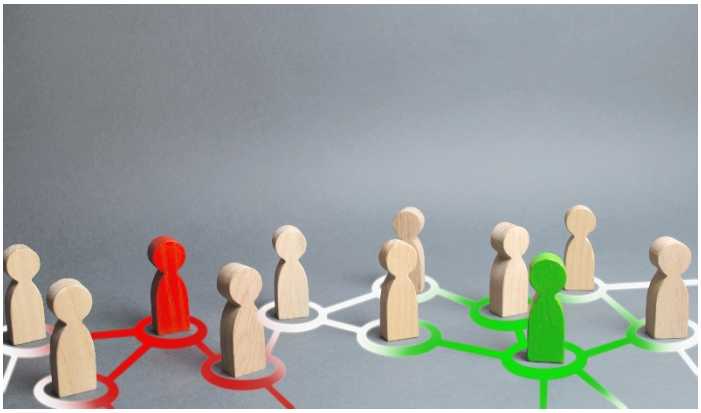
STUDY

Requested by the INGE committee

European Parliament

Best Practices in the whole-of-society approach in countering hybrid threats



Authors:

Mikael WIGELL, Harri MIKKOLA, Tapio JUNTUNEN

European Parliament Coordinator:

Policy Department for External Relations

Directorate General for External Policies of the Union

PE 653.632 - May 2021

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

STUDY

Best Practices in the whole-of-society approach in countering hybrid threats

ABSTRACT

Over recent years, the European Union has increased efforts to strengthen its resilience to hybrid threats. A model of preparedness based on the notions of 'whole-of-society', 'whole-of-government' and 'societal resilience' has gained ground in the EU's policy work. Although some progress has been made, many obstacles and challenges remain. The EU needs to address conceptual questions involved with the mapping of hybrid threats to facilitate targeted and effective countermeasures, as well as initiatives to improve societal resilience. Although the EU recognises the strategic value of resilience, the concept's precise meaning and level of added value remain vague. Its exact relationship to national preparedness and hybrid threats, as well as the whole-of-society approach requires clarification. In addition to addressing these issues, this study analyses some best practices from the whole-of-society approach by examining action taken by Finland, Sweden and Australia in this regard. The study also provides recommendations for further actions.

EP/EXPO/INGE/FWC/2019-1/LOT6/R/06
May 2021 - PE 653.632

EN

AUTHORS

- Mikael WIGELL, Programme Director, Global Security Programme, Finnish Institute of International Affairs (FIIA), Finland
- Harri MIKKOLA, Leading Research Fellow, Global Security Programme, Finnish Institute of International Affairs (FIIA), Finland
- Tapio JUNTUNEN, University Instructor, Master's Degree Programme in Security and Safety Management (SAFER), Tampere University, Finland

PROJECT COORDINATOR (CONTRACTOR)

- Trans European Policy Studies Association (TEPSA)

This study was requested by the European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE).

CONTACTS IN THE EUROPEAN PARLIAMENT

- Coordination: Ulrich JOCHHEIM, Policy Department for External Policies
- Editorial assistant: Grégory DEFOSSEZ

Feedback is welcome. Please write to ulrich.jochheim@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu

VERSION

The original English-language manuscript was completed on 06 May 2021.

This paper will be published in the European Parliament's online database, 'Think tank'.

ISBN: 978-92-846-7991-1 (pdf)
doi: 10.2861/379 (pdf)
Catalogue number: QA-09-21-109-EN-N (pdf)

ISBN: 978-92-846-7992-8 (paper)
doi: 10.2861/702047 (paper)
Catalogue number: QA-09-21-109-EN-C (paper)

Table of contents

Executive Summary v

1 Introduction 1
- 1.1 Introduction to the theme 1
- 1.2 Methodological approach and outline of the study 3

2 Improving resilience against hybrid threats in the European Union 4
- 2.1 EU policy initiatives to counter hybrid threats 5
- 2.2 Strengthening the EU's resilience against disinformation 8
- 2.3 Key obstacles and points of development 9

3 Mapping hybrid threats: a need for conceptual clarity 11
- 3.1 Hybrid Interference 14
- 3.2 Hybrid Operations 16

4 Resilience and the whole-of-society approach 19
- 4.1 Resilience as a comprehensive process 19
- 4.2 Whole-of-society approach in practice: layers of resilience 21
- 4.3 Towards an EU hybrid resilience strategy 22

5 Whole-of-society approach in practice: case studies of Finland, Sweden and Australia 27
- 5.1 Finland's comprehensive security concept 27
- 5.2 Finland's security of supply model 28
- 5.3 Finland's media literacy policy 30
- 5.4. Sweden's total defence model 31
- 5.5 Sweden's efforts against disinformation 34
- 5.6 Australia's need to counter hybrid threats 35
- 5.7 Australia's key activities to tackle foreign interference 36
- 5.8 Australia's policy against disinformation 38

6 Recommendations 40
- 6.1 Introducing shared assessment of the hybrid threat domain 40
- 6.2 Crafting a comprehensive resilience-building approach 41

6.3 Institutionalising a process of resilience assessment and monitoring 42
6.4 Measures for strengthening societal resilience 43
References 45

Executive Summary

International cooperation is of utmost importance in countering hybrid threats. Over recent years, the European Union (EU) has increased efforts to strengthen its resilience in this regard by establishing a number of policy initiatives. Tackling hybrid threats should be a continuous process whereby the development of resilience at societal, national and European levels plays a key role. Consequently, a model of preparedness based on the notions of 'whole-of-society', 'whole-of-government' and 'societal resilience' has increasingly been gaining ground in the EU's policy work.

Although some advancements have been achieved, many obstacles remain. The lack of connection and synchronisation between top-level commitment to fighting hybrid threats and the necessary working-level policies, plans and measures have led to little progress. Significant ownership and coordination challenges within EU institutions have given rise to difficulties in overcoming compartmentalised silo mentalities. This is particularly true *vis-à-vis* cooperation between military and civilian authorities. As a result, actions have been reactive and not sufficiently holistic to counter threats effectively. The EU should be a platform for sharing information and best practices between Member States (MS). This requires a joint conceptual understanding of hybrid threats, shared situational awareness and political will.

A particular problem with the EU's use of hybrid threat terminology is the way it fails to distinguish between different forms of hybrid threats, thereby making it difficult for policymakers to delineate institutional responsibilities and formulate more targeted countermeasures. Hence, the EU now needs to address some of these conceptual challenges involved with the mapping of hybrid threats. One specific question concerns the need to systematise terminology. EU hybrid threat analysis needs to solve the problem of creating analytic differentiation in order to facilitate the identification of empirical variation between different hybrid threat types.

With this challenge in mind, this study proposes a new hybrid threat taxonomy identifying three main types: hybrid interference, hybrid operations and hybrid warfare. These differ along three key threat dimensions: means (non-military, paramilitary, military), deniability (plausible, implausible, no deniability) and control aim (reflexive, functional, territorial). Framing the hybrid threat domain in this way has several advantages for the EU. In particular, it (1) presents a shared analytical tool within the EU to identify and compare different hybrid threats; (2) helps recognise institutional responsibilities based on the typology, facilitating institutional collaboration as well as coordination within the EU; and (3) helps develop countermeasures based on a clear understanding of the entire hybrid threat domain, whereby the EU's approach to counter hybrid threats can be better targeted.

Herein, resilience building is key. Societal resilience is the desired product of a well-functioning whole-of-society approach in countering complex and interconnected dangers such as hybrid threats. The EU recognises the strategic value of the resilience approach in its documents and policies. However, as with the notion of 'hybrid threats', this concept's precise meaning and level of added value remain vague. Moreover, there is no clarification of exactly how these notions of resilience and hybrid threats relate to the whole-of-society approach.

This study argues for a processual model of comprehensive resilience, offering a template for both strategic resilience planning and post-hoc evaluation of threat responses. When enhancing the societal base structures to counter hybrid threats, the three resilience process phases – resistance, continuity management and adaptation – should be planned not only as overlapping components of a comprehensive approach, but also as stages which are flexible enough to allow context-dependent variation in their interrelated weightings. Ultimately this signals an ability to deal with the long-term effects of hybrid threats as a continuous process. The resilience response to hybrid threats should be built upon the general adaptive resilience capacities of society. This will increase societal ability to absorb some of the

'slow-burning' effects of particular hybrid threats without the need to fall back on measures that would require deviation from democratic practices.

The study also argues for an understanding of resilience strategies in three ways: maintenance, marginality and renewal. These different strategic understandings of resilience can be used when planning policies and practices. Resilience building can further be divided into attributes enhancing either societal resistance or adaptive capacities, helping to clarify how the different components link together with an overarching whole-of-society approach. Hence, it provides the EU and its Member States with a tool for specifying options when planning strategic responses to hybrid threats.

This study further analyses some best practices and pitfalls associated with the whole-of-society approach. It investigates particularly policies and actions adopted by Finland, Sweden and Australia.

Preparedness in Finland is based on the notion of comprehensive security, where the vital functions of society are jointly safeguarded by the authorities, business operators, civil society organisations and citizens. The Finnish security of supply model, together with efforts to improve media literacy and mass communication, present illustrative examples of the country's approach. However, despite clear benefits being derived from the Finnish model, problems are also being experienced. Specifically, contingency planning and information sharing are still considered to be too vertical and plagued by a silo mentality. Other limitations apparent in the Finnish comprehensive security system include under-resourcing, overdependence on a few critical functions, resource competition between governmental agencies, a general lack of trust between actors and, in some cases, imprecise administrative responsibilities during normal circumstances versus crisis situations.

Sweden is a country with a long tradition in utilising a whole-of-society approach in its national preparedness efforts. Following the Cold War, Sweden in essence decommissioned its total defence system, as well as all related civil activities. These are now in the process of being re-built as part of the country's total defence capabilities. In practice, the country is drafting strategies; designating coordinating institutions; imposing additional responsibilities on central, regional and local entities; along with developing cooperation between the private and public sectors.

During recent years, Australia has been one of the most active countries worldwide in updating its legislation, policy and bureaucratic structure to manage foreign influence in the country. These responses have focused on criminalising, disrupting and deterring foreign interference. Key measures include the creation of foreign influence transparency registers, the Espionage and Foreign Interference Bill and the establishment of the National Counter Foreign Interference Coordinator position.

In recent documents and policies, EU institutions and Member States have clearly demonstrated an awareness of their need to counter hybrid threats. Current EU policies focus especially on promoting resilience as a framework to counter threats in the hybrid domain. The EU now needs to devise a set of more specific policies and measures, in addition to those already implemented, to put such a framework into practice in an effective manner. To this end, this study proposes four bundles of recommendations.

1. Introduce a shared assessment of the hybrid threat domain.
    - Establishing a shared EU hybrid threat typology which should be mainstreamed across EU policies and documents. Actions to be taken should include: initiating further development of an EU hybrid threats typology based on the conceptual model generated by the European Centre of Excellence in Countering Hybrid Threats (Hybrid CoE).
    - Implementing regular EU hybrid threat risk assessments taking into account the entire hybrid threats domain as conceptualised in the shared EU hybrid threat typology. Actions to be taken should include: implementing regular Council/Commission shared risk assessments under the responsibility of the High Representative of the Union for Foreign Affairs and Security

Policy/Vice-President of the European Commission (HR/VP); increasing staffing and resources for the Hybrid Fusion Cell as a focal point for hybrid threats assessments; as well as generating easily readable and concise classified intelligence reports for EU policymakers.

- Starting a process of joint planning for countering hybrid threats with a basis in the EU hybrid threats risks assessments. Actions to be taken should include: introducing a process of regular exercises to be developed by the Hybrid Fusion Cell in cooperation with the Hybrid CoE, based on the shared hybrid threat typology and risks assessments; developing a hybrid threats diplomacy toolbox in order to facilitate rapid and effective countermeasures; and developing recommendations for improving joint civil-military planning for hybrid contingencies.

2. Devise a comprehensive resilience-building approach.

- Creating an enabling environment for citizen activism and independent media, including civil society support and media capacity building. Actions to be taken should include: developing tools for grassroots agenda setting, such as the European Citizens' Initiative; and initiating rapid implementation of provision for revised Audio-visual Media Service Directive 2010/13/EU, which requires Member States to promote and develop media literacy skills.

- Introducing regulation and increased transparency of social media platforms. Actions to be taken should include: implementing and continually evaluating the Digital Services Act and the Digital Markets Act; developing the Code of Practice on Disinformation and monitoring implementation of commitments by the signatories.

- Facilitating processes of public-private continuity management in critical infrastructures. Actions to be taken should include: implementing the upcoming Critical Entities Resilience (CER) Directive; supporting research on the actual implications of the CER Directive with regard to hybrid threats; developing cross-border training activities and exercises; launching an awareness-raising campaign with regard to hybrid threats targeting private enterprises; and creating a funding instrument for strengthening the resilience of infrastructure and systems that underpin the EU single market.

- Assigning clear responsibilities and procedures for attributing hybrid threats within EU institutions. Actions to be taken should include: establishing obligations for all entities targeted by hybrid threats to report incidents and allow access to and analysis thereof; clarifying the division of labour with regard to attributing and countering hybrid threats between the Integrated Political Crisis response (IPCR) arrangements, the Hybrid Fusion Cell within the EU intelligence and Situation Centre (EU INTCEN) and the European Commission; along with conducting regular tabletop exercises to test and enhance the EU's hybrid threat response capabilities in cooperation with the Hybrid CoE.

- Creating a deterrence toolkit for dissuading hybrid threats, including strategic communication and sanctions preparedness. Actions to be taken should include: enhancing the security of EU institutions especially with regard to secure communications; conducting a regular review of the 2016 EU Playbook on Countering Hybrid Threats; developing a public version of the Playbook in order to raise awareness and communicate the EU's resolve in countering hybrid threats; bolstering the European External Action Service (EEAS) StratCom Teams with a focus on investing in Chinese language experts; integrating a hybrid threat evaluation as a regular element in the EU's general policy work across sectors.

3. Institutionalise a process of resilience assessment and monitoring.
    - Identifying sectoral hybrid resilience baselines for Member States and EU institutions (as called for in the EU Security Union Strategy). Actions to be taken should include: developing hybrid resilience baselines; developing measurements and joint assessment tools in line with the hybrid resilience baselines to be used by the Hybrid Fusion Cell inter alia on the general adaptive resilience capacities of Member States.
    - Introducing resilience assessments modelled on the hybrid threats assessment procedure in the Member States and a peer review process by experts. Actions to be taken should include: establishing a maturity model for the hybrid resilience baselines in cooperation with the Council and the EU Commission; defining indicators for assessing maturity; and selecting a group of experts drawn from the EU Commission and Member States to assess maturity levels in reaching the hybrid resilience baselines.
4. Introduce efforts to strengthen societal resilience.
    - Increase awareness of attributes related to society's general adaptive resilience in countering hybrid interference. Actions to be taken should include: developing measurements of general societal resilience into the joint assessment tools and baseline resilience criteria used by the Hybrid Fusion Cell; and further develop strategic analysis on the interrelationship between general and specific resilience capabilities in the context of countering hybrid interference.
    - Promoting media literacy as a key civic virtue and developing respective curricula development guidelines based on identified best practices. Actions to be taken should include: strengthening the role of critical (digital) media literacy skills, together with other civic virtues such as critical thinking and public participation, in educational programmes and curricula in each Member State; involving key national media companies within curriculum planning and creating national forums that offer further training opportunities for teachers in the field; and increasing Union-level coordination of the above-mentioned activities via a Commission-steered Media Literacy Expert Group.
    - Implementing targeted programmes aimed at integrating diasporas and minorities. Actions to be taken should include: promoting the positive role of civil society actors in public education campaigns on disinformation and media manipulation, especially those directed for ethnic minorities or vulnerable groups; increasing general awareness against disinformation campaigns by designing non-alarmist public information campaigns on the interrelationship between disinformation and societal security; as well as increasing the level of vertical/social trust within society by reducing social inequalities and deprivation.
    - Developing legislation for increased electoral transparency. Actions to be taken should include: introducing regulation concerning foreign funding of political parties and associations; and strengthening transparency of political advertisements, including on social media platforms.
    - Heightening the importance of supply and value chain resilience (e.g. science, technology, trade, data and investment sectors) in the EU's policy work on strategic autonomy. Actions to be taken should include: introducing resilience assessments in connection to the EU's trade and competition policies; and launching a debate on resilience to hybrid threats within the framework of the Conference on the Future of Europe.

1 Introduction

1.1 Introduction to the theme

European democracy is being threatened as never before. These threats are often subtle, manipulating for cover the very same European democratic values that paradoxically they are designed to subvert. Four cornerstones of European democracy – state restraint, pluralism, free media and economic openness – provide opportunities for hostile external actors to interfere in European democratic society through carefully calibrated covert means designed to undermine internal cohesion and accelerate political polarisation within Europe.

For instance, disinformation campaigns have become increasingly evident since the 2016 United States (US) elections and stepped up in the midst of the COVID-19 emergency. External actors have been deploying disinformation to aggravate the public health crisis in European countries. Exaggerated and fabricated stories of how European governments have been mismanaging the coronavirus' spread have been used to play on the anxieties of European populations. While not all these disinformation efforts succeed in persuading the public as such, the cumulative impact in sowing distrust can be very effective, rendering European states less capable of countering either the epidemic or the aggression. As another example, external actors are also offering business links to Western groups in order to generate interest convergence and cultivate loyalty. China's *Qiaowu* policy in its neighbourhood offers an example of how local interlocutors can be used to this end. The ultimate aim has been to create cracks in US alliances within the Indo-Pacific region. Europe is not exempt from these attempts and urgently needs to find means of putting up defences against such hybrid threats, without jeopardising the values that the measures are meant to defend.

The study addresses this *problématique*. As national security remains the sole responsibility of each Member State, countering hybrid threats is first and foremost a national responsibility. However, international cooperation is also of utmost importance. Over recent years, the European Union has increased efforts to strengthen its resilience to hybrid threats and has come up with a number of policy initiatives in this regard. Hybrid threat terminology has now been firmly established and seems certain to continue being used in strategic planning.

However, a particular problem with the EU's use of this terminology is the way in which it fails to distinguish between different hybrid threats. At present, the term 'hybrid threat' is being used as a catch-all for a variety of threats, making it difficult for policymakers to delineate institutional responsibilities and formulate more targeted countermeasures. Accordingly, the EU now needs to address some of the conceptual challenges involved with the mapping of hybrid threats. There is a specific concern regarding the need to systematise terminology. EU hybrid threat analysis needs to solve the problem of creating analytic differentiation to facilitate the identification of empirical variation between different types of threats, without stretching concepts to include cases that do not fulfil the reasonable criteria of specific conceptual validity.

With this challenge in mind, the study proposes a new hybrid threat typology under three main headings: hybrid interference, hybrid operations and hybrid warfare. They differ along three core threat dimensions: means (non-military, paramilitary, military), deniability (plausible, implausible, no deniability) and control aim (reflexive, functional, territorial). Framing the hybrid threat domain in this way has several advantages for the EU. In particular, it: (1) presents a shared analytical tool within the EU to identify and compare different hybrid threats, bringing some order to the terminological confusion that has marked the field in recent years; (2) helps recognise institutional responsibilities based on the typology, facilitating institutional collaboration and coordination within the EU; and (3) helps develop countermeasures based on a clear understanding of the entire hybrid threat domain, thereby enabling better targeting of the EU's approach to countering hybrid threats.

Tackling threats should be a continuous process whereby development of resilience at societal, national and European levels plays a key role. Consequently, a model of preparedness based on the notions of whole-of-society, whole-of-government and societal resilience has increasingly gained ground in the EU's policy work. Societal resilience is the desired product of a well-functioning whole-of-society approach to counter complex and interconnected threats such as hybrid ones. The main advantage of the resilience approach is that issues which are integral in developing a proper whole-of-society approach – i.e. increasing social and political trust, highlighting the culture of democratic participation and emphasising the need to increase critical media literacy – can be advocated as inherently positive societal processes.

The strategic value of the notion of 'resilience' is fully recognised by the EU. However, as with the idea of 'hybrid threats', its exact meaning and level of added value remain vague. There is no clarification of its precise link to national preparedness and hybrid threats, as well as its relationship with the whole-of-society approach. The study addresses this challenge by developing a processual understanding of comprehensive resilience, which can be utilised as a tool for strategic planning to develop a proper whole-of-society approach. To this end, this study utilises a typology of resilience strategies – resilience either as maintenance, marginality or renewal – that can be applied to trace different strategic understandings of resilience in wider governance policies and practices concerned with societal security. This typology can give the EU and its Member States a tool designed to facilitate deeper understanding by specifying exactly what kind of options there are when choosing an appropriate strategic response to hybrid threats.

The importance of clarifying and refining alternative strategic responses becomes even more evident when one looks at the various conceptualisations of resilience in key EU documents. Analysing policy responses by dividing them into attributes enhancing either societal resistance or adaptive capacities would further clarify how the different components of an overall whole-of-society strategy could link together.

The processual model of comprehensive resilience offers a template for both strategic resilience planning *and* post-hoc evaluation of responses to threats. The study argues that when enhancing societal base structures so as to counter hybrid threats, the resilience process phases should be planned as overlapping components within a comprehensive approach and kept flexible enough to allow context-dependent variation in their respective weightings. Ultimately this points to an ability to deal with the long-term effects of hybrid threats as a continuous process that would include openly reflective learning processes not only within European society, but also among like-minded societies elsewhere.

The study analyses some best practices and pitfalls associated with the whole-of-society approach. We look particularly at models developed in Finland, Sweden and Australia.

Finland has a long history and established practices in utilising whole-of-society approach in its national preparedness efforts. Therefore, the country provides an excellent example of several best practices in this regard. In Finland, preparedness is based on the notion of comprehensive security, whereby the vital functions of society are jointly safeguarded by the authorities, business operators, civil society organisations and citizens. This security of supply model and the country's efforts to improve media literacy and mass communication serve to exemplify the Finnish approach.

Sweden is another country with a long tradition of whole-of-society approach. Currently the country is re-building its civil defence by drafting strategies, designating coordinating institutions, imposing additional responsibilities on central, regional and local entities as well as developing cooperation between the private and public sectors. Hence, the country serves as valuable case study on the implementation of whole-of-society practices and how they can be utilised in building up societal resilience.

Australia provides a good example of whole-of-society activities carried out by a larger, non-European country. In fact, during recent years, Australia has been one of the most active countries in the world in updating its legislation, policy and bureaucratic structure to manage foreign influence in the country.

These responses have focused on criminalising, disrupting and deterring foreign interference. Key measures include the creation of foreign influence transparency registers, the Espionage and Foreign Interference Bill and the establishment of the National Counter Foreign Interference Coordinator position.

1.2 Methodological approach and outline of the study

This study is based on a conceptual open-source analysis that draws on earlier work undertaken by the Finnish Institute of International Affairs (FIIA) and Tampere University in Finland covering hybrid threats and societal resilience. The study utilises relevant national and EU documents, such as legislation and key strategy documents to do with hybrid threats, societal resilience and whole-of-government approaches, as well as more recent research literature on these topics. In addition, four expert interviews were conducted among senior government officials with regard to the case studies of Finland, Sweden and Australia. The interviews were conducted under the Chatham House rule. The interviewees were selected due to their broad expertise on the civil preparedness systems of the respective countries. The aim of the interviews was to provide background material for the research as well as to facilitate the identification of the most relevant data sources, research material and key actors. The hybrid threats typology presented in Chapter 3 has been assessed and discussed in a focus group meeting with senior experts, organised by the Finnish Institute of International Affairs.

Following the Introduction Chapter, the study will proceed as follows:

- Chapter 2 provides an overview of the current state of play in the EU regarding countering hybrid threats with the whole-of-society approach. This is done by taking stock of the most important EU policy initiatives, as well as highlighting key crucial obstacles and points of development in this regard.
- Chapter 3 addresses conceptual challenges involved with the mapping of hybrid threats. It presents a hybrid threats typology to systematise terminology and thereby enable the identification of empirical variations between different threat types, without stretching the concepts to cases that do not fit within reasonable validity criteria.
- Chapter 4 focuses on the interplay between comprehensive societal resilience and the whole-of-society approach. This chapter analyses how resilience should be understood in the context of hybrid threats, what elements the concept should include and how the resilience of civil society at large could be enhanced in order to deter hybrid threats in a whole-of-society manner.
- Chapter 5 maps out and analyses some of the best practices and pitfalls within the whole-of-society approach. This is done by investigating action taken in Finland, Sweden and Australia to utilise such an approach as a key element in countering hybrid threats.
- Chapter 6 provides policy recommendations for further action.

2 Improving resilience against hybrid threats in the European Union

Security remains the sole responsibility of each EU Member State, thus countering hybrid threats is first and foremost a national responsibility. Furthermore, only governments have adequate resources for effective countermeasures, including intelligence and counterintelligence agencies, uniformed services, means of communication with citizens and cyber incident response capabilities (Szymański, 2020). It is usual within any given country for national actors to have (1) a specific understanding of the political, socio-economic and historical context in which actual hybrid activities take place; (2) a better grasp of the critical vulnerabilities; and (3) shorter decision-making processes for more timely and effective responses. However, as it is often the case that hybrid threats target, utilise and are enabled by cross-border infrastructure and processes, international cooperation is of utmost importance in effectively countering these threats. In principle, well-functioning international cooperation can make the implementation of more effective measures to counter common threats possible by providing more coordinated responses, frameworks and processes, as well as by enabling states to pool and share their resources.

In addition to concrete actions taken by Member States, the EU has also increased its efforts to strengthen the Union's resilience to hybrid threats, having over recent years come up with an impressive amount of policy initiatives in this regard. These include a number of sectoral and overarching strategies, such as:

- the creation of expert bodies focusing on different aspects of hybrid threats;
- legal instruments to improve response to hybrid threats;
- information-sharing mechanisms to enhance common risk analysis and situational awareness;
- exercises and simulations to improve preparedness for hybrid attacks;
- closer cooperation with partners such as the North Atlantic Treaty Organization (NATO);
- and investments in core capacities (Fiott & Parkes, 2019).

Thematically, the biggest emphasis in the Union's policy work has been on issues related to situational awareness, cybersecurity and disinformation (Szymański, 2020). Of course, these sectors do not exhaust the list of potential risks and vulnerabilities. The current European security landscape holds a very broad spectrum of hybrid threats, as well as high levels of interconnectivity which enables tools for malicious actors to conduct hybrid activities. As the threats are numerous and cross-sectoral, several states have started to investigate or even implement a comprehensive security concept. In this regard, Finland is often quoted as the primary example. Here the notion of comprehensive security (with roots in a 'total defence' model) refers to a cooperation-based preparedness model in which the vital functions of society are jointly managed by authorities, business operators, civil society organisations and citizens (Finnish Government, 2017). This definition implies that, for the concept of 'comprehensive security' to work, it must be put into practice with whole-of-government and whole-of-society approaches. Such security approaches emphasise institutional coordination at government level, strong links between government, civil society and the private sector, civil–military cooperation, as well as constant preparation, training, exercises and education. Similar practices have been implemented in both Sweden and Australia to make comprehensive and coordinated responses to hybrid threats possible.

However, as the hybrid toolkit is constantly evolving, tackling emerging threats should be a continuous process where development of resilience at societal, national and European levels plays a key role (Bajarūnas, 2020). Hence, a model of preparedness based on the notions of whole-of-society, whole-of-government and societal resilience has increasingly gained ground in the EU's policy work. This is clearly visible in its key documents regarding hybrid threats, with progressively more explicit and frequent

reference to the respective concepts. In order to provide an overview of the current state of play in the EU regarding its countering of hybrid threats with the whole-of-society approach, this chapter takes stock of the most important policy initiatives, whilst at the same time highlighting the most crucial obstacles and areas of possible development.

2.1 EU policy initiatives to counter hybrid threats

Initially, the EU's intensified actions to counter hybrid threats were driven by Russia's hybrid warfare against Ukraine, which have been ongoing since 2014. The Union had previously formulated several policy initiatives that are relevant in regard to hybrid threats and building resilience in the EU, such as the 2013 Cybersecurity Strategy (European Commission, 2013). However, shortly after the outbreak of war in Ukraine, the EU began to react more explicitly to hybrid activities, starting with the recognition of online disinformation campaigns. In 2015, the European Council tasked the High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the European Commission (HR/VP) in cooperation with EU institutions and Member States to submit an action plan on strategic communications (European Council, 2015). As a result, the European External Action Service (EEAS) East StratCom Task Force was created to address Russia's ongoing disinformation campaigns in the EU's Eastern Neighbourhood.

An important step in the EU's policy work against hybrid threats was taken in 2016 with the adoption of the 'Joint Framework on Countering Hybrid Threats: A European Union response' (European Commission, 2016). The Communication has played an important role not only in lifting political awareness on the topic, but also in increasing conceptual clarity by providing a much-needed definition of the threats. It defines hybrid activities as 'the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare' (European Commission, 2016). As to hybrid activities' objectives, the Communication makes a general observation that 'there is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes' (European Commission, 2016).

Importantly, the Communication argued for a set of operational level actions to be carried out by the Commission and Member States. This document highlighted especially the importance of situational awareness, information exchange and intelligence sharing; it also called for Member States to conduct a survey aimed at identifying areas vulnerable to hybrid threats. Furthermore, the creation of an EU Hybrid Fusion Cell was called for, to be tasked not only with receiving and analysing classified as well as open-source information on hybrid threats, but also with stressing the importance of a sound strategic communication strategy to counter disinformation. The Communication also required Member States to consider establishing a Centre of Excellence aimed at countering hybrid threats, which was eventually set up in Helsinki in 2017. As an initial step towards developing more comprehensive response capabilities to counter threats, the 2016 Communication underlined a need for the European Commission, in cooperation with Member States and stakeholders, to improve protection and resilience of critical infrastructures against hybrid threats in relevant sectors. These included the energy networks – with a special focus on efforts to diversify energy sources; transport and supply chain security – and space. The importance of protecting public health and food security was also noted.

The 2016 Communication placed key emphasis on raising cyber security levels by improving the resilience of communication and information systems, highlighting particularly the importance of public-private cooperation. It was also stressed that essential service providers in the fields of energy, transport, finance and health, as well as providers of key digital services (e.g. cloud-computing), need to take appropriate security measures and report serious incidents to national authorities. Furthermore, the Communication highlighted the importance of the EU's anti-money laundering framework in making it possible for national Financial Intelligence Units to identify and follow suspicious money transfers and information exchanges,

while ensuring traceability of fund transfers within the Union. Another sector where public-private cooperation was underlined deals with improving resilience against radicalisation and violent extremism. Here strong emphasis was put on tackling disinformation and extremist content on the internet, highlighting the need for rigorous procedures to remove illegal content along with greater responsibility and due diligence being applied by intermediaries in the management of their networks and systems.

The Communication called for the EU's closer cooperation with NATO, arguing that this would make both organisations better able to prepare and respond to hybrid threats effectively in a complementary and mutually supporting manner. In July 2016, the President of the European Council and the President of the Commission together with the Secretary General of NATO signed a Joint Declaration defining seven specific areas of cooperation, including the fight against hybrid threats. In this regard, the declaration stated that there is an urgent need to boost the ability to counter hybrid threats, including: bolstering resilience by working together on analysis, prevention and early detection through timely information sharing; as much as is practicable, intelligence sharing between staff within different teams; and cooperation on strategic communication and response (EU-NATO, 2016). A subsequent Joint Declaration in 2018 reinforced these objectives and noted an increased ability to respond to hybrid threats (EU-NATO, 2018).

The 2016 Communication (European Commission, 2016) was followed in June 2018 by a Joint Communication on 'Increasing resilience and bolstering capabilities to address hybrid threats' (European Commission, 2018a). This later Communication reinforces a focus on: strategic communications and situational awareness; chemical, biological, radiological and nuclear threats (CBRN); together with resilience, cybersecurity and counterintelligence. The Communication argues that 'efforts to destabilise countries by undermining public trust in government institutions and by challenging the core values of societies have become more common' (European Commission, 2018a). Surprisingly, this document presenting the wording 'increasing resilience' in its title, focuses almost exclusively on governmental and EU-level actions, with only minor emphasis being placed on improving the whole-of-society approach. Solely in those sectors where this approach is explicitly visible is there any mention of the importance attached to setting up a dialogue with private actors in the supply chain, thereby facilitating cooperation in addressing evolving threats from unauthorised access to high-risk chemicals, as well as calling for online platforms and media companies to take action on the problem of disinformation.

The 2019 Joint Staff Working Document (SWD) titled 'Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats' (European Commission, 2019) concludes that the EU's counter-hybrid toolbox 'has grown to an impressive size'. The document notes that a large number of legislative proposals have been adopted, such as the Regulation for screening foreign direct investments into the EU. New response measures also include chemical and cyber sanctions regimes. Actions have also been taken inter alia in the areas of countering disinformation, election protection, cybersecurity and defence industry cooperation. The 2019 Report underlines that close coordination between EU entities and Member States lies at the core of counter-hybrid policies and importantly stresses that this should be based on a whole-of-society approach including government, civil society and private sector actors.

As an important element in developing a whole-of-society approach in countering hybrid threats, the EU has increasingly started to emphasise the notion of resilience. The 2016 Communication (European Commission, 2016) defines resilience as 'the capacity to withstand stress and recover, strengthened from challenges'. The Communication continues by stating that 'to effectively counter hybrid threats, the potential vulnerabilities of key infrastructures, supply chains and society must be addressed. By drawing on the EU instruments and policies, infrastructure at the EU level can become more resilient' (European Commission, 2016). In addition, this document highlights that 'it remains essential to strengthen the ability of Member States and the Union to prevent, respond and recover from hybrid threats in a swift and

coordinated manner'. One illustrative example of how the notion of resilience is becoming increasingly significant in the Union's policy work is the 2016 EU Global Strategy, which mentions the word no fewer than 41 times (EEAS, 2016). Here the notion is defined as a broad concept 'encompassing all individuals and the whole-of-society', 'featuring democracy, trust in institutions, and sustainable development' as well as 'the ability of states and societies to reform, thus withstanding and recovering from internal and external crises' (EEAS, 2016).

The EU's resilience work has focused strongly on its external relations, adopting in November 2017 a 'Strategic Approach to Resilience in the EU's External Action', which contains 'Ten Guiding Considerations of a Strategic Approach to Resilience' (European Commission, 2017). In regard to a whole-of-society approach, this Communication importantly places emphasis on inclusive and participatory societies' connections with accountable, transparent and democratic institutions. Conversely, it was concluded that 'shortcomings in governance, democracy, human rights and the rule of law, gender equality, corruption or the shrinking space for public participation and civil society, pose a fundamental challenge to the effectiveness of any society's development efforts' (European Commission, 2017). The Communication also highlights that 'resilient societies are underpinned by sustainable and balanced socioeconomic development that anticipates and addresses socioeconomic inequalities, vulnerabilities, and their root causes. This understanding is at the heart of the EU's approach to state and societal resilience' (European Commission, 2017). The Communication emphasises a number of building blocks for resilient societies, including: inclusive and participatory societies; economic resilience; prevention of violent conflict; a clear and principled approach to migration; as well as countering climate change and environmental degradation.

In December 2019, the European Council Conclusions on 'Complementary efforts to enhance resilience and counter hybrid threats' were adopted (European Council, 2019). These Conclusions emphasise on a number of occasions the need for comprehensive, whole-of-government and whole-of-society approaches to address hybrid threats, both at national and EU levels. The need for continually improved cooperation between relevant national authorities and EU institutions is underlined, with a strong focus on: increasing synergies and avoiding duplication of effort; voluntary information-exchange; along with training and exercises cutting across sectors. One of the key areas where the whole-of-government and whole-of-society approaches are deemed crucial is the protection of critical infrastructure, functions and services. It was also stressed that in addition to EU and national legal, regulatory and supervisory requirements governing operational resilience and business continuity, arrangements with private sector owners as well as operators of infrastructures and services should be promoted in order to guarantee the continuity of and access to critical services.

In December 2020, the Council adopted the 'Conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic' (European Council, 2020). This document highlights that threats such as malicious cyber activities, disinformation and threats to economic security require a comprehensive approach with well-functioning cooperation and coordination. The Conclusions call for a comprehensive situational awareness to deal with hybrid threats, requiring actions at national, EU and international levels in cooperation with partners – including the private sector as well as the owners and operators of critical infrastructures and services. Importantly, the Conclusions invite the European Commission and the HR/VP to develop resilience measures and related resilience indicators further, as they have the potential to become a guiding tool for Member States when developing national structures and initiatives. In addition, the Council underlines its focus on mainstreaming hybrid considerations into policymaking as well as the need to follow whole-of-government and whole-of-society approaches at national and EU level. The Council also invites the EU Commission and the HR/VP to play active roles in addressing pan-European vulnerabilities, including the security and resilience of supply chains as part of economic security.

An important recent activity has been the revision of Directive 2008/114/EC of 8 December 2008 concerning the identification and designation of European critical infrastructures (ECI Directive). On 16 December 2020, the Commission published its proposal for a directive on the resilience of critical entities. This proposed Critical Entities Resilience (CER) Directive expands the ECI Directive's scope by covering ten sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space. It aims to create an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, including hybrid threats (European Commission, 2020).

According to the proposal, Member States would be required to adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments in order to identify such entities. Critical entities would have to carry out their own risk assessments, taking the necessary measures to ensure resilience and honouring an obligation to report disruptive incidents to national authorities. At EU level, a Critical Entities Resilience Group, bringing together Member States and the European Commission, would be responsible for evaluating national strategies and facilitating cooperation and exchange of best practices, while an enforcement mechanism would help ensure that the rules are followed. According to this proposal, Member States would need to ensure that national authorities have the powers and means not only to conduct on-site inspections of critical entities, but also introduce penalties in case of non-compliance. The EC would provide complementary support to Member States and critical entities, for instance by developing a Union-level overview of cross-border and cross-sectoral risks, best practice, methodologies, cross-border training activities and exercises to test the resilience of critical entities (European Parliament, 2021).

The documents and actions presented above represent only some of the major EU actions and decisions taken to counter hybrid threats. As by default this should be a cross-sectoral and comprehensive effort, there are several other processes that are highly relevant in this regard. These include the Free and Fair European Elections Package – in line with the relevant Council and European Council conclusions –, the EU Cyber Diplomacy Toolbox, as well as work done toward the EU Strategic Compass. The European Council has established in the summer of 2019 a permanent working group named 'The Enhanced Resilience and Countering Hybrid Threats Group'. Additionally, access has been granted to the European Defence Fund for projects that aim to counter hybrid threats (Bajarūnas 2020).

2.2 Strengthening the EU's resilience against disinformation

EU actions to counter disinformation play a central role in the Union's efforts to fight back against hybrid threats and improve societal resilience. In this regard, key policy processes include the 2018 Action Plan on Disinformation (European Commission, 2018b) and the creation of the Rapid Alert System on Disinformation in 2019. The 2018 Communication on 'Increasing resilience and bolstering capabilities to address hybrid threats' underlines how disinformation harms democracies by hampering the ability of citizens to take informed decisions and participate in the democratic process. This is a major problem, given that technological developments have made possible the dissemination of disinformation at unprecedented scale and speed.

As to developing a whole-of-society approach, the 2018 Communication on 'Tackling online disinformation: a European Approach' (European Commission, 2018c) calls upon private actors, in particular online platforms and media companies, to take action against disinformation. In this regard, the Communication emphasises: enhancing transparency, trustworthiness and accountability of online platforms; guaranteeing secure and resilient election processes; fostering education and media literacy; supporting quality journalism; and countering disinformation through strategic communication. Furthermore, the Communication stresses that raising awareness and ensuring that people can

differentiate between information and disinformation is of utmost importance, as indeed is guaranteeing the delivery of quick, reliable and consistent information to the public in case of hybrid attacks.

Importantly, this Communication underlines the need for comprehensive societal resilience by correctly noting that 'the spread of disinformation is a symptom of wider social phenomena of societal tensions, polarisation and distrust. In order to tackle this problem, it is essential to tackle the key issues such as economic insecurity, rising extremism and cultural shifts that generate anxiety.' It stresses variations in the impact of disinformation from one society to another, depending on certain structural differences including education levels, democratic culture, trust in institutions, inclusiveness of electoral systems as well as social and economic inequalities. The Communication notes that fostering education and media literacy is crucial in reinforcing the resilience of societies to disinformation. EU action in this respect includes work done by the Commission-steered Media Literacy Expert Group, the Audiovisual Media Services Directive and the Erasmus+ programme on internet safety, digital well-being and digital skills.

Perhaps the most important EU document on the matter is the 2018 Action Plan against Disinformation, endorsed by the European Council in December 2018. This document bases the coordinated response to disinformation on four pillars: (1) improving the capabilities of Union institutions to detect, analyse and expose disinformation; (2) strengthening coordinated and joint responses to disinformation; (3) mobilising the private sector to tackle disinformation; (4) raising awareness and improving societal resilience. Moreover, in March 2019, the EEAS launched the Rapid Alert System 'to enable Member States and EU institutions to facilitate sharing of data, enable common situational awareness, facilitate the development of common responses, and ensure time and resource efficiency' (European Commission, 2019).

The 2019 Joint SWD states that 'the Commission continues its efforts to increase societal resilience against disinformation by reaching out to citizens with proactive messages and positive narratives on the EU's policies and values' (European Commission, 2019). It is argued that this is achieved in particular through the Commission's daily media outreach and the ongoing corporate communication campaigns *InvestEU*, *EUandME* and *EU Protects*. The EU Code of Practice on Disinformation, a self-regulatory instrument finalised in September 2018, plays a role in the work of online platforms by developing internal intelligence capabilities to detect, analyse and block malicious activities on their services. Importantly, this EU document stresses the crucial roles played by civil society and media organisations in fact-checking and research capabilities around disinformation. These actors are vital not only for increasing the transparency, accountability and trustworthiness of online media, but also for raising public awareness and media literacy skills (European Commission, 2019).

2.3 Key obstacles and points of development

As illustrated above, the EU has come up with a significant number of policy initiatives to counter hybrid threats and highlighted the need to develop a whole-of-society approach. Hence, whilst many key steps forward have already been taken, many obstacles and problems still remain. Indeed, it can clearly be seen that merely looking at present official documents paints an unrealistically rosy picture. As Pamment (2020) notes, the EU's work on disinformation, for instance, is characterised by 'a lack of terminological clarity, unclear and untested legal foundations, a weak evidence base, an unreliable political mandate, and a variety of instruments that have developed in an organic rather than a systematic manner' (Pamment, 2020, p. 5) Moreover, he continues, 'one should not underestimate the challenges posed by the different approaches of Member States and EU institutions to the disinformation problem. For example, many Member States do not recognise the problem, do not publicly attribute particular malign activities to the offending adversaries, or are under political pressure to limit support to EU-level activities to counter disinformation' (Pamment, 2020, p. 5).

This critique also reflects more generally on the EU's difficulties in countering hybrid threats. The most significant problem identified is the lack of connection and synchronisation between top-level

commitment to fighting hybrid threats and the necessary working-level policies, plans and measures[1]. Pamment (2020) points out that only certain Member States – such as Sweden, Finland, Poland, Lithuania and Spain – acknowledge hybrid threats as being a major priority. The largest EU countries, France and Germany, do not yet appear to have fully internalised this notion, whereas states such as Austria, Hungary and Italy have registered little or no concern at all.

In addition to differing understandings of this issue's severity, there are also significant ownership and coordination challenges within the EU institutions, coupled with difficulties in overcoming silo mentalities when devising strategies and responses to hybrid threats (Fiott & Parkes, 2019). This, in turn, has resulted in actions which are too reactive, displaying the absence of a holistic approach to counter these threats effectively (Pamment, 2020). Moreover, merely increasing general awareness of hybrid threats is not enough. It is widely understood and agreed that more information and experience sharing within the EU is vital. So far this has proved to be difficult. As Fiott and Parkes (2019) point out, information sharing and intelligence exchange between Member States and EU institutions are still not operating well enough. Risk assessments are often based on the lowest common denominator and proper response networks are still hampered by a lack of trust. Here the main obstacle continues to be the reluctance of Member States to share quality intelligence with each other through EU channels.

This is the case for instance with cybersecurity. Szymański (2020) notes that despite significant efforts, the EU's cooperation on cybersecurity has not been developed well enough to meet the European Commission's ambitions. This is first and foremost due to Member States regarding data cyberattacks as sensitive information. Coupled with a lack of top-down coordination and leadership, this means that hybrid attackers continue to have diverse opportunities to conduct operations (Gressel, 2019). The same applies to the Rapid Alert System. So far only a few Member States share information through the system, since a general lack of trust amongst others has led to low levels of information sharing and engagement (Pamment, 2020).

Despite all the difficulties, as Bajarūnas (2020) notes, the EU could and should become a platform for experience and information sharing between Member States. This would require a joint conceptual understanding of what hybrid threats are all about, an appreciation of how severe the problem is and above all a display of political will. Thereafter, practical steps already formulated in the 2016 Joint Framework on Countering Hybrid Threats need to be more rapidly implemented. Bajarūnas (2020) stresses that with the new strategic agenda agreed upon, the European Commission should now devise a roadmap on how to implement policy initiatives concerning resilience, hybrid threats and disinformation. He also emphasises that the EU should invest more in effective technical and intellectual methods of monitoring and analysing hybrid threats, for instance by strengthening the EU's Hybrid Fusion Cell and EEAS StratCom Units.

From the perspective of this study, developing a whole-of-society approach and societal resilience is critical. Private sector engagement is crucial on many fronts, particularly in terms of the media and IT sectors. Although this is and continues to be primarily a national task, the EU could do more to support and complement resilience building initiatives and national preparedness in Member States. Key sectors where the EU can play a vital role include: intelligence analysis; development of cyber security standards and capacities; critical infrastructure protection; and democratic resilience against information and electoral interference (Finnish Government, 2021a).

[1] See also Bajarūnas, 2020.

3 Mapping hybrid threats: a need for conceptual clarity

The concept of 'hybrid threats' has led to much controversy amongst security analysts and scholars during recent years. Some view it as helpful in highlighting emerging security challenges (Cullen, 2018; Treverton et al. 2018). Others dismiss it as a misleading analytical category, obscuring rather than explaining the changing nature of strategic competition and conflict (Cormac & Aldrich, 2018; Van Puyvelde, 2015). Yet, despite all the rage demonstrated in the latter grouping, hybrid terminology is now firmly established and seems poised to continue being used in strategic planning, as the review of EU documents and policies in Chapter 2 makes clear. The EU continues to refer to hybrid threats and regards them as key within the EU's future strategy work. Moreover, NATO has made countering 'hybrid war threats' a central task in its strategic planning (NATO, 2014). A Joint EU-NATO Declaration in July 2016 made the building of Member States' resilience and ability to counter hybrid threats a priority (EU-NATO, 2016).

Nevertheless, a particular problem with the EU's use of hybrid threat terminology lies in the way it fails to distinguish between its different forms. At present, the term is being used as a catch-all for various threats which differ widely from one another, thus making it difficult for policymakers to delineate institutional responsibilities and formulate more targeted countermeasures. Furthermore, NATO's usage of hybrid terminology does not offer much guidance, as it appears to be employing terms as 'hybrid threats', 'hybrid influencing', 'hybrid warfare' and 'hybrid warfare threats' interchangeably without drawing any distinctions[2]. This loose usage of terms creates confusion particularly between kinetic and non-kinetic threat categories, with potentially far-reaching security repercussions. Practices that rely mainly on non-military means need to be differentiated from those that involve military components, as they require different countermeasures. Treating cases such as Russia's interventions in Crimea and Ukraine together with its meddling in European elections as belonging to the same analytical category of hybrid threats not only creates conceptual ambiguity, but also risks generating unnecessary confusion concerning the level and method of response. Indeed, how the EU and NATO label such activities is not merely an academic issue but will directly affect how policymakers understand and deal with these security challenges.

Accordingly, the EU first and foremost needs to address some of the conceptual challenges involved with the mapping of hybrid threats. A specific challenge has to do with the systematisation of terminology. EU hybrid threat analysis needs to solve the problem of creating analytic differentiation, which can then facilitate the identification of empirical variations between different types of hybrid threats without stretching the concepts into cases that do not fit within the reasonable criteria of conceptual validity. Certainly, a recent conceptual model developed by the EU Commission and the Hybrid CoE is a step in the right direction (Giannopoulos et al., 2020). It provides a valuable basis on which to develop further a shared hybrid threat typology across the Member States.

With this challenge in mind, our study proposes a new hybrid threat typology using three key headings: hybrid interference, hybrid operations and hybrid warfare. These headings differ along three fundamentally important threat dimensions: means (non-military, paramilitary, military), deniability (plausible, implausible, no deniability) and control aim (reflexive, functional, territorial). Table 1 below presents the hybrid threat domain and how it compares with conventional warfare.

[2] See for instance the way in which NATO appears to use the terms 'hybrid threats', 'hybrid warfare' and 'hybrid warfare threats' interchangeably in its 2014 Wales declaration.

Table 1. Differentiating Hybrid Threats

		Hybrid interference	Hybrid operations	Hybrid warfare	Conventional warfare
Means					
	Non-military	●	○	○	○
	Paramilitary	-	●	●	○
	Military	-	-	○	●
Deniability					
	Plausible	●	●	-	-
	Implausible	-	○	●	-
Aim (type of control)					
	Reflexive	●	○	○	○
	Functional	○	●	●	○
	Territorial	-	-	○	●

Note: ○=some focus, ●strong focus

Firstly, to what extent an aggressor uses non-military, paramilitary or military means obviously needs to be a central distinguishing characteristic between different hybrid threats. Military capabilities continue to feature prominently in the contemporary conflict toolbox, but debates on hybridity and grey-zone conflict have helped highlight the way in which conflict activities are also being increasingly pursued in non-military ways, such as disinformation, economic interference and subversion (Wigell, 2019). The use of paramilitary methods and tactics is also seen to be on the rise, even by militarily powerful state actors such as China, Russia and the United States (Morris et al. 2019). Paramilitary implies semi-militarised or irregular military groups which are not formally part of a state's armed forces, such as militias, guerrillas, insurgents, terrorists, cyberhackers and private military companies. Because state actors often prefer not to engage in open conflict with adversaries for strategic reasons, they use paramilitary troops to carry out hostile activities and operations. This demonstrates how hybrid threats may vary significantly in the specific mix of tools used. Hence, for any typology of hybrid threats, 'means' needs to be a central distinguishing feature. From a practical point of view, analytically separating hybrid threats in accordance with the particular combination of means employed will help better plan defensive actions, which will require different countermeasures.

Secondly, related to the above, another important distinguishing feature of any hybrid threat is the focus put on deniability of action by the aggressor. In an open confrontation, such as in the case of conventional warfare between two or more states, deniability is not an issue. The rationale of conventional warfare in essence involves appearing as intimidating as possible and thereby compelling a target to surrender. The use of attributable force is therefore intrinsic to conventional warfare (Art & Greenhill, 2018). By contrast, in the case of irregular warfare, perhaps involving terrorists or guerrilla groups, deniability does not play any prominent part. This inherently involves self-attribution as a facet of shock-and-awe tactics (Schmid & de Graaf, 1982; Jenkins, 1975). However, as highlighted by the debate on hybridity and grey-

zone conflict, an aggressor sometimes seeks to conceal conflict activities in some way to preserve a measure of deniability. It is appropriate here to distinguish between plausible and implausible deniability. An aggressor may want actions to remain covert, hence seeking plausible deniability. Yet, even when conflict activities are such that deniability cannot be plausibly claimed, aggressors may still seek implausible deniability. Indeed, many covert actions are planned with the goal of not remaining secret. Implausible deniability allows aggressors to exploit ambiguity and communicate resolve, while not officially acknowledging the operation (Cormac & Aldrich, 2018).

Finally, hybrid threats may be designed with different strategic aims. The type of control that an aggressor strives for will frame the chosen means and role of deniability. *Reflexive control* denotes the creation of control through reflexive, unconscious responses from the target. The means are thus designed to provoke reactions that are predictable and strategically favourable to the aggressor. The aggressor might interfere in the domestic politics of a target state by seeking to shape perceptions in such a way that the state then voluntarily takes steps that unwittingly further the aggressor's agenda (Thomas, 2004). *Functional control* refers to a different type of strategic aim, which involves targeting the critical functions of a target country using more physical means. 'Critical' in particular refers to those parts of an infrastructure that provide essential and life-sustaining services required for the security and well-being of citizens and key government functions. Ideally the aim is to gain control of some vital critical infrastructure through which the aggressor can coerce or manipulate the target, but often the aggressor settles for merely aiming to interfere with or disrupt some critical function. *Territorial control* refers to the more straightforward aim of gaining broad physical presence on the ground, either directly or through proxies, in the target country, possibly by way of annexation or occupation. In practice, if this action is successful it eliminates the sovereignty of the target state.

Breaking down the hybrid threat domain into separate categories, as detailed above, has a number of advantages for the EU.

1. It serves as a shared analytical tool within the EU to identify and compare different hybrid threats, bringing some order to the 'terminological Babel' that has marked the field in recent years.
2. It helps recognise institutional responsibilities based on the typology, thus facilitating institutional collaboration and coordination within the EU.
3. It helps develop countermeasures based on a clear understanding of the threat domain and thereby better targeting the EU's approach to counter hybrid threats.

A closer look at the variety of hybrid threats should help clarify their differences and the model's analytical logic. It also sets the stage for understanding how to counter hybrid threats. Due to their different underlying strategic rationales, they require broad-based preparedness. Here, we will restrict ourselves to looking at hybrid interference and hybrid operations. Western defence cooperation makes hybrid warfare offensives an unlikely prospect in the European Union, as it would allow ample time for the EU and its Members States to deploy high-end Western capabilities, thus making little strategic sense from an aggressor's perspective (Charap, 2015).

Nevertheless, a word of caution is pertinent here. The typology depicted in Table 1 above not only helps us to differentiate hybrid threats, but also the ways in which they overlap and can be combined in strategies of escalation/de-escalation. All three hybrid threat categories combine similar elements, but to a different extent. Indeed, their 'hybridity' comes precisely from the way they combine both conventional and unconventional military as well as non-military tactics and tools to achieve strategic objectives. As we move from the category of hybrid interference through hybrid operations to hybrid warfare, the means becomes more kinetic and overt, suggesting a pattern of escalation. As such, while hybrid interference and

hybrid operations are threats in their own right, they can also entail different pre-positioning phases with escalatory potential towards hybrid warfare or even conventional warfare.

3.1 Hybrid Interference

Hybrid interference refers to the use of a wide range of non-military strategies to gain control of other states' strategic interest formation reflexively (Wigell, 2019). As such, it resembles what was referred to as 'active measures' during the Cold War and more recently in Russian strategic parlance as *gibridnaya voyna* ('hybrid warfare'). The idea of *gibridnaya voyna* is to avoid the traditional battlefield, but nevertheless aim to destroy 'the political cohesion of an adversary from the inside by employing a carefully crafted hybrid of non-military means and methods that amplify political, ideological, economic and other social polarisations within an adversary's society, thus leading to its internal collapse' (Fridman, 2018, p. 96). While maintaining diplomatic relations and thus not breaking any official war threshold, the aggressor mobilises oppositionists and radicals within the target state through a host of methods ranging from disinformation campaigns to corrupting political actors and financing subversive movements, carefully synchronised to compound the effect.

Hybrid interference avoids the use of overt military strategy in order to maintain plausible deniability. As such, it is a form of covert action that centres around the logic of 'subversion', which refers to the deliberate attempt by an aggressor state to destabilise and undermine the authority of a target state by way of local proxy actors (Breitenbauch & Byrjalsen, 2019). It specifically involves the use of disinformation and economic inducements to recruit and assist these actors inside the target country, detaching their loyalties from the target government and using them as interlocutors to transform the established social order together with its structures of authority and norms. The aim is specifically to weaken democratic governance and norms as a means of enhancing the aggressor's authoritarian standing. Not only are weakened democracies less able to confront these authoritarian aggressors directly, but they will also look less appealing as models of success and partners for others. By portraying Western democracies as corrupt and ungovernable, authoritarian regimes such as China, Iran, Russia and Turkey are less at risk of being overthrown by their own populations (Wigell, 2021).

The use of economic instruments forms a central part of hybrid interference. It may involve capturing strategic sectors within an economy, such as critical infrastructures, finance and media, by which the hybrid agent can attempt to: destabilise the target country and manipulate local economic conditions; generate unfair profits for some local stakeholders while punishing others; and thus achieve greater political influence (Conley et al., 2016). A prominent example is Russia's use of its energy resources as a means of driving political wedges between different parties both at national and EU levels (Wigell & Vihma, 2016). The Kremlin has also been channelling money into anti-EU organisations and movements to accelerate a centrifugal effect within the Union (Polyakova et al., 2016). In addition, there are a number of other economic levers available for resourceful external powers. One option is to foster links with leaders of industry and politicians by offering them business opportunities. This facilitates a web of local affiliates in positions of power, who possess an incentive to advocate on the external power's behalf and downplay any attendant threats. The deliberate use of corruption and cronyism can be used to reinforce this tendency. Corruption networks across borders facilitate the recruitment of 'fifth columnists', who act as middlemen in interfering with economic and political processes. Two reports by the Centre for Strategic and International Studies (CSIS) reveal how large economic players in the European Union, such as financial and corporate service providers, having become entangled in illicit Russian finance schemes later go on to function as 'enablers' of Russian interference, with direct consequences for democratic structures (Conley et al., 2016; Conley et al., 2019).

A key means is the use of disinformation, which pertains to the intentional distribution of false or inaccurate information into the communication system of a target country or group[3]. It is an encompassing category, covering various forms of information influence operations, whose vast reach and penetration are enhanced by the use of modern media technology. The hyper-connected nature of cyberspace works as a force multiplier, allowing external powers to plant, disseminate and lend credibility to disinformation. This has been critical in the recent success of Russian disinformation campaigns (Giles, 2016; Richey, 2017). Similar practices are also being used by China. President Xi Jinping, for instance, has embarked on a campaign of information control by targeting niche foreign media with mergers, acquisitions and partnership agreements (Hamilton, 2018).

Disinformation is central to the overall strategic objective of reflexive control for a number of reasons. First and foremost, disinformation campaigns are designed to provoke public discontent and create an aura of distrust. Russian disinformation campaigns have for instance played on the anxieties of target populations with trumped up (or actual) misdeeds by refugees and then represented European governments as either reluctant or powerless to manage the influx[4]. This has sometimes been carried out concurrently with an intentional campaign of migrant dumping to amplify the effect (Pynnöniemi & Saari, 2017). With European public opinion already divided, such offensives have led to heightened polarisation over the issue.

Hybrid interference is designed as a flexible approach, in which the tools and tactics can vary, but they will always be tailored to manipulating existing cleavages as well as sowing internal dissension in target countries and alliances. Hence, hybrid interference does not adopt a one-size-fits-all approach, but rather exploits specific vulnerabilities depending on target country contexts. The hybrid aggressor interferes in domestic politics by seeking to amplify divisions and hatred, undermining the 'civic culture' – crucial for democratic governability – by tempering the intensity of political conflicts and cleavages (Diamond, 1999). The idea is not to confront the target head-on, but to weaken its resolve more subtly by employing interference which is calibrated to undermine internal cohesion. By helping to provoke divisions or aggravate existing tensions among target populations, hybrid interference thus functions as a 'wedge strategy'. When such a strategy is successful, it will have a corruptive impact on the target's cohesion, aggravating internal divisions and conflicts, thereby weakening its potential to instigate counteractions (Wigell, 2019).

This presents a particular challenge for the European Union. The EU's open pluralism with its multitude of competing interests from 27 Members States can be exploited by driving wedges between various factions, potentially exacerbating conflicts to the point where governability is threatened. Hybrid interference is deliberately designed to accelerate the sort of politicisation and polarisation that make it hard for the EU along with its Member States to manage and process such underlying conflicts. Brexit has been a case in point, with strong indications of external interference deliberately designed to deepen underlying rifts (McGaughey, 2018).

Preventing a hostile actor from exploiting European democratic pluralism involves taking a whole-of-society approach to security with the aim of strengthening societal resilience against hybrid interference. Initiatives to counter hybrid interference, therefore, need to include various means of supporting societal resilience, such as:

- *increasing efforts to activate civil society* – investigative civil society groups and media can play a major role in detecting and monitoring hybrid interference;

[3] Disinformation needs to be differentiated from *misinformation*, 'which is the unintentional dissemination of false information'. Kragh and Åsberg (2017), p. 797.
[4] For a compilation of cases, see EU vs Disinfo.

- *fostering increased transparency* – foreign influence transparency registers, mechanisms for screening foreign investments as well as requirements for non-governmental organisations (NGOs), political parties, media and research institutes to report their sources of funding publicly will help disrupt and deter alliances between hybrid aggressors and domestic proxy groups;
- *broadening social inclusion* – policies directed toward enhancing media literacy, social cohesion and welfare, particularly by integrating diasporas and minorities, who otherwise risk being used as proxies for hybrid interference efforts.

3.2 Hybrid Operations

Hybrid operations (HOPS), sometimes called 'grey zone tactics', comprise any hybrid threat that aims to gain primarily functional and – when deemed necessary – reflexive control of a target state or area by integrating mostly non-military and especially paramilitary operations, while as a minimum requirement seeking to preserve implausible deniability. As such, the term captures activities just short of war in which state actors avoid aggressive military use of force and hence do not cross the threshold to overt conflict.

To preserve ambiguity and deniability, paramilitary forces and tactics feature prominently in HOPS. These include the use of terrorists, mercenaries and criminal networks to engage in kidnappings and assassinations so as to intimidate target populations along with the use of sabotage and cyber-attacks against critical infrastructures (Jonsson, 2018). Using radicalised local activists can be an effective way of creating a permanently operating front inside the target country (Breitenbauch & Byrjalsen, 2019). With their ready-built networks inside the target country and inherent operational deniability, these proxies can easily be activated without too much risk of direct attribution. To compound this effect, paramilitary campaigns are combined with other non-military means to achieve their objectives.

Firstly, through economic means, hybrid operators try to capture strategic sectors of the economy such as critical infrastructures that provide functional control and can be used as ready-made platforms for other hybrid measures, including paramilitary forces and tactics. Trade and investment deals are utilised to bind key interlocutors in target countries into dependency relationships, thereby providing leverage for hybrid operators (Jonsson, 2018). The deliberate use of corruption and cronyism is used to reinforce the creation of such fifth columns inside the target country (Zelikow et al. 2020). Through mergers and acquisitions, hybrid operators gain control over critical infrastructures and media, facilitating the use of other HOPS options. If ownership disclosure requirements are lenient, such activities can be hidden behind a network of proxies, shell companies and offshore accounts.

The *Airiston Helmi* case in Finland provides an illustrative case of a possible preconditioning hybrid operation. In September 2018, more than 400 Finnish police officers and military commandos raided around 20 properties in the Finnish archipelago (Higgins, 2018). The properties had been purchased by the real estate firm *Airiston Helmi* and its Russian backer Pavel Melnikov, who had been operating under various disguises while investing in Finland. The names of this company's real owners were obfuscated behind shell companies registered in the British Virgin Islands and other offshore tax havens. Despite continuing to invest millions of euros in these properties, the company appeared to have no revenues and reported losses year after year. Interestingly, all investments were concentrated on strategically located properties in the south-western archipelago, near important military installations as well as vital ports and sea lanes critical for Finland's security of supply. The properties had been equipped with helipads, large sized piers, multiple satellite dishes and sophisticated communications equipment, in addition to no-trespassing signs, motion detectors and security cameras to keep trespassers away. While the raid was officially described as a crackdown on tax evasion and money laundering, circumstances suggest that this company was operating as a cover for preconditioning hybrid operational capabilities.

Secondly, disinformation provides a key means whereby hybrid operators attempt to propel local radicalisation and subversion. The dissemination of narratives – often conspiracy theories – that support local extremist groups facilitates the cultivation of a subversive operating front inside the target country. Inciting and fuelling protest movements by disinformation, which can then be infiltrated by *agents provocateurs* to incite violence, is very much part of the paramilitary toolbox for hybrid operations.

In attempting to take advantage of any vulnerabilities, strategies are always tailored to the countries that HOPS target and the precise combination of methods will thus vary from one HOP to another. All actions are planned to preserve a measure of deniability so as not to cross over the threshold of overt conflict that may trigger counter-offensive actions. Yet, in contrast to hybrid interference, HOPS do not always seek plausible deniability. Depending on the context, implausible deniability can be useful in some HOPS because of the ambiguity it creates (Cormac & Aldrich, 2018). It allows states to communicate their resolve without escalating conflict activities into open warfare. During the Cold War, such 'open secrecy' sometimes prevented escalation. It allowed parties to manage risk by maintaining the fiction of secrecy and thereby offer an exit from tense situations (Cormac & Aldrich, 2018). At the same time, deterrence effects may be sought by conveying subtle messages about the existence of capabilities without specifying exactly how they are being used. With a view to this deterrent value of denials being implausible, ambiguity is thus preferred over strict deniability.

As an example, Cormac and Aldrich (2018) use the 2007 Israeli 'covert' strike on a suspected Syrian nuclear reactor to illustrate the logic. They argue that it was launched as a way of demonstrating resolve to other potential nuclear proliferators in the region, particularly Iran. The deterrent value of this strike depended precisely on the Israeli denial being implausible. A similar example is offered by the Salisbury poisoning case, in which Sergei Skripal – a former Russian military officer and double agent for the British intelligence services – was poisoned together with his daughter by a rare military-grade nerve agent developed in Russia. By leaving this distinct fingerprint behind, the would-be assassins wanted to convey a warning to Russian exiles seen as traitors of the Russian regime and perhaps also a broader message of its potent capabilities for conducting operations on foreign soil (Financial Times, 2018).

While hybrid operations may include reflexive control aims, more central is the aim to influence or interfere with the functionality of a target country. Cyber intrusions offer a tool which is capable of disrupting critical processes in a target state, for instance, through denial-of-service attacks on vital infrastructures such as electricity grids. Other paramilitary methods in cyberspace include data theft, data destruction, malware, or the outright capture of key systems. Ideally, the aim is to capture crucial functions through which the target country can be made dependent on the hybrid operator. Herein, economic interference offers another proven mean. A hybrid operator working in an open economic environment may be able to capture the ownership of critical infrastructures in a target country.

The European Union and its Member States are in many ways vulnerable to different HOPS. Key features of European democracy provide possible loopholes for hybrid operations. *State restraint* is an integral part of European democracy, with the rule of law governing a state's powers and functions, while simultaneously providing the necessary space for an autonomous and functioning civil society. However, when the state has been functionally restrained from 'policing' society, it has limited scope for detecting and protecting against hybrid operations. Similarly, the democratic principle of a *free media* renders it difficult for European governments to defend themselves against disinformation campaigns. Hence, by utilising a mixture of media outlets as vehicles for disinformation offensives, a resourceful hostile actor may exploit this open, deregulated media environment. The *economic openness* of European democracies also renders them vulnerable to external capture and exploitation, particularly in regard to strategic sectors within economies such as critical infrastructures. Indeed, as a strategic practice, HOPS are deliberately tailored to exploit openness in democratic economies and society.

Given the nature of HOPS, they cannot be countered by societal resilience alone. Countermeasures will need to include more direct efforts to dissuade actors from using HOPS by changing their strategic calculations, in accordance with a whole-of-society approach in which the state retains a coordinating role. These measures should involve:

- *public-private continuity management* – public-private cooperation is paramount as most critical functions of European society these days are operated and managed by private sector actors;
- *strategic communication* – enhanced attribution capabilities and communicated thresholds of response are important expedients in dissuading hybrid aggressors;
- *sanctions preparedness* – by signalling preparedness to harden sanctions in a coordinated manner, the EU can strengthen hybrid deterrence.

4 Resilience and the whole-of-society approach

This chapter focuses on the interplay between comprehensive societal resilience and the whole-of-society approach. The use of resilience as a concept has become ubiquitous within aims to survive and recover from adverse events and crises. At the same time, its exact meaning and added value implications remain vague. There is a lack of clarification about its precise link to related security discourses, such as national preparedness and hybrid threats, as well as its relationship with the whole-of-society approach. The study addresses this *problématique* by analysing how resilience should be understood in the context of hybrid threats, what elements the concept should include and how the resilience of civil society at large could be enhanced so as to deter hybrid threats in a whole-of-society manner. As previous chapters have shown, the very broad definition of hybrid threats used by EU institutions is of value when delineating the entire hybrid threat domain. However, it needs to be complemented by a better conceptual differentiation between the various threats. This is also the case with societal resilience as a strategic concept in countering hybrid threats. At present, it is defined in a loose manner without any specification of its various components and how they connect with different hybrid threats. Indeed, there is a clear need for developing the hybrid-resilience nexus, especially in terms of dissecting different strategic approaches to resilience building and more specific societal capacities upon which these strategic responses must be built[5]. Although defining resilience loosely might serve the function of providing conceptual middle-ground to close the gap between more liberal-minded and conservative approaches to EU foreign policy (Cross, 2016), a lack of analytical precision hampers the development of more targeted policies.

In order to clarify the strategic and operational value of resilience in the context of hybrid interference, Chapter 4 provides an ideal typical model of comprehensive societal resilience (Hyvönen & Juntunen et al., 2019). This model consists of two dimensions. Firstly, as a response to crises and disruptions, societal resilience should be understood as a temporal process that consists of resistance, maintaining functionality and adaptive learning. Secondly, as an attribute that cuts through society, resilience should be analysed as a 'nested' or layered attribute. Insights derived from the comprehensive resilience model are then applied to evaluate the EU's alternative strategic options for resilience building against hybrid interference.

4.1 Resilience as a comprehensive process

In common jargon, resilience is usually understood as the ability of any given referent object to withstand the immediate impact of major disruptions, regardless of whether such disruptions are societal or personal in nature. In multidisciplinary studies literature, resilience is usually understood as a complex process of adaptation and change. As an operational concept, resilience can further be divided into attributes, implying either 'systemic resistance' or 'general adaptive capacities' (Tierney, 2014; Hyvönen & Juntunen et al., 2019)[6]. Moreover, resistance itself can be categorised into attributes that represent physical or mental robustness and systemic redundance, whereas adaptive capacities stem from the resourcefulness of society as a whole (Brand & Jax, 2007; Juntunen & Hyvönen, 2014).

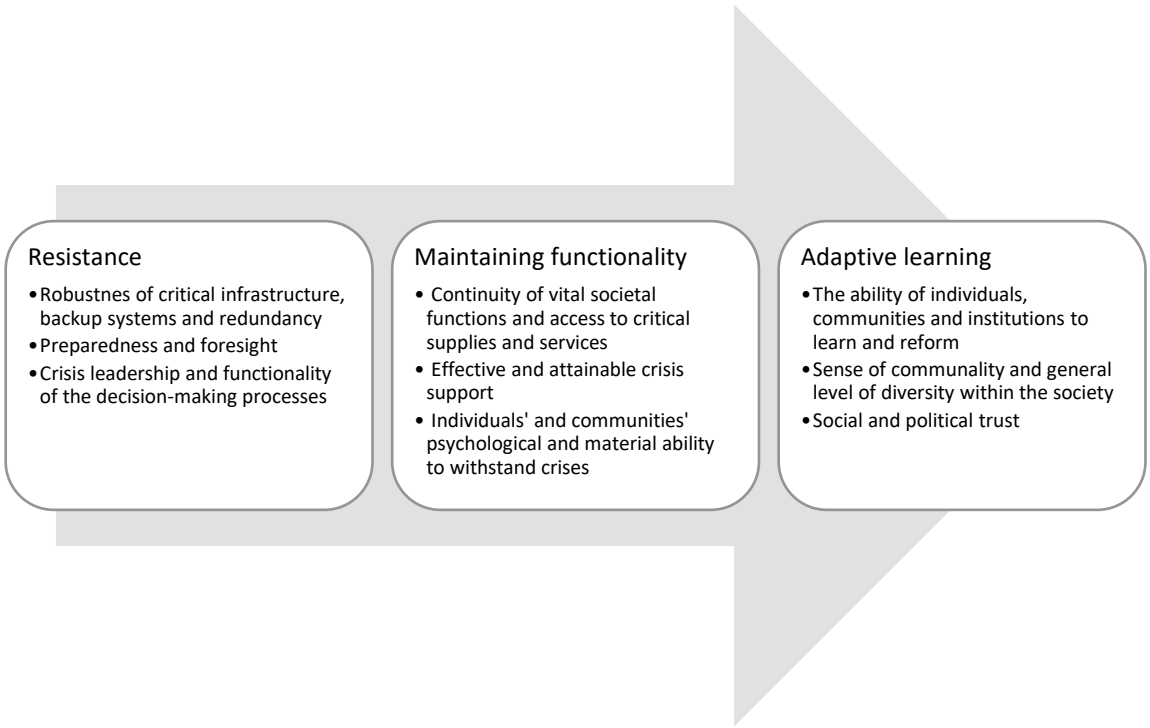
This points towards an understanding of resilience that does not merely reduce it to a capability for rapid response enforcement to restore the status quo, but rather a comprehensive process wherein an ability to manage the inevitable impacts and repercussions of crises or other major disruptions is highlighted. Processual understanding of resilience is also grounded on the notion of modern technology-dependent open societies' high level of interdependency. Together with the societal threat landscape's increasing complexity, this has decreased a general ability to foresee the likelihood and proportions of each crisis.

[5] To date, academic multidisciplinary resilience studies have to a large extent focused on themes related to global governance and non-state centric threats, such as environmental catastrophes, responses to climate crisis together with counter-terrorism policies and less on hybrid threats.
[6] Instead of resistance, Tierney uses the concept *inherent resilience* in the context of community disaster resilience.

Modern hybrid campaigns share these elements of vagueness and complexity. Indeed, reliance on deniability and ambiguity is very much a key rationale of hybrid interference.

Against this processual reading, comprehensive societal resilience consists of three partly overlapping phases: (1) attributes that increase the resistance and immunity of a system/society in order to absorb the immediate impact of the crisis; (2) resources needed to maintain general functionality and identity of a system/society while adverse conditions persist; (3) broader institutional and societal attributes not only in adapting positively to the post-threat situation, but also by initiating a reflective learning process to enhance comprehensive resiliency of a system/society to face another similar disruption in the future[7].

Figure 1: Resilience as a comprehensive process (Juntunen & Hyvönen, 2020)



This processual model should be understood as an ideal type rather than a one-size-fits-all solution to every possible threat scenario. In other words, the model merely offers a template for both strategic societal resilience planning and post-hoc evaluation of threat responses. Another important caveat to be borne in mind is the need to expand any conception of societal resilience beyond the traditional understanding of societal crises. Indeed, modern societal resilience conceptions have mostly been developed in the context of crisis management. The actualisation of hybrid threats, conversely, does not usually lead to a crisis in the traditional sense[8]. Instead of having clearly discernible spatial and temporal dimensions, hybrid threats 'merely' (or at worst) incite societal distress that *could* lead to a 'creeping crisis', in other words a crisis that has 'a long incubation time and may keep simmering long after the 'hot phase' of the crisis is over' (Boin et al., 2020, p. 120).

Within the context of hybrid threats, these stages of the resilience process are more entwined than would be expected in 'normal' crisis contexts. In other words, the processes of resistance, continuity management

[7] Similar kind of processual models of resilience building have been developed in the context of urban resilience (see Rademaker et al., 2018, 8).

[8] In Crisis Management literature, a crisis is generally defined as an event that (i) poses a threat that endangers essential values or goals of the actor; (ii) compels the actor facing the crisis to make prompt decisions under considerable stress to avoid the increasing costs of inactivity; and (iii) is relatively unpredictable both in terms of its likelihood, dynamics and societal impacts (Pursiainen, 2018).

and adaptation are not as linear as those within traditional scenarios. The actual threat potential is usually inconspicuous enough not to increase general crisis awareness, especially because it pertains to hybrid interference, which aims to provoke divisions, polarisation and societal tensions among target populations in a covert manner. Low levels of attention towards the actual threat potential and the fundamental value of respecting the transparency of democratic decision-making culture implies that counter-hybrid policies cannot rely on the sort of exceptional policy measures used in traditional crisis management contexts.

Consequently, when enhancing societal base structures to counter hybrid threats, the three resilience process phases should be planned primarily as overlapping components of a comprehensive approach. These phases should be flexible enough to allow context-dependent variations in the balancing of their weightings. Certain hybrid tactics, such as the combination of cyber-attacks and military coercion, require countermeasures that stress the need for building robust infrastructures and coordinating visible resistance measures taken by officials and governments. By contrast, more invisible and subversive hybrid interference tactics that aim to create more gradual 'wedging effects', such as disinformation campaigns, require tailored responses where emphasis is placed on the role of societal attributes along with the ability to reform and adapt.

Thus, it is important to note that improving resilience against hybrid interference cannot be reduced to attributes that aim to avert the impact of a 'wedge strategy' altogether, nor can it be planned on the basis of returning to a pre-crisis status quo as rapidly as possible. This is simply due to the creeping nature of hybrid interference, where there is no clear pre- or post-crisis state to return to. Instead, the refining of resilience responses to hybrid interference should be built upon any society's general resilience capacities. This would increase its ability to absorb the slow burning 'wedging effects' of hybrid interference without the need to employ measures that would require deviation from democratic practices. Ultimately this implies an ability to deal with the long-term effects of hybrid interference as a continuous process that would include openly reflective in-built learning processes among likeminded societies. This would then also strengthen the 'democratic deterrence' effect against potential hybrid aggressors (Wigell, 2021).

4.2 Whole-of-society approach in practice: layers of resilience

Comprehensive resilience policies should be planned to provide responses within all three phases of the abovementioned resilience process. In order to function properly this needs to be done in a cooperative whole-of-society framework that integrates the capacities and capital possessed by various private and civil society sector actors into one unified strategic planning process (Hyvönen & Juntunen, 2020). In addition to understanding this whole-of-society approach as a 'silo-breaking' model of cooperative planning between different branches of the government, it also refers to a 'panarchic' (overlapping and all-encompassing) understanding of society that is being structured along certain 'levels of analysis'. There are several heuristic typologies in academic literature which visualise these layers of resilience. One recent academic meta-analysis that was conducted to trace the dimensions of comprehensive societal resilience has suggested a division into four layers and their interconnections: (1) personal resilience; (2) community and sub-regional resilience; (3) institutional resilience; and (4) forward resilience[9].

Firstly, *individual resilience* obviously refers to people's psychological and temperamental characteristics, predispositions and competencies. This also includes social and education policies that reduce inequalities,

[9] See Hyvönen & Juntunen et al., 2019, pp. 23–25. The study was funded by Finnish Government's analysis, assessment and research activities unit and conducted in 2018–19. Although the study was conducted specially to inform Finnish decision- makers and civil society actors, the meta-analysis was based on wider academic research rooted in multidisciplinary resilience studies. There are also more complex typologies and heuristic typifications on the levels of societal resilience in the research literature. Walklate et al. (2014) finds seven layers: individual, family, communities, institutions, national level (the state), regional level and global sphere. Berkes and Ross (2016), on the other hand, discusses on five layers: individuals and families, communities, sub-national regions, national and global spheres.

thereby enhancing the social trust basis of a society. On an individual level, these further enhance the ability to withstand crises and other forms of disruptions. Research results in developmental psychology have shown, for example, that the quality of early childhood education and the ability to grow up in safe and caring surroundings correlate strongly with a later ability not only to function during personal or societal crises, but also to recover positively thereafter (Ungar, 2011; Backett-Milburn et al., 2008). In the context of hybrid interference, the role of critical media literacy as an integral civic virtue also stands out at the individual level.

Secondly, *community-level resilience* refers generally to the sense of togetherness and meaningfulness that individuals experience in their immediate livelihoods. In this sense, the quality and sustainability of vibrant residential environments also interweave with community resilience. According to Hall and Zautra (2010), resilient neighbourhoods are characterised by: a strong trusting bond between its members; regular interaction among neighbours; a relatively stable residential structure; a sense of togetherness and communality; a willingness to act on behalf of the community; and the accessibility of public spaces. As local communities are the locus of social and democratic participation, this highlights their importance in terms of accumulating social capital and trust within a society – key ingredients of adaptive societal resilience. Moreover, when planning critical infrastructure protection against possible hybrid operations, the specific needs of vulnerable communities should be stressed[10].

Thirdly, *institutional resilience* refers to social policy, critical infrastructure planning and functionality of political decision-making structures. In terms of preparing national responses to hybrid operations, this institutional level is perhaps of crucial importance. When it comes to social policy, the key sectors in enhancing resilience are welfare and education. Another vital feature of a resilient society, one that also increases invulnerability against certain methods of hybrid interference such as disinformation campaigns and election interference, is the level of political trust – understood as citizens' trust towards key institutions and officials. Finally, the level of coordination in preparedness planning between national and regional levels increases institutional resilience, as does a clear distribution of responsibility in national crisis decision-making.

Fourthly, the layer of *forward resilience* consists of foreign relations, cooperative structures and institutional arrangements. These comprise effectively planned continuity management and security of supply policies that are developed in international cooperation so as to cope with the challenges caused by increasingly interdependent global value and supply chains. Perhaps most importantly, especially in regard to the EU, international coordination of counter-hybrid planning and arrangements to share situational awareness represent vital elements in countering 'wedge strategies' – which are rarely tailored purely on the basis of certain national characteristics.

The main driver in considering counter-hybrid resilience building through overlapping and partly nested societal spheres is to highlight the interrelated nature of these layers. The layering model of this whole-of-society approach gives practitioners responsible for the policy planning of counter-hybrid measures an additional analytical tool to locate the various actors that are providing resilience building capacities either directly or indirectly.

4.3 Towards an EU hybrid resilience strategy

As reported earlier in Chapter 2, the EU already recognises the strategic value of a resilience approach in its documents and policies, not only in relation to countering hybrid threats, but also in the context of its wider strategic ambitions – such as increasing the Union's autonomy. However, analytical ambiguities remain concerning the exact meaning of societal resilience and how it should be translated into a more

[10] For a more elaborate taxonomy on community resilience and its indicators see Rademaker et al., 2018.

operational concept. Although conceptual clarity and precision need not be an objective within policy planning, there is certainly a need for more fine-grained analytical articulation of what societal resilience strategies mean in general and from the perspective of hybrid threats in particular.

Philippe Bourbeau (2013; 2018a) has presented a valuable tripartite typology of resilience strategies, which feature maintenance, marginality and renewal (MMR-typology). Although Bourbeau has developed his MMR-typology as a descriptive tool for analysing migration policies, it can also be applied to trace how the strategic value and purpose of resilience are understood in other settings related to societal security governance[11]

Firstly, *resilience as maintenance* aims to secure the existing social order and institutional setting. This type of resilience finds relevance in countering hybrid operations. Due to the highly intrusive nature of HOPS, the ambition of a maintenance strategy should focus on preventive actions by creating a compelling and deterring toolkit of countermeasures. The challenge with this approach is that the legitimation of countermeasures needs to rely on a high level of securitisation and open threat construction. This requires an institutionalised and shared process of hybrid threat assessment along with planning of countermeasures and exercising. One straightforward danger of maintenance strategies is that they tend to provoke responses which securitise the whole fabric of any society, including its day-to-day functions (Bourbeau & Vuori, 2015). This, in turn, might lead to questionable practices that obfuscate the division between normal running of democratic politics and exceptional policy measures, thus potentially endangering societal freedoms and intensifying a climate of suspicion.

Resilience as maintenance points towards hierarchical top-down counterstrategies where the combined role of governments, security officials and key EU institutions is being emphasised. The main rationale in maintenance strategies is to invest in capabilities that enhance the EU's ability to prevent and repel the intrusive and disruptive effects of hybrid threats. This is especially important in relation to direct kinetic threats, such as the use of CBRN agents as well as paramilitary and military operations. Enhancing resilience as maintenance at EU level requires continual coordination of operational level actions and up-to-date situational awareness between Member States and the European Commission. It is also important to note that public legitimation of maintenance strategies requires a solid EU level communication strategy that makes it possible to expose the gravity of threats openly and coherently so as to signal, resolve and counter disinformation.

However, with regard to hybrid interference, particularly strategies aiming at reflexive control such as malicious and corruptive investment operations, resilience as maintenance is not enough. Hybrid interference, with its focus on preserving plausible deniability, complicates attribution. Indeed, hybrid interference is intentionally designed to reduce clarity about who is doing what, or whether somebody is actually doing anything. As such, well-targeted deterrence measures are hard to apply against most forms of hybrid interference.

Secondly, *resilience as marginality* stems from the premise that a threat cannot be checked or completely prevented. This type of resilience can be useful in countering HOPS that rely heavily on subversive tactics – such as cyber intrusions and attacks against critical infrastructures in general – and cannot be disclosed fully in public due to sensitive information about critical capabilities. The idea is thus to marginalise the inherently intrusive threat in order to render it less effective. This requires high levels of intra-agency cooperation between the Member States' security officials, key international organisations such as the European Union Agency for Law Enforcement Cooperation (EUROPOL) and EEAS StratCom Units. At the same time, the marginality strategy serves the purpose of providing escalation control.

[11] See also Bourbeau & Vuori (2015).

Relying on resilience as marginality also has a downside, if used as a preclusive strategy in isolation. A challenge inherent to the process of marginalising is that it will not be dealt with publicly (Bourbeau, 2013). In other words, the authorities' public communication over the magnitude of a particular threat will not align with actual security practices, which may lead to a questionable culture of secrecy and lack of open dialogue. As such, this strategy may also entail foregoing any possible lessons that could be shared with the whole society. If relied on for a prolonged period of time, the disconnect between public security discourses and government-led practices increases, which is particularly problematic in open democratic societies trying to learn how to endure hybrid threats. If the public finds out post-hoc that the actual measures taken by government and officials were more drastic than the official justification and framing of any incident, this might lead to a severe decrease in political trust and general sense of legitimacy conveyed by key societal institutions. This latent tension in the strategy of marginality might, in turn, be exploited in the adversary's hybrid aggression strategy.

Thirdly, unlike resilience strategies based on marginality and maintenance, *resilience as renewal* actually considers disruption as an opportunity to bring out the transformative potential of a society by remodelling its structures (Bourbeau, 2013). In other words, resilience is understood as the ability and will to reform on the basis of crisis experience. Moreover, resilience as renewal emphasises the need to craft an appropriate situation-specific response. This requires: open communication on the nature of any threat; embracing whole-of-society preparedness to crisis management; and the ability to coordinate actions flexibly during and after the crisis.

Resilience as renewal strategies highlight the self-organising abilities among civil society, something that is especially crucial in countering HOPS based on tactics such as disinformation campaigns and election interference. Resilience is perceived more in a bottom-up manner, stemming from a high level of civic virtues, culture of democratic participation and strong bases of social trust.

From the perspective of this latter resilience strategy, by exposing vulnerabilities a hybrid threat would thus be seen as a 'stress test' for European democracies (Wigell, 2021). Crafting effective countermeasures would involve crafting targeted responses to those particular vulnerabilities in a reactionary manner. This calls specifically for a whole-of-society approach, aimed also at bringing societal actors into an open model of dialogue, cooperation and joint preparedness. This would mean that the relationship between governments and EU institutions would be more akin to partnership than hierarchy and the roles of civil society actors would be perceived as a crucial resource, both in the planning of counter-hybrid strategies and their execution.

While the open environment of European democracy presents loopholes for covert interference, it simultaneously provides an enabling environment for citizen activism, which can play a major role in identifying interference and a society's respective resilience (Wigell, 2021). Civil society actors are central in monitoring and exposing hybrid interference. Essential watchdog functions of the open media environment serve the same end. Investigative journalism is a pertinent example, as evidenced by novel online sources such as *Bellingcat*, whose investigations helped solve the Skripal poisoning case.

Western democracies should encourage investigative civil society groups and media to monitor and detect hybrid threats. Civil society groups are often more acutely aware of localised dynamics and more agile in their scrutiny. Through quality education on critical media literacy, civil society support and media capacity building, society's cognitive resilience can be strengthened. Specific measures should include developing rapid alert systems, media literacy programmes and training media professionals themselves in recognising fake news. In the United States, the Countering Foreign Influence Task Force of the Department of Homeland Security, in coordination with the FBI, began operations before the 2018 US midterm elections. Its focus is on raising public awareness about the inherent dangers of foreign disinformation campaigns and working with social media companies as well as academia to improve recognition and understanding, thereby helping build resilience against foreign disinformation (Wigell, 2021).

The exponential growth of open data is also changing the nature of intelligence. Traditionally a realm which has almost exclusively been governmental, this is now making private firms and civil society organisations central in monitoring and exposing hybrid interference. Especially in the digital sphere, the private sector is often a step ahead of governments in developing new analytical technologies. For example, facial recognition software, now deployed by most intelligence services, whether private or governmental, was developed by Israeli companies. The United Kingdom and the United States are increasingly emulating Israel, where government intelligence agencies are embracing the commercialisation of espionage instead of battling it (Lucas, 2019). By supporting societal and market-based mechanisms in this way, resilience can be strengthened within the confines of the democratic rule of law (Wigell, 2021).

The strategy of renewal is thus also based on explicit securitisation of a threat, albeit without the need to resort to a policy of secrecy. The main problem with a strategy of renewal lies in its tendency to use crises as scapegoats for societal reforms that have little or nothing to do with the motivation of tackling similar crises in the future. Moreover, the tendency to avert deterrence and coercion techniques that aim to repel the threat, at least partially, can lead to sentiments of defeatism, should the post-crisis renewal process fail to deliver widely accepted societal reforms.

Following from what has been discussed above, how then should the EU react in order to enhance its resilience against hybrid threats? First and foremost, the EU should aim towards adopting an overall hybrid resilience strategy that would be more capable of adapting to variations in maintenance, marginality and renewal (MMR-typology) on a threat-specific basis. The importance of clarifying and refining alternative strategic responses becomes even more evident when one looks at the various conceptualisations of resilience in key EU documents[12]. An analytical dissection of resilience building by dividing it into attributes enhancing either societal resistance or adaptive capacities would further clarify how the different components of an overall whole-of-society strategy could link together.

Secondly, a key takeaway would be to reconsider the relationship between deterrence and resilience (Sørensen & Nyemann, 2018). This points to the subtle division and relationship between, on the one hand, general societal attributes that contribute to comprehensive resilience and, on the other hand, active policies of dissuasion and open countermeasures against hybrid campaigns. It is especially important to recognise that the framing of societal resilience purely in terms of deterrence might also have some negative implications. One obvious danger is that this could lead to an over-securitisation of day-to-day societal processes.

When deterrence – understood either as dissuasion based on punishment or denial – is based on the ability to impose and signal unacceptable costs to an adversary, general resilience capabilities should *not* be understood *primarily* as a function of dissuasion. Indeed, resilience ultimately points to the ability of a system or a society to reorganise itself amid major adversity. It is about maintaining one's identity, rather than an explicit strategy of dissuasion.

Nonetheless, the ability to signal resolve is at least partly based on certain general resilience capabilities, such as social cohesion, democratic culture and the decision-making system's response time (Monaghan, 2019). Thus, the vocabulary of deterrence should perhaps be broadened to include a third mode of dissuasion alongside denial and punishment. For example, the mode of dissuasion based on resilience

[12] In the 2015 EU Global Strategy (p. 23) societal resilience is defined in the context of European neighbourhood policy as 'the ability of states and societies to reform, thus withstanding and recovering from internal and external crises'. In the 2016 Joint Framework on Countering Hybrid Threats, resilience is defined as 'the capacity to withstand stress and recover, strengthened from challenges' (p. 5), but the actual policy recommendations clearly emphasise action that would increase society's ability to marginalise the impact of hybrid operations.

could be labelled as 'deterrence by absorption', where it's main rationale would be to frustrate potential adversaries instead of inflicting unacceptable costs[13]. Furthermore, due to the subversive and deniable nature of certain key hybrid threats, incorporating key civil society actors more closely into the strategic planning process of counter-hybrid strategies is of the utmost importance. This should be done by recognising the vital roles of certain virtues in civic culture, such as critical media literacy, together with democratic deliberation and participation. Ultimately, strengthening adaptive societal resilience capacities and general levels of social trust requires constant efforts to improve life conditions and opportunities for social mobility within vulnerable and marginalised groups.

[13] See also Wigell, 2021.

5 Whole-of-society approach in practice: case studies of Finland, Sweden and Australia

Chapter 5 maps out and analyses some of the best practices and pitfalls in a whole-of-society approach. This is done by (1) investigating Finland's actions in this regard as the key element in its comprehensive security concept; (2) considering Sweden's efforts to re-build its civil defence as a part of its total defence system; and (3) looking at Australia's efforts to develop a whole-of-government and whole-of-society approach to counter hybrid threats. Herein, a number of expert interviews were conducted to advise on these countries' approaches and help make judgements about the usefulness of specific practices.

5.1 Finland's comprehensive security concept

The general principles regarding Finland's preparedness are laid out in its 2017 Security Strategy for Society. In a nutshell, the notion of comprehensive security forms the basis of this strategy, where the vital functions of society are jointly safeguarded by authorities, business operators, civil society organisations and citizens. In practice this means sharing and analysing information, joint plans and training, as well as practical everyday work. The comprehensive nature of the Finnish approach is emphasised in the Strategy by stating that 'together with central government, the authorities, business operators, regions and municipalities, such actors as universities, research institutions, organisations, other bodies and individuals form a network of comprehensive security in which the sharing of information, setting of joint objectives and commitments to cooperation can take place in a flexible manner' (Finnish Government, 2017). The Strategy defines security actors as 'all actors taking part in coordinated security work or security activities closely supporting it' (Finnish Government, 2017).

This Strategy emphasises the broad scope and cross-sectoral nature within the areas of preparedness and highlights the applicability of preparedness principles in all operational levels of society. To reflect the processual understanding of resilience as described in Chapter 4, the role of individual citizens in regard to their psychological resilience has been underlined as a fundamental factor underpinning societal security. Moreover, promoting the preparedness of households is an important part of societal resilience in Finland. To illustrate further the whole-of-society approach in the country's system, central roles are also played by non-governmental organisations – such as the Finnish Red Cross and the Finnish National Rescue Association (SPEK) – in providing services, coordinating the participation of volunteers within activities supporting authorities and maintaining special expertise in areas like contingency operations. Cooperation between the authorities, administrative branches and organisations is achieved by joint agreements, training and exercises, contingency and preparedness planning and by considering organisations' role in the preparedness process. Administrative branches, the authorities and key organisations combine to agree on cooperation arrangements required for performing strategic tasks in areas such as: prevention of risks, training, preparedness, communications, operations during accidents and disruptions, as well as the recovery process (Finnish Government, 2017).

At institutional level, the Prime Minister's Office is responsible for the government's situation awareness, preparedness and security services as well as coordination in the management of different incidents and emergencies. The Finnish government, ministries and competent authorities are responsible for preparedness related to comprehensive security, incident management and running of operations. These functions are managed on the basis of a normal mandate under existing statutory powers. Ministerial committees, meetings of Permanent Secretaries, meetings involving the Heads of Preparedness and other permanent inter-ministerial cooperation bodies may participate in preparations to manage incidents (Finnish Government, 2021b).

The Security Committee is a permanent and broad-based cooperation body for contingency planning, that works for comprehensive security by assisting the Finnish government and ministries in comprehensive

security matters. This Committee comprises 20 members and four experts from different branches of government, various official bodies and a number of business organisations. The Committee organises seminars and hearings with organisations, businesses and other contacts with the objective of generating conversation and collecting the information required for developing the security of society. If emergencies or incidents occur, the Security Committee will act as a specialist body (The Security Committee, 2021).

An important element in Finland's comprehensive security concept is training provided by the National Defence Courses. These courses bring together leaders from the military, government, the private sector and civil society for national defence education. The goal is to give participants a total overview of the country's foreign, security and defence policies, thereby improving collaboration between different sectors of society in emergency conditions and promoting networking between people working in different areas of comprehensive security. In addition to activities at national level, regional courses are also arranged. Their focus is on preparedness at the regional administrative and local levels for a variety of disruptions and emergency conditions which can face society. Here, special attention is paid to the operation of Finland's Defence Forces, civil defence, security of supply of the economy, communications and transportation. These courses promote cooperation between the regional authorities, those responsible for key tasks in emergency conditions and the communities that they represent. The target groups are people who hold leading positions in government, the private sector and civil society, together with others in key positions of major importance for national preparedness (The Security Committee, 2021).

5.2 Finland's security of supply model

Finland's security of supply model presents a good example of the country's comprehensive security concept, given that ensuring security of supply is a sector within the Finnish system where the public-private partnership is most apparent. The 2017 Security Strategy for Society underlines the increasingly important role for business operators in the preparedness process, especially for ensuring the functioning of the economy and other infrastructures such as social welfare and health care services. Consequently, the Strategy concludes that it is increasingly important to guarantee that companies can continue to operate in times of crisis.

This objective is put into practice through Finland's security of supply model. The Finnish National Emergency Supply Agency (NESA) defines security of supply as 'society's ability to maintain the basic economic functions required for ensuring people's livelihood, the overall functioning and safety of society, and the material preconditions for military defence in the event of serious disruptions and emergencies' (NESA, 2021). The security of supply concept is understood in very broad terms as covering a wide range of critical sectors under one umbrella. According to its official definition, this concept includes: securing critical infrastructures, production and services; covering energy production, transmission and distribution networks; data-communication systems, networks and allied services (including mass communication); financial services; transport and logistics; water supply; construction and maintenance of infrastructures; waste management in special circumstances; food supply; health care and basic amenities; industry; production and resources supporting military defence (Finnish Government, 2018).

A central feature in Finnish security planning has been a potential scenario whereby the country's international links and logistical lifelines through the Baltic Sea are disrupted or even cut altogether (Aaltola et al., 2014; Hakala et al., 2019). As a result, the crisis preparedness system still includes a strong emphasis on self-sufficient security of supply, including material preparedness through stockpiling. However, what should be noted is that securing the above critical sectors requires stable, reliable and well-functioning international connections. The Council of State's decision on the objectives within security of supply (Finnish Government, 2018) recognises that first and foremost this should be based on access to international markets. In addition to other international threats that could disrupt the country's supply, critical sectors are also potential targets for any malicious actor to conduct hybrid operations. From this

perspective, securing the functioning and resilience of these sectors is also an important element in deterring hybrid threats. The more resilient these sectors are, the less tempting they become as targets for hybrid activities.

Most critical societal functions in Finland are operated and managed by private sector actors, who are highly dependent on global supply chains. Consequently, public-private cooperation in supply chain management has assumed paramount importance. Due to the central role of private enterprises, complex continuity management has taken centre stage in the Finnish security of supply paradigm. This means an emphasis on supporting the business continuity management of critical enterprises (Finnish Government, 2013; 2018). As security of supply is grounded in well-functioning markets and a competitive economy, societal preparedness in this respect also requires extensive collaboration among authorities, businesses and industry organisations. In Finland, certain strategic industries are required through laws and regulations to ensure the continuity of their critical processes. However, private actors do not in general have a statutory duty to undertake measures such as preparedness planning to guarantee continuity of their critical operations amid disruptions and emergencies. Instead, continuity management activities undertaken by enterprises are determined by business requirements, contractual obligations toward customers and risk management (NESA, 2021). This operational continuity management is designed to ensure continuity in the operation of those organisations and networks that provide critical infrastructures and services. The general idea here is simple: when these critical private actors make their own operations more secure, the security of Finnish society will also improve. NESA supports these operations by providing enterprises with tools and guidelines for developing their business continuity management, for instance through the NESA's Extranet portal and the *Sopiva* project.

Together with the National Emergency Supply Organisation's (NESO) sectors and pools, NESA aims to integrate the objectives and interests of both society and the business community. The NESO sectors are industry-specific organisations with representatives from both public authorities and business life. Voluntary business participation has always been characteristic of Finland's efforts to ensure security of supply. The experiences gained during the Second World War and the models of operation established shortly thereafter form the foundations for this collaboration. From an international perspective, such cooperation has been considered a strong point of the Finnish model (Hakala et al., 2019). A key element in this model is that it facilitates the formation of quick and comprehensive situational awareness in critical sectors. This is put into practice by the NESO pools by providing sectoral situational pictures from different fields of business, which in turn help to plan and steer the national level security of supply operations. In addition to improving societal resilience, NESO pool activities provide important benefits for private actors involved, such as networking, communication and relationship building with other relevant stakeholders.

From an international perspective, the Finnish security of supply model is unique. Its operational logic and organisational structure have evolved through decades of history. It has been affected by certain historical and cultural experiences and its close connections to military defence (through the concept of 'total defence'). As such, the Finnish model is accordingly not easily exported to other countries. Different states have differing characteristics related inter alia to energy security, logistical connections, geographical conditions and security policy solutions. Largely because of these factors, most EU Member States' coordinated security of supply solutions do not match those of Finland. In many countries, for instance, managing public-private partnerships is undertaken in sectoral authorities and ministries. This is also the case with other issues that in Finland are put under one security of supply concept, such as food security, energy, cyber security or epidemic preparedness (EVPHT/P, 2013).

5.3 Finland's media literacy policy

Media literacy and mass communication are other sectors where the comprehensive whole-of-society approach in Finland is underlined. The Government's decision on security of supply (Finnish Government, 2018) stresses the importance of securing responsible media communication by stating that 'safeguarding the operating conditions and free and diverse media, which supports the security of society and responsible freedom of speech, shall be one of the priorities of the safeguarding of society.'

In this respect, a key actor is the NESO pool *Mediapooli*, which is focused on issues related to mass communication. This provides media companies with a forum for cooperation where companies and relevant authorities seek solutions together on mass communication security. Issues covered include: industrial cybersecurity; countering hybrid threats and disinformation; the technical and general continuity of media operations in special situations, during serious disturbances and emergencies; as well as sharing the best practices regarding the aforementioned matters. *Mediapooli* is also interested in the phenomena of social media and information influencing by hostile actors. As an important part of its efforts, *Mediapooli* arranges courses and exercises for journalists and media organisations (Mediapooli, 2021), one example being a workshop organised in 2019 together with the Hybrid CoE on media resilience, including ways to counter disinformation and hybrid threats (Hybrid CoE, 2019).

On a general level, it can be seen that Finland has done very well in countering disinformation. For example, one indicator is that Finland leads the media literacy index (Lessenski, 2019), a yearly ranking of European countries reflecting their level of resistance to fake news. According to this index, Finland, Denmark, the Netherlands, Sweden and Estonia are considered best equipped to withstand the impact of fake news due to the quality of education, free media and extensive trust among people (Lessenski, 2019). In addition to the joint work between business life and authorities in the *Mediapooli*, in more general terms Finland's media literacy policy is one of its key public-private partnership areas. The country has a long history of mass communication education stemming from the 1950s, but greater activity levels have been apparent since the 2000s, with the need to promote media literacy being acknowledged in an increasing number of sectors.

A significant characteristic in Finland is the multitude of actors and projects that are partly or fully funded by the ministries or other public authorities. The Ministry of Education and Culture plays an important role, having in 2019 published the document 'Media literacy in Finland' (Finnish Ministry of Education and Culture, 2019). This publication updates and extends the cultural policy guidelines for media literacy issued in 2013, highlighting the themes of social inclusion, active citizenship, critical thinking, creativity and self-expression. As an illustrative example of the whole-of-society approach in this respect, the guidelines were developed in cooperation with actors and organisations from the Finnish media literacy field. According to the 2019 guidelines, media education is planned, practised and developed in broad-based collaboration between a variety of different actors. The need for an update of these guidelines arose from changes in media culture and the broader target groups of media education, as policy guidelines highlight the need for media skills in all age groups. Finland also has a governmental media education authority, the National Audiovisual Institute (KAVI). Furthermore, the National Board of Education actively develops educational policies such as national core curricula, including media educational perspectives. The field of media literacy in Finland is wide and active, involving many national institutes, municipalities as well as regional and local actors (European AudioVisual Observatory, 2016; OKM, 2013; 2019).

To summarise, Finland leads by example in many sectors of whole-of-society preparedness and the international recognition received in this regard is well-deserved. However, despite clear benefits being demonstrated by the Finnish model, it is not without flaws. For instance, a study on Finland's security of supply concept (Aaltola et al. 2016) notes that in particular information sharing is still considered to be too vertical, in reality operating in 'silos', whereas the current security policy environment requires a more

horizontal approach. Furthermore, making enterprises truly commit themselves to the security of supply cooperation can prove to be challenging. This is especially so in situations where the enterprises in question are foreign-owned, often lacking a historical understanding and tradition of cooperation. In some of these cases cooperation is just seen as increasing bureaucracy without providing any real added value. Consequently, these actors may be unwilling to invest resources into cooperation. Another study conducted in the context of the coronavirus pandemic has also identified certain points of development in the Finnish comprehensive security system. These include: too few resources, especially at the Prime Minister's office level; dependence on few critical people; inability to work horizontally outside 'silos'; resource competition between governmental agencies; as well as a general lack of trust between actors and in some cases even unclear administrative responsibilities (Mörttinen, 2021).

5.4. Sweden's total defence model

Hybrid threats are also high on the security agenda in Sweden. The country is exposed to grey zone threats generated by non-state and state actors, related for instance to *Salafi/jihadi* influence activities, disinformation campaigns, cyberattacks and economic influence operations. As a result, the country has gradually started to improve its societal resilience capabilities. In 2018 Sweden appointed its first Ambassador and Special Envoy for countering hybrid threats situated in the Ministry for Foreign Affairs. The Ambassador's tasks consist of coordinating the activities of the foreign ministry relating to hybrid aggression, analysing the consequences of the hybrid threat environment for Sweden's foreign and security policy, representing Sweden in international cooperation and discussion on countering hybrid threats, as well as being part of the intragovernmental coordination effort to understand and counter hybrid threats (Löjdquist, 2019). Other countries like Finland have taken similar steps. This measure is important because it helps to coordinate the response action and overcome silos, especially as hybrid threats by definition are designed to make coordinated countermeasures difficult. To provide another example, the Swedish research community has also been given support for conducting policy-relevant research, analysis and training with regard to hybrid threats. Herein, a key measure has been the establishment of the Centre for Asymmetric Threat Studies (CATS) as part of the National Defence University's Centre for Societal Security (CATS, 2021). As a key element in countering hybrid threats, the research community plays an important role in raising awareness and supporting knowledge-based decision-making on the topic.

In addition to recent efforts in countering hybrid threats, it should be noted that Sweden is a country with a long tradition in utilising a whole-of-society approach in its national preparedness efforts. Following the Cold War, Sweden essentially ended military planning. The country decommissioned its total defence system and related civil defence capabilities. In practice this implied major reductions in the country's defence budget, downsizing its armed forces and refocusing security policy on terrorism and expeditionary crisis management operations instead of territorial defence (Gotkowska, 2021). However, as a result of deterioration in the Northern European security environment, Sweden is currently re-establishing its defence capabilities, with particular emphasis being put on building up the civil defence in a whole-of-society manner. While rebuilding Sweden's total defence model is a slow and costly process, progress has already been made (Hägglund, 2020). Hence, the country provides a valuable case study on the implementation of whole-of-society practices and how they can be utilised in building up societal resilience.

Total defence not only revolves around preparing Sweden for conventional war but also in planning and designing the operational capabilities for countering hybrid threats. Resources in Sweden's total defence efforts are currently being designed so that they can also strengthen society's ability to prevent and handle severe emergencies (Swedish Government, 2020). As a report from the Swedish Defence Research Agency (FOI) points out, 'state and non-state actors have acquired new ways of influencing societies without

needing to resort to traditional military force. This is why preparedness among all authorities and a reinforced total defence are becoming increasingly important' (Rossbach et al, 2019, p. 11). The Swedish Civil Contingencies Agency (MSB) has emphasised that planning for civil defence should go hand in hand with crisis preparedness and suggested that they should be defined under the common concept of civil preparedness (Hägglund, 2020). Another report by FOI argues that 'Sweden is exposed to grey zone threats and that particularly the civil defence must have the capability to withstand these threats' (Jonsson et al., 2019, p. 89). Thus, Sweden's current countermeasures against hybrid threats are being planned to build on general civil defence capabilities and the strengthening of societal resilience.

In practice, Sweden is re-establishing its civil defence by implementing a whole-of-society and whole-of-government approach, especially by drafting 'strategies, defining problems, designating coordinating institutions, imposing additional responsibilities on central, regional and local entities, and exploring the possibility of cooperation between the private and public sectors' (Gotkowska, 2021, p. 7). Sweden's security strategy for 2016–2020 highlighted, in particular: coordination and planning in civil defence; civilian support for the armed forces; and psychological defence against disinformation. A central role in these activities was given to the MSB. Importantly, the Swedish approach also recognises the role of exercising civil-military cooperation put into practice, for instance, during the 2017 Aurora national defence drills (Gotkowska, 2021).

An important step was taken in 2017, when the Swedish government tasked the Defence Commission to produce a report on civil and total defence. In December 2017, this Commission delivered its first report on 'Resilience – the total defence concept and the development of civil defence 2021-2025' (The Swedish Defence Commission Secretariat, 2017). Key areas of development identified in this report include: organisation and management of total defence; psychological defence; electronic communications and cyber security; personnel training; voluntary defence organisations; economic and total defence; protection of the civilian population; law enforcement and security; energy, food and drinking water supply, transport; financial preparedness; healthcare; research and development; and international cooperation (The Swedish Defence Commission Secretariat, 2017; von Sydow, 2018; Gotkowska, 2021). As already noted, improving general levels of resilience in these sectors is also important with regard to countering hybrid threats.

The Swedish concept defines in essence all relevant societal functions as part of total defence. Key actors include: the parliament, the government, government authorities, municipalities, private enterprises, voluntary defence organisations, as well as individuals (The Swedish Defence Commission Secretariat, 2017; von Sydow, 2018). In line with this definition, the latest 2020 Government Total Defence bill highlights how civil defence encompasses the whole of society and consequently the need for strengthening public-private cooperation (Swedish Government, 2020). Swedish law stipulates requirements for critical businesses to participate in the total defence planning process. To integrate the private sector into civil defence planning, the government underlines that enterprises important for defence efforts should be identified and regulated. Related to this, the Defence Commission has proposed the institution of a National Business Council for total defence in order to establish long-term cooperation between public and private actors at national, regional and local levels. The purpose of this Council is mutual information sharing to identify joint directions, plans and requirements for cooperation between public and private actors throughout society (The Swedish Defence Commission Secretariat, 2017). In Finland, a similar role is already played by the NESO pools, signaling the added value of such structures in facilitating public-private cooperation in a whole-of-society manner.

To illustrate the whole-of-society nature of the Swedish model even further, its total defence system highlights the importance of voluntary defence organisations as well as the key role of individual citizen resilience. According to the Swedish concept, citizens should be able to cope for a week in serious crises without the state's assistance. To this end, and in line with efforts to enhance a whole-of-society approach,

in 2018 the Swedish government sent every household a pamphlet titled 'If Crisis or War Comes' (MSB, 2018a). The purpose of this pamphlet was to enhance civilian preparedness and educate citizens on how to function in the event of a serious crisis. These efforts highlight Sweden's aim to improve societal resilience in general whilst also stressing hybrid threats.

Sweden has also taken a number of measures to strengthen cyber security as a facet of its total defence system. In 2020 the government established a cyber-security centre, its central aim being to improve coordination, especially among the Swedish Armed Forces, the National Defence Radio Establishment (FRA), the Civil Contingency Agency (MSB), the Police and the Security Service, and the Postal and Telecom Authority (PTS) (Gotkowska, 2021). Concrete practising forms once again part of efforts to uphold the total defence system, with broad civil defence exercises being held during 2020. The 'Total Defence 2020' exercise took place during 2019-2021, marking the first national Total Defence Exercise since the Cold war. This exercise was a joint effort between the armed forces and MSB, involving all elements of society: parliament, regional administrations, local municipalities, government institutions, the central bank and the corporate sector (Wheeler, 2020).

As a part of its total defence efforts, the Swedish government announced the establishment of a special agency for monitoring and evaluation of these efforts by January 2023 (Gotkowska, 2021; Swedish Government, 2020). Sweden is also rebuilding its security of supply system, with particular emphasis on establishing strong cooperation between state entities and the private sector. To facilitate this work, the Swedish government has stated that it will launch an inquiry into the scope of nationally coordinated security of supply preparedness, including its organisation and financing. In addition, the afore-mentioned National Business Council is foreseen to play a key role: 'to complement business councils in different areas of society, a cross-sectoral business council will be established during the period 2021–2025 where the business sector and trade associations can participate in the development of Sweden's total defence supply capability' (Swedish Government, 2020, p. 9).

Although Sweden has asserted its determination to re-build its civil defence, the task is not easy. There exist identified lags between the shortcomings noted in different reports and the concrete measures to tackle them. Problematically, as Hägglund (2020) notes, there is currently neither an explicit definition of security of supply nor a goal for it, making Swedish planning efforts difficult. Furthermore, the COVID-19 pandemic has increased general awareness of these problems. For instance, it has been recognised that there is no central coordination of security of supply within healthcare, where the responsibility is instead divided between 21 regions. Decentralisation has led to the situation where nobody has responsibility for the overall security of supply preparations, which was previously in the hands of the state itself or state monopolies. Many sectors and functions are also now in private hands, adding to the multitude of actors crucial for crisis preparedness and security of supply (Hägglund, 2020).

Indeed, one of the most central challenges in developing civil defence and a whole-of-society approach in Sweden is complexity within the realm of different authorities in the country. Key problems identified in the Swedish system include lack of situational awareness and uncertainties within the crisis preparedness system, particularly at national level. Sweden has three different administrative levels: national, regional and local. At national level, the government and parliament are responsible for a strategic and comprehensive crisis response. Emphasis in the administrative structure is put on the requirement for the government to apply collective decision-making. Nevertheless, the government receives its mandate from parliament, which can make the necessary actions too slow. The COVID-19 pandemic has sparked debate on the Swedish system's ability to reply quickly enough to grey zone threats and vulnerabilities. The COVID-19 emergency may thus be responsible for pushing along discussion about whether or not there is a need to make any changes to the Swedish constitution regarding crises situations (Hägglund, 2020).

Moreover, while military defence is organised by the armed forces, the civil side consists of a number of functions and a wide array of actors, ranging from private companies and municipalities to central authorities and the government. This will continue to prove challenging inter alia for coordinating efforts and formulating definitions, responsibilities, concrete goals and funding needs. There have been warning signs and increased awareness in Sweden about weaknesses in the current crisis preparedness system, particularly when it comes to large-scale crises. Sweden's decentralised system can in itself create real problems in the face of a national threat (Hägglund, 2020).

5.5 Sweden's efforts against disinformation

During recent years, Sweden has shown determination in its actions to counter disinformation campaigns. During the annual *Folk och försvar* Security Sonference in Sälen in January 2018, Prime Minister *Stefan Löfven* announced that Sweden aims to establish a new governmental agency developing and coordinating activities related to 'psychological defence' (The Local, 2018).

The new agency has been justified as a necessary response to the modern demands of total defence – a model of military defence planning that is intertwined with the wider functions of the public welfare state. The rationale for this new agency was stated to include the discovery, countering and prevention of not only national but also international disinformation campaigns during peacetime and in crises. Another key task of the agency is to support the population's awareness and ability to withstand the effects of disinformation campaigns (Kommittédirektiv, 2018).

The agency is set to be established at the latest in early 2022, with the key task of leading the coordination and development of the authorities and other actors' actions in Swedish psychological defence and to support such activities. The authority must also be directly involved in strengthening the population's resilience in relation to psychological defence (Kommittédirektiv, 2021). It is important to understand the significant contextual effect of local security cultures and inherited practices to security policy planning, including countering disinformation. Indeed, Sweden was the first Nordic country to introduce a model of psychological defence planning in the post-Second World War era, predating the whole-of-society model (Larsson, 2020).

Although Sweden's defence and security planning did go through a period of major reforms during the first two decades of the post-Cold War era (see Section 5.4), the process of reinvigorating the conception of psychological defence clearly represents more continuity than discontinuity with the past. The old model of psychological defence is merely amalgamated together with modern risk society-based thinking (Stiglund, 2020). As in the case of Finland, psychological defence, including counter-disinformation campaigns and the recognised value of public broadcasting media, was already one of the four pillars of Sweden's total defence model during the Cold War, together with military defence, economic defence and civil defence (Larsson, 2020).

The three traditional components of psychological defence are countering disinformation, enhancing crisis communication abilities of officials and population's will to defend the country. The former, related to disinformation, has significantly increased in salience over recent years. According to one influential study, the role of countering disinformation, fake news and hate speech – defined as 'deception and disinformation, including rumour-mongering and propaganda or, in other words, everything that hostile psychological warfare engages in' – has become even more prominent due to complexities in the security environment, now comprising both state and non-state actors using novel technological means (Rossbach, 2017).

The reappearance of alarmism related to psychological defence capabilities and societal functions therein was closely anchored to the recognised need for developing more robust countermeasures to election interference. Experiences derived from the foreign influence campaigns on social media witnessed during

the 2016 US elections and the Brexit referendum were cited as key catalytic events in the Swedish debate. A FOI study on the role of social media bots and fake accounts in Sweden's general election campaign in 2018 concluded that there was a clear increase in the number of social media bots that framed the Swedish electoral debate with traditionalist, authoritarian, nationalistic or anti-immigration messages. The conclusions of the study clearly pointed towards the need to enhance critical (social) media literacy levels within society at large: '[…] It is clear that the use of automated accounts for spreading various types of messages has increased markedly the closer we come to the [2018 general] election. […] The results of previous research indicate that attempts to influence are less effective if individuals are aware of them. In other words, an awareness that someone is trying to influence us can, at least to some extent, make us less susceptible to influence.' (Fernquist et al., 2018, p.12)

Conversely, the aforementioned FOI study also found that, although the use of twitter bots was widespread during the Swedish 2018 elections, they appeared to be relatively unsuccessful, at least if measured in terms of retweets by real twitter accounts. This already points at inherent resiliency towards blatant disinformation campaigns within Swedish society. In addition to capabilities indicating society's general resilience, Sweden has robust legislation against the dissemination of propaganda and other means of spreading false information in issues pertaining to Swedish military or national security. Nevertheless, it is important to note that this legislation does not allow pre-censorship or provide legal authorisation for blocking media sources, itself an important prerequisite of open democratic civic culture (Hofverberg, 2019).

The MSB has been active in increasing general awareness against disinformation campaigns. In 2013, it was already pinpointing incidents related to misinformation and increasing lack of trust towards official information channels as key future challenges to societal security (MSB, 2013). As already noted in Section 5.4, in probably one of its largest information campaigns yet the MSB produced its brochure 'If Crisis or War comes' in 2018 (MSB, 2018a). It was the first brochure about societal security and total defence to have been distributed to every household in Sweden since 1961. The brochure, available both in English and Swedish, encouraged the general public to 'be on the lookout for false information.' Moreover, the MSB has published guidebooks for public servants on how to act to counter disinformation campaigns (MSB, 2018b).

Sweden has made efforts to strengthen international cooperation in countering disinformation. In addition to its participation in societal resilience building and countering hybrid interference within the EU, it has worked closely with other Nordic countries in countering the increase of disinformation and the rise of digital insecurities in general (The Nordic Council and the Nordic Council of Ministers, 2018). Finally, it is worth mentioning that also in Sweden mainstream media outlets have joined in initiatives to address fake news contents. This cooperation led to the establishment of the *Faktiskt.se* website, a joint effort by two of Sweden's leading newspapers, *Dagens Nyheter* and *Svenska Dagbladet*, to counter disinformation and raise awareness on source criticism during the 2018 general election campaign.

5.6 Australia's need to counter hybrid threats

Over recent years, Australia has been exceptionally active in updating its legislation, policy and bureaucratic structure to manage foreign influence in the country. These responses have focused on criminalising, disrupting and deterring foreign interference (Mansted, 2021). The rapid upturn in countermeasures have gone hand in hand with increases in Chinese hybrid interference observed in Australia. An example of such interference is provided by the way in which China has attempted to drive a wedge into the US-Australian alliance through its *Qiaowu* programme[14]. The purpose of this programme is to increase support for Beijing's policy amongst Chinese diaspora with the help of various reflexive control

[14] See Wigell, 2019.

techniques, ideally using it as an interlocutor for influence. Whilst the *Qiaowu* policy has been planned by the Overseas Chinese Affairs Office and is implemented by the United Front Work Department of the Chinese Communist Party (CCP), all Chinese government agencies are required to pursue *Qiaowu* objectives (Brady, 2017; To, 2014). Through the *Qiaowu* programme money has been channelled through the Chinese diaspora in Australia to support major political parties and to cultivate loyal business networks (Hamilton, 2018).

The policy has involved using subversive means to mobilise the large Chinese-Australian diaspora as a voting bloc, to intimidate critics and protest in the streets against Australian government policy, as well as placing candidates loyal to China in parliament, local government and senior public positions. To this end, so-called 'United Front organisations' were set up in Australia, guided and supported by the CCP (Hamilton, 2018). Economic interference is used to reinforce such subversion by channelling large sums of money into these organisations, which can be used to empower targeted politicians through campaign support. Furthermore, business links are offered to certain groups to generate interest convergence. Together, these politicians and businesspeople can be used to lobby for Chinese interests and denounce critics as xenophobes and threat-mongers. In May 2016, *Liu Qibao*, a member of the Politburo and head of the CCP Central Committee Propaganda Department, signed a series of agreements with major Australian media outlets which, in exchange for money, were prepared to publish Chinese news stories provided by CCP-controlled outlets such as *Xinhua News Agency* and *China Daily*. Acquiring a strong media presence in Australia is linked with China's broader strategy of hybrid interference, in which subversive, economic and disinformation means are integrated. Economic measures may facilitate acquisition of a media presence, thereby providing channels for disinformation, which can then be used to obfuscate or reinforce subversion techniques and may in turn be used to create agents of influence that open up channels for economic interference (Wigell, 2019).

5.7 Australia's key activities to tackle foreign interference

As a result of this observed increase in foreign interference, Australia is taking hybrid threats seriously, for instance by systematically reviewing its vulnerabilities and points of weaknesses with regard to critical infrastructure, including cyber systems and civil relations (Buchanan, 2019). Significantly, in order to straddle the gap between illegitimate hybrid interference and legitimate public diplomacy, in 2017 the country started the process of creating foreign influence transparency registers. This process required individuals and entities undertaking activities on behalf of foreign principals to register, while criminalising foreign interference activities, and ultimately culminated in two major pieces of legislation: the Foreign Influence Transparency Scheme Bill (FITS) and the Espionage and Foreign Interference Bill. Both are aimed at enhancing transparency regarding foreign influence in political processes. This does not prohibit foreign actors from being involved in the country's political processes, but it does create obligations to disclose information for assessment of influences on domestic interests. As such, it informs the public about influence activities that might otherwise remain hidden, while also expanding the investigative options with regard to those actors that fail to register (Hutchens, 2018).

In more detail, according to FITS, individuals or entities are required to register certain activities if they are taken on behalf of a foreign principal. Registrable activities include: parliamentary lobbying; general political lobbying; communications activities; and disbursement activity, meaning payment of money or items of value. Moreover, there are additional registration obligations for activities undertaken by former Cabinet Ministers and recently designated position holders (e.g. former Commonwealth politicians, their staff and senior civil servants). The scheme establishes criminal offences for: failing to comply with obligations; failing to register in circumstances where a person is required to do so; providing false or misleading information; and destroying records to avoid registration obligations (Australian Government, 2021a). In short, the purpose of FITS is to provide the public and decision-makers with awareness of the

nature, level and extent of foreign influence on Australia's government, political process, economy and society. The registrable activities extend beyond political lobbying to include communications activities that influence public debate and decision-making more broadly (Mansted, 2021).

As Mansted (2021) notes, the new legislation captures only a very narrow set of hybrid activities by focusing explicitly on criminal offences. Australia's foreign interference offences target interference in the political or governmental processes rather than interference with, say, market processes. Australia's approach of defining and criminalising only a narrow set of behaviours 'was intended to avoid over-securitising foreign influence matters, and to ensure political speech was protected, while focusing resources and attention on the most pernicious activities' (Mansted, 2021, p. 7).

In 2018, the Australian government made an important addition to the country's whole-of-government efforts by creating the National Counter Foreign Interference Coordinator (NCFIC) position within the Department of Home Affairs. The NCFIC's task is to coordinate Australia's whole-of-government responses to foreign interference across federal government departments and agencies. This is done by:

- engaging with the Australian National Intelligence Community in developing assessments of the threat, vulnerabilities and consequences of foreign interference;
- administering Australia's Counter Foreign Interference (CFI) Strategy that builds on Australia's existing counter foreign interference efforts across government, to create an integrated and coordinated domestic and international programme that responds to foreign interference activities;
- coordinating outreach efforts and advice to sectors and systems at risk from foreign interference;
- and enhancing engagement with culturally and linguistically diverse communities to strengthen their ability to challenge manipulation and coercion from foreign actors.

The NCFIC also connects with likeminded countries and regional partners to forge greater levels of domestic and global resilience to foreign interference (Australian Government, 2021b). An additional step was taken in 2018 with the creation of the Foreign Interference Threat Assessment Centre in the Australian Security and Intelligence Organisation (ASIO).

Government actors play an important role in raising awareness about the topic of hybrid interference, for instance by assembling and disseminating information. The annual threat assessment conducted by ASIO's Director-General is important in this respect (Australian Government, 2020). An illustrative example of the Australian whole-of-society approach is the development of the 'Framework for the development of principles-based guidelines to counter foreign interference in the Australian university sector' (Australian Government, 2019). The framework was collaboratively generated by the University Foreign Interference Taskforce established in 2019, comprising 40 members from across government and the various sectors involved and representing overall 13 universities and 10 Australian government agencies.

However, as hybrid threats also target civil society actors, countermeasures must move beyond government-led approaches. In this regard, societal resilience will play an increasingly important role, as will 'dynamic, decentralised responses from social and economic actors' (Mansted, 2021, p. 3). At the very heart of the whole-of-society approach is guidance for decision-makers in civil society, business and government on how to respond to hybrid operations and interference. Critical societal functions are increasingly owned and operated by private actors. Hence, these actors must have a clear understanding of what hybrid threats entail, looking both at operational logic and what role enterprises can play as potential subjects of hybrid activities.

5.8 Australia's policy against disinformation

The recent influx of disinformation campaigns and increase in news consumption during the bushfire season of 2019/20, together with the coronavirus pandemic, have led to strong government level initiatives in the country (Parks et al., 2020; ACMA, 2020). The Australian Communications and Media Authority (ACMA) is responsible for regulating communications and media services, including communications infrastructure. ACMA also conducts research on current trends and issues in national media and communications environments and has statutory obligation to advise and report to the Minister for Communications, Cyber-safety and the Arts.

In addition, Australia has established whole-of-society based practices on information sharing between the various stakeholders providing critical infrastructure resilience. Especially important is the Trusted Information Sharing Network (TISN), managed by the Critical Infrastructure Centre (CIC) operating under The Department of Home Affairs. One of the key tasks of TISN is to enhance 'communication channels and networks between industry and all levels of government' (CIC, 2021), thus providing inter alia a basis for accurate situational awareness on existing vulnerabilities, for instance in relation to foreign telecoms equipment (Fjäder, 2014). Safe multi-stakeholder information sharing practices also provide solid bases for official government information towards society in crisis situations.

Based on recommendations made by the Australian Competition and Consumer Commission's Digital Platforms Inquiry and by ACMA (ACMA, 2020), in February 2021 the Australian Digital Industry Group (DIGI) released a 'Code of Practice on Disinformation and Misinformation' (DIGI, 2021a). This Code was developed in response to the government's policy of increasing efforts to counter disinformation, building on lessons drawn from a similar code developed in the European Union.

According to the Code, all its signatories will 'commit to safeguards to protect Australians against harm from online disinformation and misinformation, and adopting a range of scalable measures that reduce its spread and visibility' (DIGI, 2021b). The code is supported by ACMA and has already been adopted by a number of major social media companies such as Twitter, Google, Facebook, Microsoft and TikTok. This Code contains both mandatory and non-mandatory objectives. One key mandatory commitment is the release of an annual transparency report on enforcement of the Code. The core idea is to increase situational awareness on the role of online misinformation and disinformation in Australian society.

Media literacy skills are included for all students in the Australian curriculum, with learning outcomes tending to emphasise the role of digital media production skills, but also including 'creative and critical thinking, and exploring perspectives in media as producers and consumers' as well as 'knowledge and understanding of their active participation in existing and evolving local and global media cultures' (ACARA, 2021) However, a recent study has revealed that Australian citizens are concerned about their ability to distinguish truthful news from fake news on the internet (Parks et al., 2020). The same study showed that 66 % of Australians had experienced misinformation about COVID-19 on social media.

Moreover, research conducted by Notley and Dezuanni (2019) demonstrates that only 43 % of Australian teenagers (aged 13 to 16 years) have confidence in their ability to distinguish fake news or disinformation from true news stories, a trend further reinforced by increasing reliance on digital information sources. In Australia and Great Britain there seems to be a particularly strong demand to increase traditional critical news media literacy in a way that is applied to the context of digital media. For now, Australia's curriculum is tilting towards an emphasis on arts-based media production skills.

In addition to the lively debate about China's hybrid interference and related wedge strategies, there has also been discussion on certain commonalities between pre-2014 Crimea and the country's Northern Territories. Both regions are important strategic locations in the wider regional setting, although the geopolitical context is not entirely comparable. As Boichak (2020) points out, the two regions share

similarities in housing major critical infrastructure projects, including defence infrastructure[15]. Moreover, both Crimea and the Australian Northern Territories share a long history of colonial violence toward indigenous populations that is still visible in the major differences in living conditions among ethnic groups. These divisions provide favourable conditions for potential societal wedge strategies, should the social cohesion of the population be neglected.

On this basis Boichak (2020) suggests that, in addition to investments in physical infrastructure, there is an increasing need for strengthening civil society institutions and promoting public education campaigns on disinformation and media manipulation. This could be done by investing in projects that focus on digital literacy and digital inclusion, which represent integral components of enhancing the social cohesion that would make the region increasingly immune to externally orchestrated hybrid campaigns.

[15] See also Northern Territory Government, 2017.

6 Recommendations

The EU institutions and Member States have demonstrated an awareness of the need to counter hybrid threats, as expressed in the documents and policies reviewed in Chapter 2 of this study. Current EU policies focus especially on promoting resilience as a framework to counter threats in the hybrid domain. This provides a useful starting point for further action. However, the EU now needs to craft a set of more specific policies and measures, in addition to those already being undertaken, to put this framework into practice effectively. To this end and based on the analysis conducted in this study, we propose four bundles of recommendations.

6.1 Introducing shared assessment of the hybrid threat domain

At present, EU institutions apply the term hybrid threats as a catch-all label for a variety of activities in the so-called 'grey zone' between war and peace. The broad definition of hybrid threats used by the EU Commission is of value in delineating the entire hybrid threat domain, but it needs to be complemented by a better conceptual differentiation between different forms of hybrid threats in order to improve situational awareness, risk assessment and planning of countermeasures. Hybrid threats differ substantially in terms of their strategic aims, means and logic. EU policies need to take into account these differences so as to facilitate a better targeting of response actions.

Specific measures include the following.

a. Introducing a shared EU hybrid threat typology and mainstreaming that typology across EU policies and documents. Actions to be taken should include:

    - further developing an EU hybrid threats typology based on the conceptual model generated by the Hybrid CoE.

b. Implementing regular EU hybrid threat risk assessments taking into account the entire hybrid threats domain as it is conceptualised in the shared EU hybrid threat typology. Actions to be taken should include:

    - implementing of regular Council/Commission shared risk assessments under the responsibility of the HR/VP;
    - increasing staffing and resources for the Hybrid Fusion Cell as a focal point for hybrid threats assessments;
    - generating easily readable and concise classified intelligence reports for EU policymakers.

c. Starting a process of joint planning for countering hybrid threats with based on the EU's hybrid threats risks assessments. Actions to be taken should include:

    - introducing a process of regular exercises to be developed by the Hybrid Fusion Cell in cooperation with the Hybrid CoE;
    - developing a hybrid threats diplomacy toolbox in order to facilitate rapid and effective countermeasures;
    - developing recommendations for improving joint civil-military planning for hybrid contingencies.

6.2 Crafting a comprehensive resilience-building approach

Countering the variety of hybrid threats calls for a comprehensive and varied strategy of resilience building. The various conceptualisations of resilience need to be broken down into strategic response options – maintenance, marginalisation and renewal – as part of an all-embracing approach to resilience-building. This resilience building rests on a whole-of-society approach in which EU institutions retain a coordinating role. It harnesses market and society-based actors in an effort to pull together resources and take full advantage of European democracy's societal strengths. This is vital because in the era of hybrid threats, resilience cannot be achieved by state action alone. Countering hybrid threats requires a whole-of-society approach whereby various societal actors build resilience capacities, supporting EU institutions and Member States in maintaining preparedness as well as ensuring continuity of vital societal functions and supply lines. In this regard, the proposed Critical Entities Resilience (CER) Directive is a crucial step. The whole-of-society approach is an inclusive model of cooperation that aims to bring all relevant actors together into a comprehensive system of resilience building.

Specific measures include the following.

a. Creating an enabling environment for citizen activism and independent media, including civil society support and media capacity building (*resilience as renewal*). Actions to be taken should include:
    - developing tools for grassroots agenda setting, such as the European Citizens' Initiative;
    - rapidly implementing the provisions of the revised Audio-visual Media Service Directive 2010/13/EU requiring Member States to promote and develop media literacy skills.

b. Introducing regulation and increased transparency of social media platforms (*resilience as maintenance and renewal*). Actions to be taken should include:
    - implementing and continuously evaluating the Digital Services Act and the Digital Markets Act;
    - developing the Code of Practice on Disinformation and monitoring implementation of commitments by the signatories.

c. Facilitating processes of public-private continuity management in critical infrastructures (*resilience as maintenance and marginalisation*). Actions to be taken should include:
    - implementing the upcoming CER Directive;
    - supporting research on the actual implications of the CER Directive with regard to hybrid threats;
    - developing cross-border training activities and exercises;
    - introducing an awareness-raising campaign with regard to hybrid threats targeting private enterprises;
    - creating a funding instrument for strengthening the resilience of infrastructure and systems that underpin the EU single market.

d. Assigning clear responsibilities and procedures for attributing hybrid threats within EU institutions (*resilience as marginalisation*). Actions to be taken should include:
    - creating obligations for all entities targeted by hybrid threats to report the incident and allow access to and analysis thereof;

- clarifying the division of labour with regard to attributing and countering hybrid threats between Integrated Political Crisis Response (IPCR) arrangements, the Hybrid Fusion Cell within the EU intelligence and Situation Centre (EU INTCEN) and the EU Commission;
- conducting regular tabletop exercises to test and enhance the Union's hybrid threat response capabilities in cooperation with the Hybrid CoE.

e. Creating a deterrence toolkit for dissuading hybrid threats, including strategic communication and sanctions preparedness (*resilience as maintenance*). Actions to be taken should include:

- enhancing the security of EU institutions especially with regard to secure communications; conducting a regular review of the 2016 EU Operational Protocol for Countering Hybrid Threats (EU Playbook);
- developing a public version of the Playbook in order to raise awareness and communicate resolve in countering hybrid threats;
- bolstering the StratCom Teams in EEAS with a focus on investing in Chinese language experts;
- integrating hybrid threat evaluation as a regular element in the Union's general policy work across sectors.

6.3 Institutionalising a process of resilience assessment and monitoring

In order to develop the EU's resilience systematically, the maturity level of resilience across its various institutions and Member States needs to be monitored in a consistent manner. This requires institutionalising a processual model for measuring resilience across the Union and its Member States against a set of resilience baselines. Herein, the processual model of comprehensive societal resilience provides components – resistance, functionality, and adaptive learning – for such an approach.

Specific measures include the following.

a. Identifying hybrid resilience baselines for Member States and EU institutions (as called for in the EU Security Union Strategy). Actions to be taken should include:

- developing hybrid resilience baselines;
- developing measurements and joint assessments tools of the hybrid resilience baselines to be used by the Hybrid Fusion Cell, including on the general adaptive resilience capacities of Member States.

b. Introducing resilience assessments modelled on the hybrid threats assessment procedure in the Member States and a peer review process by experts. Actions to be taken should include:

- establishing a maturity model for the hybrid resilience baselines in cooperation between the Council and the EU Commission;
- defining indicators for assessing maturity;
- selecting a group of experts drawn from the EU Commission and Member States to assess maturity level in reaching the hybrid resilience baselines.

6.4 Measures for strengthening societal resilience

Countering hybrid interference campaigns requires a comprehensive societal approach that should not be reduced to capabilities related to preparedness and active countermeasures. In addition, it is crucial to acknowledge the importance of general societal resilience capabilities that decrease the permeability of hybrid interference campaigns from the outset. Societal resilience and resistance against hybrid interference should be planned on basis of a whole-of-society approach in which individuals, communities, institutions and international cooperation and connections (*forward resilience*) provide interrelated layers for comprehensive resilience planning. It is of utmost importance to incorporate key civil society actors more closely into the strategic planning process of counter-hybrid strategies.

Specific measures include the following.

a. Increase awareness on the importance of attributes related to general adaptive resilience of the society in countering hybrid interference (*institutional and forward resilience*). Actions to be taken should include:

    - developing measurements of general societal resilience into the joint assessment tools and baseline resilience criteria used by the EU Hybrid Fusion Cell;
    - further developing strategic analysis on the interrelationship between general and specific resilience capabilities in the context of countering hybrid interference.

b. Promoting media literacy as a key civic virtue and develop respective curriculum development guidelines based on identified best practices (*individual and institutional resilience*). Actions to be taken should include:

    - strengthening the role of critical (digital) media literacy skills, together with other civic virtues such as critical thinking and public participation, in educational programmes and curricula in each Member State;
    - involving key national media companies into the curriculum planning and create national forums that offer further training opportunities for teachers in the field;
    - increasing Union-level coordination of the abovementioned activities via a Commission-steered Media Literacy Expert Group.

c. Implementing targeted programmes aimed at integrating diasporas and minorities (*individual and community resilience*). Actions to be taken should include:

    - promoting the positive role of civil society actors in public education campaigns on disinformation and media manipulation, especially those directed for ethnic minorities or vulnerable groups;
    - increasing general awareness against disinformation campaigns by designing non-alarmist public information campaigns on the interrelationship between disinformation and societal security;
    - increasing the level of vertical/social trust within the society by reducing social inequalities and deprivation.

d. Developing legislation for increased electoral transparency (*institutional resilience*). Actions to be taken should include:
    - introducing regulation concerning foreign funding of political parties and associations;
    - strengthening transparency of political advertisements, including on social media platforms.

e. Heightening the importance of supply and value chain resilience (e.g. science, technology, trade, data and investment sectors) in the EU's policy work on strategic autonomy (*forward resilience*). Actions to be taken should include:
    - introducing resilience assessments in connection to the EU's trade and competition policies;
    - launching a debate on resilience to hybrid threats within the framework of the Conference on the Future of Europe.

References

Aaltola, Mika; Fjäder, Christian; Innola, Eeva; Käpylä, Juha and Mikkola, Harri, Huoltovarmuus muutoksessa: Kansallisen varautumisen haasteet kansainvälisessä toimintaympäristössäv, *FIIA Report* 49, The Finnish Institute of International Affairs, 2016.

Aaltola, Mika; Käpylä, Juha; Mikkola, Harri and Behr, Timo. Towards the Geopolitics of Flows, Implications for Finland. *FIIA Report* 40, The Finnish Institute of International Affairs, 2014.

Art, Robert J and Greenhill, Kelly M., 'Coercion: An Analytical Overview', in Kelly M. Greenhill and Peter Krause (eds.) *Coercion: The Power to Hurt in International Politics*, New York: Oxford University Press, 2018.

Australian Communications and Media Authority (ACMA), Misinformation and news quality on digital platforms in Australia. A position paper to guide code development. 2020.

Australian Curriculum Assessment and Reporting Authority (ACARA) Media Arts: The Australian Curriculum. 2018

Australian Government, Director-General's annual threat assessment, 2020.

Australian Government, Foreign Influence Transparency Scheme, 2021a.

Australian Government, Framework for the development of principles-based guidelines to counter foreign interference in the Australian university sector, 2019.

Australian Government, National Counter Foreign Interference Coordinator, 2021b.

Backett-Milburn, Kathryn et al. 'Challenging Childhoods: Young people's accounts of 'getting by' in 'Families with substance use problems', *Childhood* Vol. 15, No. 4, 2008, pp 461–479.

Bajarūnas, Eitvydas, 'Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond'. *European View 2020*, Vol. 19(1), 2020, pp 62–70.

Berkes, Fikret and Ross, Helen 'Panarchy and community resilience: Sustainability science and policy implications'. *Environmental Science & Policy* Vol. 61, 2016, pp 185–193.

Boichak, Olga, 'Mitigating diffused security risks in Australia's north: a case for digital inclusion', *The Strategist*, 30 Sep 2020.

Boin, Arjen; Ekengren, Magnus and Rhinard, Mark, 'Hiding in Plain Sight: Conceptualizing the Creeping Crisis', *Risk, Hazards & Crisis in Public Policy*, Vol. 11, No. 2, 2020, pp 116–138.

Boulègue, Mathieu; Orysia Lutsevych and Anaïs Marin, Civil Society Under Russia's Threat: Building Resilience in Ukraine, Belarus and Moldova., *Chatam House Research Paper*, 2018.

Bourbeau, Philippe and Vuori, Juha A., 'Security, resilience and desecuritization: multidirectional moves and dynamics', *Critical Studies on Security*, Vol. 3, No. 3, 2015, pp 253–268.

Bourbeau, Philippe, 'A Genealogy of Resilience', *International Political Sociology* 2018, Vol. 12, No. 1, pp 19–35.

Bourbeau, Philippe, 'Resiliencism: Premises and Promises in Securitisation Research', *Resilience: International Policies, Practices and Discourses*, Vol. 1, No. 1, 2013, pp 3–17.

Brady, Ann-Marie, Magic weapons: China's political influence activities under Xi Jinping, Washington DC: Wilson Center, 2017.

Brand, Fridolin Simon and Jax, Kurt 'Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object', *Ecology & Society* 2007, Vol. 12, No. 1, 23.

Breitenbauch, Henrik and Byrjalsen, Niels, 'Subversion, Statecraft and Liberal Democracy', *Survival* 61, no. 4, 2019, pp 31–41.

Buchanan, Elisabeth, 'Hybrid warfare: Australia's (not so) new normal', *Australian Strategic Policy Institute ASPI*, 2019.

Charap, Samuel, 'The ghost of hybrid warfare', *Survival*, vol. 57, no. 6, 2015, pp 51-58.

Conley, Heather A., Donatienne Ruy, Ruslan Stefanov and Martin Vladimirov, The Kremlin Playbook 2: The Enablers, Lanham: *Rowman and Littlefield*, 2019.

Conley, Heather A., James Mina, Ruslan Stefanov and Martin Vladimirov, The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe, Lanham: *Rowman and Littlefield*, 2016.

Cormac, Rory and Richard J. Aldrich, 'Grey is the new black: covert action and implausible deniability', *International Affairs* 94(3), 2018, pp 477-494.

Critical Infrastructure Centre (CIC), The Trusted Information Sharing Network (TISN). Australian Government. Department of Home Affairs. 2021.

Cross, Mai'a K. Davis, 'The EU Global Strategy and diplomacy' *Contemporary Security Policy*, Vol. 37, No. 3, 2016, pp 402–413.

Diamond, Larry, Developing Democracy: Toward Consolidation, Baltimore: *Johns Hopkins University*, 1999.

Digital Industry Group Inc. (DIGI), 'Disinformation code'. 2021b.

Digital Industry Group Inc. (DIGI), Australian Code of Practice on Disinformation and Misinformation, 2021a.

EEAS, Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy, 2016.

EU-NATO, Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg, 2016.

EU-NATO, Joint declaration on EU-NATO cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 2018.

European Audiovisual Observatory, Mapping of media literacy practices and actions in EU-28. 2016.

European Commission and High representative of the Union for Foreign Affairs and Security Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final, 2013.

European Commission and High representative of the Union for Foreign Affairs and Security Policy, Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, 2016.

European Commission and High representative of the Union for Foreign Affairs and Security Policy, A Strategic Approach to Resilience in the EU's external action, JOIN/2017/021 final, 2017.

European Commission and High representative of the Union for Foreign Affairs and Security Policy, Increasing resilience and bolstering capabilities to address hybrid threats, JOIN/2018/16 final, 2018a.

European Commission and High representative of the Union for Foreign Affairs and Security Policy, Action Plan against Disinformation, JOIN/2018/36 final, 2018b.

European Commission and High representative of the Union for Foreign Affairs and Security Policy, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint

Communication on increasing resilience and bolstering capabilities to address hybrid threats, SWD (2019) 200 final, 2019.

European Commission, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. COM/2020/829 final, 2020.

European Commission, Tackling online disinformation: a European Approach., COM/2018/236 final, 2018c.

European Council, Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions (10 December 2019), 14972/19, 2019.

European Council, Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic, 14064/20, 2020.

European Council, European Council meeting (19 and 20 March 2015) – Conclusions, EUCO 11/15, 2015.

European Parliament, Proposal for additional measures on critical infrastructure protection / after 2020-9. Legislative train 02.2021, 2021.

EVPHT/P, Esitys valtioneuvoston päätökseksi huoltovarmuuden tavoitteista 2013: perustelumuistio. Työ- ja elinkeinoministeriö, 4/12/2013.

Fernquist, Johan, Lisa Kaati, Nazar Akrami, Katie Cohen and Ralph Schroeder, Bots and the Swedish election. A study of automated accounts on Twitter, FOI Memo 6466, 2018.

Finnish Government, Government Report on EU Policy Strong and united EU – towards a more sustainable European Union. 2021a.

Finnish Government, Prime Minister's Office webpages. 2021b.

Finnish Government, The Security Strategy for Society. 2017.

Finnish Government, Valtioneuvoston päätös huoltovarmuuden tavoitteista 857/2013, 2013.

Finnish Government, Valtioneuvoston päätös huoltovarmuuden tavoitteista, 1048/2018, 2018.

Finnish Ministry of Education and Culture, Media Literacy in Finland, 2019.

Fiott, Daniel and Parkes, Roderick, Protecting Europe: The EU's response to hybrid threats. EUISS. Chaillot Paper 151, 2019.

Fjäder, Christian, 'The nation-state, national security and resilience in the age of globalization', *Resilience: International Policies, Practices and Discourses,* Vol 2(2), 2014, pp 114–129.

Garnaut, John, 'How China Interferes in Australia: And How Democracies Can Push Back', *Foreign Affairs*, 2018.

Giannopoulos, Georgios; Smith, Hanna and Theocharidou, Marianthi, eds., The Landscape of Hybrid Threats: A Conceptual Model, European Commission JRC and Hybrid CoE, 2020.

Giles, Keir, Handbook of Russian information warfare, Nato Defense College, 2016.

Gotkowska, Justyna, Sweden's security: the long way towards total defence. OSW, 2021.

Gressel, Gustav, 'Protecting Europe against hybrid threats.' ECFR Policy Brief, 2019.

Hakala Emma., Mikkola Harri et al., Suomen huoltovarmuus ja Baltian alue: Tiivistyvät yhteydet muuttuvassa turvallisuusympäristössä. *FIIA Report 61*, The Finnish Institute of International Affairs, 2019.

Hall, John Stuart and Zautra, Alex J., 'Indicators of Community Resilience: What Are They, Why Bother?' In Reich, J., Zautra, A.J. & Hall, J.S. (eds..), *Handbook of Adult Resilience*. London: *Guilford*, 2010, pp 350–371.

Hamilton, Clive, 'Silent invasion: China's influence in Australia'. Melbourne: *Hardie Grant*, 2018.

Hofverberger, Elin, Government Responses to Disinformation on Social Media Platforms: Sweden, Library of Congress, 2019.

Hutchens, Gareth, Sweeping Foreign Interference and Spying Laws Pass Senate, *The Guardian*, published on 28 June 2018.

Hybrid CoE, Countering disinformation: News media and legal resilience, 2019.

Hyvönen, Ari-Elmeri and Juntunen, Tapio et. al, Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi, Publications of the Government's Analysis, Assessment and Research Activities 17/2019. Helsinki: Prime Minister's Office, 2019.

Hyvönen, Ari-Elmeri and Juntunen, Tapio, 'From 'Spiritual Defence' to Robust Resilience in the Finnish Comprehensive Security Model., in Larsson, Sebastian & Rhinard, Mark (eds.), Nordic Societal Security: Convergence and Divergence. London: *Routledge*, 2020, pp 154–178.

Hägglund, Mariette, Rebuilding Sweden's crisis preparedness: Lack of clarity impedes implementation, *FIIA Briefing Paper 283*, The Finnish Institute of International Affairs, 2020.

Jenkins, Brian M., 'International Terrorism: A New Mode of Conflict', in David Carlton and Carlo Schaerf (eds.), International Terrorism and World Security, London: *Groom Helm*, 1975

Jonsson, Daniel, Ingemarsdotter, Jenny; Johansson, Bengt; Rossbach, Niklas; Wedebrand, Christoffer; and Eriksson, Camilla, Civilt försvar i gråzon. FOI, 2019.

Juntunen, Tapio and Hyvönen, Ari-Elmeri, 'Resilience, Security and the Politics of Processes', *Resilience: International Policies, Practices and Discourses,* Vol. 2, No. 3, 2014, pp 195–206.

Juntunen, Tapio and Hyvönen, Ari-Elmeri, 'Koronakriisi, informaatio ja resilienssipolitiikka', *Kosmopolis*, Vol. 50, No. 2, 2020, pp 72–92.

Kommittédirektiv, En ny myndighet för psykologiskt försvar. Beslut vid regeringssammanträde den 16 augusti 2018, Dir. 2018:80, Stockholm: Justitiedepartementet, 2018.

Kommittédirektiv, Inrättande av Myndigheten för psykologiskt försvar. Beslut vid regeringssammanträde den 18 mars 2021. Dir. 2021:20, Stockholm: Justitiedepartementet, 2021.

Larsson, Sebastian "Swedish total defence and the emergence of societal security", in Larsson, Sebastian and Mark Rhinard (eds.), Nordic Societal Security: Convergence and Divergence. London: *Routledge*, 2020.

Lessenski, Marin, The Media Literacy Index 2019, *Open Society Institute Sofia – European Policies Initiative (EuPI) Policy Briefs*, n 55, 2019.

Lucas, Edward, 'The Spycraft Revolution: Changes in technology, Politics, and Business are all transforming espionage. Intelligence Agencies Must Adapt – Or Risk Irrelevance', *Foreign Policy*, April 27, 2019,

Löjdquist, Fredrik, An Ambassador for Countering Hybrid Threats. *RUSI Commentary*, published on 6 September 2019.

Mansted, Katherine, 'The domestic security grey zone: Navigating the space between foreign influence and foreign interference', *Occasional Paper,* Australian National University, 2021.

McGaughey, Ewan, 'Could Brexit Be Void?', *King's Law Journal* Vol. 29, No. 3, 2018, pp 331-343.

Mediapooli, *Mediapooli webpages*. 2021.

Monaghan, Sean, 'Countering Hybrid Warfare So What for the Future Joint Force?', *Prism*, Vol. 8, No. 2, 2019, pp 82–98.

MSB, Countering information influence activities: A handbook for communicators. Karlstadt: Myndigheten för samhällsskydd och beredskap. 2018b.

MSB, If crisis or war comes. 2018a.

Mörttinen, Matti, Valtioneuvoston ydin kriisitilanteessa — Covid-19-pandemian paineet suomalaiselle päätöksenteolle. Sitra, 2021.

NATO, Wales Summit Declaration, *Press Release 120* of 5 September 2014.

NESA, National Emergency Supply Agency. *Webpages.* 2021.

Northern Territory Government, Infrastructure Strategy, 2017.

Notley, Tanya and Dezuanni, Michael, 'Advancing children's news media literacy: learning from the practices and experiences of young Australians', *Media, Culture & Society*, 41(5), 2019, pp 689–707.

OKM, Hyvä medialukutaito: Suuntaviivat 2013–2016, 2013.

OKM, Medialukutaito Suomessa: Kansalliset mediakasvatuslinjaukset, 2019.

Pamment, James, The EU's Role in Fighting Disinformation: Taking Back the Initiative. *Carnegie Endowment for International Peace*, 2020.

Parks, Sora et al., Digital News Report: Australia 2020. Canberra: University of Canberra, 2020.

Polyakova, Alina; Laruelle, Marlene; Meister, Stefan and Neil Barnett, 'The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom', Washington, DC: *Atlantic Council*, 2016.

Pursiainen, Christer, 'The Crisis Management Cycle', London: *Routledge*, 2018.

Pynnöniemi, Katri and Saari, Sinikukka, 'Hybrid Influencing – Lessons from Finland', *Nato Review*, 28 June 2017.

Rademaker, Michael et al. Making cities in conflict areas more resilient. Netherlands Institute of International Relations 'Clingendael', 2018.

Richey, Mason, 'Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation', *Asia Europe Journal* Vol 16, no 1, 2017, pp 101-113.

Rossbach, Niklas H., Psychological Defence: Vital for Sweden's Defence Capability. FOI Memo 6207. Offprint from Strategic Outlook 7, 2017.

Rossbach, Niklas H.; Öhrn-Lundin, Josefin; Jonsson, Daniel K; Sundberg, Anna; Olsson, Sofia; Gustafsson, Jakob; and Trané, Camilla (eds.), *Sweden's total defence – challenges and opportunities*. Strategi Outlook 8, FOI. 2019.

Schmid, Alex P. and de Graaf, Janny, Violence as Communication: Insurgent Terrorism and the Western News Media, London: *Sage*, 1982.

Stiglund, Jonathan, Threats, risks, and the (re)turn to territorial security policies in Sweden, in Larsson, Sebastian and Mark Rhinard (eds.), Nordic Societal Security: Convergence and Divergence. London: Routledge, 199–221. 2020.

Swedish Government, Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025), 2020.

Szymański, Piotr, 'Towards greater resilience: NATO and the EU on hybrid threats.' *OSW Commentary*. 2020.

Sørensen Heine and Nyemann, Dorthe B., 'Going Beyond Resilience. A revitalised approach to countering hybrid threats', *Hybrid CoE Strategic Analysis 13*, 2019.

The Local, Sweden to create new authority tasked with countering disinformation. Published on 15 January 2018.

The Nordic Council of Ministers, Nordic fightback against fake news. Published on 30 October 2018.

The Security Committee, The Security Committee webpages. 2021.

The Swedish Defence Commission secretariat, Resilience - The total defence concept and the development of civil defence 2021-2025, 2017.

Thomas, Timothy L., 'Russia's reflexive control theory and the military', *Journal of Slavic Military Studies*, Vol 17, No 2, 2004, pp 237-56.

Tierney, Kathleen J., 'The social roots of risk: producing disasters, promoting resilience'. Stanford, CA: *Stanford University Press*. 2014.

To, James Jiann Hua To, 'Qiaowu: Extra-Territorial Policies for the Overseas Chinese', *Brill*. 2014.

Ungar, Michael 'The Social Ecology of Resilience: Addressing Contextual and Cultural Ambiguity of a Nascent Construct', American Journal of Orthopsychiatry, Vol. 81, No. 1, 2011, pp: 1-17

Van Puyvelde, Damien, 'Hybrid War – Does it Even Exist?' NATO Review, 2015,

von Sydow, Björn, Resilience: Planning for Sweden's "Total Defence". NATO Review, 2018.

Walklate, Sandra Lyn; McGarry, Ross and Mythen, Gabe, 'Searching for Resilience: A Conceptual Excavation', *Armed Forces & Society*, Vol. 40, No. 3, 2014, pp 408–427.

Wigell, Mikael and Vihma, Antto, 'Geoeconomics versus Geopolitics: The Case of Russia's Geostrategy and Its Effects on the EU', *International Affairs*, vol. 92, no. 3, 2016, pp 605-627.

Wigell, Mikael, Democratic Deterrence: How to Dissuade Hybrid Interference, *The Washington Quarterly,* Vol 44, No 1, 2021, pp 49-67.

Wigell, Mikael, Hybrid Interference as a Wedge Strategy, *International Affairs,* Vol 95, No 2, 2019, pp 255-275.

PE 653.632
EP/EXPO/INGE/FWC/2019-1/LOT6/R/06

Print ISBN: 978-92-846-7992-8 doi: 10.2861/702047 QA-09-21-109-EN-C
PDF ISBN: 978-92-846-7991-1 doi: 10.2861/379 QA-09-21-109-EN-N