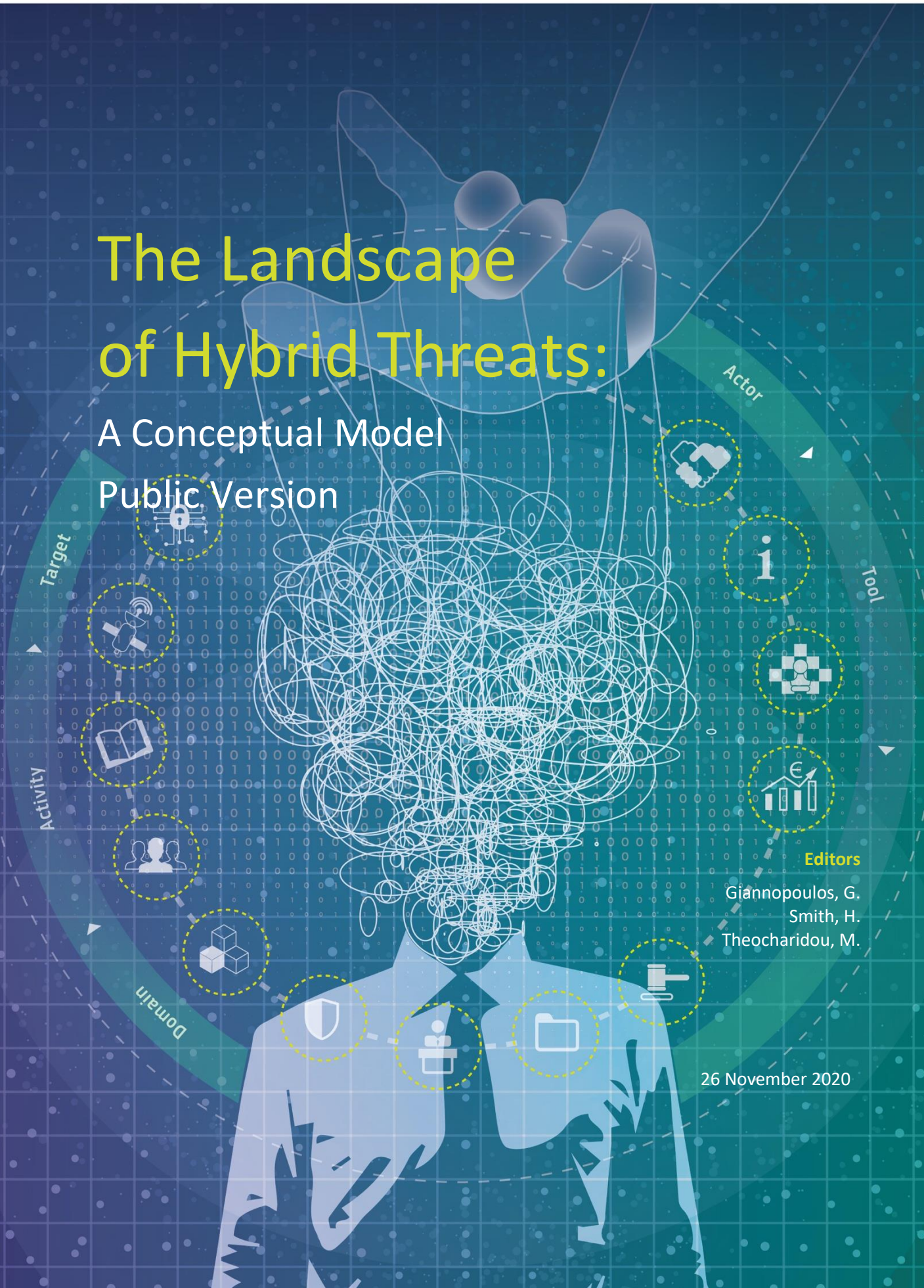
European Commission

Hybrid CoE

The Landscape of Hybrid Threats:

A Conceptual Model

Public Version



Editors

Giannopoulos, G.
Smith, H.
Theocharidou, M.

26 November 2020

Contact information
JRC
Name: Georgios GIANNOPOULOS
Address: via E. Fermi 2749, 21027, Ispra (VA), Italy
Email: georgios.giannopoulos@ec.europa.eu
Tel.: +390332786211

Hybrid CoE
Name: Hanna SMITH
Address: Lintulahdenkatu 5 A, 00530 Helsinki, Finland
Email: hanna.smith@hybridcoe.fi
Tel.: +358505385549

Science Hub
https://ec.europa.eu/jrc

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

JRC123305

Ispra: European Commission, 2020

How to cite this report: Giannopoulos, G., Smith, H., Theocharidou, M., *The Landscape of Hybrid Threats: A conceptual model*, European Commission, Ispra, 2020, PUBSY No. 123305

Content

The Landscape of Hybrid Threats
Foreword by Commissioner Mariya Gabriel

The events of 2020 have reminded us to always be prepared for the unthinkable, and that, in times of crisis, science and robust evidence must be at the heart of the decisions we take to protect citizens' lives and livelihoods.

This holds true for the coronavirus crisis but it also extends to many other domains, including Europe's security. We made a big step forward in creating a future-proof security environment in 2020, as the EU adopted a new Security Union Strategy in July. Many of its pillars are forward looking, designed to tackle hybrid security threats that are continuously evolving and bringing increased uncertainty over what the future holds. EU security research is a cornerstone of the Security Union enabling innovation in technologies and knowledge. A solid, scientific approach will help us fully understand these challenges and take the right decisions to protect all of Europe's citizens. The Joint Research Centre's multidisciplinary expertise - and the evidence and knowledge contained within this report - are an instrumental part of these efforts.

We can no longer rely on the certainties of the past. Alliances are changing and strategic interests are shifting, dictating new doctrines and approaches to international problems. Our neighbourhood is still far from being stable. Rising and revisionist powers are challenging our shared values and our democratic institutions, making it difficult to take a step back, consider things objectively, and understand the changes we are going through. We must find our compass to guide the EU and its Member States through these choppy waters and maintain our prosperity, our values and our way of life.

This will require a collective effort. The complexity of the threats we are facing continues to evolve. Adversaries may use all kind of tools to achieve their objectives, from information manipulation, to terrorist attacks, cyber attacks and the exploitation of vulnerable groups in society. In many cases, these actions remain below the level that would allow our sensors to detect and expose them.

Fortunately, the EU has the capacities and know-how to build its resilience to hybrid threats. Our advantage is that we ground our policy actions in science and evidence. This report, a collaboration between the JRC and the European Centre of Excellence for Countering Hybrid Threats, will help us to acknowledge the problem, understand it in depth and design our response accordingly. The fruit of major efforts to gain a deep understanding of hybrid threats, the report provides a comprehensive characterisation of these threats, analysing the strategic thinking of state and non-state hybrid actors and exploring the toolbox these actors may use against EU countries.

This is only the beginning. We have a long and exciting way in front of us, and I am confident that we will take the right actions to lead us to a more secure and more resilient Europe.

I commend the efforts of the JRC, together with the Hybrid Centre of Excellence and wish you enjoyable reading.

Acknowledgements

The editors would like to thank the former European Council Friends of the Presidency Group for Countering Hybrid Threats (FoP) currently the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats for their support and collaboration. Their support, comments and corrections have been valuable in driving this study to be useful for practitioners, as well as for the EU and Hybrid CoE member states. Moreover, were it not for the insights of the peer-review meeting held in Brussels (May 2019), this report would have been much poorer. We would like to thank Mikael Wigell, Andreas Herberg-Rothe and Aurel Sari for their constructive critique and valuable ideas from the international relations and legal perspective. Tibor Toth reminded us about the importance of historical perspectives, and we credit him with one of the central ideas in the report, namely that "*hybrid is always a combination but not all combinations are hybrid*". Bas Keijser from TNO encouraged us by demonstrating the insightful thinking emanating from TNO and gave us ideas on how to enhance the phases section as well as the whole characterisation. The EDA and EUMS reminded us how important the military aspect is for the landscape of Hybrid Threats. FRONTEX provided extremely useful insights with respect to the links between migration and Hybrid Threats, a highly sensitive and divisive topic at the EU level. The ESDC helped us to see how the report should be improved in order to be useful for training and conducting exercises. We hope we fulfilled their expectations. Both JRC and Hybrid CoE staff have provided critical support throughout the process. Without their assistance, the concept creation would not have been possible. Many of the elements have been gathered from JRC and Hybrid CoE colleagues' insights and thinking, as well as suggestions for improvements. The Hybrid CoE's communities of interest – Hybrid Influencing, Strategy and Defence, and Vulnerabilities and Resilience, as well as the teams working on JRC reports (Security and Defence, and Resilience to name the most relevant ones) have been invaluable sources of ideas and information. Without this support, the report would have never been born. We would like to thank the members of the Interservice Group of European Commission on Hybrid Threats for their comments and suggestions.

The workshops in Ispra and Helsinki for the authors were always executed in a good spirit and with the will to go the extra mile. The constructive and inspiring debates benefitted the concept creation. The editors would like to extend deep gratitude to the dedicated team of authors.

The case-study authors Dr. Patrick Cullen, Norwegian Institute of International Affairs, Dr. András Rácz, Deutsche Gesellschaft für Auswärtige Politik, and Dr. Magnus Normark have performed a Herculean task in uncovering difficult cases and analyzing how Hybrid Threats are manifested. They also contributed significantly to the concept of Hybrid Threats and hybrid warfare, pointing out linkages, missing parts and unclear passages, especially relating to Russia, China, and non-state actors.

Dr. Georgios Marios Karagiannis made a huge contribution in describing a series of domains and tools of hybrid threat activity, an essential aspect for understanding Hybrid Threats. Without Cristina Juola's deep dive into Russian and Chinese language literature on influence creation, threat perceptions, world views and status building, this report would not have been as rich in material and the concept as convincing. Käsper Kivisoo added a practitioner's perspective to the many different project workshops and put the authors through their paces in the process. Dr. Johann Schmid ensured that the hard end of Hybrid Threats, hybrid warfare activity, was covered, perhaps not sufficiently from the military perspective, but enough to provide a basis for further development. Dr Josef Schroefl helped us in understanding the escalation potential, how the military can also be a target domain, and the importance of cyber. His long-term and in-depth knowledge of the subject is hopefully accurately reflected in the report.

The editors would like to thank the report's strategic advisors: Former JRC's Director General Vladimir Šucha, current JRC's Director General Stephen Quest, JRC's Directorate E Director Dan Chirondojan, Former Hybrid CoE Director Matti Saarelainen and the current director Teija Tiilikainen, and Georg Peter, Head of Technology Innovation in the Security Unit leading the JRC's efforts in Hybrid Threats, for their support, knowledge and engagement from day one. Their efforts provided the solid foundation that the report was built upon. We remain indebted to them.

Georgios Giannopoulos

Hanna Smith

Marianthi Theocharidou

Strategic advisors

Stephen Quest	EC – JRC
Vladimir Šucha	former EC – JRC, currently EAC
Dan Chirondojan	EC – JRC
Teija Tiilikainen	Hybrid CoE
Matti Saarelainen	former Hybrid CoE
Georg Peter	EC – JRC

Editors and Authors

Georgios Giannopoulos	EC – JRC
Hanna Smith	Hybrid CoE
Marianthi Theocharidou	former EC – JRC, currently ENISA

Authors

Cristina Juola	Hybrid CoE
Georgios Marios Karagiannis	EC – JRC
Käsper Kivisoo	Hybrid CoE
Johann Schmid	Hybrid CoE
Josef Schroefl	Hybrid CoE

Case-study authors

Patrick Cullen	Norwegian Institute of International Affairs
András Rácz	Deutsche Gesellschaft für Auswärtige Politik
Magnus Normark	Swedish Defence Research Agency (FOI)

Contributors

Thomas Barbas	EC – JRC
Jon Filipek	EC – CNECT
Joaquim Fortuny-Guasch	EC – JRC
Naouma Kourti	EC – JRC
Georgios Koutepas	CERT – EU
Elisabeth Krausmann	EC – JRC
Gian Luigi Ruzzante	EC – JRC
Holger Fabian Sahl	FRONTEX
Aurel Sari	Exeter University
Guido Tintori	EC – JRC
Ana Lisa Vetere	EC – JRC
Jukka Savolainen	Hybrid CoE
Rainer Jungwirth	EC – JRC

Executive summary

In recent years, the topic of Hybrid Threats has dominated the security landscape in Europe. Whereas it may be considered a new topic by several stakeholders, in actual fact it is not. It is as old as conflict and warfare, but **repackaged and empowered by changing security environment dynamics, new tools, concepts and technologies targeting vulnerabilities in several domains** in an unprecedented manner. This new reality increases the **outreach and effectiveness** of today's Hybrid Threats in achieving highly strategic and **overarching objectives** such as **undermining public trust in democratic institutions, deepening unhealthy polarization both nationally and internationally, challenging the core values of democratic societies, gaining geopolitical influence and power through harming and undermining others, and affecting the decision-making capability of political leaders.** As a consequence, it is no surprise that today's Hybrid Threats belong to the sphere of **serious and acute threats** posed to the EU, NATO and their member states, and are recognized as such by policymakers across Europe and beyond.

Addressing Hybrid Threats effectively requires a common understanding by practitioners, policymakers and politicians, early identification of the hybrid threat activity, the identification of gaps in prevention, preparedness and response, and the development of the right actions in order to bolster resilience both at a national and at a European/NATO level. To this end there is significant ongoing work being done at the academic, policymaking and operational level. At the academic level, new scientific knowledge is being produced. At the EU policymaking level, two Joint Communications have paved the way for acting in this area, and Hybrid Threats are recognized in a number of security-related policies, such as the EU Security Union Strategy adopted in July 2020. In EU and NATO member states significant changes have already been made at the national level, but more are needed. At the operational level, the EU has conducted the largest ever tabletop exercise on Hybrid Threats (Parallel and Coordinated Exercise, PACE 18) in collaboration with NATO. These efforts leave no doubt about the importance of Hybrid Threats for the EU.

A careful analysis of these actions reveals that our understanding about Hybrid Threats and how they express themselves still draws very much on past experience. Since a solid conceptual basis has been lacking, it has hindered relevant stakeholders in improving their understanding of Hybrid Threats, while making it more challenging to design and implement effective comprehensive measures to address this very complex phenomenon both national and international levels.

In order to address this gap, the Joint Research Centre of the European Commission (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki have joined forces to develop a conceptual model for characterizing Hybrid Threats accompanied by a framework for analysis.

The proposed conceptual model provides a narrative with a corresponding visual representation depicting the main concepts and factors and, more importantly, the relationships between them. More specifically, the conceptual model's analytical framework is developed around four main pillars: **actors (and their strategic objectives), domains, tools, and phases**. This structure enables us to grasp the time variable of Hybrid Threats and identify the way in which an actor can employ a series of tools to affect the targeted country in order to achieve a series of objectives. The proposed framework is not the mere listing of the above-mentioned pillars, but aims at identifying the links between them as well as providing a flexible framework, a blueprint, that can be adapted to the needs of each EU and NATO member state. The proposed conceptual model's analytical framework is validated against a number of real case studies in order to assess its validity and its analytical value. Although it would be convenient to establish the analytical framework on the basis of past experience, we refrained from doing so in order to deliver a concept for Hybrid Threats and analytical framework that is future-proof, handles the test of time and that describes the concept of Hybrid Threats against the background of current security environment dynamics, while taking into consideration the evolving nature of the threat.

In particular, the conceptual model puts much emphasis on actors. It aims at understanding their drivers by studying their motives, doctrines, open source intelligence and literature, which duly provide pieces of evidence for their objectives and strategic culture. A deep understanding of actors' objectives is an excellent proxy for forecasting possible future activities. The conceptual model focuses on state and non-state actors and the case studies demonstrate the diversified nature of their activities and modii operandi.

An essential factor of the conceptual model is the identification of the various tools that enable state

and non-state actors to create Hybrid Threats. Despite the extensive list of tools that have been included and analysed in the present document, the objective was not to develop an exhaustive list of tools but rather to provide examples and a framework of what tools could look like so as to enable member states and international organizations to adapt the framework to their needs. Such an approach serves the purpose of avoiding a conceptual handcuffing, which would restrict stakeholders rather than broaden their view. We are expecting that the end users of this report will also be in a position to propose other tools that are not currently listed and associate them with actors, domains and phases.

The term "Domains" is used throughout the document in order to characterize instruments of national power. A concerted effort has been made to achieve balance between granularity and the analytical value of generalization, and to this end 13 domains have been considered. All case studies demonstrate combinations of different domains, so alternative approaches exist both in consolidating and expanding the list. As in the case of tools, it would be useful to observe an evolution of the concept with fewer or more domains according to the strategic, operational and analytical needs of the end users. The number of domains in this report highlights the complexity of the threat. The 13 domains also show the importance of a comprehensive approach, which combines civil and military thinking.

A description of the phases of Hybrid Threats is fundamental for their complete conceptualization and central for the analytical framework. It is an essential element for raising awareness, providing arguments for stakeholders in order to act even during periods of low activity since this low activity might simply be part of the first priming phase, where little is observed. The timeline of hybrid threat activity does not necessarily exhibit a monotonic escalation, but it might oscillate between priming and destabilization phases without reaching a full escalation. This is due to the fact that an actor might achieve the desired objectives without full escalation. The phases also show what is the difference between traditional influence as part of international politics and interference and influence, which meddles in a state's internal affairs in unwelcomed and unacceptable ways by disguising the true intent, sometimes also the real actor, and using covert means.

A recurring question to which this conceptual model sought to provide concrete answers is the hybridity of certain actions or, in other words, what makes a threat hybrid. In fact, this aspect constitutes the glue that holds the variables of the present conceptual model together. The combinatory and persistent strategic nature of a threat (involving several tools in a variety of domains for extended periods), the manipulation of thresholds of detectability, the problems of attribution and activation of response mechanisms, and the ambiguity and exploitation of the seams of democratic states are the adhesive elements that render an activity hybrid.

The conceptual model is expected to constitute an important element for both operational as well as strategic thinking at the EU and NATO levels and their member states, which is sorely needed. It will complement ongoing efforts and existing policy initiatives as well as provide an ex-post *raison d'être* based on scientific evidence. In addition, it will facilitate common understanding and raise awareness of the relevant authorities on the issue of Hybrid Threats. Given the importance of early detection and attribution in order to counter Hybrid Threats, the conceptual model will provide a comprehensive guide to those variables that authorities should look out for in order to identify the onset of a hybrid threat activity that can turn into Hybrid Threat at an early stage. It will also serve as a basis for extracting vulnerability indicators across domains, facilitating sound risk management as well as building capacities for bolstering resilience. Finally, the conceptual model will support the development of exercise scenarios as well as the identification of areas that require further research work (e.g. emerging and disruptive technologies).

1 Introduction

1.1 Concept

In recent years, the topic of Hybrid Threats has dominated the security landscape in Europe. Whereas it may be considered a new topic by several stakeholders, in fact it is not. It is as old as conflict and warfare, but **repackaged and empowered by changing security environment dynamics, new tools, concepts and technologies targeting vulnerabilities in several domains** in an unprecedented manner. The evolution of the available tools increases the **outreach and effectiveness** of Hybrid Threats in achieving several highly strategic and **overarching objectives** such as **undermining public trust in democratic institutions, deepening unhealthy polarization both nationally and internationally, challenging the core values of democratic societies, gaining geopolitical influence and power through harming and undermining others, and affecting the decision-making capability of political leaders.** As a consequence, it is no surprise that today's Hybrid Threats belong to the sphere of **serious and acute threats** posed to the EU and its member states and are addressed as such by policymakers across Europe.

The fast pace with which this concept of Hybrid Threats **is evolving** is reflected in the literature, in the proliferation of research groups and organizations working on the topic, and also in the evolution of the **language** used in the relevant policy documents. The **Joint Communication** on Hybrid Threats published in 2016 focuses on a series of **actions** to be carried out by the Commission and member states in order to counter Hybrid Threats at a more **operational** level. The Joint Communication **JOIN(2018)16** "*Increasing resilience and bolstering capabilities to address Hybrid Threats*" released in June 2018 provides a more **strategic** view on the topic, clearly delineating the importance of strategic aspects such as bolstering **resilience** as a means of countering the effects of Hybrid Threats.

An inherent characteristic of Hybrid Threats entails blurring traditional **dichotomies** and creating **ambiguity**. Individuals have an inherent preference for thinking in dichotomies (true/false, friend/enemy, etc.) and decision-making is largely based on such a way of thinking. Ambiguity on the other hand hinders decision-making at an individual and a collective level by creating confusion and distrust. Being "**under the radar**" as much as possible is one of the characteristics of hybrid threat activities. Hence it is necessary to shed light on the blurred **boundaries of disciplines** and provide the means to facilitate comprehension and decision-making.

We are confronting a totally **new situation** today. The core values of Western societies, including **openness** and **democratic decision-making**, are being manipulated in order to **compromise** these very values. The struggle for geopolitical power and influence further accentuates the significance of Hybrid Threats.

The conceptual model for Hybrid Threats needs to take into account current technological and **socioeconomic** megatrends and answer a series of existential questions: How can we bolster resilience to counteract the erosion of the core values of Western democratic societies when these very values might be the means of **undermining** their own existence? How can we ensure that the struggle for geopolitical power will not undermine the level of prosperity of EU countries? And finally, how we can safeguard the resilience of the decision-making capability of EU member states?

1.2 Scope and objectives

The main scope of this document is to establish a conceptual basis for describing Hybrid Threats and to confirm the validity of its analytical framework by means of case studies and an in-depth literature review of Russian and Chinese strategic thinking. In addition, the conceptual model seeks to address a series of overarching objectives in order to better characterize Hybrid Threats.

The first objective of the conceptual model is **to arrive at a common understanding among the various stakeholders of the concept of Hybrid Threats**.

The second objective of the conceptual model is **to support designing the right actions in order to address and counter Hybrid Threats**. In this respect, the conceptual model's analytical framework should be considered as a point of reference for policymakers in order to design effective and efficient policies and actions, especially when it comes to detection, questions of attribution and resilience building.

The **third objective** of the conceptual model is to provide a **context** and basis for further development of the Hybrid Threats concept at the academic, political and operational level.

It is also important to state what this report will not offer. First of all, it does not aim to provide a

universal definition of Hybrid Threats. The concept should reflect an understanding that the threats are changing and evolving.

This report does not aim to become a threats assessment or risk assessment tool, nor a methodology. There is no estimation as to if or when hybrid threat activity occurs and which tools may be used again, and what kind of effects and impact those activities and tools may have.

To conclude, given the complexity of the topic, the combination of exploitation of **vulnerabilities**, attack vectors and number of actors involved, a conceptual model will be extremely useful for providing an abstract yet very powerful representation of the Hybrid Threats ecosystem. This will support the efforts of policymakers in the EU and member states to establish a common understanding, improve detection, preparedness, attribution, addressing vulnerabilities, and ultimately bolster resilience.

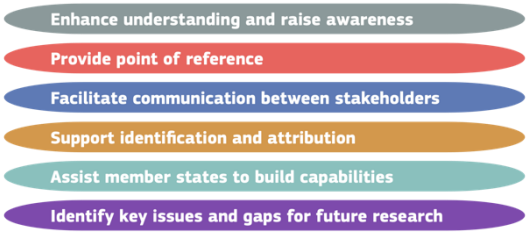


Figure 1. Summary of objectives

1.3 Audience

The previous paragraphs have already put forward some ideas regarding the recipients of this conceptual model. The proposed model aims at addressing strategic issues both at a national and an international level. To this end, the model should further a common understanding and better communication among EU institutions and agencies with a more operational role. Furthermore, it should prove useful for the academic community in fostering innovative research in areas where knowledge gaps are identified.

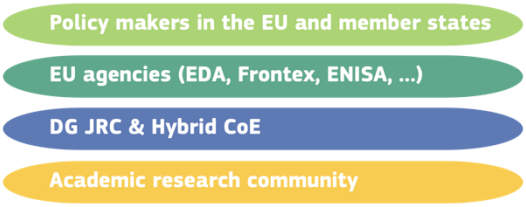


Figure 2. Audience

1.4 Methodology

This model (the report) is a product of the close collaboration between the JRC and Hybrid CoE from July 2018 to July 2020. The collaboration was facilitated by periodic meetings and brainstorming sessions both within each organization and jointly. A visiting scientist from Hybrid CoE worked in the JRC for a period of three weeks to strengthen the collaboration.

1.4.1 Expert team

In order to tackle the complexity of this report's conceptual work, a team of experts from both organizations was formed, comprising the editors, the authors of the report, and the authors of the case studies. This multi-disciplinary group embodies a range of backgrounds and expertise, namely engineering, security, emergency management, defence, military studies, public administration, social science, international relations, and political science, among others. The experts were intentionally chosen to ensure that the complexity of the problem is addressed from multiple viewpoints such as civilian vs. military, technical vs. social, and so on. Moreover, the review process described below contributed to the inclusion of multiple perspectives and expertise.

1.4.2 Literature review and analysis

In order to support the conceptual model creation, the expert team reviewed the literature on Hybrid Threats. They were assisted in their initial desk research by the JRC's TIM Technology Editor tool.[1] They focused on previous scientific work on hybrid warfare, but also expanded their study to other works that reflect the civilian side as well. The references at the end of the document constitute a starting point for further reading.

To support the case studies, the literature research was also conducted in Russian and Chinese to compare the visible activities with what is being written on the topic in these languages in order to

[1]TIM Technology Editor allows its users to create and visualize datasets about specific technological issues. It brings together datasets such as patents, scientific publications, and EU grants. More information on the JRC's Tools for Innovation Monitoring is available at: https://ec.europa.eu/jrc/en/scientific-tool/tools-innovation-monitoring.

gain a more comprehensive understanding of the actors' point of view and to minimize our own potential biases and misperceptions of their actions. The literature review was also used to support the analysis of the actors' objectives and intentions.

1.4.3 Model design

The conceptualization was conceived based on a series of iterative sessions, which reflected the progress of the research conducted by the expert team.

In the initial stages of the work, various types of conceptual models were reviewed. These covered other scientific topics but were examined in terms of visualization techniques and analytical properties.

Moreover, previous research conducted by the JRC on conceptual modelling was reviewed, such as the work on resilience by Manca, Benczur, and Giovannini (2017), MCDC's Countering Hybrid Warfare project (Monaghan, Cullen, and Wegge 2019; Cullen and Reichborn-Kjennerud 2017), the project "*Russia and Hybrid warfare: definitions, capabilities, scope and possible responses*" (Renz and Smith, 2016) and the initial efforts by Hybrid CoE on the conceptualization of Hybrid Threats provided the basis for this work.

1.4.4 Case studies

Three case studies were chosen to verify the theory and research behind the conceptual model[2]: The first two case studies focus on state actors that are relevant to the current security environment in Europe and across the Atlantic. Non-state actors are discussed in the third case study.

1.4.5 Review process

The process for developing the conceptual model was backed-up by a 4-stage review process that was carefully designed to take on board the views of the various stakeholders who are among the final recipients of the conceptual model. The reason for engaging in such a thorough review process is the highly political nature of the topic and its complexity. In particular, the political dimension of Hybrid Threats might prevail over its academic foundation and, as a consequence, it was paramount to have policymakers on board even at the early stages of the model's development. In addition, the review process did not take place at the end of the drafting process. It was conducted iteratively, an agile type of development process designed to ensure that the model was aligned with the expectations of the audience of this product.

The editors of this report have work hard to accommodate the comments, correct mistakes and consider new aspects. Any shortcomings in this report are the editors'.

1.5 Structure

The report is structured as follows.

Section 2 describes the **concept** of Hybrid Threats, followed by the **analytical framework** and its main components.

Section 3 focuses on actor**s**, their objectives and their types (state, non-state). The **domains** that are targets are analysed in Section 4, followed by the **tools** that can be applied to each domain. These are analysed in more detail in Annex A. Section 5 discusses the **phases** (and the types of **activity** observed in each phase). The report concludes with a summary and outlook for future work.

[2] The case studies have been classified "EU RESTRICTED" and therefore are not included in the open version of this report.

2 Hybrid threats conceptual model

2.1 Background

This report's conceptualization of Hybrid Threats builds on the conceptualization of hybrid warfare/war in the earlier academic literature. The terms, Hybrid Threats and hybrid warfare/war are sometimes used interchangeably, which is one of the reasons why the concepts can appear confusing. In addition, the concepts have been examined through many different disciplinary lenses: international relations, strategic studies, security studies, military studies, history and political science to name a few. This multidisciplinary analytical mosaic also blurs the picture of what the concept of Hybrid Threats actually entail. In this report the concept of Hybrid Threats is used as an umbrella concept, while hybrid warfare/war is part of the activity occurring under the Hybrid Threats umbrella.

Frank Hoffman, often regarded as the father of the hybrid warfare concept, has said that his formulation draws on several schools of strategic thinking, making the concepts (hybrid warfare and Hybrid Threats) intellectual synergies (Fridman 2018). Indeed, the concepts have evolved over time. In Hoffman's concept, which focused on non-state actors like Hezbollah and Al-Qaida, their tactical and operational military activities are directed and coordinated within the main battlespace to achieve synergistic effects (Fridman 2018), and to include tactics used by transnational networks like transnational organized crime and state actors. At the time Frank Hoffman started to use the “hybrid warfare” label, it was only one of many labels, which also included “New Wars”, fourth-generation warfare and asymmetric warfare amongst others. These were being used by analysts to conceptualise changes in contemporary warfare in line with the idea that war had become “substantially distinct” from older patterns of conflict (Berdal 2011).

There are plenty other concepts that describe new forms of conflict/warfare: “surrogate warfare”, “grey zone activity”, “raiding”, “unrestricted warfare” (origins Chinese), “reflexive control” (origins Russian), “new generation warfare”(origins Russian), “competition short of conflict”, “active measures” (origins Russian), “non-linear warfare”, “asymmetric warfare”, “compound warfare” “ambiguous warfare”, “political warfare”, “information warfare”, “cyber warfare”. All of these are trying to describe very similar actions than the Hybrid Threats concept – interventions and operations targeted against states and institutions with multiple means. **The concept of Hybrid Threats, however, is the only one that raises the issue of systemic vulnerabilities of democratic systems as particular targets and clearly argues for comprehensive approach with civil-military cooperation from the very beginning.**

The concept of Hybrid Threats has been increasingly debated in the academic circles. A recent Google Scholar search for the terms Hybrid Threats and Hybrid Warfare produced roughly 9,990 results, with most publications - some 6,970 - produced since 2014 (Babbage 2019). This is an indication that the Hybrid Threats concept is here to stay. But it does not mean that the concept is fully accepted and understood. The list of question is long:

- **What are Hybrid Threats?**
- How are they positioned inside security literature?
- Is there anything new in the concept?
- What theory is behind them or should theory be developed?
- Which methodologies should be used when performing research related to Hybrid Threats?
- And where are the sources for that research?

In addition to the scientific and military context, the terms Hybrid Threats and hybrid warfare are also used in a political context which started with the annexation of Crimea in 2014. Political use of Hybrid Threats refers to manipulative, unwanted interference through a variety of tools: spread of disinformation/misinformation, creation of strong (but incorrect or only partially correct) historical narratives, election interference, cyber-attacks, economic leverage, to name just a few. Some of the activities may not even be illegal per se. Since Hybrid Threats are characterized as a combination of action, in academic analysis one action alone does not make the activity hybrid and in some cases even the threat aspect can be questioned. These actions and activities alone strictly speaking do not qualify them to be Hybrid Threats. However, they do belong to the landscape of Hybrid Threats. This means that as a political concept, Hybrid Threats can be seen as unacceptable foreign interference in sovereign states’ internal affairs and space.

This means that we have today at least three main emphases for the concepts: **military**, **academic** and **political**. All of those three emphases are good to

keep in mind. This report will put the main emphases to the academic/scientific approach while the military and political ways are integral part of the approach.

Hybrid Threats is a broad overarching concept that includes many types of activity: interference, influence, operations, campaigns and warfare/war. All of these activities can be seen as unwelcome interventions of one sort or another to a country's internal space. We need to keep in mind that the term Hybrid Threats is a Western concept used to discuss a security dilemma that states face which either have a democratic state system or are in the democratization phase. This is how the context is framed in most of the Western literature relating to Hybrid Threats. The concept has penetrated to Russian and Chinese writings today, but they did not use the name "Hybrid Threats/Hybrid warfare" before it was widely discussed in the Western security debate. The characterization of Hybrid Warfare can be found in both the Russian and the Chinese literature. They claim that Western countries are using hybrid warfare against them. This claim is often done without giving a context, with strong support for the state's official line. The references used from Western literature ignore the fact that the used references describe the action by a hostile actor against the Western countries. This fact is not mentioned.

The report identified three phases with different intensity of action and nature of the threat. This means that an escalation potential exists. These phases are explained later in this document. The activities and phases follow a rather conventional understanding, with slight modifications, of how a threat is constructed and how it might escalate. The activities and phases in themselves do not characterize a threat as hybrid, but they belong to the landscape of Hybrid Threats and are therefore also an integral part of understanding the nature of the threat element of Hybrid Threats.

A major ongoing debate concerns old (Williamson and Mansoor 2012) versus new ways of exerting interference and influence. In this debate both, those that argue that there is nothing new relating to Hybrid Threats and those that see Hybrid Threats as a fully new security challenge, have a point. As Mikael Wigell, senior researcher at the Finnish Institute of International Affairs, has argued, "*many scholars and analysts contest the utility of the hybrid label, criticizing it for conveying little that is new, for being imprecise, or outright misleading. When coupled with the term `warfare', critics warn, there is the danger of unnecessarily militarizing the language of international politics with potentially dangerous consequences*" (Wigell 2019). What this boils down to is bearing in mind that from the point of view of military-strategic thought, the analytical utility of the "hybrid warfare" concept is contested (Renz and Smith 2016)(Kofman and Rojansky 2015) and, as a tool to analyse military capabilities, its usefulness is very limited. **However, the concept of Hybrid Threats does not seek to explain policy or strategy or to analyse capabilities. The concept characterises Hybrid threats as force multipliers and/or a coercion tactic used to support a policy or strategy that is not delivering the desired results.**[3]

There is nothing new about seeking influence and trying to advance strategic interests through interference. However, in the landscape of Hybrid Threats the conventional logic is broken. We expect to experience influencing activities by states in international politics all the time. Influencing also occurs among friends and allies. Influence can even be welcomed if it is done transparently. Since Hybrid Threats are force multipliers and leverage-building mechanism as well as coercive actions, in a Hybrid Threats landscape we often see interference occurring before unwelcomed and covert influencing. This challenges the conventional view that influence is softer, essentially trying to convince somebody to do something, while interference is seen as a form of coercive action. When it comes to the Hybrid Threats landscape, we often witness interference first as action by an outside actor, carried out inside a state. The goal is to build influence through interference. It also means that an actor that uses interference to build influence is to some extent weak or in another way unable to influence other states or international organizations. Therefore, they need to "strengthen their hand". If interference has been successful new form of the influence has been built and new leverage has been created, which in turn will be used to push the target to make decisions that will ultimately inflict self-harm. This type of activity can blur the lines between policies that are difficult but acceptable, and tactics that can become a threat if not countered in time.

Mixing different types of tools is not a novel idea. When taking an in-depth look at the idea behind Hybrid Threats, it is evident that we have to consider why state and non-state actors engage in this kind of activity. Why do EU and NATO countries

[3] See for example: ``[...]so-called hybrid methods are used alongside more usual deterrence policies [...]'' (van der Putten et al. 2018)

seem to be on the defensive? And how are democracies challenged?

We need to consider that in today's international system there may well be some new tools that we have not encountered before. Old tools might be used in a new way, or in a different context from what we are used to and surprising combinations can be created. This can challenge even the best prepared countries. The state of affairs in current world politics also shapes the possibilities. New actors will emerge and old actors will resurface. In this kind of security environment we seek explanations, definitions, name to define the situation and ways to respond.

When the concept Hybrid Threats is used to describe the threats that democratic countries face in the 21st century, it can equip us with tools to understand the novelty behind such threats, and why they are used against democratic and democratizing nations. "*There is nothing new about Hybrid Threats, but today's far-reaching globalization, hyperconnectivity and digitization have vastly amplified their effectiveness and their impact. As a result, we are now living in a new twilight zone between war and peace*"(Meessen 2018). This is the reason why we speak not only about the changing nature of conflict/war, but also about the changing nature of peace.

So the question remains: What turns an action into Hybrid Threats?[4] Ostensibly, it is when a hostile actor **deliberately combines and synchronizes action, specifically targeting the systemic vulnerabilities in democratic societies** in ways that have roots in tactics with which authoritarian states, revisionist powers, rogue states and non-state networks that are seeking to undermine democratic state system have been trying to maintain their power, exert control and weaken opponents. This point is further developed in the next section. Furthermore, there is **a malign intent behind the action**, characterized by the following:

- Using multiple synchronized tools (in principle, non-military) to create linear and non-linear effects (Cullen and Reichborn-Kjennerud 2017);
- Creating ambiguity (covert and plausible deniability) and hiding the real intent;
- Exhibiting deliberate threshold manipulation when it comes to detection and response (Cullen and Reichborn-Kjennerud 2017);
- Exploiting the seams of democratic society as well as between different jurisdictions;
- Often including a distraction element, such as action in one place, and a target somewhere else (centre of gravity analysis, Schmid, 2017).

2.2 The analytical framework and its elements

There are four **main pillars**, which all need to be examined to be able to construct a full understanding of the landscape of Hybrid Threats:

- **Actors** (and their **strategic objectives**)
- **Tools** applied by the actor
- **Domains** that are targeted, and
- **Phases** (including the types of **activity** observed in each phase)

In this section the basic structure/visualization of the analytical framework of the conceptual model is introduced, which captures the above-mentioned pillars and demonstrates their links in a dynamic way. The proposed representation is powerful since it can be used in different perspectives.

One can regard this representation of the analytical framework as a storyteller. An actor (state or non-state), that has objectives but limited ability or limited possibilities to reach them, can apply a variety of tools to a series of domains to perform a certain type of activity, in order to achieve a series of objectives and affect the target. It provides a visual narrative of Hybrid Threats and it is adaptable to each country. In addition, it offers a very powerful representation for each individual actor, tool, domain or activity. For example, an analyst is able to identify visually which tools are applicable in specific domains and which domains are pertinent to specific activities. This model combined with quantitative information from intelligence, media-monitoring tools, as well as other sources of information can be transformed into a comprehensive risk assessment and resilience tool that can provide a holistic view of a country's security posture against Hybrid Threats.

Before delving into the analysis of the framework's elements, it is important to remind the reader about the baseline assumption concerning the hostile actor's **modus operandi**:

[4] This section draws on: (Cullen and Reichborn-Kjennerud 2017; Monaghan, Cullen, and Wegge 2019); (Schmid 2019); (Hoffman 2007; Mattis and Hoffman 2005; Hoffman 2010); (Fridman 2018); (Renz and Smith 2016); the Russia and Chinese literature review conducted by Cristina Juola as a part of this report's original language research.

An actor selects a combination of **tools** to achieve **strategic objectives.** These form the Hybrid Threats toolbox, which may vary depending on the actor in question (state actor, non-state actor) and its target. Each tool **targets one or multiple domains** or the **interface** between them. Tools can exploit, or even create a **vulnerability** in one or more **domains**, or take advantage of an **opportunity**. The objective can be achieved either by the **direct effect** of the tool on the domain or due to **cascade effects**. Activity in one domain may be aimed at affecting a completely different domain from the one where the activity was detected.

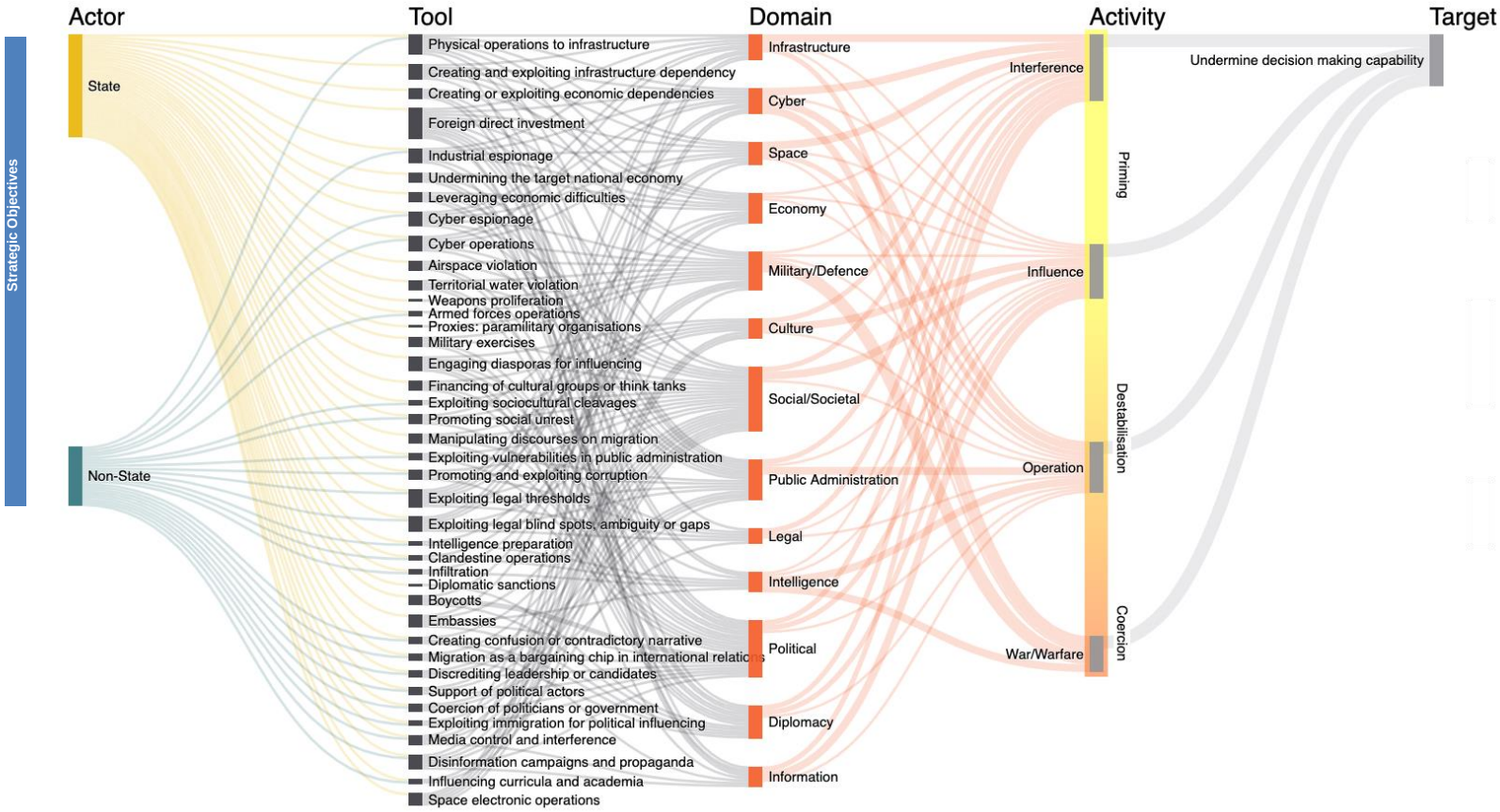


Figure 3. Visualization of the conceptual model

2.3 Potential usage of the model's analytical framework

The aim of the proposed analytical framework is not to limit stakeholders to a specific analytical perspective but rather to broaden their view and provide a powerful representation of the issue at hand. At the same time, the aim is to offer a flexible and expandable analytical framework for covering future needs. Given the fact that Hybrid Threats are dynamic in nature and hostile actors may use different tools, the futureproof aspect constitutes an essential requirement. In order to implement this notion of flexibility, the analytical framework describes the main Hybrid Threats variables that have to be considered by stakeholders, but the range of values of these variables can be adapted according to the needs of the end user:

- The analytical framework covers the **varied timeline** of **hybrid threat activity**, the plethora of **tools** that can form the hybrid threat toolbox of a hostile actor and, in parallel, the **domains** that can be compromised.
- The **flexibility** and **adaptability** of the model's analytical framework enables its applicability in various settings and for different purposes.
- Potential **actors** that have strategic interests in the focus area can be identified and closely monitored.
- The **link** between **actors** and **tools** indicated by the analytical framework provides the means to quantify the capabilities of actors and monitor their evolution over time.
- Looking at the **tools** in isolation one can immediately identify which tools have been used in the past, which are still candidates for becoming hybrid threat tools and which are the most successful ones.
- Regarding **domains**, the analytical framework allows to perform a structured analysis of their vulnerabilities. In the same fashion as tools, it will be possible to enable a time series analysis of vulnerabilities in a way that will even make it possible to quantify the progress in mitigating vulnerabilities and improving the security posture (Giannopoulos et al. 2018).
- **Early detection** of Hybrid Threats is essential for countries. The conceptual model's analytical framework offers a **blueprint** for **establishing** the **links** between **actors**, **tools**, **domains** and **objectives** to help analysts to visualize and contextualize information for the purposes of detection and attribution, and to inform decision-makers accordingly.
- The combination of tools and their application in specific domains can be an excellent **source of inspiration** for countries in order to identify **possible hybrid threat scenarios** and develop exercise scenarios. **Exercises** are an essential element in enhancing preparedness and response as a part of bolstering resilience across society.
- **Raising awareness** and establishing a common understanding are part of the process of building resilience.
- The conceptual model will provide a basis for **developing administrative structures to tackle Hybrid Threats**. The proposed conceptual model with the concept and analytical framework, paves the way for transforming security from a silo-based approach to an ecosystem-based approach where all relevant disciplines have to be addressed in a synergetic way.
- Hybrid threats require a **multi-layered response** given their supranational character. The conceptualization of Hybrid Threats provides the basis for developing strategies as well as policies that should enhance overall resilience in the long run.
- **Information sharing** and **joint intelligence** efforts are essential in order to identify threats aimed at several countries and/or organizations and alliances.
- The conceptual model provides food for thought on **future research** calls, in order to develop the necessary knowledge in areas where **gaps** are identified.

3 Actors

3.1 Strategic objectives

The international security environment is clearly changing and evolving, and Hybrid Threats are very much connected to this. Security itself as a concept is not very well defined and is also continuously developing. Around the time of the Cold War, security consisted of military issues, but since the end of the Cold War security can be defined more broadly (Baldwin 1997) involving different dimensions and levels such as the individual, family, society, state, organizations, international system, environment or humanity. Different countries and regions view the concept of security differently and hence threat perceptions are also different.

The changes we have witnessed during the last decade or so have shown that non-democratic states or states that challenge their own democracy might have difficulties in reaching their strategic goals through transparent traditional influencing using foreign policy, diplomacy, trade deals, legal agreements, and so forth. At the same time, the international world order has also been in turmoil. The great power competition is growing in intensity and scope, and competition of values and narratives has been reborn. In the Cold War time we had communism versus capitalist competition mostly based therefore on economic systems. The democratic state system was seen as the best suited ground for functioning economy but not as necessity. The end of Cold War is seen as a proof of the strength of market economy. This type of thinking has dominated the world politics for a long time. China's new path after the Cold War combining the one-party system with capitalist economic system was for a long time seen as something positive. Therefore today there is not a competition between economic system but state systems with similar economic systems. In other words, we are talking about a democratic state system versus an authoritarian state system. This means a re-evaluation of existing alliances and partnerships. It will put a strain to global trade and create new dividing lines inside societies. Consequently we now have more players seeking to gain, regain or renegotiate their status and challenge the normative world order.

Since the world has become more complex and more connected, analysis has been moving from resource-based power (the hard power of the economy and the military) towards relational power. Relational power refers to the power to change others' beliefs, attitudes, preferences, opinions, expectations, emotions and/or predispositions to act. This means that influencing in international affairs has become more complex and multidimensional, as opposed to merely being based on material power (Smith 2017). Objectives are no longer only about competition with and/or defeat of competing states but include non-state actors as well, while practices are no longer about the military acquisition of territory but about control of the population (Kaldor 2018). As a consequence direct use of a military-centric approach is virtually excluded or may not apply. In this type of situation, the idea of hybridity, combining new and old tools in a creative way, becomes an attractive tactic for those lacking the capabilities or opportunities to push their strategic interests otherwise. This type of power is termed the power of the weak. If a weaker actor can cleverly combine the tools it has, hence creating a force multiplier, it can challenge even the strongest. Moreover, in the best-case scenario for the hostile actor, the combination helps to reach its strategic goals without detection, resistance and response. At the same time, using Hybrid Threats can lower and minimize the risk of total or open escalation or conflict. This type of tactic can exploit the opportunities that a changing security environment provides, as well as create new vulnerabilities and increase leverage for future use.

If by using a combination of tools, the desired effect is achieved, it can challenge the targeted state's sovereignty while giving the hostile actor the possibility to advance its own strategic interests in a traditional zero-sum game spirit.

Hence, actors who resort to hybrid threat relating activity will try to influence the target's decision-making algorithm. The decision-making may be small-scale in the form of business deals, or local decisions made by individuals during elections, decisions made by practitioners who formulate policies and legislation, or those made by law enforcement officials. If the operation is successful, it might entail only some of the elements that make a threat hybrid in nature. This means that the activity may cause damage on its own and needs to be detected and countered at an early stage. For this reason, it is important to study the actors behind hybrid threat activity.

3.2 Actor types

The activity behind Hybrid Threats is undertaken particularly by actors with more or less authoritarian or totalitarian views of power. The aim is to target the systemic vulnerabilities of democracies while using all the tools that an authoritarian state has at its disposal. Democratic

states can also encounter interference and influence operations from democratic states, but there are significant differences compared to the actions taken by authoritarian states.

In many of the explanations and definitions relating to the concept of Hybrid Threats, both state and non-state actors are mentioned as actors engaging in Hybrid Threats activity to intervene in other states' internal space to enhance their own strategic interests, sometimes even by violent means. The use of hybrid threat activity as a support mechanism for different policies to advance strategic interests has been attributed to states like Russia, China, Iran and North Korea, to non-state actors like Hezbollah, Al-Qaeda, and ISIL, as well as to several proxy actors, transnational organized crime syndicates, ideological movements and profit-making "freelance" actors.

Frank Hoffmann makes a point about the actors and the way they construct an effective mechanism: "*Hybrid wars can be conducted by both states and a variety of non-state actors. These multi-modal activities can be conducted by separate units or even by the same unit but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict*" (Hoffman 2010, 444). The situation Hoffman talks about here refers to warfare activity. In Hoffman's analysis the actor can be both state and non-state actor. However, in most of his writings the emphasis is on non-state actors.

Ronald O'Rourke puts it a different way, but somewhat mirrors Hoffmann's views while presenting three actor groups; revisionist powers, rogue states and transnational threat organizations: "*Three main sets of challengers—the revisionist powers of China and Russia, the rogue states of Iran and North Korea, and transnational threat organizations, particularly jihadist terrorist groups—are actively competing against the United States and our allies and partners. Although differing in nature and magnitude, these rivals compete across political, economic, and military arenas, and use technology and information to accelerate these contests in order to shift regional balances of power in their favour. These are fundamentally political contests between those who favour repressive systems and those who favour free societies* "(O'Rourke 2018). In O'Rourke's analysis the rivalry between two different state system becomes clear. When it comes to state actors, he differentiates the revisionist states and rogue states. This report will only take a closer look at Russia and China, but there should also be closer look at states that O´Rourke calls rogue states. The non-state actor part is also only a snap-shot and more work on that front needs to be done to learn more about the objectives and ways non-state actors are able to challenge democratic societies.

As a consequence, it is central to get an idea of who is behind Hybrid Threats activity and why. When examining "who" – namely the actors – the picture relating to Hybrid Threats becomes clearer while simultaneously becoming more complex. There are many actors with very different strategic aims and strategic cultures. Even if one of the common denominators is to undermine democracy, there are also specific short and long-term goals at play. Hybrid threats are always tailored to the respective target and hence an operation cannot always be directly transposed from one context to another.

3.2.1 State actors

One factor that is common to actors is that they are all one way or another seeking to challenge rule of law principles one of the main core values of democracies. During the past decade, "*powerful and ambitious authoritarian regimes, which systematically suppress political pluralism and free expression to maintain power at home, have been increasingly applying the same principles internationally*" (Walker and Ludwig 2017). Authoritarian states have multiple strategies in their domestic politics to maintain and hold onto power. These domestic political strategies seem to adhere to a logic similar to the one identified in the landscape of Hybrid Threats. Authoritarian states have weaknesses that they try to cover up. One of the central weakness is that in authoritarian state system, power transition should always happen inside of the regime and therefore the first objective of the regime is preservation of power. This is one of the variables that differentiates the behaviour of authoritarian states compared to democratic states. Authoritarian regimes don't believe that influence without coercive methods will work, so they use interference to build leverage, recruit middlemen, manipulate information and create fear factors within their own countries. In international politics, the logic is that authoritarian states fear democratic states, as the authoritarian political elite see the democratic state system as an existential threat to their power position. Therefore, they need to try to undermine and weaken the capabilities of democratic states. Furthermore, authoritarian states often lack the attractiveness and/or resources to influence democratic states or alliances to co-opt them to do what they want.

Manipulative interference in the information domain is one of the main assets. Information may reshape citizens' beliefs about social fundamentals and discourage them from taking collective action against the regime (Chen and Xu 2017). This means that authoritarian countries play with information in order to instil trust in their own regime, to discourage any collective action, and to sow distrust among domestic societal actors. Furthermore, the relationship between the state and the media is completely different from that in democratic states. In authoritarian states, the media can seldom express criticism towards the government unless the government has vetted that criticism. Criticism and dissatisfaction are often expressed in different ways, such as through satire, culturally embedded humour, and memes. In democracies, the media are supposed to point out the shortcomings of the regime, act as an observer of society, and awaken societal debate. The media landscape has changed significantly in democratic states during the last decades, opening up new avenues for outside actors to interfere in debates that are domestic in nature. These changes that have effected most to create new media landscape are 1) anyone can be news creator 2) new platforms 3) the new possibilities of content confusion, 4) the increased reach of content beyond localities, national borders and cultural contexts, 5) altered media business models and revenue logics, and 6) an economic structure that is based on data, personal information and surveillance (Valaskivi 2018). All of the above-mentioned changes have created vulnerabilities in democratic societies. In countries that the information environment is more controlled the vulnerabilities are not the same, although new platforms do challenge also authoritarian regimes although not by an outside actor but by their own citizens.

Another characteristic of authoritarian regimes is seeking to control society by putting power into the hands of a "middleman". In the Soviet Union, the police had the power to control nearly every aspect of Soviet citizens' daily lives: individuals could not move, take a holiday, travel abroad, register their cars or obtain a driving licence without authorization from the police (Shelley 1996). This type of societal control translates into a strategic culture that sees any authority as an instrument of power. It also enables the real controller to blend into the background.

The use of law should not be overlooked when examining the way in which authoritarian regimes have sought to control their societies. Authoritarian regimes are typically based on the rule **by** law, where the legal system is used as an instrument of repression and social control, not the rule **of** law, where the exercise of public authority is subject to checks and balances (Ginsburg and Moustafa 2008). These insights into the internal use of law as a tool to seek legitimacy and control are highly indicative of how authoritarian regimes are using legal arguments. As Tiina Ferm has argued: "*In the era of Hybrid Threats, laws have become a toolbox used to create influence by potential hostile actors. This means that laws have a new significant but very complex role in threat maps. When an adversary operates across legal boundaries and masks its actions, the decision-making processes of the opponent are undermined*" (Ferm 2017). This fundamentally different approach to the internal use of law is also reflected in how democratic States and authoritarian regimes view and employ law in their external relations. Democratic societies typically rely on domestic and international legal processes to promote and propagate their own democratic and liberal values in the international arena. Authoritarian regimes often perceive this as a threat to their political survival and thus favour a more traditional, Westphalian approach that puts a premium on non-interference. In addition, authoritarian regimes have fewer inhibitions to using law in order to gain an asymmetric advantage, for example by turning the checks and balances of democratic societies against themselves, by leveraging the compliance of democratic States with the law, by exploiting legal uncertainties and thresholds, and by evading accountability and attribution for violations of the law.

Authoritarian states can erode the line between public and private (business and individuals) in a different way than in democratic state system and force business or individual to act in favour of the state. According to the Chinese 2015 National Security Law, states have the right to "impose broad obligations on citizens and corporations to assist and cooperate with the government in protecting national security. The principal obligations are set forth in Article 80 and include, for example, reporting information on activities that may damage national security, protecting and providing (to the authorities) evidence on activities that may damage national security, protecting national secrets, and providing data, information, and technological support or assistance to security agencies, law enforcement agencies, and the military. Citizens and corporations providing such

assistance and cooperation enjoy legal and other protections".[5]

The job of untangling commercial objectives and geo-political goals is a complex one.[6] If a state has declared that its companies are part of its other policies as in case of Russia's energy strategy published under Putin's presidency, then the link between state interests and business needs to be taken seriously. Russia's energy strategy states that "*significant energy resources and powerful fuel-energy complex are instruments for conducting domestic and foreign policy*", and that "*the role of the country on global energy markets to a great degree determined its geo-political influence*" (Lough 2011), This is not to say that companies never work with the state in democracies, but that cooperation is very different from what was described above.

When it comes to the room for manoeuvre in international politics, the fundamental difference between democratic states and authoritarian regimes, as well as actors that see democracy as threat to their interests and power and hold fundamentally different ideas about the content and rule of law (e.g. sharia law of ISIS, Westphalian sovereignty for China) needs to be highlighted. Democratic states have normative rule of law-based constraints that cannot easily be changed. The media, civil society, parliamentary overview and independent courts all act as checks and balances with regard to political and military power. This means that covert operations and clandestine operations by democratic states are more heavily regulated and thus exceptional and limited, compared to authoritarian states. Very often powerful democratic states rely much more heavily on an open power projection (economic and military) rather than on any kind of combination whose parts collectively make it useful and strong, but requires careful priming and long-term strategic patience.

On occasion, democracy promotion has been discussed in terms of Hybrid Threats. This is a false perception. Funding NGOs that promote democracy in undemocratic countries or in countries that are in the process of democratization do not have anything to do with Hybrid Threats. Firstly, this is a transparently declared aim and, secondly, measures to push authoritarian states towards democracy often are connected to regimes that have themselves committed to certain rules and principles (Helsinki final act, ECHR, Budapest memorandum etc.). Democracy promotion challenges authoritarian state systems, but through more open competition.

In their report from 2016, Dengg and Schurian provide a clear explanation of the type of force that Hybrid Threats constitute (Dengg and Schurian 2016). They take as an example Austria's involvement in Bosnia-Herzegovina, which is a policy of multi-dimensional enforcement of interests affecting the targeted countries' security sector, judicial system and economy. The policy is designed to help the country in its own efforts towards a peaceful and democratic future. The policy may not always be universally appreciated, but it is openly declared, its aims are transparent and, even if multi-dimensional, it does not combine different elements in an imaginative way, connecting dots and amplifying effects against the countries' will. In this way, Dengg and Schurian come to the conclusion that "*a hybrid threat with the same broad approach would rather aim at the contrary; internal destabilization, disintegration, public fear and disturbance, economic volatility and diplomatic isolation to enforce one's own interests. A hybrid threat must therefore be designated as a type of covert, coercive or corrupt use of force*" (Dengg and Schurian 2016).

It is worth mentioning, albeit only fleetingly, that concepts like soft power and public diplomacy have also been suggested as tools that have been used to push states' strategic interests. Both concepts are a positive force, and their ability to co-opt is based on voluntarism. Yet Joseph Nye, the "father" of the soft power concept, has pointed out that both Russia and China have got the soft power concept wrong (Nye 2013). Perhaps it is not so much that the two countries have got the concepts wrong, but rather that they understand them differently based on their own strategic culture. Public diplomacy in the Russian context is, in fact, part of its strategic thinking related to active measures and historical interference tactic, and is therefore understood very differently from the way in which public diplomacy is dealt with in the Western literature.[7] Hence, instead of soft power or public diplomacy,

[5] "China Enacts New National Security Law", Covington, July 2, 2015. Available at: https://www.cov.com/~/media/files/corporate/publications/2015/06/china_passes_new_national_security_law.pdf (accessed 20 July 2019).

[6] Henderson, James. Rosatom – competitive commercial actor or tool of Russian foreign policy? , Hybrid CoE Research Report;https://www.hybridcoe.fi/wp-content/uploads/2019/10/Nuclear-Research-Report-2019_web.pdf

[7] See, for example, the discussion on public diplomacy versus active measures in Kragh and Åsberg (2017).

we should be analysing the action and activity from the statecraft perspective.

Since this report makes an argument that Hybrid Threats are a Western academic concept and singles out some state actors in particular, Russian and Chinese strategic thinking will be examined a bit more in detail.

3.2.2 Russian strategic thinking

The Russian language literature that was reviewed for this report suggests that Russia's strategy is built in a way that individual actors have their own stake in the operation and want to pursue independent goals, which are in line with Kremlin's overall strategic objectives. Therefore, letting the strings develop independently of state control and then pulling them together could actually be seen as an inherent characteristic of the Russian strategy.

Vladimir Lepskiy, the co-founder of Reflexive Control and Processes magazine and an expert of Russian academy of sciences, has written about "*self-regulating groups*". In one of his articles he proposes a new model for controlling Russia internally. The basis of the model is clarifying a set of specified values and ideas, which would be prudent in the face of challenges from the West (economic and technological), as the subjects (the population) would be a coherent mass with a shared mindset and vision of future development (Lepskiy, 2015). In Lepskiy's view through patriotic upbringing this idea could be easily extended beyond the borders of Russia, to encompass what formerly belonged to the Russian Empire or Soviet Union. The fact that the Russian leadership has signalled out this attitude could be and has been taken as a sign by both business elites (oligarchs) and various non-state actors (hackers) that the Russian leadership is in favour of certain activities, for instance the purchase of assets in these regions. This indirect approach empowers the Russian leadership to retain strategic and operational flexibility, i.e. it does not have to stick to any rigid, detailed plans, but may pull the strings according to the actual needs and possibilities.

Lepskiy has elaborated the mechanism behind self-regulating by writing about "polisubjekts", a term mostly used in pedagogy, to analyse the interactions of pupils with one another. "Polisubjekt" in Lepskiy's writings can be understood as analysing a specific group as one comprehensive body, that has unity through the intimate interactions of its subjects and their uniform development. The "polisubjekt" functions as a single whole, as one organism based on the unity of its subjects and their interactions, capable of adapting (as a unit) to different circumstances and interacting with other subjects within the community to pursue the mutual course of development (Lepskiy, 2017). Connected to his writings on civilizational uniqueness and the Russian civilizational superiority, it could be argued that the "Russianness" is the connecting element, which ties all Russians to securing the Russian national strategic interest and strategic objectives given by the top leadership. Here naturally comes the difficult question of what in fact is "Russianness" can be seen as connecting elements and which topics the Russian leadership could be using to try to find support among Russian to that extend that self-regulation and "polisubjekts" thinking entails? Two themes emerge above others: deep sense of Russia as a Great Power and a need to protect that identity (*Greatpowerness*) as well as historical complex relationship with the Western countries and feeling of Russia as an underdog in European/Global politics (*anti-Westernism*). Both themes have given tools for Russian political elite to find those that are ready to push forward the strategic interests that today's Russian regime has.

Reflexive control

The Hybrid Threats concept is not Russian, but as Russia is seen as an actor behind the Hybrid Threats relating activity, it is good to take a look of Russian concept of reflexive control that is deeply in-rooted in Russian strategic thinking. It should be noted that in Russia military, political elite and security services are very strongly interlinked and therefore there is connection from the military strategic thinking and security services to political culture and how to seek control (Smith and Juola (eds.), 2019). G.L.Smoljan – a long-time student of Vladimir Lefebvre, the Soviet mathematician who coined the term – reflects on Lefebvre's understanding of reflexive control. The process can be described as reverse psychology: prompting the opponent to do something that he will perceive as being harmful to the manipulator, while actually taking a decision that has been prepared before-hand by the manipulator. *"Do whatever you want with me, just don't throw me into a thorny bush" said the rabbit to the fox. The fox did just that and the rabbit was saved in the thorny bush*. The opponent is manipulated into believing that the decision was made of his own free will. Reflexive control is informational influence and requires the study of human consciousness and will (Smoljan, 2016).

Smoljan identifies **manipulation** as the basis of reflexive control. It can be understood either as the

***art* of manipulating** individuals and social groups (families, social groups, countries, civilizations), or a specific ***method* of social control**. Smoljan identifies four levels of influence: direct manipulation of the target, manipulation of relationships within a social group, manipulating the scale, order and significance of certain information or events and manipulation of the target's subconsciousness (Smoljan, 2016). However, any one method applied by itself can easily be discovered. **Traceless manipulation** is therefore achieved through a **combination of methods that are constantly changing, while the overall level of intensity remains constant and just below the threshold of detectability**. Successful manipulation "*is capable of decisively damaging the normal functioning and livelihood of social institutes, governmental structures, public organizations, coherence of a community and individuals as such*" and is capable of "*deeply transforming individual, group and mass consciousness*" and so bring about changes in the moral-political and socio-psychological climate in the community (Smoljan, 2013).

Smoljan also analyses the texts of military experts who have used the term. S. Leonenko sees that reflexive control requires **sufficient knowledge about the enemy**. Him and F. Chausov have both identified reflexive control as intentionally providing tailored information that would influence the decision-making of the enemy towards a desired outcome. This is a **coordinated process** (specific place, timing, methods, aims and mission) **with an identified goal and accordingly aligned operations**, and includes the ongoing anticipation of a certain outcome. M.D. Ionov (who has earlier referred to reflexive control as "*control over the enemy*", *управление противником*), sees successful reflexive control as the **culmination point of an information operation**. This includes **pressure over the leadership** (demonstrations of military might, sanctions, ultimatums, provocations, military intelligence, raising defence readiness etc.), **confusing situational awareness of enemy through falsified information** (appearing strong where weak and vice versa – maskirovka, covert operations, bluff, provocations in irrelevant areas, hiding critical connections and links between operations, creating false distractions, leading the target out of a conflict in a way that benefits the manipulator etc.),[8] **influencing the decision-making** of the enemy by falsifying doctrines and providing falsified information, and **changing the timing of decision-making** through surprise (military) action or providing critical information that prompts early and not-well-thought-through decisions (Smoljan, 2013).

Preparations of reflexive control includes playing out scenarios of potential reactions and anticipate certain responses and outcomes. Main challenges include discovery of subversive activity by the opponent, especially considering the new technological advances that allow for more comprehensive information gathering, and the resulting change in the opponent's behaviour.

Understanding the very principle and logic of reflexive control is highly important in order to gain a deeper insight into Russian activity that is conceptualized today in the Western academic literature as Hybrid Threats.

3.2.3 Chinese strategic culture[9]

China's ambitions to expand its influence are seen in its official statements and action. It is almost as China would be building its strategy and global ambitions in line with old Halford Mackinder's heartland theory that see the global power and control to be based on the control of the sea lanes linking Europe, Asia and Africa.[10]One good example of how these ambitions are reflected in China's policies is the goal to become a "Sea Power Nation".[11] Establishing China as a sea power nation has been declared a national strategic objective[12] and it is reflected in the statements of the Chinese leadership.[13] Discussions in Chinese state-affiliated

[8] The same is described by Sun Tsu as the "art of deception" (Chapter 1*: All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.*)

[9] This section is based on insights and writings from Matti Nojonen, Professor of Chinese Culture and Society at Lapland University, Finland and Juliette Genevaz is the China research fellow at the Institute for Strategic Research (IRSEM, Paris)

[10] Halford J. Mackinder,1942, Democratic ideals and reality, National Defence University Press, Washingto DC, https://www.files.ethz.ch/isn/139619/1942_democratic_ideals_reality.pdf

[11] For an English analysis see eg. China's "Sea Power Nation Strategy", Wu Xiaoyan, Asia Paper, June 2014. Institute for Security & Development Policy, Sweden. [http://isdp.eu/content/uploads/publications/2014-wu-chinas-sea-power-nation-strategy.pdf] accessed 12.6.2019.

[12] The 18th National Congress of the CCP put forward the strategic goal of building up sea power, and the 19th National Congress announced that "adhering to the coordination of land and sea and accelerating the construction of sea power" is a strategic objective, and an important attribute of "socialism with Chinese characteristics" in the new era.

[13] President Xi Jinping for instance has recently stated: "The blue planet humans inhabit is not divided into islands by the oceans, but is connected by the oceans to form a

research institutions are being held on how "*to guarantee the accelerating process of constructing China as a sea power nation*". As with most of the Chinese statements, the discussions emphasize China's growing role in international affairs and the world's need to readjust.

One of the most known Chinese thinkers, referred to almost always in the Hybrid Threats context, that captures the subtle and indirect aspect of characterization of Hybrid Threats is Sun Zu, a Chinese strategist from the late sixth century BC. His work *The Art of War* states that "*war is deception*" involving the **art of successfully leading the enemy astray**, and ideally winning the war without the need to resort to arms. As in the Russian context, the Chinese context also includes **indirect measures**. These **indirect strategies** are important and are used in human interactions to avoid the "loss of face". In the West, such measures might easily be perceived as lying or delaying action, whereas in the East it is seen as courtesy.

In the book *On Strategy Studies* (2006) published by PLA, the authors outline three factors that determine the strategic behaviour of the Chinese military: strategic thinking, strategic environment and military capacity. In analysing Chinese strategic behaviour, they argue that the tradition, understanding and practice of stratagems is the dominating pattern of Chinese strategy work. Based on the book, characteristics of the "**supraplanning**" thinking and practices are: a) resourcefulness and decisiveness; b) deep Stratagems and distant deliberations; c) comprehensive planning and preparations; and d) flexibility and ingenuity. In addition to this dominant asymmetric approach, there also exists a deeper undercurrent of Chinese strategic thinking that is particularly applicable in the context of hybrid/strategy practices. Traditional Chinese strategic thinking provides a dialectic view of the strategic environment and work consisting of dynamic self-generating properties, such as "weakness and strength", and "clandestine manoeuvres and open operations". In this tradition concepts are not strictly defined, but rather remain borderless and ambivalent. Importantly, concepts can at the same time be nouns and verbs; in other words, they can be both abstractions of cognitive processes as well as actual practices.

This tradition stands in stark contrast with the Western tradition where concepts are always nouns and separated from practices, definitions are precise, and eventually concepts are imposed on an environment to mould or control the processes. In the Chinese tradition concepts are on the one hand abstractions of thinking, and on the other hand, practices that are part of unfolding configurations. Consequently, as concepts are parts of constantly changing configurations, they are flexible and inherently responsive to minor environmental changes. When an agent activates one concept, he immediately understands that it not only alters its surrounding environment and adapts to the changing configurations, but also instantly sensitizes and changes properties of its conceptual pair. The process is instant and organic, not causal or mechanistic. The conceptual pair, "clandestine manoeuvres and open operations", exemplifies this dynamism. The opponent is engaged with open operations that will provide opportunities to apply clandestine manoeuvres; clandestine manoeuvres will always alter the balance of power on the field, and consequently, there will be new possibilities to use open operations in engaging the opponent that will lead to novel clandestine manoeuvres. Importantly, this cycle is endless.

Three warfares concept

The Chinese concept of ***Three Warfares*** describes well the Chinese way of thinking when it comes to the activity that is place into the landscape of Hybrid Threats in the Western literature. The concept is comprised of Psychological Warfare, Public Opinion Warfare, and Legal Warfare, and was first made official in the revisions of the PLA's Political Work Regulations in 2003.

Psychological Warfare is defined in Chinese strategic theory as operations that achieve political and military aims through influencing targets' psychology and behaviour through the distribution of specific information. In this the "targets" are practitioners and decision-makers. The media used to disseminate this information varies according to operational need and can include broadcasting and person-to-person as well as the use of specialist equipment. Psychological operations cover both offensive operations against a target's psychology and defensive operations to counter enemy psychological attacks. Methods of Psychological Warfare include deterrence, coercion, deception, instigation, seduction, bribery, inducement and confusion. It should be stressed that these methods arise from theoretical and doctrinal descriptions.

community with a shared future, where people of all countries share weal and woe," supporting the point that countries should cooperate on mutual security threats. Lu Hui, "Xinhua Headlines: Though oceans apart, a shared future across blue waters", 8.6.2019, *Xinhua*. [http://www.xinhuanet.com/english/2019-06/08/c_138126882.htm] accessed 14.6.2019.

Public Opinion Warfare is defined as operations to influence both domestic and international support by the use of selective information delivered through different media. Here the theories relating to how to control masses applies. Mass media including the internet and traditional sources such as broadcasting and newspapers are the main sources of disseminating information; however, more pervasive methods such as the use of international organisations and academic forums can be used to influence more targeted audiences. Achieving social harmony according to the Chinese mindset has big differences to the liberal democratic system. For instance, the values of equality, transparency and free speech are replaced by values of tight social control. Doug Young has researched the role of media in the Chinese context – which differs greatly from that in liberal democracies. Rather than allowing media to pinpoint inadequacies of social order and playing the role of the "watchdog", the CPP views media as a tool for influence, control and intelligence gathering. Mass media is used to frame public opinion in a way that enhances the positive, credible and legitimate image of the CCP and China[14] and supports CCP objectives on national and international levels. State media outlets work as a mouthpiece of the CCP and they are copied by other media outlets. Media bureaus get instructed from the state level on what to report and what not. The aim is to "*create an impression of consensus in a number of ways …. to ensure that all media outlets carry out the same message*". (Young 2013, p39) Even international issues can be portrayed in a way to support CCP objectives, which means that state media controls public reactions to international events (examples include boycott of Chinese citizens of Japanese and South Korean goods after certain events in state-to-state relations). Specific tools that are used by the CCP-led media to frame public opinion can be picked up in Young's analysis. These include direct top-down control, a bias towards positive stories, heavy use of slogans to convene the message and censorship of negative stories. (Young 2013)

Legal Warfare is used to describe the technique of manoeuvring to gain legal superiority by using or modifying domestic and international law to gain political initiative or military advantage. Rather than viewing law as a method of rational order-making, legal warfare looks for ways to use legal advantage to influence targets by delivering the effects of defeat, deterrence or defence via legal means, including through national or international arbitration.

3.2.4 Non-state actors

State actors are the most talked about in the context of Hybrid Threats today. However, the concept originated from actions engaged in by weaker non-state actors to challenge stronger parties through the use of smart tactics. As states are still the most powerful challengers of another state or alliance, we largely think in terms of countering states in the Hybrid Threats landscape. But it would be a potentially fatal omission if non-state actors were not treated with equal seriousness.

A quick review of the existing literature on Hybrid Threats reveals that the specific feature of non-state actors in hybrid threat campaigns has not been the central focus for researchers and academics, despite the concept originating from non-state actions. Indeed, one of the first uses of the concept of hybrid warfare was related to non-state actors. William Nemeth studied the first Chechen War (1994–1996) and how the confluence of modern political theory and technology with traditional ancient customs and ideologies in a decentralized, devolving society created a unique ability to wage war, which he then called hybrid warfare (Nemeth 2002).

Non-state actors in the Hybrid Threats context constitute entities that play a part in international relations and that exercise sufficient power to interfere, influence and cause change without any affiliation to the established institutions of a state. The role of non-state actors has changed along with the changes in international politics as a result of globalization and new connectivity. The changes have bolstered network-based action to such an extent that it can even challenge nation states and put pressure on democratic governments. Non-state actors exert influence through interference, sometimes slowly and in a subtle way, as the case study on Salafis in Sweden shows.

3.2.5 States operating through non-state entities

Typically, the approach adopted by states acting through non-state actors for hostile purposes is referred to as "proxy warfare". When Frank Hoffman, inspired by Nemeth, introduced the concept of hybrid warfare into the public debate in

[14] Front pages are reserved for politicians and their positive contributions, bias towards positive stories – the aim is to raise legitimacy and credibility of leaders.

2005 (Mattis and Hoffman 2005), he connected it to the Iranian use of Hezbollah in its long-term, low-intensity conflict with Israel. More recently, attention has been paid to the proxy warfare challenges brought to the forefront by state support for fighting rebel factions in contemporary conflicts such as those in Iraq, Syria and Yemen to either promote their own policy interests and/or counter those of other states.

States acting through third parties, or activity cloaked thus, for the purposes of influencing and exercising hostile measures against other states is certainly not a new phenomenon. Using other entities to influence, manipulate and obstruct can have several advantages, providing insights into the conceptual understanding of non-state manifestations of Hybrid Threats campaigns. The active non-state entity can take many different shapes and may be manifested through a direct construct by the foreign state or a long-term ally formed through established relationships and mutual dependencies. It can also be shaped through a short-term alliance for achieving common objectives in relation to a local or specific issue, or simply through the exploitation of "useful idiots" that may not be aware that they serve a purpose in a Hybrid Threats context. States with a strong and long-term interest in influencing, manipulating and creating events in other countries to promote their interests will probably seek to utilize all of the above in a systematic fashion.

3.2.5.1 States acting covertly

States directing activities through non-state entities exploit the opportunity to conduct activities of a harmful nature against other countries covertly. This has the advantage of making it more difficult for the targeted states to detect the harmful state related activity and respond before it occurs, but also of impeding the targeted state's ability to attribute the harmful operation to the foreign state behind the event or series of events. Acting covertly through a third entity might even contribute to the foreign state being able to achieve its desired objectives without the targeted state being aware that it has been subjected to harmful activities. The Russian Federation's use of the Pro-Russian nationalist group Night Wolves MC in the early phase of the annexation of Crimea, in February 2014, can serve as an example. The Night Wolves Sevastopol chapter was utilized to collect intelligence, distribute propaganda and organize protests prior to the annexation, thus serving as an important covert part of the Russian offensive capability. During the annexation, the Night Wolves came to play a small but active part in armed operations and intimidation measures, hence providing another useful advantage of using entities with an established capacity for employing violent means.

States acting in a covert mode also provides for the ability to **deny and refute** any potential accusations of involvement in the events. This would be convenient for foreign states with an interest in performing activities in politically sensitive areas. The deployment of Private Military Corporations (PMCs) for risky operations in conflict zones, or in support of regimes where deniability of involvement is of vital interest, serves as a relevant case. Many states have employed PMCs in conflict zones over the years and a recent case of relevance from a European perspective would be the Russian PMC Wagner Group, which has reportedly been observed in the conflict in Eastern Ukraine as well as in Syria, South Sudan, the Central African Republic, and most recently in Venezuela. As Margarethe Klein has observed: "*Although Russian PMCs form a diverse group of actors, they provide the Russian leadership with a useful instrument for acting as a force multiplier for the Russian armed forces, for pursuing hybrid operations under the guise of plausible deniability, and for making inroads into regions from which Russia has been absent for a long time"* (Klein 2019).

Although the Wagner Group has the highly unique feature of being intimately linked to the Russian military intelligence and security structures through individuals in the corporate leadership, and sources of funding, training, equipment and transport to the area of operations, PMC entities in general are always difficult to identify when they appear on the ground. Professionally trained, well-equipped and well-organized personnel without any form of identifiable marking, acting in an area of operation with support and direction from a foreign state intelligence service, create challenges for the targeted state in terms of understanding the nature and scope of the threat. The growing market for private security corporations for hire, potentially by state regimes with dubious objectives, has become a source of considerable concern. This is particularly worrying as many corporations recruit professionally, state-trained and experienced individuals who, while in the service of the corporation, may very well end up in situations where they contribute to harmful operations against their own countries.

3.2.5.2 Gaining access to critical sectors and specific skillsets

Another feature of relevance for Hybrid Threats activities is the opportunity to deploy entities in the target state with certain skillsets suited to specific activities. The ability to enter the market within critical infrastructure sectors in the targeted state would be a highly useful advantage in order to exert influence and conduct obstructive measures that would have considerable consequences. Access to vulnerable sectors in the target state can be gained through direct investments by existing businesses or the creation of new business entities for the specific hostile purpose. The Airiston Helmi real-estate company in Finland is an instructive case that could potentially have served as a very suitable overt entity for making strategically important investments and for preparing properties for future use to the detriment of the targeted state. Besides the occurrence of international financial crime schemes, this case entailed Russian citizens purchasing properties with highly unusual security features, advanced technical equipment and exceptional capabilities for housing a large number of individuals and large transport platforms in a strategically important geographical area in the Finnish archipelago. The properties are located in an area traversed by the majority of cargo vessels en route to Finland, where the Finnish coastal fleet is based with all the naval combat vessels, and in the vicinity of key seabed communication cables. This case serves to clearly illustrate one of the many features of Hybrid Threats manifested through non-state actors when thinking about how foreign states can act through third parties to influence, interfere in or obstruct states' affairs to give rise to negative consequences or to establish the ability to do so when desired.

Another example of states exploiting the skillsets and access procured by private entities for influencing activities was the Russian interference in the US presidential elections in 2016. With the support of data from highly qualified business companies such as Cambridge Analytica and the use of information outlet entities such as WikiLeaks, the Russian intelligence-linked hacker entity known as the Internet Research Agency was able to exert considerable influence over American voters in regard to the two presidential nominees (Lapowsky 2019; Mueller 2019).

Leverage building through overt business entities, often operating within legal boundaries, makes it difficult for law enforcement and security services to identify such occurrences and, if they do, to allocate resources to take appropriate action.

3.2.5.3 Exploiting criminal networks

Even criminal organizations with operations and networks in the target state are a very useful entity for foreign state activities in a Hybrid Threats context. Exploiting criminal organizations could include utilizing established smuggling networks, the ability to provide forged documents, financial crime schemes or simply their ability to threaten, intimidate, pressure or harm strategically important individuals or groups in a specific situation for political purposes. The Iranian relationship with the powerful and multifaceted terrorist organization Hezbollah is a case in point, where the organization's operatives have been present and active in Europe for many years as one part of its criminal enterprises and terrorist activities, with tentacles extending to almost every corner of the world. As such, it has become a useful entity with which Iran can track potential targets of strategic interest and intimidation operations.

States' exploitation of non-state actors embedded in the target state or target audience as a force multiplier will most likely be an integral and growing part of Hybrid Threats manifestation in the future.

3.2.5.4 *Non-state actors using hybrid means*

Between 2002 and 2014, when the concept of Hybrid Threats became a widespread political term, it was used also in connection with transnational organized crime, terrorism and insurgency.[15] Hybridity from this point of view is characterized by the interpenetration of a wide range of non-state actors including any combination of insurgent or terrorist networks; organized crime groups; social groups such as clans, tribes or ethnic groups; and ideologically or religiously motivated organizations, all of which may be backed covertly or overtly by states and/or legitimate businesses (Schroefl and Kaufman 2014). Few of these extremists, terrorists and criminal groups have thus far conducted operations against Western states or indicated a capacity and strategic proclivity to launch coordinated and systematic campaigns by different means to target vulnerable sectors in society for their own objectives. Most terrorist and criminal groups operating in Western states tend to rely primarily on violence or the threat of violence and hence do not reach the strategic threshold to present Hybrid Threats since there is not a creative

[15] See Vergani and Collins 2015; Pacheco 2009; Bunker 2013; Fernández 2009.

way to combine a diverse range of means across multiple domains.

Advances in social media and cyber tools have increased opportunities to influence and manipulate target audiences, and they have clearly been used in hybrid campaigns by state actors. To some extent, this is also the case in relation to organizations such as the Islamic State, which are guided by radical, anti-democratic agendas to punish "infidels" and the "heretic lifestyle" in the West, and to promote their agenda among Western populations. But the ability to perform such actions in order to inflict harm against Western societies has thus far been limited, apart from those terrorist attacks perpetrated by sympathizers inspired by the propaganda and narratives spread by such organizations. However, one example of activities conducted by radical followers of conservative Salafi/Jihadi ideology can serve as a clear and growing challenge of a Hybrid Threats nature.

When harmful activities occur in a coordinated and systematic manner, it is highly likely that there will be manifestations through non-state actors. Our initial ability to understand whether or not these activities are related to covert state direction and support will be very limited. From several viewpoints, not least the political one, knowing who the initiator of harmful events is, will be of utmost importance for determining the response and how to counter these threats in the future. For this reason, it is imperative for academics and researchers to not only focus on current events linked to states within the Hybrid Threats domain. It is also important to achieve an increased understanding of the diversity of Hybrid Threats in order to be able to meet the ever-changing manifestations of future security challenges and to limit their impact.

4 Domains and tools

As mentioned earlier, hybrid threat activity targets a state in multiple domains by applying **combinations of tools.** Each tool targets **one or multiple domains**, or the **interface** between them, by creating or exploiting a **vulnerability** or taking advantage of an **opportunity**. This is why it is important to identify the areas of interest or critical functions that a state should ensure are resilient against hybrid threat activity, as they relate strongly to national security and the decision-making capability of a state.

The list of domains is presented below, while potential tools of hybrid threat activity are described in Section 4.2 and in more detail in "**Fehler! Verweisquelle konnte nicht gefunden werden.**".

4.1 Domains

In selecting the domains for the conceptual model (see Figure 4. Domains), the following main aspects were considered.

(a) In all groupings and acronyms[16] that stand for instruments of national power, the underlying logic has stemmed from the military. Before the introduction of the concept of Hybrid Threats, the mainstream approach has always included military intervention and physical occupation as a precondition for taking over an independent country. According to this report, substantial control by an actor over the target can be achieved without necessarily engaging in open military activity. Alternatively, actors may use a hybrid threat strategy to weaken the target state with no intention of physical control in any way. This means a military-centric approach may not deliver an accurate picture of the whole spectrum of current threats and challenges.

In all conceptual work, it is important to strike a balance between granularity and the analytical value of generalization. It might be worth noting that there are still several subdomains and all of the case studies demonstrate combinations of different domains, so alternative approaches exist both in consolidating and expanding the list of domains.

(b) Currently, there is no prevailing or universal approach to structuring instruments of national power. There is no compelling reason to select any existing concepts from the multitude of approaches that are used in parallel and that do not fully comply with the requirements of describing the Hybrid Threats.

(c) Although the number of domains (thirteen) might be considered high, reducing the number and merging them into larger categories would fail to convey the complexity of the coordinated activity that has been described in the three case studies.

(d) Last but not least, this list was based upon a decision by the expert team and the consensus within the group that emerged through the iterative process of creating the model and compiling the report. Moreover, it has been validated though a series of review meetings with external reviewers.

It should be stressed that this remains an open list, and is not the last word by any means. Users of this conceptual model may choose to limit the number of domains by merging some, or increasing the number by further refining the detail. An accurate understanding of each specific situation will be the cornerstone of an adequate response and of bridging the gaps in resilience.

Not every tool and activity that targets a domain may be classified as hybrid threat. Similarly, not all assets within a domain are equally important for a hostile actor. Hybrid threat activity, targeting the domains and using the domains as a medium, described in the following sections would be qualified as such by the simultaneous use of multiple tools, in a coordinated campaign designed to exploit vulnerabilities or opportunities and, consequently, to undermine the opponent's decision-making process, while maintaining a degree of plausible deniability.

In the sections that follow (4.1.1 to 4.1.13), each domain is briefly described, highlighting which components of the domain may be targeted by hybrid threat activity, as well as the links between domains.

[16] Examples include:
DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement Instrument of National Power ("National Military Strategic Plan for the War on Terrorism" 2006; U.S. Joint Chiefs of Staff 2017).
MPECI: Military, Political, Economic, Civilian and Informational Instruments of power, MCDC Countering Hybrid Warfare Project (Monaghan, Cullen, and Wegge 2019).
PMESII: Political, military, economic, social, informational and infrastructure vulnerabilities of a target system, MCDC Countering Hybrid Warfare Project (Monaghan, Cullen, and Wegge 2019).

The domains should not be examined in isolation, as an effect on one domain may cause cascade effects in another. This is particularly important when considering the effect of hybrid threat activity on a domain. Earlier MCDC work observes that "a series of synchronized, low-observable or unobserved events […] normally only become apparent once their cumulative and non-linear effects begin to manifest themselves". In MCDC's analytical framework (Monaghan, Cullen, and Wegge 2019), action targeting one domain is further analysed to allow for the depiction of the first and second-order effects on other domains

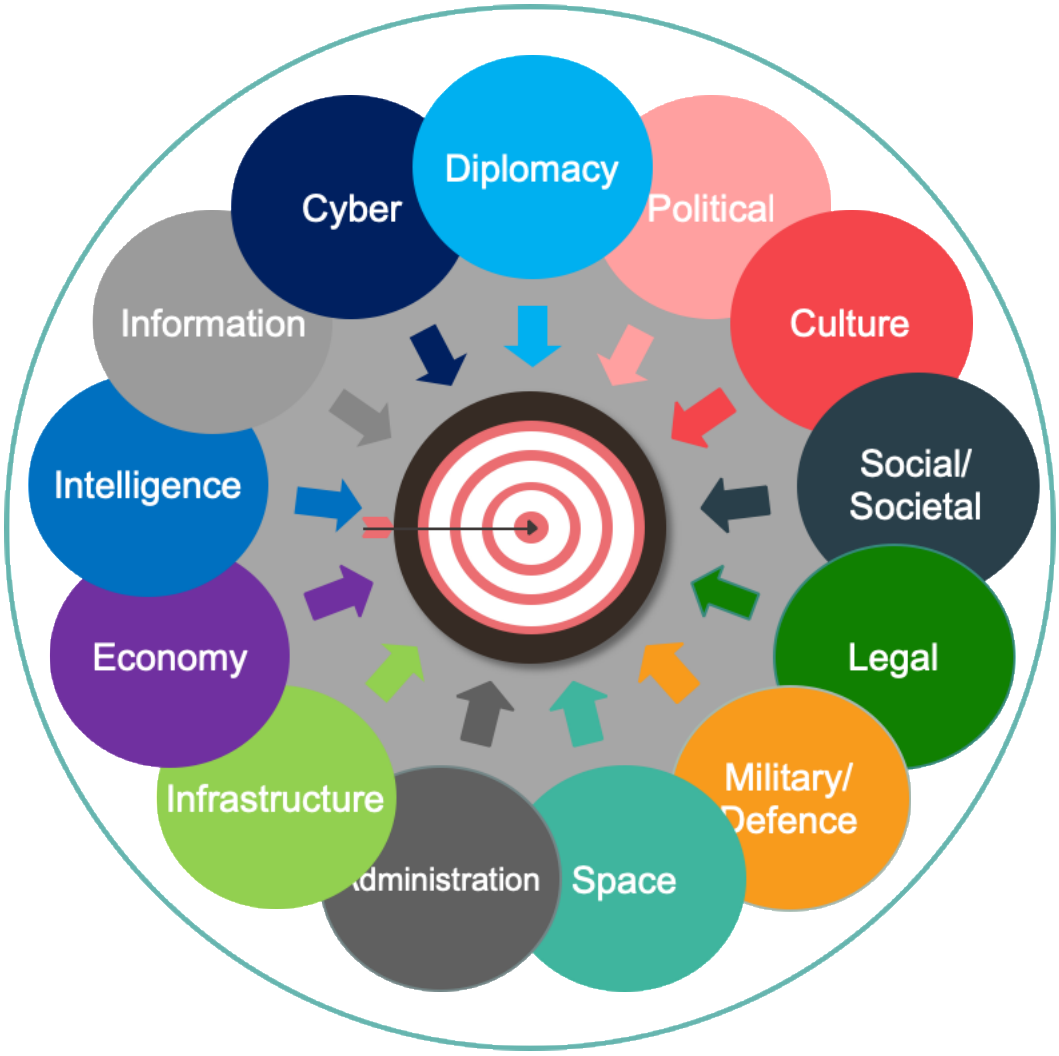


Figure 4. Domains of the conceptual model[17]

4.1.1 Infrastructure

While there is no commonly accepted definition of critical infrastructure (CI), all definitions emphasize the contributing role of CI to society, or the debilitating effect in the case of disruption.[18] A European definition regards 'critical infrastructure' as:

"An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (Council of the European Union 2008).

[17]Figure 5. got its inspiration from Schmid, Johann. "Hybrid Warfare – a very short introduction". COI S&D Concept Paper. ISBN: 978-952-7282-20-5, Helsinki, May 2019, page 7.

[18]CIPedia©, 2019. Available at www.cipedia.eu (Accessed 21 July 2019).

The more recent NIS directive (European Parliament and Council 2016) places the emphasis on the provision of essential services and their continuity. Irrespective of the nature of the hostile actor (state or non-state), infrastructures, essential services and supply chains can be attractive targets in order to intimidate and apply pressure.

The activities could aim to:

(a) degrade the quality of the offered goods and services (e.g. reduce availability, reliability)

(b) destroy key parts of an infrastructure,

(c) increase their cost of operation,

(d) affect the demand, putting the infrastructure under pressure,

(e) reduce/remove redundancies and cause one-sided dependencies on the hostile actor,

(f) acquire or limit access to key resources needed for their functionality (raw materials, technology, expertise, etc.), and more.

Any tool that can create or exploit a vulnerability in an infrastructure (home-grown vs injected vulnerabilities) and achieving one of the above effects could potentially be used as part of the hybrid toolbox. Note that vulnerability is often sector-specific, can also be temporal (e.g. increased demand for a service due to a natural disaster[19] or service degradation due to normal ageing of the infrastructure), or recurring (cyclical) based on specific conditions.

The infrastructure domain can be regarded as a 'mega-domain', as it includes several sectors. When using the model, it could be split into several subdomains, if needed.

4.1.2 Cyber

The cyber dimension plays an exceptional and highly specific role concerning Hybrid Threats today, not least because anything of significance that happens in the real world, including every political and military conflict, will also take place in cyberspace. For national security planners, this includes cybercrime, propaganda, espionage, influencing, terrorism and even warfare itself. The nature of national security threats has not changed, but cyberspace provides a new delivery mechanism that can increase the speed, diffusion, and power of an attack, and ensure anonymity and undetectability. The low price of entry, anonymity, and asymmetries in vulnerability mean that smaller actors have more capacity to exercise power in cyberspace than in many more traditional domains of world politics.

This domain refers to the information environment, consisting of the interdependent networks of information technology infrastructures (including hardware, software, data, protocols), and information including the internet, telecommunications networks, computer systems, and embedded processors and controllers.[20] The tools that can be applied by an hostile actor aim at causing degradation, disruption, or destruction of the networks, or aim to access data and information. Access to information may also be the objective of an hostile actor in order to collect intelligence and reduce detectability.

4.1.3 Space

Space-based services include navigation, communications, remote sensing, and science and exploration (Defense Intelligence Agency 2019). There is increasing concern about hybrid threat activities in space due to the fact that several countries have been developing counterspace capabilities with multiple state actors (Weeden and Samson 2019; C4ADS 2019).[21] The effect of hybrid operations in space not only affects the military/defence domain, but can also have a significant impact on civil commercial activities, as these increasingly rely on space capabilities. In fact, most of the tools that can target the space domain exploit the linking of space assets to other domains described in this report, and the potential cascade

[19] Natural hazards in particular have been found to pose a threat to vulnerable infrastructure. Impacts can lead to extensive service outages and supply-chain effects, major accidents with hazardous-materials releases (so-called Natech accidents), as well as possibly prolonged service recovery times (Krausmann, Girgin, and Necci 2019; Karagiannis et al. 2017). This problem is exacerbated by climate change. What is more, natural hazards, such as earthquakes, floods or storms can cause multiple and simultaneous infrastructure incidents over extended areas, increasing the risk of cascading effects. This can create a heavy drain on limited emergency-response resources (including the police and military) in situations when power, water, fuel etc. might not be available due to the natural-disaster effects (Krausmann, Necci, and Girgin 2017).

[20] Based on DOD Dictionary of Military and Associated Terms (June 2018).
In the military literature, the term 'cyber' is used in a wider sense, referring to the use of the internet and computer technologies for operations in the so-called fifth domain. NATO recognized in July 2016 that cyberspace is a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea (and even also in space). 'Cyber operations', 'cyber war' and 'cyber attacks' are examples of such operations, depending on their intensity. For a classification of 'cyber conflicts', see Schmitt 2012.

[21] For China's and Russia's counterspace capabilities, see Harrison, Johnson, and Roberts 2018; PSSI 2018.

effects if they become compromised, even temporarily. This domain is closely related to the military/defence, economy, infrastructure, information and intelligence domains (sections 4.1.1, 4.1.4, 4.1.5, 4.1.10, and 4.1.13).

4.1.4 Economy

The economy as a domain of Hybrid Threats is defined as the production, distribution and consumption of all goods and services for a country, and includes its economic development and distribution of wealth (NATO 2013). Economic statecraft, or the pursuit of foreign policy objectives by leveraging the security externalities of economic interactions (Baldwin 1985; Norris 2016; Reilly 2013) has been a traditional source of state power and influence.[22] In today's globalized society, economic relationships are inherently susceptible to state-borne manipulation, and are routinely exploited by several countries as a means of first resort for strategic purposes (Blackwill and Harris 2016; Iancu et al. 2016). Economic policy instruments such as sanctions, taxation, embargoes, trade agreements, asset freezing, sterilized interventions, subsidies, tariffs, sovereign lending and debt forgiveness are all employed in this context (Fabre 2018; Norris 2016).

In light of the need to maintain deniability and avoid the provocation of an open military conflict, the exploitation of the economy domain would rarely have the same objectives as an open military campaign.

The objective of a hybrid threat action on the economy domain is to comprehensively weaken the target state, undermining public confidence in democracy and the government. For instance, economic measures or policies can be used to add political pressure (Blackwill and Harris 2016), or economic coercion can seek to modify a state's foreign policy stance, or to weaken the resilience of its economy, society and security (Iancu et al. 2016). The priming phase can last for decades (see section 5.1).

The tools associated with Hybrid Threats seeking to affect the economy domain are none other than the instruments of international economic policy. The ubiquity of these issues in international relations is what makes the economy one of the first possible targets of a hybrid threat campaign. At the same time, it is what allows for a prolonged priming phase and makes it so difficult to tell whether an action constitutes part of Hybrid Threats or not.

In the context of Hybrid Threats, the economy domain is closely related to other domains. These diverse and complex relationships stem by and large from the activities of firms that may be controlled or influenced by an actor prone to use Hybrid Threat activity. First, energy and other infrastructure dependencies may generate economic dependencies and/or become a tool for exerting economic pressure. For instance, Russia has been leveraging its position as a natural gas exporter not only against Ukraine, but against the European Union as well. Second, infrastructure development usually entails capital projects that attract Foreign Direct Investment (FDI), the intent of which may be dubious. Third, economic difficulties and/or inequalities can be leveraged to influence the outcome of elections (Giles et al. 2015). Fourth, economic difficulties, such as a balance of payments (BOP) crisis or rising sovereign debt, can be used as a narrative to undermine the legitimacy of a government or even to justify the actions and/or geopolitical position. Lastly, corruption in the political and social spheres undermines economic security, as the affected country becomes less competitive in the global market.

4.1.5 Military/Defence

In military defence operations, the task of the military is to preserve independence as well as the inviolability and unity of the homeland territory, particularly for the maintenance and defence of sovereignty.

In times of peace, the military joins civil authorities for exercises and assistance purposes. In order to be able to respond quickly to terrorist attacks, to assistance requests from civil authorities (in the event of flood damage, avalanches, etc.), as well as to changes in the immediate vicinity of the home country, military forces need to maintain a presence.

A country's military and defence capabilities constitute a cornerstone of its own existence and projection of power. In both recent and ancient history, superpowers have combined economic with military power and enhanced defence capabilities. Furthermore, military capabilities are a prerequisite for a country to be perceived as an important player in the global geopolitical arena. There are examples of countries that are regarded as superpowers (e.g. Russia) despite their economic weakness, while other countries with a much stronger economy and potential for growth are not regarded in the same way due to a (maybe only

[22] Blackwill and Harris employ the term "geoeconomics", an adaptation of "geopolitics" (Blackwill and Harris 2016).

perceived) lack of capabilities in the military domain. Compromising a country's military and defence capabilities can be a very effective means of increasing influence, exerting pressure, and, in certain cases, preparing the ground for future military operations. Compromising a country's military defence capabilities triggers a reaction by the affected country leading to increased defence costs and depletion of resources. It is an implicit way of exerting also economic pressure. It can also push the target to escalate by responding to action that is seen hostile. This might be the goal of the action.

4.1.6 Culture

This domain entails the use of cultural statecraft by an aggressor to support an objective through hybrid threat activity. The scope of cultural statecraft may be internal, external or both. Internally, cultural statecraft involves "the use of cultural and civilizational themes in an effort to define fundamental elements of a national identity", whereas as a foreign policy strategy, it endeavours *"to promote culture as a means to project an attractive image abroad"* (Wilson 2016).

Although similar to the concept of soft power (Nye 1990), cultural statecraft differs fundamentally in origin. Whereas soft power is born out of an autonomous civil society, cultural statecraft is essentially a state endeavour. It targets specifically issues belonging national identity, history and religion. Like cultural statecraft, the culture domain of Hybrid Threats originates from the state. However, it is aligned with and intended to support hybrid threat activity.

4.1.7 Social/Societal

The social/societal domain is used typically to generate, deepen or exploit sociocultural cleavages, which will spawn the social upheaval necessary for hybrid threat activity to proceed or succeed. Contentious issues, such as unemployment, poverty and education are always subject to debate in Western societies, and thus offer an easy target. However, issues that can create or sustain a crisis are particularly attractive. Examples include the recent economic downturn, irregular immigration and terrorist attacks (active shooter incidents, cyber-attacks, CBRNE incidents).

The ultimate goal of the action in this domain will be to influence the way society works in the target state to create favourable conditions for hybrid threat activity.

4.1.8 Public Administration

Public administration is purposefully construed in its widest possible sense as "*the process of translating public policies into results"* (Kettl 2018). The politics-administration dichotomy is emphasized as a fundamental feature of European societies (Wallace, Pollack, and Young 2015). In other words, public administration exists to implement the law and rules. Although clear in theory, this concept may be hard to apply in practice. First, in interpreting the law to bring it to life, administrators may inadvertently make value judgements that may be political in nature. Second, public administration naturally contributes to policymaking by evaluating existing policies and organizing the formulation of new ones.

4.1.9 Legal

For present purposes, the legal domain refers to the aggregate of legal rules, actions, processes and institutions, including both their normative and physical manifestation, that are or may be utilised to achieve legal or non-legal effects in the context of a hybrid threat campaign (Sari 2019a).

Law is a societal system. This means that all states, together with a large number of other national and international actors, rely on law to pursue their interests. Authoritarian states are no exception: they regularly use law for a variety of reasons, including as an integral component of hybrid threat activities.

An actor may choose from a broad range of legal tools to support a hybrid threat campaign, including exploiting legal thresholds, gaps, complexity and uncertainty; circumventing its legal obligations; avoiding accountability; leveraging rule-compliance by the targeted state; exploiting the lack of legal inter-operability among targeted nations; using its own regulatory powers under domestic law; and utilizing the law and legal processes to create narratives and counter-narratives (Savolainen 2018; Sari 2019a).

While some of these tactics may involve violations of the applicable rules of domestic or international law, not all of them do. What distinguishes the use of law as an instrument or component of Hybrid Threats is not necessarily its illegality or illegitimacy as such, but the following features.

First, actors that want to undermine democratic or democratizing states employ law with the aim of targeting specific vulnerabilities in democratic societies. For example, relying on the right to freedom of speech creates space for disinformation campaigns. Second, law is utilised to achieve

disruptive, subversive or other malign effects in or against the targeted nation that undermine its interests and further the interests of the actor Third, in many cases law is employed in a manner that is abusive or otherwise corrosive to the rule of law. Fourth, law is often used to achieve effects in other domains, in particular (but not only) in the information space, while activities in other domains may be designed or exploited to achieve effects in the legal domain.

Overall, authoritarian actors are employing law as an instrument or component of hybrid threat activities in order to legitimize their own behaviour and maintain their own freedom of action and to delegitimize their target's behaviour and restrict its freedom of action.

4.1.10 Intelligence

According to Lowenthal (2015, 10), *intelligence is the process by which specific types of information important to national security are requested, collected, analyzed and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities*. Intelligence provides decision-makers with situational awareness, a must for strategic and security-related decisions. Therefore, intelligence activities need to be designed and implemented to meet the need identified by decision-makers or implied by their policy guidance.

Intelligence in the modern world is derived from several disciplines, including Open-Source Intelligence (OSINT), Signals Intelligence (SIGNIT), Geospatial or Imagery Intelligence (GEOINT or IMINT), Measurement And Signature Intelligence (MASINT), Cyber Intelligence (CYBINT) and Human Intelligence (HUMINT).

An actor using Hybrid Threats may use intelligence in two principal ways. They will usually employ their own intelligence capabilities to support planned or ongoing hybrid threat activities, or they may attempt to affect the target state's intelligence operations. In both cases, the actor seeks to undermine the target state's capability to develop and maintain situational awareness.

To the extent that intelligence can support and has been used to support a wide range of hybrid threat activities, it can be understood to be related to all other domains. Nevertheless, it has a strong connection to the information domain (section 4.1.13), mainly because disinformation campaigns can be orchestrated or facilitated by intelligence agencies. By the same token, CYBINT and MASINT play an increasingly important role in intelligence gathering. Therefore, this domain is strongly related to the cyber and space domains as well (sections 4.1.2 and 4.1.3). In addition, the purpose of intelligence support for hybrid threat activities, whether it is used to implement clandestine operations in support of hybrid threat activities or to blur the target state's situational awareness and/or create deception, is to undermine the decision-making capabilities at the political level and the ability of public administration to implement policy (sections 4.1.8 and 4.1.12).

4.1.11 Diplomacy

Here, diplomacy is construed in its international dimension as the conduct of international relations. Foreign policy has traditionally focused on security (Wallace, Pollack, and Young 2015). In fact, normative theories of international relations justify war as a defensive measure against provoked aggression, subject to the constraints of proportionality and the protection of non-combatants (Viotti and Kauppi 2012).

Hybrid threat activities, especially those in the diplomacy domain, are designed to create divisions either in a state or international level, support any information campaigns and meddle in decision-making process. The following sections discuss the tools employed in this context, including diplomatic sanctions, boycotts, the use of embassies and the creation of confusing or contradictory narratives.

The diplomacy domain has strong ties to the political domain (discussed below in section 4.1.12). Although foreign policy has tended to be regarded as distinct from domestic politics, the two are very closely intertwined, mainly because of the need for negotiators in international politics to have their decisions ratified by their domestic constituencies. Therefore, diplomacy and domestic politics become a two-level game, requiring decision-makers to develop "win sets" of solutions that can be defended in the international and domestic arenas (Putnam 1988). In authoritarian states the foreign policy is to support the domestic politics. Diplomacy domain in this case becomes almost as a battleground for negotiated reality.

Besides its close relationship to domestic politics, diplomacy in the context of Hybrid Threats is also related to the economy (section 4.1.4), social (section 4.1.7) and legal domains (section 4.1.9). Diplomatic sanctions and boycotts are either predominantly economic in nature or are designed to inflict a major impact on the economy of the target state.

4.1.12 Political

In the context of Hybrid Threats, the political domain encompasses the actors, organizations and institutions that exercise authority or rule within a territory through the application of various forms of political power and influence (NATO 2013). In modern democracies, officials are either elected by the people or their representatives or appointed by those elected. The political system is expected to be representative of the cultural, historical, demographic and sometimes religious factors that form the identity of a society. Citizens' rights, elections and parliamentary accountability are usually the distinguishing factors in a democracy (Newton and van Deth 2010).

Actors may attempt to exploit the political domain to influence the target state or establish favourable conditions for the conduct of hybrid threat activity. Political power may be used either from within a country or in the diplomatic arena. In the latter case, the activity may be a standalone effort or combine the political power of various actors to exert a greater effect. The tools of this domain target democratic processes, political organizations, and persons.

The political domain is strongly connected to diplomacy (section 4.1.11), mainly because of the capability of foreign policy to have a strong bearing on domestic politics. The relationship between the two is often described as a "two-level game" (Putnam 1988). This domain is also closely linked to public administration (section 4.1.8) because the latter exists to implement public policy, but can also affect policymaking. In addition, some tools of the political domain endeavour to change the public's perception of political choices and/or actors. Therefore, the tools of the information domain (4.1.13) can be used to support hybrid threat activities seeking to exploit the political domain. Furthermore, the actors, to the extent that they want to avoid an open confrontation, will keep seeking to exploit legal gaps and operate in the seams between national and international law. In this sense, it is the legal domain (section 4.1.9) that shapes the environment in which an actor may attempt to exploit the political domain. Lastly, the success of several tools in this domain is contingent on the surreptitious nature of the activities involved. Therefore, actors behind the hybrid threat tend to use their intelligence services, which are able to orchestrate and implement these activities thanks to their capability to conduct clandestine operations and their sometimes vast networks.

4.1.13 Information

Weaponizing information arguably remains the hallmark of Hybrid Threats and nonlinear strategies. It is used to undermine the perception of the security of the people by pitting political, social and cultural identities against one another. The purpose of the action is to exploit identity politics and allegiances, thus dividing influential interest groups and political alliances. Confusion and disorder ensue as people feel more insecure. By virtue of its low intensity and potential for deniability, Hybrid Threat activities designed to exploit this domain are generally low-risk, allow for a trial-and-error approach, much like the agile processes used in technology firms, and have a relatively low cost, with some even being open to outsourcing.

Cyber disinformation/(black) propaganda/fake news is false information, which is also intended to give the impression that it was created by those it is supposed to discredit. It is typically used to vilify, embarrass or misrepresent someone/the target. Fake news in social media is not just a post that has been liked, shared or followed; rather, it is a powerful technique of multiplying cyber propaganda. In the wake of the financial and economic crisis of the years after 2008, the local press in the US almost collapsed. The internet became the leading and determining substitute medium. A medium and source of information that can be considered highly critical. The tools of this domain seek to shift the political discourse, to create or promote narratives, and to manipulate public opinion and sentiment. In addition, they may impair freedom of opinion and expression. Freedom of expression encompasses respect for media freedom and pluralism, as well as the right of citizens to hold opinions and to receive and impart information and *ideas "without interference by public authority and regardless of frontiers"*.[23] However, public authorities in democratic countries are expected to educate citizens regarding the threat of disinformation and protect them against activities aimed at manipulating their views and covertly influencing their decisions.

The information domain is strongly linked to the culture and society domains (sections 4.1.7 and 4.1.6) because disinformation campaigns and other tools in this domain seek to affect the homogeneity of the target state's culture and society. It is also influenced by the intelligence domain (section

[23] European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 10, https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed June 21, 2019).

4.1.10), as information obtained via cyber or traditional espionage can be leaked to influence public opinion, perceptions, and discourse. Moreover, to the extent that one goal of the information domain is to undermine the political discussion and processes in the target state, it can also be related to the political domain.[24]

4.2 Tools

In each domain above, we described the ways in which an actor might bring about an effect. Moreover, this effect can span various domains, as they are strongly connected to each other.

In Table 1 we present an indicative list of tools that can be used by a hostile actor to achieve its objective, together with the potentially affected domains. Each manifestation of a tool does not necessarily constitute hybrid threat activity. For example, a cyber operation may be part of hybrid threat activity or not. This has been discussed extensively in Section 2, when describing the concept of Hybrid Threats. It is worth reiterating therefore that ***"hybrid is always a combination of tools but not all combinations are hybrid"***.

The list of tools presented is extensive, but remains an open one, as (a) there may be undetected hybrid threat activity we have not considered, and (b) Hybrid Threats evolve and we may observe new tools being used in the future. A detailed list of these tools, together with a description and examples can be found in Annex A.

Table 1. Tools of hybrid threat activity

Tool	Affected domains
Physical operations against infrastructure	Infrastructure, Economy, Cyber, Space, Military/Defence, Information, Social/Societal, Public Administration
Creating and exploiting infrastructure dependency (including civil-military dependency)	Infrastructure, Economy, Cyber, Space, Military/Defence, Public Administration
Creating or exploiting economic dependencies	Economy, Diplomacy, Political, Public Administration
Foreign direct investment	Economy, Infrastructure, Cyber, Space, Military/Defence, Public Administration, Intelligence, Information, Political, Legal
Industrial espionage	Economy, Infrastructure, Cyber, Space, Intelligence, Information
Undermining the opponent's national economy	Economy, Public Administration, Political, Diplomacy
Leveraging economic difficulties	Economy, Public Administration, Political, Diplomacy
Cyber espionage	Infrastructure, Space, Cyber, Military/Defence, Public Administration
Cyber operations	Infrastructure, Space, Cyber, Social/Societal, Public Administration, Military/Defence
Airspace violation	Military/Defence, Social/Societal, Political, Diplomacy
Territorial water violation	Military/Defence, Social/Societal, Political, Diplomacy
Weapons proliferation	Military/Defence

[24] For instance, during the 2016 US presidential election campaign, the information leaked on candidate Hillary Clinton and her campaign was obtained via cyber attacks and was published on WikiLeaks and several Russian-sponsored sites (such as Guccifer 2.0 and DCLeaks.com). In a similar vein, the Kremlin leaked stolen files from Emmanuel Macron's campaign 48 hours before the 2017 French presidential election (Treverton et al. 2018).

Tool	Affected domains
Armed forces conventional/sub-conventional operations	Military/Defence
Paramilitary organizations (proxies)	Military/Defence
Military exercises	Military/Defence, Diplomacy, Political, Societal
Engaging diasporas for influencing	Political, Diplomacy, Social/Societal, Culture, Intelligence, Information
Financing cultural groups and think tanks	Societal, Culture, Political, Diplomacy
Exploitation of sociocultural cleavages (ethnic, religion and culture)	Social/Societal, Culture
Promoting social unrest	Infrastructure, Social/Societal, Economy, Political
Manipulating discourses on migration to polarize societies and undermine liberal democracies	Social/societal, Culture, Political, Legal
Exploiting vulnerabilities in public administration (including emergency management)	Public Administration, Political, Social/Societal
Promoting and exploiting corruption	Public Administration, Economy, Legal, Social/Societal
Exploiting thresholds, non-attribution, gaps and uncertainty in the law	Infrastructure, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
Leveraging legal rules, processes, institutions and arguments	Infrastructure, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public Administration, Legal, Intelligence, Diplomacy, Political, Information
Intelligence preparation	Intelligence, Military/Defence
Clandestine operations	Intelligence, Military/Defence
Infiltration	Intelligence, Military/Defence
Diplomatic sanctions	Diplomacy, Political, Economy
Boycotts	Diplomacy, Political, Economy
Embassies	Diplomacy, Political, Intelligence, Social/Societal
Creating confusion or a contradictory narrative	Social/Societal, Information, Diplomacy,
Migration as a bargaining chip in international relations	Social/Societal, Diplomacy, Political
Discrediting leadership and/or candidates	Political, Public Administration, Social/Societal
Support of political actors	Political, Public Administration, Social/Societal
Coercion of politicians and/or government	Political, Public Administration, Legal

Tool	Affected domains
Exploiting immigration for political influencing	Political, Social/Societal
Media control and interference	Information, (Media) Infrastructure, Social/Societal, Culture
Disinformation campaigns and propaganda	Social/Societal, Information, Political, Cyber, Culture, Public Administration
Influencing curricula and academia	Social/Societal, Culture
Electronic operations (GNSS jamming and spoofing)	Space, Cyber, Infrastructure, Economy, Military/Defence

5 Phases

In this report the Hybrid Threats is the overarching concept that includes a spectrum of activities. This part of the report will try to clarify the role of different activities in the landscape of Hybrid Threats; interference, influence, operations/ campaigns and warfare/war.

When studying the literature relating to changing character of war and how our security environment has been changing, it is clear that the analyses push the characterization of Hybrid Threats towards strategic-level thinking and the fact that there are different types of activity with different degrees of intensity, long timeframes, and changed geography, coupled with the fact that actors behind the Hybrid Threats might either have material constraints or other reasons why they seek to support their policy with questionable action. They act in the **shadows** or in the **grey zone** between acceptable and unacceptable and legal and illegal, with a **combination of tools** to strengthen their effort as already pointed out in this report.

Erin Simpson's paper *"Thinking About Modern Conflict: Hybrid Wars, Strategy and War Aim"*' (Simpson 2005) looked at Hybrid Threats from a more strategic perspective and highlighted the strategic ends while de-emphasizing the ways and means. She reviewed the relationship between time, cost, and strategy. Her conclusion was that resource endowments and geography are integral to developing strategic choices. This supports the idea that those diverting to questionable activity to achieve their strategic goals, seek cost effective and long-term solutions to maintain or enhance their power and status in world politics. It is also clear that strategic culture plays important role when it comes to the methods that are used to insert influence.

In this part of the report the different type of Hybrid Threats activity is put also in a timeline, which also underlines the fact that there is the escalation potential in Hybrid Threats that covers both short-term and long-term possibilities. The timeline has three different phases. The three phases named here are **priming, destabilization and coercion**. All of the phases have a strong psychological component. The activities, interference, influence, operations/campaign and warfare/war, in the different phases overlap in some cases. There may or may not be **escalation**. **There may also be de-escalation**, meaning that the activity can also move backwards, confusing situational awareness and disguising the real aims of the action. This is distinctive of the landscape of Hybrid Threats. The escalation and de-escalation can be horizontal and vertical, meaning that the combination of tools and how they are used, is adjusted to the situation and need. As the MCDC countering hybrid warfare report *"Understanding hybrid warfare"* observes, "*synchronization allows the hybrid warfare actor to `escalate or `de-escalate' horizontally rather than just vertically, thus providing further options for the attacker"* (Cullen and Reichborn-Kjennerud 2017).

The identification of the phases and the activity in them is based mostly on Russian and Chinese language literature reviews done by the Hybrid CoE. The literature that was reviewed reflects a strategic way of thinking as well as various approaches to competition, conflict and war. Furthermore, to tackle the cognitive component of the ideology behind the use of Hybrid Threats several psychological theories have also been studied for this report.

Since the **intent** behind conducting any hybrid threat activity, as mentioned earlier, is to **harm, undermine or weaken the target**, it is an indication that we are talking about tactics not policies. Due to the fact that Hybrid Threats activity is planned to support existing policies, condemning the action also becomes more challenging; how to differentiate a policy from unacceptable and/or illegal action? How to attribute action if it's denied even with evidence? How to negotiate about something that is created for the purpose to harm?

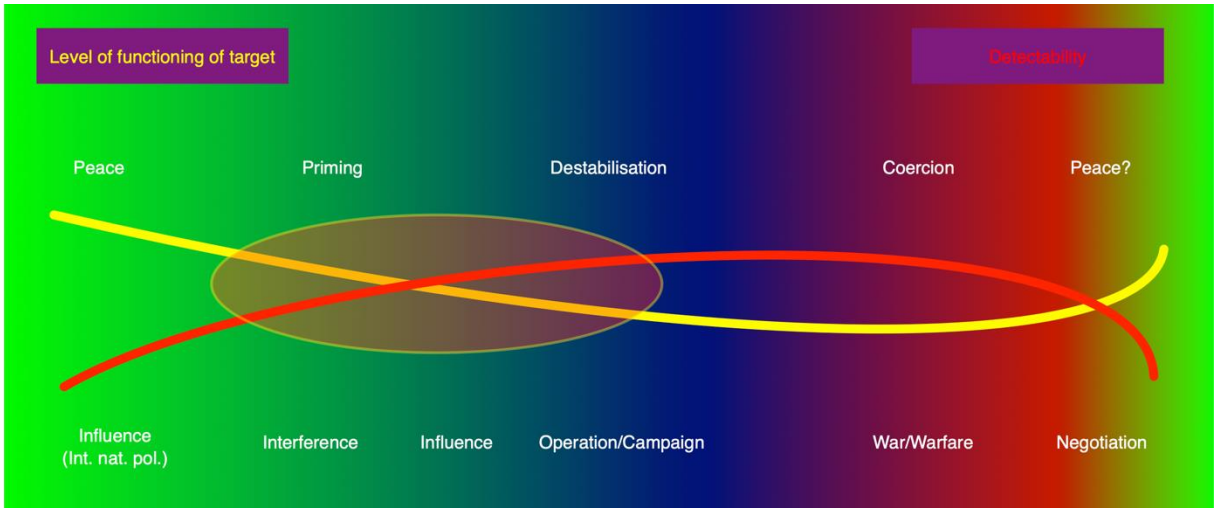


Figure 5. Phases and activities

5.1 Priming

In the priming phase, the actor's ultimate goal is that the target will voluntarily make harmful choices and decisions. If there is already in this stage a plan that involves escalation toward a military conflict the actor will seek to infiltrate and predisposition its capabilities in the internal space of the target state. This aim is pursued through interference, which blurs situational awareness. The actor has plenty of strategic patience at that point. In security and military studies, the preparation phase is often referred to as preconditioning or shaping. Shaping involves any series of actions taken in anticipation of an engagement or tactical operation designed to promote the accomplishment of strategic objectives. The meaning behind such action is to enhance success by negating or mitigating potentially adverse effects while strengthening or increasing potentially favourable factors. "*This means that such activity focuses on any factor or combination of factors that may influence the outcome and can involve any or all echelons of a tactical organization. For example, that the control of a piece of terrain has been determined critical for success. The force that occupies and reinforces it before the onset of the operation gains a defensive advantage. Such actions can be decisive in nature*" (Heal 2008). Even if preconditioning and shaping are terms from security and military studies, in the case of Hybrid Threats, they are suited, since the actors, authoritarian states, have interlinked relationship with military and intelligence.

In this report, shaping/conditioning is referred to as priming. Priming is better suited to the nature of Hybrid Threats activity as it also takes account of the civilian dimension, which is central both as a target and to countering Hybrid Threats. Even if the activity is designed from the outset to avoid open conflict or war, but the force multiplying effects and tactics behind the activity are underpinned by military-like thinking, as mentioned typical of authoritarian state's strategic culture, where the power elite is dependent on intelligence services and military. Hew Strachan has also made this point in relation to Russia: "Putin has an understanding of strategy that is more military and operational, not least in its readiness to see strategy as something that is not reactive but proactive, and which requires a state to take the initiative and to exploit the vulnerabilities of others. In other words, Putin has understood strategy as a soldier would rather than as a Western politician" (Strachan 2016).

Therefore, the military option should not be side-lined and kept in mind from the beginning. It is virtually impossible to know for sure whether warfare activity will become a part of the strategy to successfully achieve the intended aim or not. This fact might not be known to the actor either in this point.

The Russian literature review gives also a convincing insights of how the idea of priming is seen from the Russian perspective. Valery Sobolnikov (Собольников 2015) argues that the **main structural element** in hybrid warfare (note: term used in the Russian literature) is **psychological interference**, which is a comprehensive set of different forms, methods and means to control the psychological characteristics and behaviour of humans and communities, and the ability to shape their value systems and perceptions of the world view. In Sobolnikov's view, Hybrid Threats activity can be conducted in all spheres of society through the use of various tools and technologies, yet their

aim remains the same: psychological influence over the target. **Psychological interference** is therefore the common denominator (the "structural layer") of Hybrid Threats activity in all domains and spheres, and provides the lens through which operations should be perceived in space and time. Psychological influence **entails transforming the consciousness and behavioural patterns of the target person or group**; the manipulation of a particular society or community, of its governing characteristics, views, values and shared norms towards a direction that will **push the target state to make a decision desired by the aggressor** in a given situation.

Andrey Devjatov, a long-time KGB agent and author of numerous intelligence-related publications, also views psychological influence as an integral part of achieving victory in the contemporary confrontation, which he calls the "*war of meanings*". He advocates an overarching, above-state intelligence network, which is tasked with influencing minds towards a Russian values-based world order (as opposed to being limited to information gathering). He also argues that the Russian cultural heritage, linguistic structure, perception of paradox and abstract thinking provide Russia with a competitive advantage to develop and implement such a model, and enable Russia to successfully use socio-humanistic technologies, which he sees as the main weapon to control people in the digital age(Девятов 2013)

Socio-humanistic technologies are referred to by multiple authors in the Russian literature review. Sergey Ustinkin and Anatoliy Rudakov (2017) describe socio-humanistic (or socio-humanitarian) technologies as one of the tools for achieving psychological influence. Socio-humanitarian technologies are employed for the purpose of gaining control over the process of identification at the personal, community or national level by creating a primed information environment. The process is incremental **but in the long term has the potential to destabilize the socio-political sphere of a state**. The strategy becomes successful when individuals from all layers of society (students, expert circles, business and political elites) start to think and act in a way desired by the actor behind the activity without the actor's direct commands. Decision-making and the population are targeted and influenced through external interference below the threshold of detectability in a way that is harmful to the target state, which is one of the main characteristics of a Hybrid Threat.

In the Western social psychological literature, priming is an action that aims to facilitate a change in an organization or an environment (Oyserman and Lee 2008; Molden 2014). The idea behind priming is that it will have a long-term effect on the attitude or behaviour of an individual, a group or an organization. The priming technique facilitates testing cultural factors by clarifying what is salient and accessible to the participants at the point that a judgement is made, or behaviour engaged in. There seems to be a certain level of agreement among social psychologists *"that the mere exposure to socially relevant stimuli can facilitate, or prime, a host of impressions, judgements, goals and actions, often even outside of people's intention or awareness*" (Molden 2014). It is important to note that evaluations of the effects of priming in social psychology research are still highly diverse. However, given the strong emphasis in the Russian literature and in Chinese strategic thinking on the role of psychology, examining the Hybrid Threats mechanism through the lens of psychology makes sense. For example, in the Russian literature review Bartosh, one of the most active authors on the topic, refers to the concept of attrition warfare (Бартош, А.А. 2018). This type of warfare is aimed at wearing down and exhausting the enemy's resources by keeping it in a constant state of alertness. This type of action is regarded as interference. Bartosh refers to a very long-term strategy which, as he puts it, is "*a war of meanings and nerves"*, and a reference to transforming existing values and behavioural patterns, destroying existing systems such as "language codes" and replacing them with new ones, mobilizing the masses in one's own society and demobilizing the enemy's masses. To this end, Bartosh sees attrition warfare as an influence-building strategy through a set of interference actions. The aim for the action as he argued already in 2013 is the "self-disorganization and self-disorientation of the target state"(Bartosh 2013) .

The priming mechanism involves two components: 1) The "excitation" of representations in memory by some process of spreading activation through a semantic network of associations; and 2) The use of excitations or accessible representations to encode information about a social target that was subsequently received (Molden 2014). In relation to the priming phase, domains like information, culture, diplomacy, politics, society, cyber, intelligence, economy and public administration are highly important. For example, it has been shown that in harmful information activities conducted by foreign state actors, they study a society, its divisions, controversies and problems, and attempt

to disrupt perceived areas of tension using illegitimate methods (Pamment, Nothhaft, and Agardh-Twetman 2018). Another often-cited area is cyber. Activities in cyberspace can harm infrastructure, while information-gathering by hacking, different types of disruptions, and overloading are also part of the toolkit to find ways to build influence. Priming can also target individuals or different types of communities, especially those that do not feel included in the country they inhabit. Moreover, in international relations, trying to interfere in and disrupt existing normative frameworks in order to gain more influence belongs to the priming phase. Action relating to economic factors may also be part of this type of activity. Building leverage through economic means has long roots when seeking ways to exert influence: conditionality relating to loans (Mattlin and Nojonen 2011), foreign direct investment (FDI), ownership relating to property or business.

The question of exerting influence is an important one. Influencing is part of traditional state policies and most states try to influence in the international politics. However, there are two kind of influencing, the one that is more open with clear goals – conventional influencing – and then there is influencing that is part of the Hybrid Threats – often referred to as Hybrid Influencing. In international politics influential states are able to effectively deploy a broader portfolio of instruments of influence to modify the beliefs and/or the behaviour of other states. It is this ability that lies at the heart of effective statecraft – one that protects and promotes national interests – in today's globalized world (Moyer et al. 2018). Statecraft based on resources and openly declared goals to influence states is in the Hybrid Threats perspective a conventional way to try to build influence. It still has its place.

From the Hybrid Threats perspective, the statecraft is the ability to creatively and cost effectively combine different means to build influence without targeting and negotiating directly with a state. The methods first targets population, local level and institutional level through interference, and then once the actor has managed to wedge itself into targets internal space, it will start inserting its covert influencing. This can bring the desired result slower but with more lasting effects. Roselle, Miskimmon, and O'Loughlin (2014) point out that "*if people believe, for example, that the promotion and protection of human rights is important, desirable, and right or proper, it is more difficult to legitimize actions perceived to be in conflict with that consensus. Creating a shared consensus to force another to do something can be much more difficult than using hard power, but there is reason to believe that the results can be more lasting"*. This means that without some level of attraction, there is no influence. Authoritarian states hold little natural attraction for people that live in democratic states. Neither Russia nor China call themselves authoritarian states, but rather states with their own democracy. In Russia, the term sovereign democracy is still often used, while in China the term is socialist democracy. The reason why democracy is variously named, especially in authoritarian states, is that regime has an inherent weakness in those states with an authoritarian state system. They are in constant need to legitimize their power both internally and externally. This means that all policies, strategies and tactics have a largely top-down approach. Therefore, when it comes to states like Russia and China, we cannot talk about soft power, as often has been talked about those policies, but rather cultural statecraft (Forsberg and Smith 2016)- a top-down approach, which also duly implies a need for control. From the perspective of Hybrid Threats, this is a highly important distinction and helps to uncover the working and thinking behind the use of the Hybrid Threats mechanism.

From these perspectives, it seems that a certain type of interference is needed as the first face in priming phase, especially if there is no natural or pre-existing influence. Some good examples of how interference might form a basis for influence creation in the Hybrid Threats domain are given by Charles Parton in his analysis of Chinese actions. As he points out: "*There is nothing covert, coercive or corrupt(ing) about purchasing routers and other equipment for UK telecommunications from Huawei (China's largest telecommunications company), nor about The Telegraph accepting £750,000 a year to include a supplement from the CCP's China Daily. But it is possible to conceive that Huawei might, in future, if it has not already, covertly collect data via the UK's systems, or that The Telegraph, if in future it finds itself in financial trouble, might be less willing to offend the CCP by forthright reporting on matters such as abuses in Xinjiang, Tibet or other sensitive issues"* (Parton 2019).

As Parton (ibid.) goes on to say: "*A major tool of interference is to create dependency on Chinese funding (or to imply that it may be withdrawn). Often this promotes self-censorship and self-limiting policies, to avoid losing financial support. Another is to get Chinese who can be trusted to advance the CCP's interests, whether in universities, the media, politics or business. A further tactic is 'elite capture', the appointing of former politicians, civil servants, businessmen, or high-profile academics/think-tank personnel who retain influence in their home*

countries to positions in Chinese companies and think tanks or to affiliated posts in Chinese universities. Often paid very generously for their advice, they risk becoming more amenable to CCP aims." These activities are not illegal or unacceptable, but when activated with given need or opportunity and combined and used in synchronization, they start to create an effect that harms and undermines the democratic state system, sovereignty and functionality of the target state. As Wigell has argued, "*Such subtle means of interference can involve deniable cyber operations, disseminating false information, financing anti-government groups, infiltrating agents of influence, corrupting political actors, and offering economic inducements to selected actors, ideally to lure them into making a - conscious or unconscious - political bargain with the hybrid agent*" (Wigell 2019). In this way, interference is *"a strategy for the mostly covert manipulation of other states' strategic interest"* (ibid.). Influence, therefore, is created through different forms of interference, which can even in some cases include the use of military power in the form of airspace violations and military exercises. Both Russia and China have also demonstrated their military capabilities and willingness to use them in Russia's case in Syria and in China's case in "*through the use of its coast guard to intimidate rival claimants to rocks and reefs in the South China Sea"* (Shevchenko and Larson 2019).

The interference itself might not yet be hybrid as such. The activity starts becoming hybrid, when it starts fulfilling the criteria for Hybrid Threats. When opportunity, necessity or impatience present themselves, the created influence will be used. At this point, the activity will become more detectable and also hybrid. Even if detectability grows, harm has already been done and it becomes harder to respond and contain the activity. In some cases, the desired affect can even be achieved at the end of the priming phase. If so, the effect will have been accomplished by the target making decisions and responding in a way that has been beneficial for the aggressor. In the end, it will have proved to be a very cost-effective tactic and it will be very difficult to attribute to the real actor behind all the activity due to the force-multiplying effect of a mix of tools and domains which blurs the situational awareness.

5.2 Destabilization through operations and campaigns

The destabilization phase is a stage that the actor intensifies the activity in the manner of a campaign (multiple operations), or to use for one operation with the aim of archiving the designated goal. Unlike in the priming phase, that aims to prime and by default gain something; information, positioning, testing information, learning or an advantage, in the destabilization phase there is pre-planned aim.

It is difficult to detect when an actor is switching the mode. In the destabilization phase, the activity becomes more visible, aggressive and possibly involves more violence. This happens either according to the actor's need or an opportunity that presents itself, or due to the actor's frustration with the status quo situation. In this phase, the activity pushes the limits of acceptable and unacceptable, as well as legal and illegal action. One of the aims of a hostile actor in using the mechanism behind the Hybrid Threats is the dissolution of fixed categories of order (Schmid 2019). This means that there is a multi-layered effort designed to destabilize a functioning state and polarize its society (Pindják 2014). This would not be possible without the priming phase.

Even if the activity becomes more visible, an official admission on the part of the actor does not exist ("plausible deniability") and may be very difficult to attribute evidentially. When evidence of the activity is based on classified information, public and open evidence-based attribution becomes virtually impossible. This is a clear advantage for the actor behind the activity. Here, the information and public domains are relatively central space for action. If the discussions and debates relating to events are held in open public domains, while the information and facts are classified, the democratic states become underdogs and the idea behind "the power of the weak" kicks in.

In the destabilization phase more energetic narrative promotions, clear disinformation and propaganda, as well as the activation of bots, algorithms and cyber-attacks like the overloading of public and private services, blocking and malware planting, among others can be experienced. Furthermore, so called on-line to off-line starts to happen, meaning something that has been promoted in social platforms and in the virtual world becomes active in a form of protests or even riots. This more open and aggressive action is aimed at the destabilization of the targeted society. In some cases, the society being affected is used to influence the real target as a planned second-order effect (where attention is focused in one place, but the real target is elsewhere). Examples of this type of tactic can be found in military and strategic literature relating to wars like Vietnam, the Kosovo war of 1999, and the wars in Iraq and Afghanistan. In the case of the Vietnam War, US public opinion became a decisive factor in influencing the real

target - the US government - to end the war (Schmid 2017). In the case of Kosovo, a successful military operation was shadowed by public opinion and opposition in the NATO countries, which also favoured Milosevic at home. In the cases of Iraq and Afghanistan, terrorism was used in an attempt to change the public opinion in countries that sent troops to the two countries (Schober 2009). Even if these are examples of kinetic military action, the idea of polarizing the population and degrading the trust between state and society, as destabilizing effects, applies in Europe today, along with the ideas underpinning the use of Hybrid Threats-related activity. Here too is present the idea that through other levels to target the state level and push it to make decisions harmful for itself.

Furthermore, destabilization activity exploits the different seams or grey zones between areas that are traditionally seen as separate, but which in today's security environment are closely interlinked and intertwined. This includes the seams between external and internal security, state and local-level connections, perceptions relating to friend and enemy, civil-military, areas of different authorities' jurisdictions, different legal frameworks, virtual world versus concrete world and even understandings relating to war and peace. In these seams, the activity may yet again touch upon many different domains, including legal, information, public administration, military, societal, political, economic, cyber, space and infrastructure. The difference in terms of the priming phase is particularly related to response; In respect of the destabilizing phase, we are already talking about the need to respond and defend. This is also one of the reasons why the focus in the destabilization phase is on the different seams. During this phase, the sectoral response will be inadequate, as the actor behind the activity acts according to long-term strategic interests even if the target seems to be short term goal.

During the destabilization phase, there is a deliberate push to force decisions under pressure. Now the hostile actor knows what it wants, there is a clear aim: business contract; voting result (elections and referendums); EU or NATO-level decisions; hampering a bilateral deal; block, delay or reverse a decision to use the military; decisions relating to sanctions regimes; any multilateral decision, even one relating to sports (status question); a country's strategic decisions to join or reject alliances and/or normative international rules, and so forth. All of the short-term goals are linked to longer-term strategic aims. When making above mentioned types of decisions, the correct situational awareness and broad-based information as well as the possibility to assess different perspectives over time would be an ideal decision-making basis. In reality, this is seldom the case, and the situation becomes even more complex if an outside actor applies pressure.

If the desired effects are not achieved, the activity either reverts to priming to wait another and better opportunity, to tailor a better combination or create new vulnerabilities, or then escalation will ensue. This depends on several factors: the importance of strategic goals, responses and further opportunities.

5.3 Coercion through hybrid warfare

The last phase is coercion. The activity has now moved beyond under-detection and under-attribution and can be labelled hybrid warfare/war. Hybrid warfare represents the “hard end” of the escalation spectrum of Hybrid Threats activity. Principally, hybrid warfare is a combination of covert and open military operations, combined with political and economic measures, subversion, information/disinformation operations and propaganda/fake news, the covert or open deployment of special forces, as well as military assistance or open military action, including cyber-attacks as part of the whole orchestration.

While it potentially makes use of all strategic domains (politics, diplomacy, intelligence, information, military, economy, technology, culture, legal, societal, public administration, cyber and space), hybrid warfare includes the use of force as its defining element. From terror, sabotage and subversion to guerrilla warfare, conventional warfare and even the nuclear domain, all possible levels of escalation can be included or even combined. In this connection, the use of force is not only an additional element in a Hybrid Threats scenario, it also changes the entire nature of the conflict and turns it into war. In this phase, the nature of the activity is *“an act of force to compel an enemy to do one's own will”* (Clausewitz 1976).

Basically, one can argue that this kind of warfare is nothing new. Such struggles often involve strategies and tactics of asymmetric warfare, the weaker combatants attempting to use strategy to offset quantitative or qualitative deficiencies in their forces and equipment. This is in contrast to symmetric or military-centric warfare, where two powers have comparable military power and resources and rely on tactics that are similar overall, differing only in details and execution.

According to a comparative war study by Ivan Arreguín-Toft (Arreguín-Toft 2001):

1. the weaker parties won in more than 30% of all wars examined;
2. there is a tendency for these to become increasingly victorious.

Those conducting hybrid warfare activities are usually in some ways weaker actors/states or actors avoiding openly declared war. Thus, it can turn into a war between belligerents whose relative military power differs significantly, or whose strategy or tactics differ considerably. This is typically a conflict between a standing, professional army and an insurgency, or resistance-movement militias who often have the status of unlawful combatants.

In the literature dealing with hybrid warfare, the terms "guerrilla warfare", "insurgency", "counterinsurgency", "irregular warfare", "unconventional warfare'', "rebellion", "terrorism" or "counterterrorism" - that is, essentially violent conflict between a formal military and an informal, less equipped and supported, undermanned but resilient and motivated opponent - are frequently used to describe the activity. The past vocabulary highlights why we need new terms to describe evolving trends in security and military affairs.

The warfare activity feature of the landscape of Hybrid Threats has been designed to resemble a new challenge and to include a surprise element since "*Hybrid War is not a standardized mix of various types of confrontation, but a sometimes unorganized, radial resistance which does not follow military tactics but creates its own environment of war, usually fully disregarding ius in bello and any other rules"* (Habermayer 2011). As Habermayer goes on to say, "*But the commander in the field looks for some valid `rules of war' that tell him what he can or cannot do. What he is not looking for are political statements coming from his own country, usually thousands of kilometres away from the place where 'the action is', or limiting Rules of Engagement which often favour the attacker who does not follow such limitations. It does not matter if such a manual is called strategy, doctrine or a tactical guideline"* (ibid.). This again highlights how democratic states have possibly weakened the link between civil-military-political axes in the post-Cold War era, and why a hostile actor would be successful in using the mechanism behind Hybrid Threats even against a militarily superior state or alliance.

What the military refer to as the "battlespace" is becoming increasingly difficult to define, and to defend, over time. Advances in technology are normally evolutionary, but they can also be revolutionary: artillery extending beyond the front lines of battles; rockets and airplanes crossing national boundaries and, today, as part of hybrid warfare activity, cyber-attacks that can target political leadership, military systems, and ordinary citizens anywhere in the world, during peacetime or war, with the added advantage of attacker anonymity. Furthermore, the way proxies and non-state actors are instrumental for the Hybrid Threats relating activity and especially when it comes to on-line to off-line activity, blurs the picture even further and shows how the "battle" can be over before crosses a threshold for war.

Hybrid warfare activity as part of the landscape of Hybrid Threats is a product of the 21st century, which exploits the new opportunities created by changes in the security environment such as new status competition; evolving power sources; new types of networks and interdependencies; changes in armed groups; shifts in narratives from political ideology to moral populism and single issues that challenge the democratic state system; deliberate violence against civilians with the goal of destabilization; and technological innovations that also enable cyber activities and a new media landscape.

Hence, even if the roots of warfare have remained unchanged for centuries, and ideas of how to win a war follow similar patterns, warfare is still evolving. Ongoing changes in the security environment will always affect strategic thinking and bring new features to the overall security landscape.

6 Summary and outlook

This report establishes that the European security environment has changed, and it is clear that democratic systems are being challenged. Hybrid threats have become an integral part of European security. Despite the fact that such threats are high on the political agenda, the understanding of them by various stakeholders (states, institutions, disciplines, and other relevant actors) differs considerably.

The report has taken a highly comprehensive look at Hybrid Threats and is the first of its kind to conduct a fusion of multidisciplinary analyses combining military, academic and policy views concerning Hybrid Threats. The most profound is the fact that the whole topic is viewed from the perspective of actors engaging in Hybrid Threats and, as a consequence, it offers a conceptual basis for targeted countries on how to address such hostile activities. However, it does not claim to have covered all of the aspects and domains relating to Hybrid Threats. Indeed, it has shown how complex an issue the landscape of Hybrid Threats is. This also means that no single entity can address Hybrid Threats. A comprehensive and holistic approach needs to be adopted. This should reflect a so-called whole-of-government or, even better, a whole-of-society approach, bringing civil, military and political actors together, and duly leading to a new security ecosystem.

The report has attempted to characterize Hybrid Threats, to enhance understanding, and to raise awareness among stakeholders as a first step in addressing these threats. It also provides a reference point for discussion at the EU and NATO levels, as well as in their respective member states. The report has shown that there are severe gaps between the Western understanding of Hybrid Threats and the way in which other states, such as Russia and China, view influence, threats and status competition. This is clearly an area that future research should also address. This is particularly important when we are looking for strategic objectives, intent, early warning signs and indicators. One feature of early warning signs and indicators is naturally internal information exchange and activity monitoring but, as the case studies in this report indicate, early warning signs can be identified in the narratives, doctrines and debates that are produced in the native language space.

The conceptual model covers the key elements that form the landscape of Hybrid Threats: (a) the **actors** that apply hybrid mechanisms, (b) the **phases** of a hybrid campaign, (c) the **tools** applied, and (d) the **domains** targeted, in order to achieve the hostile actor's strategic objectives. In addition, it provides arguments about hybridity – what makes a series of activities part of a Hybrid Threat. This is crucial in order to avoid common misconceptions according to which isolated activities are labelled as part of Hybrid Threats. At the same time, the authors of this report have tried to strike a balance between a detailed description of the concepts and avoiding analytical "straitjacketing", duly maintaining openness and flexibility. The present framework is not an attempt to establish an absolute truth about Hybrid Threats, but rather a call for critical thinking on the topic. Therefore, this report provides elements to support the work of stakeholders in this area – be it operational or more strategic – in both national and international arenas.

The case studies provided the validation needed for such a complex concept and not the foundation upon which the model would be built. This is a crucial element, and the authors went to great lengths to avoid being caught in the conceptual trap of self-fulfilling prophecies offered by past or current cases of Hybrid Threats.

Nevertheless, the authors recognize that there are still limitations and gaps that need to be addressed. For example, it considers individual actors and not multiple actors collaborating in order to achieve specific objectives. While there is still no evidence of hostile actors collaborating, some recent geopolitical developments might require further analysis and conceptualization in the short term. This aspect is partially covered through the notion of proxies, but it is not powerful enough from an analytical perspective to describe a full-fledged strategic collaboration between actors. Moreover, further analytical work is needed to observe with more clarity and detail the cascading effects of hybrid threat activity, as the combined use of tools may cause multiple effects, which in some cases may be unexpected or even detrimental to the hostile actor.

The operationalization of the model can be expressed in several ways. The most profound is to use it as a basis for vulnerability assessments and detection activities across domains, as well as to support the development of a process for the attribution of Hybrid Threat activity to an actor, which is always a political decision based on evidence.

The latter requires a better understanding of the hostile actor's doctrines, motives and narratives. The present conceptual model includes this aspect and also provides the necessary evidence through the case studies. It would be a very useful spin-off

product of this framework and clear proof of raising awareness and triggering practical activities if countries were to engage towards thoroughly understanding hostile actors objectives before Hybrid Threat activities take place.

The prioritization of activities towards building whole-of-governance and whole-of-society resilience is an essential element for countering Hybrid Threats, and the present work aims at supporting such efforts. Resilience measures can be designed and applied only if areas of action and the respective vulnerabilities have been identified. This report's notion of tools and domains provides a guide for such national plans. Furthermore, a whole-of-society approach requires close collaboration between political (local government, political parties), civil (citizens, businesses, volunteers, NGOs, cultural groups, schools, church etc.) and military domains, and the common understanding of Hybrid Threats offered by the present model is essential in order to support this collaboration. However, much more needs to be done since we are at the very beginning of this process, at least at the EU level.

It is expected that the conceptual model will be applied practically in order to develop scenarios for large-scale exercises at the national and international levels. An increased number of countries are embarking upon such activities with a view to improving their resilience posture, while PACE 18 (EU/NATO Parallel and Coordinated Exercise) is a notable example of such collaboration at the international level.

Interestingly enough, the approach offered by the conceptual model may also trigger changes at the governance level within countries. The complexity of the topic and the need to connect the dots from various sources requires governance structures with the capability to collect and analyse information from various jurisdictions within the government. This also addresses an important aspect of Hybrid Threat activity that exploits the seams of democratic institutions and even the lack of information-sharing among relevant authorities. A scaled-up effort in this area would also positively affect the way that intelligence gathering and sharing takes place at the national and EU/NATO levels.

Hybrid threats may morph into full-scale crises (see Ukraine), and to this end crisis management mechanisms should be adapted accordingly. It is expected that the Hybrid Threats element will be referenced more frequently in national risk assessments, and national emergency and crisis management plans. In particular, cyber crisis management mechanisms could benefit from the conceptual approach in order to put cyber-attacks into the right context. It is important to distinguish between cyber activities that are uncoordinated and isolated events, and cyber activities that form part of a wider plan with the objective to extract critical information about infrastructures or the personal data of political leaders and decision-makers. At the EU level, there are already some elements in this direction with the "Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises"[25].

It is expected that more attack surfaces and advanced concepts for the weaponization of society will emerge in the short or medium term. While a conceptual model cannot forecast what these attack surfaces are likely to be, or which dependencies will be exploited, it already aims at raising awareness around this topic. Policymakers should be aware of the fact that new technologies (e.g. 5G) might introduce new vulnerabilities, which could potentially be exploited by adversaries. Although it is not possible to prescribe such an attack scenario in detail, it is paramount that policymakers invest in monitoring and exercises to build capacities against such hybrid threat attack vectors.

Furthermore, the authors strongly believe that the conceptual model will help to enrich the mindset of security stakeholders by demonstrating the need to thoroughly consider societal aspects, perceptions, and elements of mass psychology. This shift in the security mindset requires changes in the education and training of the respective professionals, security stakeholders, and the public at large.

The latter is linked with research and education. The conceptualization of Hybrid Threats in this report provides the context and basis for the further development of the Hybrid Threats concept at the academic, political and operational levels. Several of the concepts presented here cannot be fully addressed with existing knowledge, and hence a careful gap analysis would uncover those areas that would benefit from research in the future.

At the highest strategic level, the authors would like to highlight the need for further actions in three areas: identification of gaps in existing security-

[25]Commission Recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, C(2017) 6100 final

related policies at the EU and NATO levels; the development of a hybrid diplomacy toolbox (in analogy to cyber diplomacy toolbox); and maintaining/enhancing EU/NATO collaboration in the domain of Hybrid Threats.

The conceptual model is fairly comprehensive in its identification of the various elements involved in Hybrid Threat activity and, as a consequence, existing security policies across the spectrum should be mapped against the aspects provided by the framework so as to identify potential gaps and areas that are not thoroughly addressed.

In analogy to the cyber diplomacy toolbox, Hybrid Threats diplomacy toolbox should be considered as an option for further development at the highest political level. It should be considered mainly as an element for responding to Hybrid Threat activities conducted by hostile actors.

With respect to EU/NATO collaboration, the case of Ukraine clearly demonstrated the need to reinforce the links between the two organizations. However, this enhanced collaboration should not only take place in the final phases of escalation but also during the priming phases. Awareness of the importance of the initial phases of Hybrid Threats provides the right arguments for engaging in further activities that would help to improve resilience and counter potential hostile actors.

References

Arreguín-Toft, Ivan. 2001. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security* 26 (1): 93–128. https://doi.org/10.1162/016228801753212868.

Babbage, Ross. 2019. "Stealing a March: Chinese Hybrid Warfare in the Indo-Pacific: Issues and Options for Allied Defense Planners Volume II: Case Studies." *Center for Strategic and Budgetary Assessments* II: 1–51. https://csbaonline.org/uploads/documents/Stealing_a_March_Annex_Final.pdf%0A25.

Baldwin, David A. 1985. *Economic Statecraft*. Princeton: Princeton University Press.

———. 1997. "The Concept of Security." *Review of International Studies* 23 (1): 5–26. https://doi.org/10.1017/S0260210597000053.

Bartosh, Aleksandr. 2013. "Purpose and Mechanisms of the Controlled Chaos Model." *Nezavisimaya Gazeta*, 2013. https://nvo.ng.ru/concepts/2013-09-27/6_chaos.html.

Berdal, Mats. 2011. "The 'New Wars'' Thesis Revisited.'" In *The Changing Character of War*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199596737.003.0007.

Blackwill, R D, and J M Harris. 2016. "The Lost Art of Economic Statecraft." *Foreign Affairs* 95 (2): 99–110.

Bunker, Robert. 2013. *Mexican Cartel Essays and Notes: Strategic, Operational, and Tactical*. *A Small Wars Journal-El Centro Anthology*. iUniverse.com.

C4ADS. 2019. *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*. C4ADS innovation for peace.

Chen, Jidong, and Yiqing Xu. 2017. "Information Manipulation and Reform in Authoritarian Regimes*." *Political Science Research and Methods* 5 (1): 163–78. https://doi.org/10.1017/psrm.2015.21.

Clausewitz, Carl. 1976. *On War (Edited and Translated by Michael Howard, Peter Paret)*. Princeton: Princeton University Press,.

Council of the European Union. 2008. "Council Directive 2008/114/EC of 8 December 2008 on the Indentification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection." *Official Journal of the European Union*, 75–82.

Cullen, Patrick J, and Erik Reichborn-Kjennerud. 2017. "MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare."

Defense Intelligence Agency. 2019. "Challenges to Security in Space."

Dengg, Anton, and Michael N Schurian. 2016. "On the Concept of Hybrid Threats." In *Networked Insecurity – Hybrid Threats in the 21st Century*, edited by Anton Dengg and Michael N Schurian, 25–80. Vienna: National Defence Academy, Vienna.

European Parliament and Council. 2016. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union."

Fabre, Cécile. 2018. *Economic Statecraft : Human Rights, Sanctions, and Conditionality*. Cambridge: Harvard University Press.

Ferm, Tiina. 2017. "Laws in the Era of Hybrid Threats." *Hybrid CoE Strategic Analysis*.

Fernández, Luciana M. 2009. "Organized Crime and Terrorism: From the Cells Towards Political Communication, A Case Study." *Terrorism and Political Violence* 21 (4): 595–616. https://doi.org/10.1080/09546550903153399.

Forsberg, Tuomas, and Hanna Smith. 2016. "Russian Cultural Statecraft in the Eurasian Space." *Problems of Post-Communism* 63 (3): 129–34. https://doi.org/10.1080/10758216.2016.1174023.

Fridman, Ofer. 2018. *Russian Hybrid Warfare-Resurgence and Politicisation*. London: Hurst.

Giannopoulos, G, M Theocharidou, G Theodoridis, and P Gattinesi. 2018. "Developing Vulnerability and Detection Indicators for Hybrid Threats." *JRC Technical Report, JRC109791*.

Giles, Keir, Philip Hanson, Roderic Lyne, James Nixey, James Sherr, and Andrew Wood. 2015. *The Russian Challenge, Chatham House Report*. London: Chatham House, the Royal Institute of International Affairs.

Ginsburg, Tom, and Tamir Moustafa. 2008. *Rule by*

Law: The Politics of Courts in Authoritarian Regimes. Cambridge: Cambridge University Press.

Habermayer, Helmut. 2011. "Hybrid Threats and a Possible Counter-Strategy." In *Hybrid and Cyber War as Consequences of the Asymmetry*, edited by Josef Schröfl, Bahram M Rajaee, and Dieter Muhr, 249–72. New york: Peter Lang.

Harrison, Todd, Kaitlyn Johnson, and Thomas Roberts. 2018. "Space Threat Assessment 2018, A Report of the CSIS Aerospace Security Project."

Heal, Sid. 2008. "Shaping Operations." *The Tactical Edge*.

Hoffman, Frank G. 2010. "'Hybrid Threats': Neither Omnipotent Nor Unbeatable." *Orbis* 54 (3): 441–55. https://doi.org/10.1016/J.ORBIS.2010.04.009.

Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Iancu, Niculae, Andrei Fortuna, Cristian Barna, and Mihaela Teodor. 2016. *Countering Hybrid Threats : Lessons Learned from Ukraine*. Washington: IOS Press.

Kaldor, Mary. 2018. *Global Security Cultures*. Cambridge: Polity.

Karagiannis, Georgios Marios, Stamatios Chondrogiannis, Elisabeth Krausmann, and Zehra Irem Turksezer. 2017. *Power Grid Recovery after Natural Hazard Impact*. Publications Office of the EU. https://doi.org/10.2760/87402.

Kettl, Donald F. 2018. *Politics of the Administrative Process*. 7th ed. Los Angeles: CQ Press.

Klein, Margarethe. 2019. "Private Military Companies – a Growing Instrument in Russia's Foreign and Security Policy Toolbox." *Hybrid CoE Strategic Analysis*.

Kofman, Michael, and Matthew Rojansky. 2015. "A Closer Look at Russia's 'Hybrid War.'" *Kennan Cable*, no. 7.

Kragh, Martin, and Sebastian Åsberg. 2017. "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." *Journal of Strategic Studies* 40 (6): 773–816. https://doi.org/10.1080/01402390.2016.1273830.

Krausmann, Elisabeth, Serkan Girgin, and Amos Necci. 2019. "Natural Hazard Impacts on Industry and Critical Infrastructure: Natech Risk Drivers and Risk Management Performance Indicators." *International Journal of Disaster Risk Reduction*, April, 101163. https://doi.org/10.1016/J.IJDRR.2019.101163.

Krausmann, Elisabeth, Amos Necci, and Serkan Girgin. 2017. "Natech Emergency Management: Rising to the Challenge | EU Science Hub." IChemE - UK Institution of Chemical Engineers.

Lapowsky, Issie. 2019. "House Probes Cambridge Analytica on Russia and WikiLeaks." *Wired*.

Lough, John. 2011. "Russia's Energy Diplomacy." *Chatham House*.

Lowenthal, Mark M. 2015. *Intelligence : From Secrets to Policy*. 6th ed.

Manca, Anna Rita, Peter Benczur, and Enrico Giovannini. 2017. "Building a Scientific Narrative Towards a More Resilient EU Society Part 1: A Conceptual Framework." https://doi.org/10.2760/635528.

Mattis, James N, and Frank G Hoffman. 2005. "Future Warfare: The Rise of Hybrid WarsNovember 2005 Vol. 131/11/1,233." *Proceedings*, November, 18–19.

Mattlin, Mikael, and Matti Nojonen. 2011. "Conditionality in Chinese Bilateral Lending." In *BOFIT Discussion Papers*, edited by Laura Solanko. Bank of Finland.

Meessen, Rick. 2018. "How Gaming Can Raise Our Awareness of Hybrid Threats." *TNO Insights*.

Molden, Daniel C. 2014. "Understanding Priming Effects in Social Psychology: What Is "Social Priming" and How Does It Occur?" *Social Cognition*. Vol. 32.

Monaghan, Sean (Ed.), Patrick Cullen, and Njord Wegge. 2019. "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare."

Moyer, Jonathan D, Tim Sweijs, Mathew J Burrows, and Hugo Van Manen, eds. 2018. *Power and Influence in a Globalized World*. Atlantic Council.

Mueller, Robert S. III. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Washington D.C.: U.S. Department of Justice.

"National Military Strategic Plan for the War on Terrorism." 2006. US Department of Defense.

NATO. 2013. *Allied Command Operations Comprehensive Operations Planning Directive Interim V2.0*. Belgium: North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe.

Nemeth, William J. 2002. *Future War and Chechnya : A Case for Hybrid Warfare*. Monterey: Naval Postgraduate School.

Newton, K, and J W van Deth. 2010. *Foundations of Comparative Politics: Democracies of the Modern World*. 2nd ed. Cambridge: Cambridge University Press.

Norris, William J. 2016. *Chinese Economic Statecraft : Commercial Actors, Grand Strategy, and State Control*. Ithaca: Cornell University Press.

Nye, Joseph S. 2013. "What China and Russia Don't Get About Soft Power." Foreign Policy. 2013. https://doi.org/10.2307/1148580.

Nye, Joseph S. 1990. "Soft Power." *Foreign Policy*, no. 80: 153. https://doi.org/10.2307/1148580.

O'Rourke, Ronald. 2018. "A Shift in the International Security Environment: Potential Implications for Defense - Issues for Congress."

Oyserman, Daphna, and Spike W S Lee. 2008. "Does Culture Influence What and How We Think? Effects of Priming Individualism and Collectivism." *Psychological Bulletin* 134 (2): 311–42. https://doi.org/10.1037/0033-2909.134.2.311.

Pacheco, Fernando Celaya. 2009. "Narcofearance: How Has Narcoterrorism Settled in Mexico?" *Studies in Conflict & Terrorism* 32 (12): 1021–48. https://doi.org/10.1080/10576100903319797.

Pamment, James, Howard Nothhaft, and Henrik Agardh-Twetman. 2018. "Countering Information Influence Activities." Swedish Civil Contingencies Agency.

Parton, Charles. 2019. "China-UK Relations Where to Draw the Border Between Influence and Interference?" London.

Pindják, Peter. 2014. "Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together?" *NATO Review*.

PSSI. 2018. "Europe's Preparedness to Respond to Space Hybrid Operations."

Putnam, R D. 1988. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42 (3): 427–60.

Putten, Frans-Paul van der, Minke Meijnders, Sico van der Meer, and Tony van der Togt, eds. 2018. *Hybrid Conflict: The Roles of Russia, North Korea and China*. The Netherlands Institute of International Relations 'Clingendael''.'

Reilly, James. 2013. "China's Economic Statecraft: Turning Wealth into Power." Syndey.

Renz, Bettina, and Hanna Smith. 2016. "Russia and Hybrid Warfare - Going beyond the Label." *Aleksanteri Papers*.

Roselle, Laura, Alister Miskimmon, and Ben O'Loughlin. 2014. "Strategic Narrative: A New Means to Understand Soft Power." *Media, War & Conflict* 7 (1): 70–84. https://doi.org/10.1177/1750635213516696.

Savolainen, J. 2018. "Legal Resilience Workshop, Helsinki, Finland." European Centre of Excellence for Countering Hybrid Threats.

Schmid, Johann. 2017. "Hybride Kriegführung in Vietnam – Strategie Und Das Center of Gravity Der Entscheidung." *Zeitschrift Für Außen- Und Sicherheitspolitik* 10 (3): 373–90. https://doi.org/10.1007/s12399-017-0659-4.

———. 2019. "The Hybrid Face of Warfare in the 21st Century." *Maanpuolustus*.

Schmitt, M. 2012. "Classification of Cyber Conflict." *Journal of Conflict and Security Law* 17 (2): 245–60. https://doi.org/10.1093/jcsl/krs018.

Schober, W W. 2009. "Conflict Communication in Times of Asymmetric Warfare." In *Winning the Asymmetric War : Political, Social and Military Responses*, edited by Josef Schröfl, Sean Michael. Cox, and Thomas Pankratz, 141–52. New York: Peter Lang.

Schroefl, Josef, and Stuart J Kaufman. 2014. "Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War." *Studies in Conflict & Terrorism* 37 (10): 862–80. https://doi.org/10.1080/1057610X.2014.941435.

Shelley, Louise. 1996. *Policing Soviet Society: The Evolution of State Control*. London: Routledge. https://doi.org/10.4324/9780203991589.

Shevchenko, Alexei, and Deborah Welch Larson. 2019. *Quest for Status: Chinese and Russian*

Foreign Policy. Yale University Press.

Simpson, Erin M. 2005. "Thinking About Modern Conflict: Hybrid Wars, Strategy, and War Aims." In *Paper Presented to the Annual Meeting of the Midwest Political Science Association*. Chicago: Palmer House Hilton.

Smith, Hanna. 2017. "In the Era of Hybrid Threats: Power of the Powerful or Power of the 'Weak'?" *Hybrid CoE Strategic Analysis*.

Strachan, Hew. 2016. "Civil-Military Relations and the Making of Strategy: The Democratic Dilemma." In *After "Hybrid Warfare", What next?-Understanding and Responding to Contemporary Russia*, edited by Bettina Renz and Hanna Smith, 29–32. Valtioneuvoston kanslia.

Treverton, Gregory F, Andrew Thvedt, Alicia R Chen, Kathy Lee, and Madeline Mccue. 2018. "Addressing Hybrid Threats."

U.S. Joint Chiefs of Staff. 2017. "Joint Warfare of the Armed Forces of the United States - Joint Publication 1."

Valaskivi, Katja. 2018. "Beyond Fake News: Content Confusion and Understanding the Dynamics of the Contemporary Media Environment." *Hybrid CoE Strategic Analysis*.

Vergani, Matteo, and Sean Collins. 2015. "Radical Criminals in the Grey Area: A Comparative Study of Mexican Religious Drug Cartels and Australian Outlaw Motorcycle Gangs." *Studies in Conflict & Terrorism* 38 (6): 414–32. https://doi.org/10.1080/1057610X.2015.1004891.

Viotti, P R, and P R Kauppi. 2012. "International Relations Theory." In , 5th ed. New York: Pearson.

Walker, Christopher, and Jessica Ludwig. 2017. "The Meaning of Sharp Power: How Authoritarian States Project Influence." *Foreign Affairs*.

Wallace, Helen, Mark A Pollack, and Alasdair R Young. 2015. *Policy-Making in the European Union*. 7th ed. Oxford: Oxford University Press.

Weeden, Brian, and Vicotria Samson, eds. 2019. *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation.

Wigell, Mikael. 2019. "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy." *International Affairs* 95 (2): 255–75. https://doi.org/10.1093/ia/iiz018.

Williamson, Murray, and Peter A Mansoor, eds. 2012. *Hybrid Warfare: Fighting Complex Opponents from Ancient World to the Present*. Cambridge University Press.

Wilson, Jeanne L. 2016. "Cultural Statecraft in the Russian and Chinese Contexts: Domestic and International Implications." *Problems of Post-Communism* 63 (3): 135–45. https://doi.org/10.1080/10758216.2015.1132630.

Young, Doug. 2013. *The Party Line: How The Media Dictates Public Opinion in Modern China*. John Wiley & Sons Singapore Pte. Ltd.

Бартош, А.А. 2018. "Стратегия и Контрстратегия Гибридной Войны" [Strategy and Counterstrategy of Hybrid War." *Военная Мысль* 10: 5–20.

Девятов, А. 2013. "Путь Правды — Разведка." *Moscow, ООО Издательство «Волант»*.

Собольников, В В (2015). 2015. "'Место и Роль Психологического Воздействия в Стратегии Ведения «гибридных» Войн НАТО,' [Place and Role of Psychological Influence in Strategies of Conduct of 'Hybrid' Wars of NATO]." *Гуманитарные Проблемы Военного Дела* 4(3): 25--31.

List of abbreviations

APT	Advance Persistent Threat
CBRN	Chemical, Biological, Radiological and Nuclear
CI	Critical Infrastructure
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
FDI	Foreign Direct Investment
FYROM	Former Yugoslav Republic of Macedonia
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
HT	Hybrid Threats
JRC	Joint Research Centre
MS	Member State(s)

List of figures

List of tables

GETTING IN TOUCH WITH THE EU

In person

There are hundreds of Europe Direct information centres all over the European Union. You can find the address of your nearest centre at: http://europea.eu/contact

By phone or email

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

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls)

- on the following standard number: +32 22999696, or

- by email via: http://europa.eu/contact

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all of the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications
You can download or order free and paid EU publications from EU Bookshop at: http://bookshop.europa.eu. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).