institutions that facilitate people`s access to resources, learn from past events and develop means to cope with threats (Keck & Sakdapolrak, 2013). Analysis by public administration of what has changed, how it is changed and

what are the implications for democratic states, is important in understanding the changing nature of the hybrid threat environment (Treverton et al., 2018). However, making a distinction between what is unusual, intentional, and possibly hostile, and what is simply normal but perhaps unusual can be difficult. Having a shared understanding of this across public administration and government can be even more challenging (Hybrid CoE, 2020a).

To provide a solution to this dilemma, it can be useful to determine assessment guidelines that give a broad overview of the different sectors and elements that should be taken into consideration in any possible assessment as well as baselines on what 'normal' looks like. This kind of approach would highlight the cross-sectoral information flow in public administration and whole-of-government effort.

Legal domain

Part of the Governance space.
Through the Legal domain the ground rules of all other domains are set and controlled. The Legal domain is of particular importance, as through the principal of checks and balances it directly protects all foundations of the Ecosystem that were proposed (e.g., rule of law, freedom, equality and justice and so on).
Connected to: Political, Public Administration, Military, Infrastructure, Information, and Social/Societal.



The impact of a major crisis, in this case the COVID-19 crisis, on the legal domain was also examined by the European Commission in the 2020 and 2021 Rule of Law reports. While the 2020 Rule of Law report points at different vulnerabilities in the legal domain created by the COVID-19 crisis the 2021 Rule of Law report concluded that the 'national systems showed considerable resilience'. However, it also gives suggestions on how resilience could be improved in the future (European Commission 2020g; 2021c).

Governance space

There are two approaches regarding resilience in the Legal domain. First, societies have dictated their fundamental principles and values or way of life as it was intended, in their legal system and laws. Usually, any legal system introduces some hindrances or friction against change, such as qualified majority. These are called 'checks and balances'. They are relevant in countering malign hybrid influence against democracies: through law the adversary can potentially seriously damage any society or even remove it from the alliance of democracies. Secondly, because laws set the way rule of law based societies work, many parts of the resilience against hybrid threats depend on laws. The adversary may seek weaknesses in the legal domain and exploit them in a damaging way. Resilience can be improved by improving the legal context (Sari, 2021). Resilience of the law against hybrid threats means the capacity of the Governance space to follow the laws, to maintain the separation of powers and to observe the key values and principles. When things fail, responsibility shall be defined sooner by the government or later by a new, freely elected parliament.

Civic space

A society in constitutional crisis is shaking at its foundations and this makes it possible for any protest and even revolutionary potential to flare up. Recent years have brought many surprises, for example, when Spain was grappling with Catalan independence claims, Britain with Brexit and the United States in the aftermath of the 2020/21 presidential election. From the viewpoint of this paper, all three crises were managed well. The legal domain managed to sustain or adapt to the situations. None of these societies lost their democratic principles, and they followed the rule of prevailing laws. Separation of powers worked as was expected. The Legal domain was resilient enough to sustain democracy.

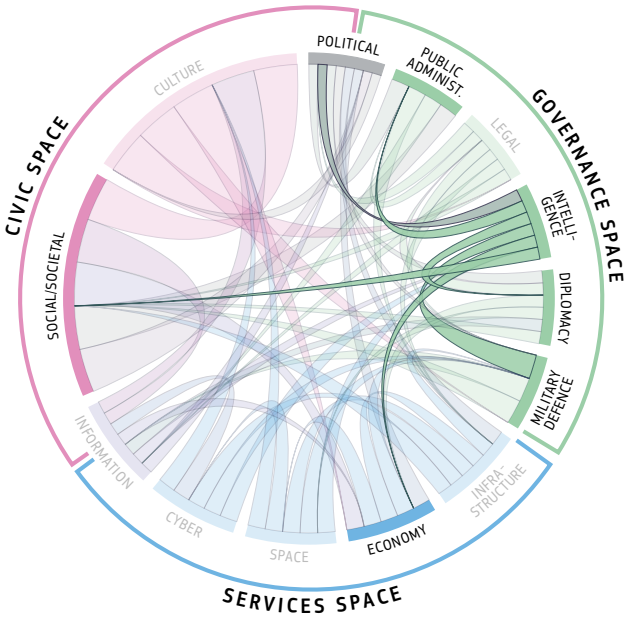
Services space

Some of the vulnerabilities to hybrid threats were born along with the openness of democratic open-market societies. Openness also facilitates free business competition. However, this openness is also a vulnerability during a hybrid threat. Legislation must take this into account, always balancing the need for security against the need for freedom and openness

Defences against hybrid threats could also set operational or technical requirements for the involved parties, be it authorities or private sector entities such as companies maintaining critical infrastructure. This cost, when it touches the private sector, will immediately become an element in market competition. If other countries in the same single market area allow cheaper standards, this can draw investments. Within the EU single market there are common rules to avoid such a situation. For example, recently the European Commission has proposed two important pieces of legislation: the proposed Directive on 'Measures for a high common level of cybersecurity across the Union' aims at establishing serious resources and competences for joint preparedness in the cyber-domain. The second proposal concerns 'the resilience of critical entities' and aims at a categorisation of entities and the activation of public-private cooperation. These pieces of legislation will improve resilience against hybrid threats in a decisive manner.

Intelligence domain

Part of the Governance space.
Connected to: Military, Political, Public Administration, Diplomacy, Economy, and Social/Societal.



Governance space

In the context of hybrid threats, the intelligence domain contains an array of potential tools, vulnerabilities and processes that can be exploited by hybrid threat actors.

Intelligence processes and products are increasingly preparing for a better understanding of how vulnerabilities develop and critical interdependences accumulate incrementally. On a systemic level, intelligence services may need to continuously expand their domain of action in as many policy sectors as possible, both to get a better foresight knowledge base and to sensitise a more diverse array of actors to security thinking in a hybrid threat context.

Services space

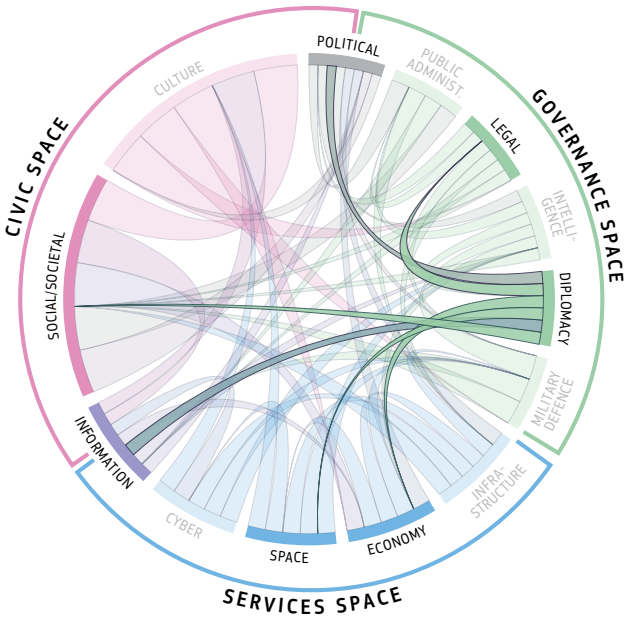
Intelligence services must be intent on nurturing a knowledge base for foresight – one of the foundations of the Services space – in order to increase resilience. This is key for intelligence to be providing the main observation and identification capability through which policymakers can anticipate trends and outliers of diffused surprise. The intelligence domain undergoes massive changes like all domains, due to the increased use of large datasets which are widely available and the available technologies such as AI which can help in rendering these datasets useful and help analysts to get the best out of these datasets. This also enables intelligence services to expand the diversity and versatility of their analytical expertise. Institutionally and in terms of process, national intelligence approaches can gain from business intelligence approaches and can also get support from the private sector. It is expected that in the future the standard of the intelligence processes might be different, with more involvement from the private sector and businesses, as we have seen in the case of the Ukraine crisis in 2022.

Civic space

Preparing for diffused surprises, in the Governance as well as Services space, requires engaging with and opening intelligence doors to those actors that possess the knowledge stocks and are linked with the relevant resources. Academia, think tanks and private analysis companies would represent such actors. The added value and resilience of the intelligence domain must also take account of the radical shift that digitalisation and big data have brought to the fore as well as adopt new technologies that can facilitate horizon-scanning and leverage OSINT. The massively available stocks of individual data render the social world computable to unprecedented levels. Individual traces and signals online can, with powerful algorithms, provide good foresight and prediction of individual behaviours. This societal aspect is also a direct competition variable for national intelligence services and their methods.

Diplomacy domain

Part of the Governance space.
Connected to: Legal, Political, Social/Societal, Information, Economy, and Space.



Diplomacy in world politics refers to a communication process between international actors that seek through negotiations to solve a conflict short of war and it is also related to attempts to manage and to create order within the global system (Smith & Baylis, 2001). Today and relating to hybrid threats, the scope of these negotiations is part of many different disagreements, since the peace/war dichotomy is no longer as we have known it.

Governance space

The communicative and bargaining potential of diplomacy at EU level is especially relevant since Ukraine and Brexit. Forceful attempts at border changes by Russia in Ukraine in 2014 were a paradigmatic shift. **It pushed the EU to reason in terms of geopolitics and strategic stability**. The twin realisation for the EU that it has a territory

and a population to protect against a host of threats has contributed greatly to the EU's geo-political shift, as a prerequisite for the definition of its interests. The effort to shape the Strategic Compass is a mere expression of this effort.

Distinguishing the threshold between foreign interference activities and legitimate diplomacy (public or non-public) relies on a concrete and correct geopolitical self-conception.[20] The EU cyber diplomacy toolbox is an example of the use of diplomacy (coordinated sanctions regime at EU level) in order to bring pressure to bear on external actors having inflicted a cyber-attack on the EU. The conception of diplomacy at play is intertwined with a bargaining / communicative function. The paradigm of imposing costs on adversaries or disruptive actors is as a way of manifesting position, agenda and will to act. This is a precedent in the EU collectively defining its interests and the means to defend them. Resilience-building in the Diplomacy domain at EU level must account for the need for inclusive decision-making and the need to take common decisions in a crisis. The question and debate around the amount of risk European states are willing to share together in collective solidarity is determining Europe's resilience to internal and external shocks.

Services space

The Diplomacy domain is connected to the Services space through the Economy domain. The Economy domain plays a crucial role in international diplomacy, due to economic interests and interconnections. The economy domain is also crucial in building resilience in the diplomacy domain: firstly, economic sanctions could be part of the response mechanism to hybrid threats, dissuading a threat actor. Secondly, building awareness of economic ties to third countries will make it possible to identify strategic connections that could be targeted by malign actors to exert pressure on the EU in the Diplomacy domain. Fostering strategic autonomy, screening of foreign direct investments and diversifying supply chains support resilience-building.

Civic space

Sharing the risk against external shocks, natural or man-made is difficult: risk sharing is greatly affected by a small number of states more exposed to risk on behalf of the whole. EU foreign affairs stances are a product of calculation between risk acceptance and risk sharing. The intergovernmental method in crisis tends to be slow and to lower the common denominator of the position adopted. However, the added value of the intergovernmental method is not always clear to citizens but, despite its inherent latency overall, it offers more sustainable and well-founded decisions. Governments need to make sure that this is adequately communicated.

Military/defence domain

Part of the 'Governance' space.
Connected to: Intelligence, Information, and Social/Societal.

Hybrid threats in the Military/defence domain are often manifested through territorial or airspace violations to test the preparedness and response of the targeted country and to put pressure on the resources. Resilience in the Military/defence domain is sometimes thought as being equal to 'deterrence by denial' (Watkins, 2020; Schmid, 2019): The Military/defence domain has a very interesting place in the hybrid threats landscape, given the fact that the use of military capabilities in a covert manner lies within the remit of hybrid threats, even when these operations are far below the threshold of declared warfare. It is true though that in the military domain (e.g., NATO) the concept

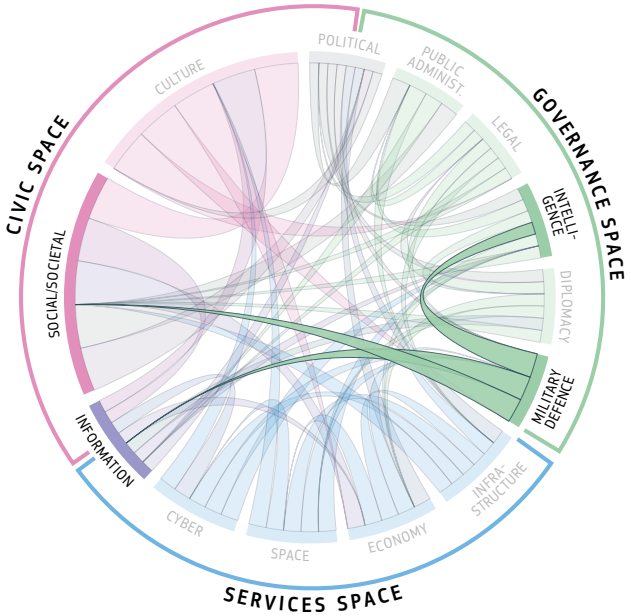
20 In other words, free after Sun Tzu: 'you have to know the enemy and you have to know yourself'

of hybrid threats has a different viewpoint, focusing more on warfare and how this can be used to destabilise and make a country more reliable, while the EU concept – although it considers military means – focuses more on other dimensions of hybrid threats, before the systemic use of military means. To this end, in the timeline of hybrid threats presented in the conceptual model, the EU's approach is positioned more in the priming phase, where the use of military tools is plausible but at a rather low intensity.

Governance space

The escalation spectrum of hybrid threats implies that all possible levels of escalation can be included or even combined (Schmid, 2019). While the current hybrid threat environment offers tools that are less expensive, less risky, more deniable and maybe even more effective than open military clashes, this has not diminished the urgency to prepare for open conflict (Giles, 2019). In fact, the more prepared the armed forces are for high-intensity conflicts, the more resilient they are also for the challenges brought by hybrid threats. This is why EU Member States must reassess their conventional warfare capabilities to provide national and collective defence, while at the same time protecting themselves against downward escalation (Schmid, 2019).

It is the regulatory frameworks that govern the deployment of military resources in response to security incidents that cannot be addressed effectively through law enforcement means. However, security incidents that exceed the capabilities of the civilian security services, but are outside the mandate of the military, might create challenges and delay decision-making.[21] The review of legal traditions in order to ensure timely reaction and the use of force in suddenly emerging extreme situations is key to decreasing the ability of the hybrid threat actor to cause ambiguity by silently operating in the grey areas.



Civic space

In militaries across Europe, the decline in the use of conscription followed the end of the Cold War as large-scale warfare was seen unlikely. Militaries were downsized and professionalised in favour of voluntary forces. The highlighted prioritisation of participation in international military missions in many cases meant dismantling traditional national defence (Hellquist, & Tidblad-Lundholm, 2021).

The social and cultural implications for the military domain should be considered. Much of the research on military resilience focuses on psychological resilience of individuals and military units, which also relates to morale (Britt & Oliver, 2013). Indeed, psychology and morale become important domains exploited as centres of gravity in the hybrid warfare context (Schmid, 2019). Influencing, disintegrating or destroying the opponent's psychological constitution, particularly their willingness to fight and their morale in constant uncertainty are key factors of success in hybrid warfare (Schmid, 2021).

Also, public trust in armed forces as an institution and support for their operations is important. In a hybrid environment that is characterised by

21 For example, who would be responsible to counter military grade armed militia or 'little green men' without insignia sponsored by another state?

uncertainty, complexity, and ambiguity, one can argue that national defence shall happen in an institutionally stable operational environment. During the possible military response to hybrid threats, there should be preparedness to handle public perceptions. It should be kept clear what a hybrid adversary's potential interests are, while counter-narratives should have been exercised in advance. In the hybrid realm it is important to be prepared to send the right messages, immediately that attribution becomes apparent, and continuing until it is confirmed by most of the alliance.

Services space

Regardless of an individual or collective focus relative to the social view, systemic focus is essential where resilience is strongly influenced by external factors. The capacity of states to use their military power in an effective and timely manner is dependent on civilian resources and operators (Roepke & Thankey, 2019). This entails a vulnerability that is not directly within the military: any serious disruption of the civilian critical systems can prevent or delay the build-up of the desired military power. These privately owned critical systems are strongly interdependent and vulnerable to hybrid operations. The aim could be to cause devastation in such systems to prevent timely build-up against an adversarial manoeuvre somewhere, not necessarily in the targeted country.

During the destabilisation phase a hybrid threat actor may aim to delay or reverse a decision to use the military (Cullen et al., 2021). So, any of these achievements would delay the deployment of military capabilities and help the adversary to collect its military gains before the response starts, meaning that the respondents are facing a *fait accompli*.

The relationship between military and civilian systems is basically two-fold. In the first case disturbances in the society may hamper the decision itself (a decision cannot be made or would be negative). In the second case, the actual capability to deploy forces would be disrupted.

SERVICES SPACE

The Services space contains the Cyber, Infrastructure, Economy and Space domains, as well as the Information domain, which is also part of the Civic space.

The Services space consists of systems, infrastructure, supply, logistics and value chains that are dependent on the private sector, while being essential to the society's life overall.

Infrastructure domain

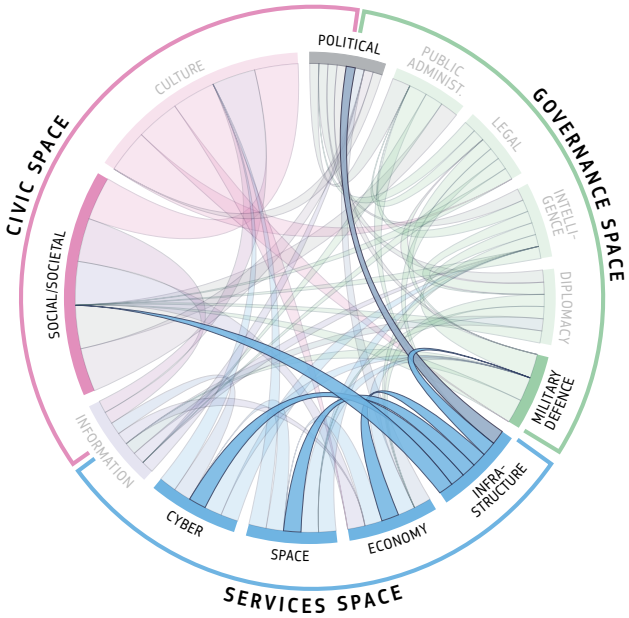
Part of the Services space.
Connected to the following domains: Social/Societal, Military, Political, Economy, Space, and Cyber.

In 2020 the European Commission published a proposals for a directive to enhance the '**resilience of critical entities providing essential services in the EU**' (COM(2020)829). Twenty different sectors are covered that are part of different domains (e.g., Energy, Transport in the Infrastructure domain, Banking and Financial market infrastructures in the Economy domain, but also including Public Administration and Space). This confirms our understanding that the Infrastructure domain is integrated over different spaces as well as that the term 'Resilience' has high awareness, as well as 'Maturity' in the Infrastructure domain.

Services space

Technical and organisational resilience are well understood and implemented in critical infrastructure protection. There are different safety levels and fallback options implemented that would be triggered as a crisis carries on, **irrespective of the causal event**[22] but rather looking at mitigating/controlling the consequences. Also, adaptive capacities are regularly implemented, as after each event it will be analysed and the processes and plant response will be improved.

Resilience of critical infrastructure in general could be seen as a sequence of events, starting from 'engineering resilience', through 'adaptive resilience', to 'transformative resilience': in a first step after a disruption 1) the operator tries to cope and preserve structures and functions, which gives time for the next step, in which 2) the system adapts, but is still preserved. 3a) After the event, when the shock has settled, a controlled transformation can start, using lessons learned and defined processes. This may lead to further adaption or to a transformation, depending on the conclusions from the lessons learnt[23]. 3b) In any case an uncontrolled transformation 'in a rush' under stress should be avoided. However, **in the environment of hybrid threats the infrastructure may be under constant stress.** The answer to this situation could be again adapting and introducing continuous processes to evaluate the level of resilience at all levels – just as continuous improving through near misses at a technical or adaptive level, the society should continuously assess which kind of transformation is needed and desirable.[24] Here, resilience in the infrastructure



domain is closely related to the Civic space as well as Governance space.

Civic space

The Infrastructure domain is connected to the Services space through the Social/Societal domain as a functioning and reliable services provided by Infrastructure is crucial for the wellbeing of the whole society. Regarding the resilience of Infrastructure, it must be noted that the adaptive capacities of society should not be underestimated and may well play an essential role. For example, if an essential service like electricity cannot be provided for some time, a well prepared, (i.e. resilient) society is more capable of coping with this situation than a less prepared society.

Lastly, when it comes to 'transformation' it should be also noted that a single infrastructure

22 In this sense, safety and security are closely connected: For example, many nuclear power plants are designed to withstand an accidental plane crash. Obviously, they will also withstand a plane crash that is caused by e.g., a terrorist attack. A high level of safety can support security to mitigate consequences of an event.

23 For example, after a massive flood that destroyed parts of important infrastructure the conclusion might either be that the dams protecting the infrastructure were not high enough, such that the infrastructure could be rebuilt at the same place but with improved protection (adaption). The result could also be that the infrastructure cannot be protected at all at the given position, i.e. it would have to be rebuilt elsewhere or a new infrastructure system that is resilient to such events must be developed (transformation). The conclusion could also be that in a whole of a society picture the old infrastructure is no longer fit for purpose and a completely new system would be established.

24 For example, climate change will also require adapting infrastructure, as the discussion around 'climate resilient infrastructure' shows. There are many technical options to mitigate the consequences of climate change, to make infrastructure resilient against the consequences and to reduce the degree of climate change. Each will require a 'transformation' — but foremost in the societal domain since society has to decide which techniques are desirable and acceptable or not.

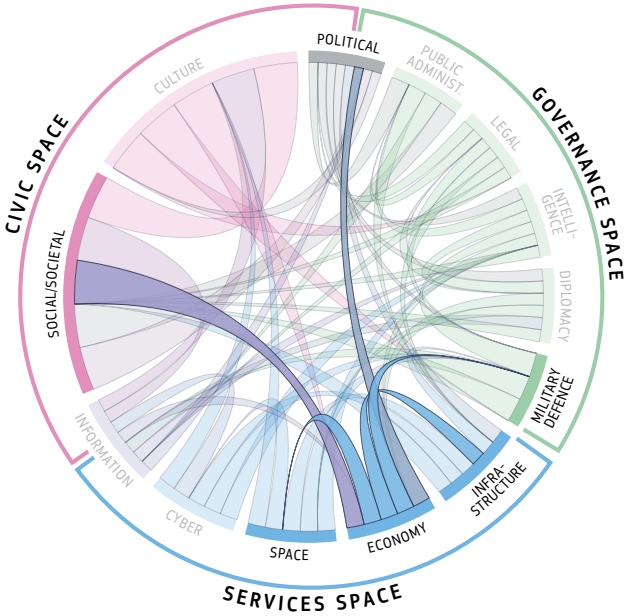
will not be able to undergo transformation. **Transformation in this case should rather be understood from a Civic and Governance point of view**. This means that the same or a similar service for the society will be provided in a different way – or society may conclude that the service is no longer required at all. In any case, transformation of an infrastructure means that it may cease to exist. Hence, it does not make sense to speak about 'transformative resilience' when it comes to 'critical infrastructure'. However, the term makes sense when speaking about 'essential services' as defined in the EC proposal for a directive on the resilience of critical entities. A good example is the Green and Digital Transition: it will not only change the type of infrastructure that will provide essential services like electricity but society as a whole.

Governance space

The Infrastructure domain is connected to the Governance space through the Public Administration and Military domain. Both domains rely for a proper functioning on services provided by the Infrastructure domain. The foundations of the Governance space, stability and rule of law on the other hand are indispensable to create the environment in which essential services can be provided from the Infrastructure domain. Hence, a resilient infrastructure will benefit the Governance space as well as a resilient Governance space will increase the resilience of Infrastructure. Lastly, Public Administration sets the framework in which Transformation in the Infrastructure domain can happen – for example, the green and digital transition is a process driven and supported *inter alia* by the European Commission.

Economy domain

Part of the Services space.
Connected to: Social/Societal, Military, Political, Infrastructure, and Space.



Services space

Vital systems supporting a modern economy are interlinked. While economies rely upon these efficient but complex interconnected systems delivering goods and services, making the system as cost effective as possible[25] has reduced the resilience of key systems to shocks and allowed failures to cascade from one system to others (Hynes et al., 2020). In globally interconnected economies, shocks or stresses originating from hybrid threats can turn into economic downturns through cascading effects and contribute to growing inequalities, polarisation of society as well as the erosion of trust.

In the hybrid threat context, the notion of economic resilience should be understood as a broad systemic-level concept, which consists of the security of supply of critical services, products and raw materials, market-access security, access to finance, trade route access, systemic-level economic security, socio-economic security, and critical infrastructure protection. In other words, the term would describe safeguarding national/multilateral

25 For example, not pricing in resilience measures.

critical economic functions (Aaltola et al., 2016). To increase resilience in the Economy domain the foundation of the Services space – Foresight and Reliability/Availability – are crucial.

Globalisation and an open-market economy have reached a dominant conceptual position. Return to protectionism and governmental control of markets functioning is hardly desirable and even harmful from a resilience point of view, as EU countries` economic resilience is dependent on the proper functioning of the EU single market and international trade in general (The Security Committee, 2017). Developing resilience through international co-operation and within an open international economic system is vital to build systems that are designed to facilitate recovery and adaptation, while keeping markets open and upholding the benefits from an open, interconnected global economy (OECD, 2021).

Civic space

In the hybrid realm, an adversary may have an interest in creating market disturbances, not only for their own economic benefit but to sow dismay, mistrust and ultimately weaken societal resilience within a targeted society (Cullen et al., 2021). It is not just immediate supply of goods and services that matter. The vitality of an economy has a longer-lasting impact on a society's prospects. The more trade potential, the more investment, the more activity, the better foundation for collection of taxes and the better development of the public sector. Positive prospects increase trust and vice versa. In the field of hybrid threats, adversarial interests often benefit from fading trust in the targeted societies. Undermining the opponents` economy and prospects would often entail erosion of trust and activity and eventually portray the image of a failed state, thus generating further vulnerabilities to hybrid threats (ibid.).

Citizens should have the belief or expectation that institutions will act in favour of one's well-being. Trust is necessary for cohesiveness of societies, public policy implementation and reforms, compliance with taxes and government regulatory measures. These are all key components of economic resilience (OECD, 2021). Ultimately, the socio-economic wellbeing of citizens is a precondition for societal resilience.

Governance space

Alternative approaches to economic integration that do not adhere to liberal market economy norms are aiming to weaken the established rules of international institutions (Hybrid CoE, 2020b). Hybrid threat actors can directly or indirectly control certain economic assets in a target state and exercise political influence through them on the government and decision makers. Hence, an economy needs adherence to common rules and norms and strong institutions to supervise this adherence to ensure resilient market-based global openness.

Institutions and their policies have an important role in increasing a society's capabilities to anticipate, plan and respond to hybrid threat activities targeting the Economy domain. Poor policy, short-term institutional-design decisions and regulatory failures may lead to the chronic build-up of stresses in the economy and society in general. Such build-up ultimately manifests itself in the form of economic recessions or with major consequences for public trust in government and its institutions and providing fertile ground for further leverage of the economic difficulties.

In the era of hybrid threats, states are increasingly claiming control over disciplining trade, investment, and finance flows. However, detailed governmental planning and state-led policies can create bureaucratic solutions causing frictions and hampering market economy. Institutions need to adapt in order to enable the development of future-focused approaches to regulation, which is often fragmented and non-coordinated vis-à-vis hybrid threats. Cascading effects could be best avoided by harmonising the regulative frameworks in the

EU. Vital societal and economic functions cannot be secured by the state alone, requiring a comprehensive whole-of-society approach to security and involvement of the private sector in the resilience process (European Parliament, 2021).

Space domain

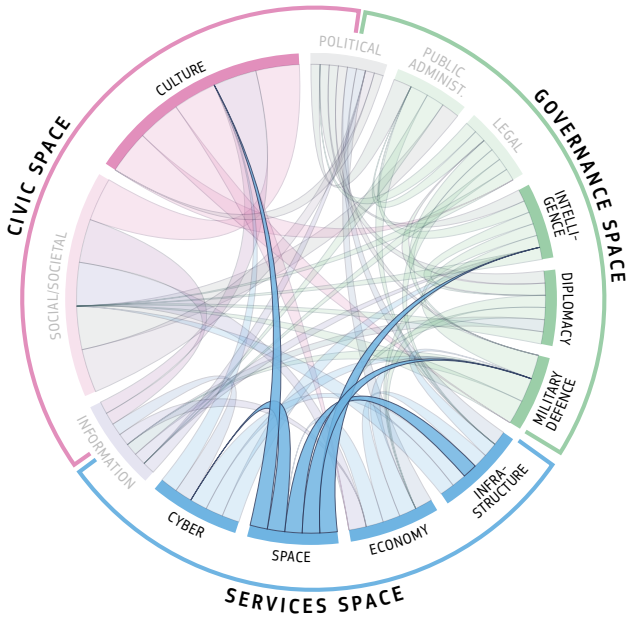
Part of the Services space.
Connected to the following domains: Intelligence, Military, Infrastructure, Cyber, and Culture.

Services space

Space is highly important and has become an essential pillar of our economy and society. Today satellites provide broadcasting (TV), global connectivity, positioning and navigation, monitoring, mapping and more – functions that, to a greater or lesser extent, are used by almost everyone almost anytime, across individuals, companies, and governments. Overall, space enables great economic growth in many 'downstream' sectors that use space systems services and data. The increasing digitisation, robotisation and connectivity will further increase the daily role of space in our economy and society. Furthermore, space has a well-established and growing role in defence, global environmental monitoring, and other government responsibilities.

In the context of hybrid threats, the space domain can be the target of malicious attacks seeking, for instance, to interfere or spoof space-based services used in EU critical infrastructures and networks. Other activities of concern are cyber- or physical-operations against EU space assets and ground-infrastructures, foreign direct investment in EU strategic space companies, creating and exploiting infrastructure dependency, or intentionally producing space debris, endangering satellites and potentially denying access to space.

Regarding the space infrastructure dependency and the EU strategic autonomy, it is important to underline the need to monitor the state of the art of disruptive technologies that can be adopted



in the space domain, as for instance, quantum technologies enabling secure communications or ultra-stable clocks.

Governance space

The EU has recognized this key role of space and clear objectives have been set: maximising the benefits of space for society and the EU economy, fostering a globally competitive and innovative European space sector, reinforcing Europe's autonomy in safe and secure space access, and strengthening the role of Europe as a stronger global actor.

Public administration bodies implement the legal frameworks which is key to ensure and increase resilience in the space domain. In the specific case of the EU and the satellite navigation programmes, the European Commission is leading a number of actions aimed at increasing inbuilt system resilience. For instance, monitoring of the industrial supply chains, the introduction of new and more resilient satellite navigation services for

civilian users, and a further increase of the system and service resilience in the second generation of Galileo. Furthermore, the European Commission is also assessing alternative and backup positioning, navigation and timing (PNT) technologies that could be activated in case of an outage of Global Navigation Satellite System (GNSS) services. A follow-up action in this context, a deployment of a minimal backup infrastructure providing PNT services in the EU, could help substantially increase the resilience of the EU economy and is thus an option under investigation. Finally, it must be noted that government-authorised and military users in the EU have access to the Galileo Public Regulated Service, which provides enhanced resilience against malicious attacks such as jamming and spoofing.

The European Commission has also taken multiple legislative actions aimed at protecting and increasing the resilience of EU space infrastructure. The EU Space Programme Regulation requests Member States to protect ground infrastructure to the level of national Critical Infrastructures and calls for stringent cybersecurity measures (Council of the European Union, 2021). The update of the CI and NIS Directives will further integrate resilience requirements for several domains, including space. A risk assessment and the implementation of relevant mitigation actions are requested.

An additional initiative that will raise resilience in the space domain in the EU is the Action Plan on Synergies between civil, defence and space industries (European Commission, 2021d).This plan includes two flagship projects that are expected to become game-changers. The EU space-based global secure connectivity system, aimed at providing access to high-speed connectivity through multi-orbit space infrastructure, and the EU Space Traffic Management initiative, which should help manage space traffic more efficiently, guaranteeing the safety, security, and sustainability of space operations.

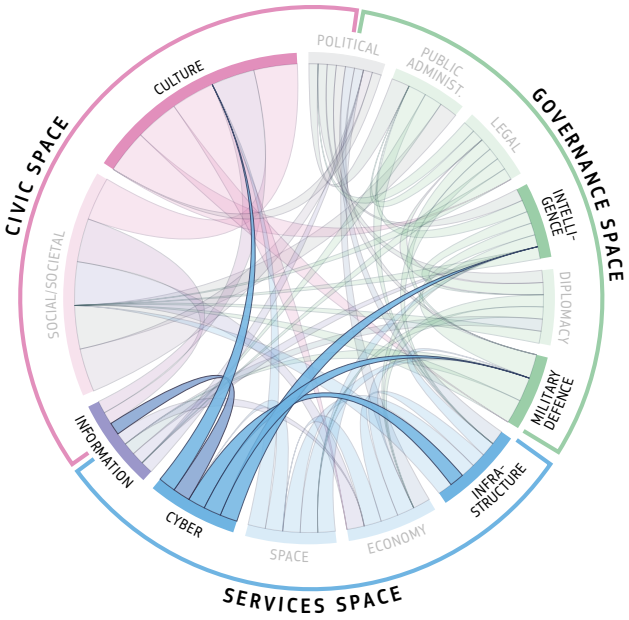
Civic space

Among the space-based services, global satellite navigation systems (GNSS) are a variant, providing positioning, navigation and timing (PNT) services globally and with continuous availability. Today, space-based PNT has become a so-called utility or service that has to be available at all times. Critical infrastructures such as transport systems (aviation, railways, maritime, road), telecommunications networks, energy distribution networks, and financial services rely on space-based PNT for the provision of precise timing and synchronisation services. An outage of PNT triggered maliciously can lead, among other effects, to the disruption of essential services used by individuals (e.g., mobile voice and data connectivity, banking services, geo-location on mobile devices…) and thus have an enormous impact on our society and economy.

The benefits of increased resilience in the space domain are multiple. Firstly, since space-based services such as GNSS are key enablers in many economic sectors, contributing to more than 10% of EU GDP in the EU (European Commission, 2017) increasing its resilience will also strengthen our economy and society. Likewise, it will also benefit defence and security operations, and thus improve our protection against external attacks. Finally, it will enable the introduction of new space-based services and applications that can bring further economic and social benefits in a safer manner with an enhanced robustness.

Cyber domain

Part of the Services space.
The cyber dimension plays an exceptional and highly specific role concerning hybrid threats. Although it is imaginable to construct a hybrid threat campaign that does not include a cyber component, this has rarely happened. To this end, the Cyber domain is a great enabler for hybrid threats and can serve as entry point, which however does not mean that it is connected to all other domains.
Connected to the following domains: Intelligence, Military, Infrastructure, Information, and Culture.



Cyber security is both a technical and a socio-economic problem, and thus cannot be solved by technical means alone. It requires the proper integration of humans, procedures, and technology to safeguard pivotal cyber assets.

Services space

The domains in the Services space are connected directly or indirectly (i.e. through other domains) to the Cyber domain and may be targeted by cyber tools. Generally, the term 'cyber resilience' refers to the ability of a system to survive as a whole under adverse and sudden cyber events. It could be said that cyber resilience is the intersection of information security, business continuity, and organisational resilience. Cyber resilience incorporates the ability 'to prepare, withstand, recover and adapt to stresses, attacks or compromises on cyber resources' (Bodeau and Graubart, 2017). Cyber resilience can encompass ICT systems, entire organisations, and even society as a whole. In the latter situation, the notion of resilience also embraces a societal perspective, which links to society's capacity to survive adverse influences from its environment and still function and continue to deliver societal well-being to current and future generations (Bodeau and Graubart, 2017).

Governance space

The domains in the Governance space are connected directly or indirectly to the Cyber domain and may be targeted by cyber tools. It is difficult to distinguish in which cases, for example, a cyber-attack targets the Cyber domain – from which the impact spreads to the political domain – and in which cases the political domain was targeted. The domains in the Governance space might suffer from different attack vectors. For example, the Public Administration domain could be targeted by a cyber-attack on the administrative systems. The Political domain could be targeted by a 'hack and leak' campaign[26] to influence elections. They will benefit from general cyber resilience measures, as described below.

Civic space

The domains in the Civic space are connected directly or indirectly to the Cyber domain. Interference in the Cyber domain might result in loss of trust of society towards decision makers, as well as service providers. Furthermore, the ever-evolving digital technologies inevitably influence Culture and Society. Building cyber resilience in the Civic space is related to establishing digital competencies within the society.

26 A 'Hack and Leak Campaign' describes a situation in which sensitive data is stolen through a cyber attack and afterwards leaked. Sometimes part of the stolen data will be manipulated before leaking, which makes it extremely difficult for the target to clarify the circumstances.

ACKNOWLEDGEMENTS

We would like to thank the following external experts
who contributed with case studies or background papers to this report:

- Ruben Arcos, Departamento de Ciencias de la Comunicación y Sociología, Universidad Rey Juan Carlos, Madrid
- Jukka Aukia, European Centre of Excellence for Countering Hybrid Threats, Helsinki
- Dimitar Bechev, Visiting Scholar, Carnegie Europe and Lecturer, Oxford School of Global and Area Studies
- Irina Busygina, Higher school of economics, St.Petersburg
- Teresa Loreth, Institut für Theoretische Informatik, Mathematik und Operations Research, Universität der Bundeswehr, München
- Markus Peltola, Finnish National Defense University, Helsinki
- Claire Pershan, EU Disinfo Lab, Brussels
- Stefan Pickl, Institut für Theoretische Informatik, Mathematik und Operations Research, Universität der Bundeswehr, München
- Matti Puranen, Finnish National Defense University, Helsinki
- Jarno Välimäki, European Centre of Excellence for Countering Hybrid Threats, Helsinki
- Arseniy Svynarenko, Finish Youth Research Society, Helsinki

Also, we would like to thank the following JRC colleagues who supported
this report by providing material and valuable insights:

- Peter Benczur
- Vytis Kopustinskas
- Luca Galbusera
- Salomé Petit-Siemens
- Stefano Ruberto
- Joaquim Fortuny Guasch
- Monica Cardarilli
- Igor Nai Fovino
- Georgios Kambourakis
- Martin Larcher
- David Anderson
- Fabiana Scapolo
- Philip Taylor
- Juan Carlos De La Rosa Blul
- Concetta Fazio

- Rocco Silverii
- Filippo Sevini
- Cristina Versino
- Lucia Vesnic Alujevic

We would like to thank our “brainstorming group”:

- Petri Uusikylä, University of Vaasa, Finland
- Tuomo Kuosa, Futures Platform, Helsinki
- Eero Kytömaa, Ministry of Interior, Finland
- Markus Peltola, Finnish National Defense University, Helsinki

We would like to thank all colleagues and external reviewers involved in the process of making this report possible through offering room for discussion, advice, insights, expertise, reviews or support in many other capacities, specifically:

- Geraldine Barry, Joint Research Centre
- Laura Giulia Cassio, Joint Research Centre
- Dan Chirondojan, Joint Research Centre
- Anne-Mette Jensen-Foreman, Joint Research Centre
- Georg Peter, Joint Research Centre
- Sönke Mahrarens, European Centre of Excellence for Countering Hybrid Threats, Helsinki
- Hasit Thankey, NATO, Brussels
- Teija Tiilikainen, Director, European Centre of Excellence for Countering Hybrid Threats, Helsinki

We would like to thank all Member States delegates of the Horizontal Working Party on Building Resilience and Countering Hybrid Threats and especially the French Presidency for their support, discussion and comments.

An early report draft was also circulated among all European Commission’s Directorates-General and also the European External Action Service (EEAS). We are greatful for all the comments, observations and insights we received.

Special thanks to the JRC colleagues who helped with the design process:

- Marina Pinilla Redondo
- Kathleen James
- Barbara Mortara

Finally, we would like to thank the teams working with us for the final promotion and launch event.

This report is part of the series **Facts4EUFuture**

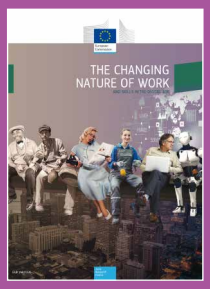
https://ec.europa.eu/jrc/en/facts4eufuture

ARTIFICIAL INTELLIGENCE: a European perspective

BEYOND AVERAGES: fairness in an economy that works for people

BLOCKCHAIN NOW AND TOMORROW: assessing multidimensional impacts of distributed ledger technologies

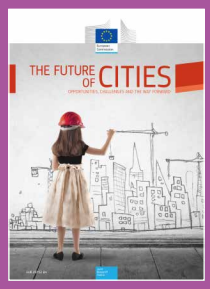
CHINA: challenges and prospects of an industrial and innovation powerhouse



CHANGING NATURE OF WORK and skills in the digital age

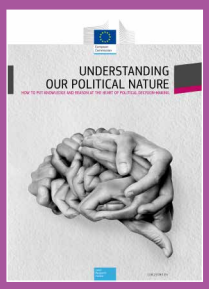
CYBERSECURITY – OUR DIGITAL ANCHOR: a European perspective

DEMOGRAPHIC SCENARIOS FOR THE EU: migration, population and education

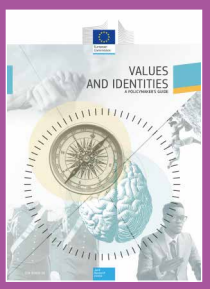


FUTURE OF CITIES: opportunities, challenges and the way forward

FUTURE OF ROAD TRANSPORT: implications of automated, connected, low-carbon and shared mobility



UNDERSTANDING OUR POLITICAL NATURE: how to put knowledge and reason at the heart of policymaking



VALUES AND IDENTITIES: a policymaker's guide

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 at: ***https://europa.eu/european-union/contact_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**, or
- 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 at: ***https://europa.eu***

EU PUBLICATIONS

You can view or order EU publications at: ***https://op.europa.eu/en/publications***
Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre, see ***https://(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 at: ***https://eur-lex.europa.eu***

OPEN DATA FROM THE EU

The EU Open Data Portal (***http://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