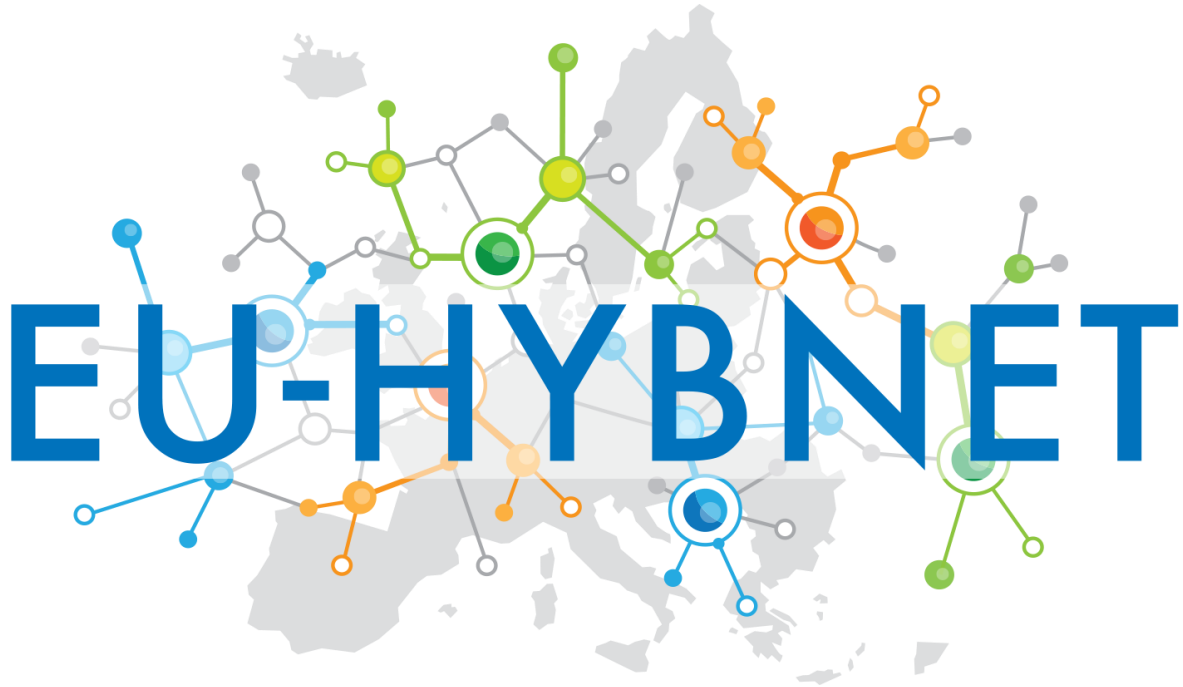

2ND FUTURE TRENDS WORKSHOP REPORT

DELIVERABLE 3.15

Lead Author: UCSC

Contributors: LAU
Deliverable classification: PUBLIC

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme, H2020-SU-SEC-2019, under grant agreement No. 883054

D3.15 2ND FUTURE TRENDS WORKSHOP REPORT

Deliverable number	**3.15**	
Version:	**1.0**	
Delivery date:	**31.5.2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public (PU)**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	**Sabina Magalini**	**UCSC**
Contributors:	**Rachele Brancaleoni, Daniele Gui, Justyna Karolina Kielar**	**UCSC**
	Päivi Mattila, Tiina Haapanen	**Laurea**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	16.05.2022	Rachele Brancaleoni, Daniele Gui, Justyna Karolina Kielar, Sabina Magalini/ UCSC	First draft, text to all chapters
0.2	17.05.2022	Rachele Brancaleoni/ UCSC	Internal review
0.3	30.05.2022	Rachele Brancaleoni/ UCSC	Text editing
0.4	31.05.2022	Päivi Mattila/ Laurea	Review and text editing. Final review.
0.5	31.05.2022	Tiina Haapanen/ Laurea	Final text editing
1.0	31.05.2022	Tiina Haapanen/ Laurea	Submission

DISCLAIMER

Every effort has been made to ensure that all statements and information contained herein are accurate; however, the Partners accept no liability for any error or omission in the same.

This document reflects only the view of its authors and the European Commission is not responsible for any use that may be made of the information it contains.

TABLE OF CONTENTS

1. INTRODUCTION

The Future Trends Workshop (FTW) is an annual event organized as part of EU-HYBNET (Pan-European Network to Counter Hybrid Threats) project. Its purpose is to address expected future manifestation and evolution of hybrid threats so that we not only look into innovations and solutions for today but also for tomorrow. It is one of the events arranged under EU-HYBNET Task (T) 3.4 "*Innovation and knowledge exchange events*".

The second EU-HYBNET Future Trends Workshop was organized by the Catholic University of the Sacred Heart of Rome, Italy (UCSC), and it took place as a hybrid event (in-person and on-line) event on 5th April, 2022 in Rome. This deliverable reports the methods and outcomes of the workshop.

1.1 STRUCTURE OF THE DELIVERABLE

This document includes the following chapters:

Chapter 2: *Future trends in the EU-HYBNET project*. This chapter explains how the annual Future Trends Workshop contributes to the objectives of the project, and why the future-oriented thinking has a special role in countering hybrid threats.

Chapter 3: *Methods*. This chapter explains what kind of information was gathered in the workshop, how this was done, and how it will be used.

Chapter 4: *Outcomes of the workshop: perceptions on future of hybrid threats.* This chapter presents the three trends that the participants considered most relevant for the future of hybrid threats.

Chapter 5: *Workshop participants and feedback*. This chapter includes the main content of feedback, and the main lessons learned.

Chapter 6: *Conclusions and way ahead*. This chapter explains how the data gathered in the Future Trends Workshop will be used in the project. This is important for the EU-HYBNET Work Package (WP) 3 "Surveys to Technology, Research and Innovations" Innovation mapping to pan-European practitioners and other relevant actors (industry, academia, NGOs) gaps and needs to counter hybrid threats.

2. FUTURE TRENDS AND EU-HYBNET PROJECT

The Future Trends Workshop (FTW) is part of the EU-HYBNET project T3.4 "*Innovation and knowledge exchange events*". Its purpose is to strengthen the future-oriented thinking among participants, and to provide a platform for out-of-the-box ideas, that might open new possibilities in countering hybrid threats. The workshops also supports to look into innovations and solutions to counter hybrid threats for today but also for tomorrow.

The Catholic University of Sacred Heart (UCSC) was the organizer of the second workshop in collaboration with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) leader of the Future Trends core theme, one of the four project core themes (others being Cyber and Future Technologies led by L3CE, Resilient Civilians and Local Administration led by UiT, and Information and Strategic Communication led by URJC). The Future Trends core theme's relevance stems from the paradigm of hybrid threats itself.

As the security environment becomes increasingly complex, so does the detection of emerging threats. Hybrid threats are by nature difficult to detect, as the hybrid threat actors operate below the threshold of open conflict, on multiple channels simultaneously, and are not always clear in relation to each other. Hybrid threats also evolve in time, due to technological advances and new ways to build resilience, and deter and counter the threats. Without detection, however, countering becomes impossible, and we would be always two steps behind, inevitably on the losing team.

These complexities are managed first and foremost by building a global, dynamic overview on evolving security issues. Foresight, especially the detection and analysis of trends is a crucial capability in this regard. To understand trends of hybrid threats or those affecting their evolution, a multidisciplinary approach is needed, and signals in every domain are relevant. Therefore, we need to bring together different actors – pan-European security practitioners, government practitioners, local administration, non-governmental organisations, academia and private sector, industry and SMEs – to learn from each other. The event took place before the second EU-HYBNET Annual Workshop in order to ensure a large participation of all stakeholders.

Due to the central role of the project four core themes, including the core theme on Future Trends, foresight and trends assessment is present in every phase of the project to some extent. However, the Future Trends Workshop is the only specific event dedicated to increase this capability. The Future Trends Workshop contributes especially to one of the project objectives (OB7), which is *to create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats.* One of the goals under OB7 is Goal 7.2 *to empower European practitioners, industry, SME and academic actors to recognise important innovations/trends.* The event was designed to contribute to that goal, with the focus on identifying and analysing possible trends and innovations to answer the future needs of pan-European security practitioners' and other relevant actors. The participants learned from high-level and panellist speakers how megatrends could affect European security. In the second part of the workshop, they got to share from their own perspective in smaller groups their opinions which were fuelled with diverse input they had been provided in beforehand. The work in small groups aimed at understanding the contexts of hybrid threats and trends as parts of megatrends, drawing a broad picture of the

environment in which potential innovations could be imagined. The participants' task was to define, what they thought are the most relevant trends affecting future of hybrid threats. The event was virtual and public, and therefore accessible to any interested stakeholder.

The table below highlights how the FTW in general will contribute to the project content and will support each EU-HYBNET Work Packages (WP) to proceed in their work.

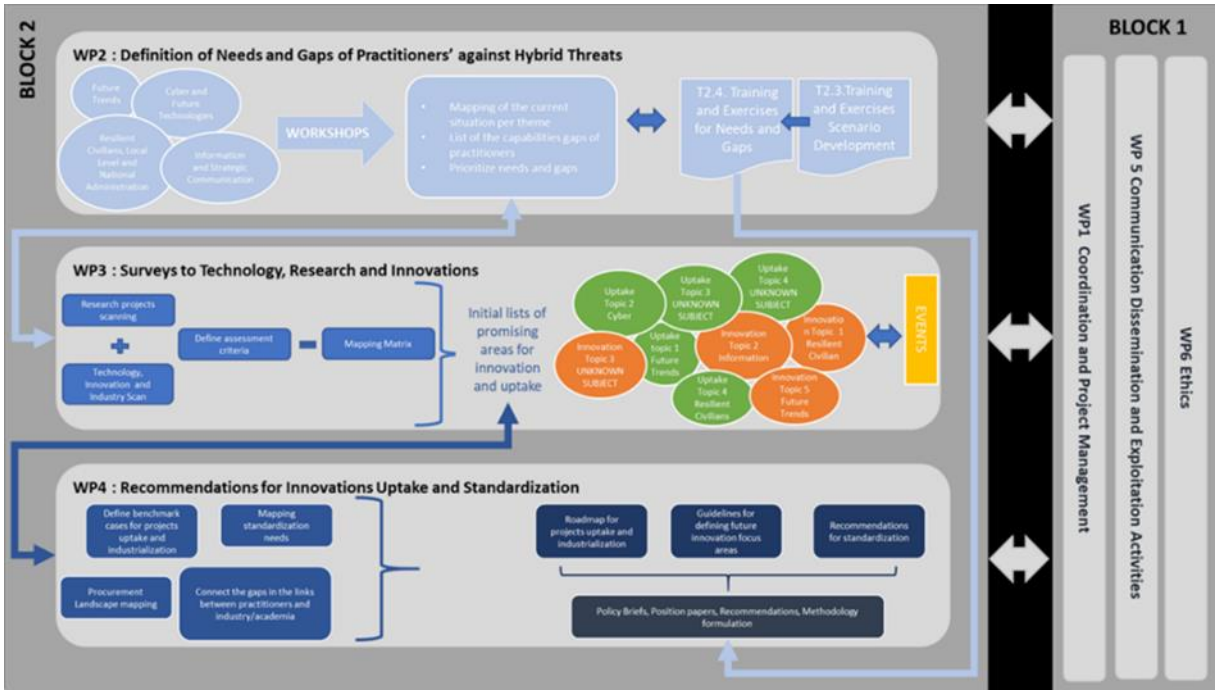

Figure 1 : EU-HYBNET Structure of Work Packages and Main Activities

The organisation of the FTWs are directly linked to **project Objective (OB) 1**: *To enrich existing network for countering hybrid threats and ensure long term sustainability,* and supports project **OB5**: *To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network*, **OB6**: *To foster capacity building and knowledge exchange on countering hybrid threats* and **OB7:** *To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats*. The OB Key performance indicators (KPI) for the network extension is the amount of events organised, which was set to a minimum 3 events every year. The detailed connection between the project objectives and the organisation of events within EU-HYBNET KPIs are described below.

Table 1 : EU-HYBNET Objectives 1, 5, 6 and 7

OB1: To enrich the existing network countering hybrid threats and ensure long term sustainability			
Goal		**KPI description**	**KPI target value**
1.3	To arrange and host events where practitioners, industry, SME and	Events are organized to attract European actors	At least 3 events every year where

	academic actors can engage in information sharing	willing to participate in professional exchanges	over 100 actors, all professionals in specific areas, will engage in information sharing
OB5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network			
Goal		**KPI description**	**KPI target value**
5.2	To set up community forums that will empower the European network to engage in productive exchanges on research and innovation, needs/gaps, uptake, policy issues, standardisation	Events for practitioners, industry/SMEs/academic actors are organised; forums established in relation to 4 core themes	-At least 3 events per year; at minimum100 participants -Innovation arena (IA) and Web site are in use by at least 4 forums (see KPI for Goal 5.1)
OB6: To foster capacity building and knowledge exchange on countering hybrid threats			
Goal		**KPI description**	**KPI target value**
6.1	To arrange dialogue sessions for EU practitioners, industry, SME and academic actors to strengthen capacity and hybrid threat knowledge exchange	Events are organised to communicate the new hybrid threat knowledge; and on latest best practices	-At least three yearly events are executed with a minimum of 100 participants each time
OB7: To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats			
Goal		**KPI description**	**KPI target value**
7.2	To empower European practitioners, industry, SME and academic actors to recognise important innovations/trends	Events are organised on innovations and future trends	-At least 2 events yearly where information on innovations and future trends is shared
7.5	To interact with a wide circle of European stakeholders, share information; and explore possibilities for engaging Network synergistically	Events are structured to facilitate interactions among stakeholders to establish synergies	-At least 2 events yearly where over 100 actors will meet - Newsletter, published every 6 months w. 60 new readers yearly

2.1 BENEFITS OF HOLDING THE FUTURE TRENDS WORKSHOP AT A MEDICAL UNIVERSITY

The EU-HYBNET Project has decided to perform the Future Trends Workshop inside a University Hospital. The fact that the Academy of Medicine is involved in the problems of hybrid risks is a novelty but also an aspect that probably anticipates the future. Hospitals as critical infrastructures can be

potentially an object of direct interest for the organizations that aim to destabilize the social fabric of a Country, even if we do not yet know what the specific targets will be.

On the other hand, since patients and people working in hospitals are the expression of the population, they are also potential object of malicious interventions aimed at changing their attitude towards health issues through disinformation and occasionally through the constitution of insider threats. We are very aware of this. During the recent Covid-19 epidemic, healthcare operators have had the opportunity to interact with subsets of the population strongly oriented against our therapeutic choices and who strongly rejected the proposals of the experts. The reason for this motivation was, as they strongly declared, “the lack of trust in our opinion and the certainty that others, such as Big Pharma, politicians, etc. enriched themselves on the population’s skin”.

Hospitals have therefore already grappled with a population of patients who, in addition to refusing preventive care, such as vaccines, have surprisingly widened the refusal to hospitalization and life-saving treatments once struck by the disease.

Having suffered the damaging effects at the level of vital organs such as the lungs or circulation, forced to go to Hospitals, they extended their total distrust to other therapies as well. Hospitals have had to face situations in which young patients at risk of death refused artificial ventilation, putting doctors in serious embarrassment in having to respect on the one hand the choice of the patient but knowing that the refusal – even if validated by signatures and assumption of responsibility - nevertheless represented the antechamber of death.

This interaction took place with a group of the population that was largely self-referring in judgment and probably influenced by inaccurate information transmitted through the media and who lived in what is defined as a “knowledge bubble”.

All these characteristics could recur in the future with other types of patients and create difficulties or even impossibility for Hospitals to carry out their function. Also, for this reason the Workshop on hybrid risks is of great interest. Healthcare workers participating not only as mere spectators but also as objects and victims of disinformation and other types of hybrid attacks due to this recent experience.

3. METHOD

This chapter describes the objectives of the event, what kind of information was gathered and how.

3.1 OBJECTIVE AND FOCUS

The main objective of the event, as the 2nd Future Trend Workshop (FTW), was to gather information from participants on what they thought were the most important elements that could impact the future context in which hybrid threats will manifest. The given time span was twenty years on. The reflections that ensued will support future assessment of EU-HYBNET results: defined gaps, needs, solutions and innovations. The purpose of bringing participants together to small working groups was to enable discussion and exchange on hybrid threats and trends in a more intimate environment and setting. The setting aimed at empowering out of the box ideas, which are needed to discuss trends and signals.

Future trends workshop aims to fulfil the project objective 1 (OB1), which is to enrich the existing network countering hybrid threats and to ensure long term sustainability. The public nature of the event enabled any European actor to join the project activities, making the project more attractive for new members to apply. The event provided arena for networking and information sharing, also contributing to project objective number 5 (OB5), which is to support conditions for enhanced interaction with the network. Moreover, enabling future-oriented thinking directly supports the sustainability of all ideas and solutions that the project produces.

By defining the trends that the participants deem most important in impacting the future of hybrid threats, the workshop also fulfils the project objective two (OB2), which is to define the common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours. The trends will support defining the most critical gaps and needs, which will be mapped in the beginning of the next cycle. One specific goal (Goal 2.3) under this project objective is to gather and define insights on trends, which the event did.

The focus of the Future Trends Workshop was developed in close collaboration with all the EU-HYBNET core theme leaders: Hybrid CoE, UiT, L3CE, and URJC. The topic of the meeting was: Are democracies on the edge?

Group/Trend 1: Changing populism: what are the forms of populism? How will populism evolve, and will it be a determining political movement in the future?

Group/Trend 2: Instrumentalization of social networks: what are current social networks? How will the galaxy of social networks look like in the future? Will information virality models give and deepen social networks' future harm potential at systemic levels?

Group/Trend 3: Constitution of international groups: what narratives and topics unite and create movements transnationally? How can this be used as a tool by outside actors? Are these likely to grow into political force or are they more of a disruption?

The topics were chosen in relation to the identified gaps and needs under each core theme. They were considered relevant contexts for the future manifestations of hybrid threats, in which the trends

emerge. The group themes were chosen based on discussion of the most important lines of research and investigation pertaining to the project four core themes.

3.2 WORKSHOP STRUCTURE

The event organisers arranged a full-day hybrid workshop: in person, within UCSC premises and online, on Zoom platform. The event consisted of two parts: the first part with a keynote speech and a panel of high-level experts and a second part more interactive where the participants were divided in three groups.

The keynote and panel served the purpose of inspiring and introducing everybody to the selected approach. The topics of the keynote and panel were related to the topic of the event and included a keynote speech by Jonas Cederlöf from DG DEFIS and two panellists: Lauri Tierala from the European Digital Media Observatory (EDMO) and Georgios Kolliarakis from the German Council on Foreign Relations.

The second, more interactive part consisted of three (3) breakout sessions, during which participants worked on a shared collaboration platform. Each breakout session had three phases: 1) pre-reading and questionnaire 2) discussion on presuppositions and how they might be challenged and 3) defining what belongs to different levels of possible and/or desired change.

Full workshop agenda is in Annex III.

PRE-READING AHEAD OF THE WORKSHOP

Each registered participant had to indicate the three groups in order of willingness to participate. The list of participants was reviewed by UCSC and Hybrid CoE in order to assign every participant to the most appropriate group. Participants received background reading produced by the experts at the Hybrid CoE. The purpose of the pre-reading material was to provide food for thought, a context for emerging threats, and an introduction to the trends. Pre-reading text is in the annexes of this deliverable.

DISCUSSION ON DRIVERS OF CHANGE AND DISRUPTIVE EVENTS

Breakout sessions built on the background paper highlighting a series of themes and ideas by the theme leaders that served as chairs and as rapporteurs. Discussions in breakout sessions focused on what drivers of change, undercurrents or disruptive events might shape the future of the topic of the session.

Each rapporteur was also provided with questions that were useful to guide the conversation and the debate.

4. OUTCOME OF THE WORKSHOP: PERCEPTIONS ON FUTURE OF HYBRID THREATS

After the meeting opening by Dr. Hanna Smith (The European Centre of Excellence for Countering Hybrid Threats/ Hybrid CoE) and Dr. Sabina Magalini (Universita Cattolica del Sacro Cuore/ UCSC), Mr. Cederlöf from DG DEFIS gave his keynote speech.

Mr. Cederlöf reflected on the title of the workshop "Are democracies on the edge?" considering different ways of understanding its meaning. War history as well as ongoing crisis raise the attention on the fact that everything can be weaponized while the concept of hybrid threats remains very important, especially thanks to its holistic approach. Kinetic war can affect population and countries far away from the actual war. Mr. Cederlöf briefly presented the DG DEFIS and its activities, among these DG DEFIS is the coordinator of counter-hybrid threats activities in the European Commission. He underlined the importance of the Defence Package and of the Hybrid Toolbox noted in it.

The panel discussion involved Mr. Tierala and Mr. Kolliarakis and was chaired by Dr. Hanna Smith.

The speech of Mr. Tierala included the following points and key take-aways are listed below:

1. How to define the phenomenon of disinformation
2. What EDMO is
3. What are we seeing now regarding Ukraine

1. Disinformation includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.

Disinformation does not cover issues arising from the creation and dissemination online of illegal content (notably defamation, hate speech, incitement to violence), which are subject to regulatory remedies under EU or national laws, nor other forms of deliberate but not misleading distortions of facts such as satire and parody.

Disinformation examples from the first phases of the war between Russia and Ukraine were identified by fact checking of news by EDMO. Various trends of false negative narratives were identified:

Trend 1: questioning of the war from its reality to its motives, Trend 2: unsubstantiated information about fighting and surrender, Trend 3: disinformation on the humanitarian crisis, Trend 4: distorted representation of Ukrainians, Trend 5: supporting frame for Russian invasion of Ukraine.

There were claims that CNN was giving false news: this was untrue.

Drivers of disinformation are: changes in information eco-system that are giving more power to the social media systems, which are more difficult to control; polarization within societies and loss of trust in Institutions (this phenomenon varies in Europe from one MS to another).

Basic to the Information Eco-system: to consider there is a Filter Bubble, which is the result of personalized search, where a website algorithm selectively determines what information the user would like to see, based on profiling of that user (location, previous click behaviour and search history, etc.). In this way, users will not see information that contradicts their own point of view. This isolates

users in their own cultural or ideological bubble. The choices the algorithms make are not transparent. However, this is business, and this is how platforms make money. One very active ongoing discussion is on how researchers can access the data generated by the platforms: are they available, are they raw data, aggregated data, etc.? The filter bubble is not illegal as such, and it is difficult for legislators to regulate it. These are some questions we are asking ourselves presently. A code of practice on disinformation has been issued in the previous years by the European Commission and it led to the funding of EDMO. This code of practice signed in 2018 is not working perfectly and it is being updated. War has shifted funds but the code is in the final phase.

2. EDMO's key activities

EDMO is a multi-stakeholder network bringing together researchers, fact-checkers and media literacy practitioners from many MS in Europe (not all yet). It is independent from MS administrations, Commission and Industry. It is funded by the Commission but also from independent entities such as Facebook, Google, etc. as part of their fact-checking policies. It is helpful to know who they are. It has six pillars: 1) Setting-up a secure online collaborative platform for fact-checkers and researchers supporting the analysis of disinformation campaigns and a web portal (this is up and running for fact-checkers but it will be opened to researchers in disinformation this year); 2) creating a governance body which ensures public trust regarding the work of EDMO and which works on a framework on access to data for research purposes (with an Executive and Advisory Board representing the wide community working with disinformation); 3) supporting and facilitating coordination of independent fact-checking activities, 4) mapping of fact-checking activities in Europe and searchable directories aggregating fact-checkers and media literacy material (mainly supporting cataloguing of fact checking activities, but hopefully driving joint research); 5) supporting and facilitating the coordination of academic research activities and creating a repository with relevant peer-reviewed scientific literature; 6) providing relevant academic input and policy analysis support (code of practice is being updated).

One activity now is to define how to measure the compliance of the platforms.

National EDMO Hubs will be put in all MS. They combine an academic aspect and journalistic fact checking aspect. Spain and Italy are particularly strong and in Italy RAI (National Radio Broadcasting Station) is part of the Hub. Call of new Hubs was completed in March 2022 and before the end of the year 2022 a Hub in Germany will be funded.

3. Reflections due to the situation in Ukraine

The main threat in the last two years was related to Covid-19, but presently it is related to war in Ukraine. In many Member States the threat comes from the National Administration.

Presently there is an intent to collaborate with Ukrainian fact-checkers. There is an EDMO taskforce on Disinformation about the war in Ukraine, which focuses on disinformation in EU and EEA Countries as well as in the western Balkans. Some actors who were not collaborating with EDMO before have begun collaborating after the start of the war. The taskforce aims to steer and collect material to help understand disinformation trends in the war in Ukraine, quickly identify and understand the disinformation trends in the current crisis to help foster societal resilience and inform and contribute to evidence-based policymaking. The Taskforce also aims to identify relevant datasets needed to understand the disinformation campaigns.

Presently EDMO is not tasked with collaborating with Countries outside the EU.

One recent example is the fact-checking on the images from Bucha that the Russian Government affirmed were not real; instead their truthfulness was proved. The war has brought a new phenomenon. The birth of fake fact-checkers has been identified. Something never heard of before which takes some innovative thinking. There is a site called WarofFakes.com, close to 200.000 subscribers on Telegram, set up by Russian individuals. We do not know if there is Government support or not. It is high-level and produces a lot of content quickly and rapidly, and they mix genuine fact checking stories with absolute lies. Published stories that Zelensky escaped to Warsaw, that the pictures coming from Bucha are actually fake, etc. They use exactly the same methodology European fact-checkers use, and it is really amazing. We must really pay attention.

What is next? What to do we expect on disinformation related to the War? Three aspects were highlighted:

1. Covid-19 disinformation community is more susceptible to Russian Propaganda. Communities which have been most exposed to Covid-19 disinformation are now more likely to be main recipients of pro-Russian disinformation. This permeability is heightened by some political figures who were previously purveyors of Covid-19 disinformation and are now active spreaders of Russian propaganda. While this is still marginal, it could extend to larger sections of the political spectrum.

2. Disinformation on discriminatory practices Vs Russian national in the EU and Russophobia. “Russophobia” represents a real problem, especially in Eastern Europe. This sentiment is being amplified into unsubstantiated discriminatory actions taken by public institutions in the EU against Russian nationals, including denying them equal healthcare treatment. In Paris there is a campaign against “stop hating Russians”.

3. Disinformation regarding refugees, which is the most worrying at the moment because there has been a great benevolence towards refugee, but as time goes on and they stay in MS maybe the situation will change.

The speech by Mr. Kolliarakis included the following topics:

1. **Hybridization as a wicked problem: the challenge of forward-looking security policy in democracies**

While the previous orator has spoken about Fact-checking, facts that have already happened, which is backward looking, because things have already happened, foresight or forward looking is just imagination of what might come, it is speculation. Foresight however is very important for policy-making because otherwise policies are limited to their timespan based on the past. Hybridization is a phenomenon of change, it is a moving target.

Much of what said comes from individual frustration of things that might work better but do not.

Deliberation in democracies: slow – checks and balances (3 +1). This is a slow process, because aside from the legislative, executive and judicative powers, there is also the press particularly the Boulevard

Press which creates the "sentiment". This Boulevard press is the one that determines nightmares in the government at 6 o'clock in the morning.

Coalition-making & Compromises: Political vs. Fact-driven. Is the possibility of making majorities to push a decision, which more often than not is based on political compromise and not on fact, which may lie out there for long and not be considered. And at the end of the day decision are taken on majorities and these are dependent very much on crowds.

Planning horizon: short termism. The planning horizon of a democracy is 4-5 years maximum. Politicians need to be re-elected. Dictatorship does not face this issue. Authoritarian systems do not care about internal criticism and public media expressions. This is even more complicated when we have to consider the multilateralism of the European level of decision making. When we go to international level it is even slower. To exemplify when we reach the definition of what a hybrid threat is this hybrid threat might have changed. The time lag problem is a pacing problem.

Modus operandi: RE-active; bureaucratic inertia; lag of multilateral forums. There are many reasons why this modus operandi is re-active and not proactive, because we have to have the proof that the fact has happened to have the legitimation for a Head of state to go in front of the cameras to say we need one billion euros of funds for research, or defence in the latest case. And this comes too late.

2. **What is a sociotechnical system?**

Co-evolution of technological and societal, **democracies as hybrid socio-technical organisms: emergent effects; blurring of traditional boundaries**; not specifically human/machine, it is something much more because it has an aggregate level that produces **emergent** properties in the system. To exemplify from the first days of war there was posting of the satellite movement of troops in the field, which is completely new not seen in the past and has to be monitored. This hybridization of socio-technical systems that are organisms and as such alive, blurs some social boundaries of what is technical and what is human and physical.

3. **Policies: piecemeal & Fragmentation vs whole-of-government**

Contemporarily there are in place several policies which make very good sense even though fragmented. All policies tackle some aspects of hybrid threats from one perspective, however they do not communicate in a coherent consistent way to produce what we say a cross-cutting coherent view such as the whole-of-government view.

EU: not found yet equilibrium within the triangle of competitiveness – security – fundamental rights. In the recent years in the EU we have more and more the effort to reach that whole-of-government, but we are not there yet. One aspect is this competing perspective between economical and industrial interest or sovereignty, security, contemplation also into fundamental rights. All this is important, but the equilibrium is not there yet neither in the EU or in the MS.

Masterframes: technology as context for society vs society as context for technology

One very important aspect on which to reflect are those paradigms that are usually behind every policy paper and every analysis, for example that that specific technology is a context for society (that we have some technological developments that force us to act or to react in a certain way) and the other

way of considering society as the context for the development of technology which is the real innovation. This is an open question.

Wicked problems are those in which the areas of complexity, uncertainty and value divergence (or ambiguity) merge together. We have several priorities but they do not sync together very harmoniously.

Security policy in this definition can be viewed as a wicked public policy problem. Security domain is different from healthcare or education and in that it presents the following problems which are not seen in other contexts.

Hammer-Nail Bias: the definition of the problem depends on available solutions and not vice-versa (e.g. "High-Tech-fix solutionism"). We have some instruments and we describe the diagnosis of the problem in a way that matches the available instruments. If we invest a significant amount of money into innovation we tend to grasp hybrid threats as a predominantly technological challenge and we miss a big part of the picture. However, it must be recognize that the EU Security research program is very technologically oriented and in this way surely creates a bias.

Moving target: the definition of the problem depends upon other moving targets (i.e. regulatory frames, policies, perceptions, attitudes): What is the meaning of an "asset"? What happens between tangible and intangible assets that we have to protect? What is "criticality"? How do we measure it? Is it a stable zone or does it change in time? These methodologies are in a strict sense missing right now.

Reflexive dynamics: when a security challenge is communicated to the public a reflexive dynamics is generated that causes often a self-fulfilling prophecy. The problem of which the public was unaware starts existing and is automatically transformed (i.e. self-fulfilling/ self- defying prophecies). Even if it is an old problem (Robert K. Merton, 1940) today it is transformed in terrorism/counterterrorism, cyber operations that are not announced so not to create problems. Many problems are not announced so they will not create undenounced unwanted effects.

2nd order effects: solutions we deploy may trigger themselves non-anticipated/non-intended effects, and may generate new problems (i.e. "security paradox"). It is like with medication, it creates new problems because it has side effects.

This is something we have to have in mind when we tackle the development of popularism and of networks in the future. How to intervene on the social networks so as not to create further problems.

These are the challenges we have to bear in mind for a forward-looking security policy.

Anticipation: prerequisite for Strategy: grasp change, mutation, trans-formation. Anticipation is a non plus ultra for strategy at all. In that respect most strategy papers that carry the title of strategy do not deserve that title at all, because they just express an impression or a snapshot, but they do not go further to describe which is our goal and which is our roadmap to reach that goal.

"Future" as Discourse(s) in the PRESENT may become highly politicized or get captured by particularistic interests. Future in that respect is not something in the future but it is here and now. It is a discursive element that we use in our deliberations, in our policy papers, that can be captured by

certain political ideologies or certain particularistic interests in order to navigate into one or the other direction.

"Future" as ARTEFACT has less purchase value than (backward-looking) "Evidence" At the same time I repeat what I said at the beginning that future is a little problematic as artifact because it does not have this weight of evidence. It is very hard to "earmark" budget for example on the grounds of foresight alone. If you have a certain case, you can say one hundred billion now, before that critical event, that catastrophe, that crisis has occurred it is very hard to say we have to invest in defence because it is a matter of time that something will happen. That's why we are here in the EU seeing that we have built some of this, but after something bad has happened we can accelerate.

Stakeholder interface (Decision makers – Experts – Practitioners): diverging logics, Languages, Interests, time horizons for action

And obviously we have all kind of stakeholders involved in that game, not only politicians, not only technocrats and policy makers, not only civil society organizations, not only experts, not only industry, and all those actors have different logics, languages, different interests and different time lines but also different resources and different strength of voice in that sort of decision finding.

Why do we assist to Strategic surprise: lack of imagination? Blindness? Deafness?

At the end of the day, we are always taken by surprise by such events. And the question that has risen here is has this been a failure of imagination? Has someone been speaking and we were not listening adequately? Or have all those signals been out there and we have been blind?

The example of the Platypus or Ornithorhynchus was a hybrid creature. It has DNA of reptile, it has fur, it lays eggs, it also produces milk and feeds the babies. And Platypus in the 19th century has triggered major conflict among experts, and professors were trying to kill each other because this creature was breaking the categories and classification silos of zoology, and it was very difficult to grasp what this "thing" was. Is it a mammal or a reptile? This is the same problem of our categories that have this piecemeal approach, the mandates of the organizations and the institutions and so on.

4. Forward looking activities for policy making

Foresight, horizon scanning, trend analyses, scenario planning as forms of policy advice.

This is a major difficulty we all face in order to render those forward-looking insights into meaningful useful, and usable policy advice, exactly for the design of policies that can survive the next 5, 10 or 15 years.

Sensitize for "weak signals"; reduce "blind spots"; break conceptual silos; recast "definitions"

A major task there for us is to somehow receive weak signals that are in the periphery of the horizon, reduce blind spots we do not see very clearly at all, break conceptual silos such as the definitions.

Mobilize awareness and resources for issues not on the radar: How to transform an issue into a priority of the policy agenda?

And also mobilize awareness and resources. Awareness is a resource in itself for issues that are not very clear on the radar of decision makers. The agenda setting rendering an initially important issue into a policy issue is not automatic or in itself evident. There are very many problems out there that are not prioritized policy issues. So, this is a task in that process to help decision and policy makers to make a correct or a more realistic prioritization on the policy agenda.

From making SENSE (What) towards making USE (how): thorny trade-offs.

So, from making sense of bits and pieces that something might take place we can identify that a new form hybridization will be there in 5 or 10 years. For example, we have the issue of satellite imaging in social media network or what Lauri has referred to the fake fact-checking that fall exactly in that Millenia old game of doping and anti-doping, terrorism and counter terrorism. This is an innovation and counter innovation race. We know it since Millenia, and we live in that. We need to be aware of that game. Moreover, the decision making has to do with dirty and painful trade-offs. We have to prioritize, and we cannot have it all. And this is something that is better done in advance than running after something bad happened.

The "Collingridge dilemma" of anticipation

Of course, a major difficulty here is that the later, the more evidence we have about something at a later stage, the more confident we are about the positive and the negative impacts. But sometimes we need to take action early on, and early on at an early stage where we have a rather high/big possibility of control this foresight, this evidence is very poor. So, policy makers procrastinate and do not act very early and they also have good arguments because they do not have a solid case out of evidence so to speak to be able to state their needs in the present. This is a fundamental difficulty we have to bear in mind.

Animals we use at foresight to describe certain phenomena:

- The red herring: false indication of a trend that misleads us
- The black swan: a phenomenon or an event that strikes abruptly has major impact, but we were not expecting it. High impact – low probability events.
- The grey rhinos: low intensity events that however are cumulating and after a certain point of time they reach tipping point and then the impact is massive; the issue of climate change is of this kind or the issue of respiratory pandemics. We had for many times many warnings but there was inaction.
- The black elephant: extremely disagreeable issue that everyone knows somehow and sees, but it is very difficult to touch, it has a political value, it is very thorny so that is why we let it there. We do not speak about the elephant in the room.

What happens most of the time in foresight exercises we have several categories of possible outcomes.

The plausible outcomes are a subcategory of the possible outcomes, the probable outcomes are an even smaller category of the possible and probable outcomes, and we have also if we have done our strategic foresight exercise correctly, our preferable outcome and most of the time what slips out of our conceptual nets is the impossible and the implausible events. We think it is ridiculous to have them on our plate and that is why we get surprised when they happen. It's a long list of events in the recent history of the past decade for example when the American Department of Defence tasked with

Hollywood script writers (end of the 90s) to come up with security scenarios, they had a paper about flying objects falling into buildings. This scenario was discarded as implausible. It happened in 2001. There has been a study in the context of the European Security Research that collected several foresight projects (16 + 10). I was involved and in 2010 foresight was dealing with right wing populists, extremist parties, overturning the European order. Those scenarios we did not find in the project reports. They had gone to the Annexes because they had been discarded as irrelevant. This is a self-inflicted blindness.

When we have this cognitive scheme of known knowns, known unknowns, unknown knowns and unknown unknowns it is very useful when we design policies. We have the known knowns, we have some certitude, we also have some certitude about things we do not know, we speculate about an area which has to do with the unknown knowns things that we do not know we do not know. There has been a lot of buzz in the recent years about those unknown unknowns such as the black swan. What I am more intrigued about is the suppressed knowledge the unknown knowns or the insights we somehow know but we suppress, distracting our view from them, and that makes the process really complicated in terms of nasty surprises. An example of how "inconvenient information is kept out rather than kept in.." in organizations is what happened in 2008 when in the previous years all the CEOs that were warning against the financial bubble were fired. The bias of denial, distraction, dismissal and diversion are at the basis of this behaviour.

5. **"Futures" literacy for forward-looking policy**

Minerva's owl: anticipation as prerequisite for preparedness as prerequisite for readiness as prerequisite for resilience.

Minerva's owl flies in the dark and learns from hindsight, it comes too late for the anticipation-preparedness-readiness-resilience cycle.

Operationalize resilience: cycle of preparedness-prevention-mitigation-recovery needs cross-sectoral approach (s.EU Resilience Dashboards). To operationalize resilience we always have to have in mind the whole cycle.

The best solutions to this are seen to be following:

Build up a Multi sectoral Forward Looking (FL) Community-of-practice beyond "experts": Upstream-downstream: internal sponsors (policy makers); inter-institutional brokers those gatekeepers; external political champions. The multiplicity of actors is necessary to move a case, to create a window of opportunity, to draw attention in order to push an issue that otherwise would have been discarded for one or the other reason and make it visible and auditable.

Dare to think inconvenient facts outside the "comfort zone": interplay mindset and muscle.

We will never build up capacity, build defence, or cyber-defence or hybrid tools unless we adjust our mindset to the fact that things are in a flow and we need to become more agile if we want to make our democracies more resilient in the years to come.

After the panel presentations "questions and answers" (Q&A) session took place and it included the following questions:

Q: How long will it take for big organizations such as NATO, the EU or even Germany with the Lander to make a system where we can fully understand the complexities of both hybridity and also security as a whole?

A: There is a difficulty in the uptake of new technologies by big organizations, this is mostly because there is a lack in political willingness. Usually the political class feels the pressure and act faster when something that was considered improbable happens.

Q: How is fighting disinformation and dealing with social media collaborating to fight hybrid threats?

A: Social media platform are not doing enough for autoregulation. Regulating companies should think again if this continues not working.

Q: How do we assess that a narrative is disseminated with a malicious intention or if it comes just from someone who was wrongly informed?

A: It is not so important to know where the fake news is coming from but rather what is driving it.

Q: Two-thirds of radicalizations come from big social media companies such as Facebook and Twitter. However, there are also other giant companies from Russia and from China. Is the danger coming more from the isolation of these companies in their own countries rather than from the globalization of the platforms?

A: Censorship is not the first line of action in fighting propaganda. The appeal to the European Court of Justice will tell if banning of Russian media outlets in Europe was the right choice or not.

Q: Should we strengthen political will and responsibility? In this way we are just asking for more authoritative leaders. It's a Catch 22 phenomenon.

A: It is Political pressure and not foresight that is forcing politicians in Europe to change attitude. That development has been ongoing for some time. The reasons for this is because the liberal democracies are diminishing and in qualitative terms because of the rise of percentage of populism inside democracies of western type. If politicians do not want to implode they must become more responsive. Criticism comes from all those parties that affirm that democracies do not perform. This message is more tailored for politicians than for policymakers which are technocrats.

Q: Can policies promoting media literacy create unintended effects of deepening distrust in those communities impacted by the information?

A: On media literacy, EDMO is mapping media literacy in Europe and Mr. Tierala is not so worried. Healthy dose of scepticism is more efficient than nihilism and also more diffuse. EDMO is also running media literacy training.

Q: Can you please provide example of some known known which might become important?

A: The known knowns are the base which should take us to the unknown knowns. Democracies on the edge is a challenge but also the possibility of getting a quick response is important. But to have reaction

we need evidence. How to bridge this gap? We need an agenda setter but we need to know against what we are acting.

To summarize the above mentioned aspects highlighted in the presentations and the identified phenomena (namely "are democracies on the edge?") it can be sated that they formulate three megatrends, considered having most relevant hybrid threat implications in the mid-term future: changing populism, instrumentalization of social networks, and constitution of international groups.

TREND 1 – CHANGING POPULISM

The group discussion was conducted by Dr. Gunhild Hoogensen Gjørv, Professor at UiT, The Arctic University of Norway. The group started reading and revisit some of the definition provided in the background paper. Find below some of the important points raised during the group discussion and presented in the final plenary session.

Precising the definition of populism. There is in the concept of populism the redefinition of ourselves as the people vs the elite or an authority that is not addressing or reflecting the grievances of the main group. This is the departure point. The highlight is that there is a sense of grievance in this political approach of understanding politics. It has benefits for democracies, because it is an approach that allows people to express their grievances and if they are many (a collective) they can bring forward this grievance. It's a very important democratic process. However, populism can often simplify things, because it becomes an us against them. It can reduce problems without exploring the nuances between them. Sometime reductive kinds of problems are more attractive for populisms. The problem in populism are the grievances that expose vulnerabilities that can be used as a force multiplier for third party or external influence that can use these weaknesses to "polarize" people and manipulating the sentiments within. This is the goal, acting on the people through their grievances.

Populism can go right or left, and because populist tactics can be used also by mainstream parties, they in reality span a spectrum of population. Populist tactics may also attract fringe groups. It is important to monitor popularism but more so to identify in what situations popularism is manipulated and successively weaponized. It is important to identify what aspects of popularism resonate more inside the movements and are easier to weaponize. There are characteristics tied to the person, race, class, economics, gender, sexual orientation.

It should not be suppressed but we must be aware on how it can be used to enhance a threat.

To summarize:

- **Populism is not itself a problem**. It is a democratic expression, but it should be considered as something that can be weaponized. It can expose vulnerabilities that can be used to enhance a threat. It may be also recognized as a 'symptom' of the distrust of the people in authorities.
- **Us vs. them: population vs. elite/authorities.** The perception of authority can represent a trigger mechanism: "power out there forces you to do something you don't want to do". Clearly this is not part of the healthy centre-periphery debate

- **Third party** possibility of getting to know the weakness and start manipulating them or use them as force multiplier to polarize people.
- **Sense of grievances can be exploit to manipulate and multiply the sentiments within populism.** There is a sense of grievance in this political approach: it has its benefits for democracies because it is an approach that allows people to express their grievances giving power to people that has a similar feeling. At the same time this can bring to populism because it can often simplify problems, reducing it without exploring the nuances in them. Reductive types of problems can be attractive in politics embedded in populism and therefore populism itself it isn't the problems.
- **Spectrum of understanding populism**: populism movements vs. populism tactics. Many mainstream political parties are using populism tactics without being populist movement.
- **Content of populism and enemy images used by populist movement.** Content of populism include Anti-EU, anti-capital, conspiracy theories while Jews and homosexuals are usual target groups in populism. Harnessing one narrative to support another, for example anti-vaxx to support anti-NATO.
- **Tackling populism.** Many needs were expressed including: improve governance through a bottom-up approach, having a good technological monitoring, increasing the knowledge base of users, regulating social media with ethical standard.

TREND 2 – INSTRUMENTALIZATION OF SOCIAL NETWORKS

The group discussion was led by Evaldas Bruze from the Lithuanian Cybercrime Center of Excellence for Training, Research & Education.

- **Weaponization of social media.** To understand how information through social media works we need to monitor them constantly and identify their technological shifts. Only in this way we will identify how they can be "weaponized". The basis of this possibility of weaponization relies on the hyper connectivity. One example 2 days after the war started there was an input of 1.5 million pre- prepared information put online by both sides (Russia and Ukraine). It does not matter who is right and who is wrong it is a figure, 1.5 million information content pushed through 2 days. It works, it makes influence, it is a completely separate "war-zone" currently established. The conclusion is "information can work as a weapon".
- The need of **cyberoffensive defence forces or a defence line organization.** This is not only for military people but for all citizens because it is a way to respond, to be resilient, not to be misled. However, some integration of military doctrine will be necessary. We expect, in the future, huge developments on this part: for example, we should attempt to regulate the algorithms, or not to feed them in some way
- **Inter and intra institutional collaboration as well as with civil society in resilience building.** We are all very well interconnected in Cyberdomains. During the war in Ukraine we saw how vulnerable infrastructures are, how quickly they were damaged and blacked out. We need to be more responsive in these parts, more de-fragmented and more oriented to risk mitigation.
- **Social media phenomena.** In social media there have been a lot of cyber related activities organized:

  - **IT army of Ukraine.** They targeting pooled resources or simply computers and phones on any main infrastructure and it really worked. This means that we have to monitor that phenomenon.
  - "**Cyberstars**". Nowadays is fashionable to become a Cyberstar, a cyberactivist and hacker, claiming that you are performing criminal activities and these will not be recognized as crime especially among the youngsters or people from higher social classes.
  - **"Rebranding" of the major hacker groups**. To name the biggest re-branding we can think of Anonymous, one of the biggest threats some months ago and now they are back in some brightly shining "uniform of the hacker". In many ways they are perceived as good guys working on the bad side and in criminal acts.
- **Cultural/social/psychological aspects of the so called "youngsters".** These aspects are not so greatly highlighted and discussed in security aspects. They are patient, they are disciplined, and they are loyal. Moreover, they act without following the rules of geography and not even those tied to their European heritage if the case, of those of their social establishment. This is a phenomenon that does not even have a name yet but must be considered.

These phenomena might be contrasted by crowd sourcing bounty programs for students for identifying gaps in the systems, and by backing them up with security organization with policies and regulations.

- **Social media platforms have power:** Another aspect of more societal, social media, as a technology nature is the understanding of platforms and how to consume them. We are now understanding that social media platforms are not only companies but they are a kind of "power". Now we have not only USA based technological giants but also Asia giants and there is an ongoing Russian speaking diaspora which imposes some kind of information dominance. Social media will not stop developing and it is a huge business, whatever we will be regulating they will continue going towards higher profits, and higher consumer market. Setting more rules will make the system more sophisticated and there will be other ways in which they will be avoided we cannot say how the click economy will work and how the content economy will work. We have to reach a huge regulating mechanism implying sanctions or other systems on service providers in order to balance the system.
- **The importance of media literacy.** It is a real necessity and it deals not only with kids and adolescents but also with adults. Critical reading is the scope, how to teach people to do critical reading, how can we help them differentiate differ really good content from fabricated content which is journalistic. In general, the majority of people will say that they can distinguish good content from propaganda but they don't and we need that a large part of consumers knows the difference. We have to train and educate everyone that we are living in a complex world.
- **The future of technological advancement.** We have AI, ML algorithms. There is an increase in "shadow profiling" that is growing constantly. Recent papers show there are 500 points on which our behavior can be profiled. Around 50 to 100 are known and there have been huge workshops dealing with these topics. We have also the Metaverse, multi-metaverse environment where we will have social media, block chain, NFTs, and gaming industry joining into one together also with online commerce. Which will hold as well additional attributes such as complete decentralization, absence of single authority of controlling and governance, and with the consequences of this.

- **Do we want to have an EU media platform?** All the participants agreed and would like that it be governed by the code of ethics of good journalism, that it be built on the trust principles, must be regulated with high level of compliance and with adequately balanced sanctions or other measures that can guarantee very trustable, clean content. A great will in this direction has been expressed.

TREND 3 – CONSTITUTION OF INTERNATIONAL GROUPS

The group discussion was chaired by Ruben Arcos, professor and researcher in the Department of Communication Sciences and Sociology of the Rey Juan Carlos University (URJC).

- **Which issues are likely to make online community coalesce?** Virtually anything could be employed, and any topic can become an issue that can be exploited. Anything that can trigger a reaction of fear is likely to represent a potential issue that lately can become the core for debate to form international groups. Moreover, every cospirational theory can be part of it. Examples of issues include technophobia, meaning people may be vulnerable or can feel that their job is threaten by technology or AI; policies around diversity and inclusion can trigger grievances of some groups (eg. incels); antidemocratic and antiegalitarian ideas; hostility against EU and transnational organizations of people that may fear that sovereignty and autonomy has been threaten and that they will not have the control on their country.
- **The role of social media.** Algorithms of social media play a role, as soon as a person become interested in (or was just searching) a particular thing, he/she will entry in this filtered bubble being invaded with information on that thing, preventing the person from finding contradictory opinions.
- **Use of an already established and polarized group.** The group could be primed for various reasons by authoritarian actors, so the forums of this community can be fed by news and information not specifically pertaining to the main topic but on political or economic situation. The research point should be how to avoid that already established groups (possibly funded by authoritarian actors) exploit and radicalize these groups.
- **Information (is not seen yet) as a critical infrastructure:** information and data sharing is a critical point, especially within the private sector and between private-public sector. Private operators are not willing to share their vulnerabilities or information about previous attacks because these can be used by a competitor. The innovation should tackle this issue considering the data environment and the sector from which they are coming from; then the innovation can support in the elaboration of vulnerability assessment improving the security of the infrastructure.
- **Addressing the online before it becomes offline:** developing a stakeholder mapping based on key issues through a horizon scanning and early identification, developing indicators or indications of online extremism to prevent online radicalization. Furthermore, AI can be used to map interconnections of those stakeholders and actors.
- **Ideas for preventing radicalization:**
    - **Focus groups as honeypot for observing online communities.** Creating and orienting online conversation to observe the interactions and behaviors as well as the feelings that they elicit can be useful to better develop responses.

- **Train chatbots to use information from online conversation.** This needs to comply with current ethical principles and legal regulations.
- **Anticipating and identifying radicalized groups through intelligence cooperation.** Super forecasting of what topics may be likely to become issues from which online groups can be established.

TRENDS OVERVIEW

In general the Future Trends Workshop provided plenty of views of future manifestation of hybrid threats. However, some key topics were to highlight as a conclusion of the discussions and findings.

It is needed to highlight the importance of populism in hybrid threats because we were looking for the activity that targets minds and uses people. How can populism be used against us, and what types of platforms are utilized for this, what kind of environment turns populism into a threat. Populism must be accepted because it is part of democracy, but it can be used against us in different ways. It also exposes our vulnerabilities and it is a force multiplier.

We can also see this new issue of behaving profiling that, if looked with 'hybrid threat lenses' can be one used as priming activity. It sounds harmless to do profiling but what type of a threat this could be in the future. The same is losing the content context in this case anything can become a topic that divides us and can be turned against us in case we lose the content context.

Interestingly new kinds of narratives can be used to form new networks, the interconnectiveness. There are some surprising connections like those who believe in natural medicine might find friends in anti-NATO discussions and from that into more dangerous groups.

The speed and the volume of the internet exchanges is enormous and it represent a challenge for those who want to identify and tackle the unhealthy populism.

There is the trend of 'cyberstars', individuals turn into warriors: those who never thought about going to the battlefield now accepts to sit at home and fight through their laptop. Out of this could be born something like a bounty program for students for identifying gaps in the system.

The response to these threats should start from a new type of trust building. Policy makers should revisit the social contract; the feeling of inclusion must come back into our perception for democratic societies. The strength of democracies is that we feel safe to be who we are in the society we live in.

5. PARTICIPANTS, FEEDBACK AND LESSONS LEARNED

The event was arranged as a hybrid event taking place in person and on-line (Zoom platform). The event was semi-public, meaning that all the people who registered as well as their organization were pre-checked. The event was announced for all interested participants from EU and Associated Countries. It was advertised on EU-HYBNET website (https://euhybnet.eu) and social media from February 2022 onwards until mid of March.

A total of 56 organization registered for the event, most of them decided to participate online, 25 in person while 8 had representative both online and in person. 15 EU countries were represented and 3 non-EU countries (namely Georgia, Turkey and UK). Most of the organization represented the academic world while 14 the practitioners' side, 8 organizations were SMEs and 7 represented NGOs.

Out of 96 participants, 15 responded to the feedback questionnaire that has been shown before the closure of the event and sent via mail few days after it. All the responses came from people who attended the workshop in presence, we received no answers from online attendees. Participants were satisfied with the event and with its topic (average rating 4.47/5). Participants generally considered the event worthy of their time, with no difference between those who attended in presence and online.

They assigned a very high rating to the organization of the event (average rating 4.67/5), and to the helpfulness of the staff (average rating 9.27 out of 10).

The selection of the speakers was considered very good with an average rating of 4.53 on 5.

Positive feedbacks included the fact that the event was held in presence, allowing human contact, proximity and the possibility to easily networking; keynote speech and panellists were interesting, especially regarding the 'wicked press' concept.

Neutral and negative feedbacks mentioned the feeling that there were many interesting topics and that attendees were able to follow only one discussion group; during the closing panel there were many ideas presented and a participant had difficulties in following the topics mentioned in discussion groups other than the one they attended. Another comment mentioned the fact that the discussion was too high-level.

The room set-up, the room temperature and the room dislocation were also part of the negative feedbacks. Interestingly UCSC has used the same rooms for both days (Future Trend Workshop and Annual Workshop, which took place the day after) and there were no negative comments on the Annual Workshop questionnaire. Moreover, the organization of the event received a pretty good score.

Most of the respondents will be likely to participate in one of EU-HYBNET in future (14 out of 15).

6. How likely are you to partecipate in one of our events in the future?

Somewhat likely	3
Somewhat unlikely	1
Very unlikely	0
Very likely	11

6. CONCLUSIONS AND FUTURE WORK

The Future Trends Workshop achieved its primary goals of creating networking opportunities and to empower European practitioners, industry, SME and academic actors to recognize important trends, also to consider innovations that could deliver solution to counter hybrid threats in the future. Importance of foresight and its different use cases in addressing hybrid threats was highlighted to the participants during the panel. Interaction and mutual learning were enabled especially in the small group working sessions.

According to the feedback, the participants found the event worth their time, and were inspired for the opportunity that the workshop provided, especially concerning the keynote speech and the panel discussion. Feedback confirmed that the in presence events are absolutely important, especially for networking and discussion. This was also the first EU-HYBNET event in presence, since the project started during the pandemic (May 2020).

The discussions brought to the table the technical aspects of hybrid threats as well as innovations but also how we can think differently or learn a way to affect the other people's thinking and measures to counter hybrid threats.

The main purpose of identifying the trends is to provide a framework in which the project can assess the future relevance of project outcomes, policy recommendations and innovations. The trends can be used as exploratory frameworks in the next phases of the EU-HYBNET project, and can be addressed as a part of the Task 2.1, Needs and gaps analysis, as additional categories of identified gaps. The trends can be further tested in the research articles in Task 2.2, Research to support increase of capacity and knowledge, or in research produced outside the project plan. The identified trends and future innovations can be explored more in-depth in the coming Future trends workshops. These frameworks can also be taken into account for the recommendations in terms of innovations esp. in EU-HYBNET Task 3.1 "Definition of target areas for improvement and innovations". The relevance of the trends and innovations to the trends lies in the fact that they overarch all four core themes and needed future innovations to practitioners needs, and aim for understanding threats and vulnerabilities and technical and non-technical, human science based innovations that are shared by them.

ANNEX I: LIST OF ACRONYMS

DG DEFIS	Directorate-General for Defence Industry and Space
EDMO	European Digital Media Observatory
EEA	European Economic Area
EU	European Union
EU-HYBNET	Empowering a pan-European Network to Counter Hybrid Threats –project; funded by the European Commission, Grant Agreement number 883054
FTW	Future Trends Workshop
HYBRID CoE	European Centre of Excellence for Countering Hybrid Threats
KPI	Key Performance Indicator
L3CE	Lithuanian Cybercrime Center of Excellence for Training, Research & Education
MS	EU member state
NATO	North-Atlantic Treaty Organization
NGO	Non-Governmental Organization
OB	Objective
SME	Small and Medium Enterprise
T	Task
UCSC	Università Cattolica del Sacro Cuore
UiT	The Arctic University of Norway
URJC	Rey Juan Carlos University
WP	Work package

ANNEX II: LIST OF PARTICIPANT ORGANISATIONS

Organisation	Type of Actor
The Kosciuszko Institute Association	NGO
Smartlink	SME/Industry
TNO	Academic/Research and Training Organization
Cyber Security Bureau of the Ministry of Defence	Practitioner (Government, local or national)
European Defence Agency	Practitioner (Government, local or national)
Academic Centre for Strategic Communication	Academic/Research and Training Organization
Research Institutes of Sweden	Academic/Research and Training Organization
Satways	SME/Industry
Polish Association for National Security – PTBN	NGO
Defend Democracy	NGO
Laurea UAS	Academic/Research and Training Organization
G4S	SME/Industry
Nord University	Academic/Research and Training Organization
Combitech AB	SME/Industry
EDF	Academic/Research and Training Organization
Foreign Affairs Institute	NGO
Erasmus Network "I Mediterranei	Academic/Research and Training Organization
AIT Austrian Institute of Technology GmbH	Academic/Research and Training Organization
European Security and Defence College	Academic/Research and Training Organization
Istituto Affari Internazionali (IAI)	Academic/Research and Training Organization
DG DEFIS	Practitioner (Government, local or national)
Quo vadis Europe	Academic/Research and Training Organization
KEMEA	Academic/Research and Training Organization
Europol	Practitioner (Government, local or national)
European Digital Media Observatory	Academic/Research and Training Organization
Hybrid COE	Practitioner (Government, local or national)
Centre for Peace Studies	Academic/Research and Training Organization
German Council on Foreign Relations	Academic/Research and Training Organization
Fraunhofer IAIS	Academic/Research and Training Organization
L3CE	Academic/Research and Training Organization
HENSOLDT Analytics	SME/Industry
University Rey Juan Carlos	Academic/Research and Training Organization
Friends of Europe	Academic/Research and Training Organization
German Aerospace Center (DLR)	Academic/Research and Training Organization
EOS	SME/Industry
DG HOME	Practitioner (Government, local or national)
VOST Portugal	NGO
Fortinet	SME/Industry
EC-JRC	Academic/Research and Training Organization
Dataminr UK	SME/Industry

European Institute for Counter Terrorism and Conflict Prevention	Academic/Research and Training Organization
Joint Research Centre - European Commission	Academic/Research and Training Organization
The Ministry of Ecological and Solidarity Transition	Practitioner (Government, local or national)
Polish Platform for Homeland Security	NGO
National Intelligence Academy Mihan Viteazul	Academic/Research and Training Organization
Directorate for Civil Protection	Practitioner (Government, local or national)
Bundeswehr University Munich	Academic/Research and Training Organization
UCSC	Academic/Research and Training Organization
PLV - Valencia Local Police	Practitioner (Government, local or national)
Ministry of Defence	Practitioner (Government, local or national)
The International Centre for Defence and Security	Practitioner (Government, local or national)
The Internal Security Agency	Practitioner (Government, local or national)
Maldita	NGO
Central Office for Information Technology in the Security Sector	Practitioner (Government, local or national)
Estonian Information System Authority	Practitioner (Government, local or national)

ANNEX III: WORKSHOP AGENDA

EU-HYBNET

Agenda

2nd EU-HYBNET Future Trends Workshop: democracies on the edge?

Tuesday 05 April 2022 | 09.00 a.m. – 04.00 p.m. CEST

In presence at UCSC (Meeting room 5: plenary – Meeting rooms 3,4 and 5: breakout sessions)
On line via Zoom call

Time	Topic	Speaker(s)
08.30-09.00	Welcome and Registration	
09.00-09.10	*Welcome words*	Hanna Smith, European Centre of Excellence for Countering Hybrid Threats
09.10-09.15	*Practical information*	Sabina Magalini, Università Cattolica del Sacro Cuore
09.15-09.30	Keynote Speech: "Are democracies on the edge?"	Jonas Cederlöf, DG DEFIS
09.30-09.45	**Q&A from the audience**	
09.45-10.00	**Leg stretch break**	
10.00-11.20	Panel discussion	*Chair:* Hanna Smith, HCOE *Discussants:* • Lauri Tierala, European Digital Media Observatory • Georgios Kolliarakis, German Council on Foreign Relations
11.20-11.40	**Break**	
11.40-12.50	Breakout sessions: Meeting Room 5 - *Populism* Meeting Room 4 - *Social Network* Meeting Room 3 - *International Groups*	*Chairs:* • Evaldas Bružė, Lithuanian Cybercrime Center of Excellence for Training, Research & Education • Gunhild Hoogensen Gjørv, The Arctic University of Norway

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

		• Rubén Arcos, Universidad Rey Juan Carlos
12.50-13.50	**Lunch break**	
13.50-14.50	Breakout sessions: Meeting Room 5 - *Populism* Meeting Room 4 - *Social Network* Meeting Room 3 - *International Groups*	
14.50-15.10	**Leg stretch break**	
15.10-15.50	Closing panel	*Chair:* Maxime Lebrun, HCOE *Rapporteurs:* • Evaldas Bružė, L3CE • Gunhild Hoogensen Gjørv, UiT • Rubén Arcos, URJC
15.50-16.00	Closing remarks	*HCoE and UCSC*

Hanna Smith

She is the Director of Research and Analysis at the Centre of Excellence for Countering Hybrid Threats and visiting professor for the academic year 2020–2021 at the College of Europe, Bruges. Dr Smith is an expert on hybrid threats, Russia and Eurasia and Great Power identity, with research interests including security studies, international relations and institutions, as well as regional and Nordic cooperation. Her latest publication is *Strategic Culture in Russian Neighbourhood* (Lexington 2019) with Katalin Miklossy (eds.).

Jonas Cederlöf

Description to come.

Lauri Tierala

Lauri Tierala is Programme Director at EDMO, European Digital Media Observatory. He is based in Italy, at the European University Institute's School of Transnational Governance which hosts the secretariat of the EDMO. Until recently, Tierala was a partner and senior advisor at Miltton, a public affairs and communications consultancy. Previously, he was responsible for global and European public affairs at the airline Finnair. He brings a long track record in European politics, having previously served in the European Parliament and the European Movement, among others, and worked as a special advisor on EU affairs to the Finnish Prime Minister.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

EU-HYBNET

Georgios Kolliarakis

Georgios Kolliarakis works with the German Council on Foreign Relations (DGAP) as Advisor for Research Strategy. Georgios has a track record in public policy analysis, with a particular focus on strategic and organizational aspects of security policy, including security research, and science, technology & innovation policies (esp. Dual-Use). He has led a series of pilot interdisciplinary research projects, and advises national ministries and international bodies, including various UN agencies, the European Commission, the Council of Europe, and the OECD, on issues of anticipatory security governance, foresight, and transfer of evidence to policy. Georgios is a member of the International Network for Government Science Advice, and belongs to the DIN Standard Interdisciplinary Working Committee on Artificial Intelligence (Sociotechnical Systems) and the World Economic Forum`s Expert Network. After his engineering studies at the Technical University of Athens, Georgios earned a master's degree in political geography at the University of Bonn, and a PhD in International Relations (Security & Strategic Studies) at the Ludwig-Maximilians-Universität Munich.

Maxime Lebrun

Maxime Lebrun, Senior Analyst, Research and Analysis. Prior to taking up his post at the European Centre of Excellence for Countering Hybrid Threats, Maxime worked at the Baltic Defence College in Tartu as a Lecturer in War and Conflict Studies and as Acting Department Director. During that time, he was also a Non-Resident Research Fellow at the International Centre for Defence and Security. Maxime holds a master's degree in International Relations from Sciences Po Lyon with a specialization in strategic, military and security studies from Sciences Po Aix-en-Provence.

Evaldas Bružė

Description to come.

Gunhild Hoogensen Gjørv

Gunhild Hoogensen Gjørv is Professor of Critical Peace and Conflict Studies with a specialization in Security Studies and International Relations at the University of Tromsø- The Arctic University of Norway. Gjørv's research has interrogated the interactions and tensions between perceptions of state and human security in a variety of contexts, with a particular focus on civil-military interaction (out of area operations, as well as Norwegian defence), and Arctic perceptions of security. She currently serves on board for the Norwegian Institute of International Affairs, and previously on boards for the Norwegian Research Council, and the International Arctic Science Committee.

Rubén Arcos

Dr. Rubén Arcos is a professor of communication sciences at URJC and a member Ciberimaginario. He is co-founder and co-director of IntelHub, an international network for the study of intelligence. He is a freelance contributor to Jane's Intelligence Review and Deputy Editor of The International Journal of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Intelligence, Security, and Public Affairs. He is a member of the Hybrid CoE's information expert pool. His main research interest are intelligence, strategic communication and hybrid threats.

Sabina Magalini

Senior Surgeon of the Emergency and Trauma Surgery Unit at the Fondazione Policlinico Universitario Gemelli (FPG) and Assistant Professor of Surgery at the Rome Catholic University School of Medicine (UCSC). She is also an Associate Researcher of the Italian National Council of Research (CNR-IASI); Fellow of the American College of Surgeon, of the American Association for the Surgery of Trauma and of the European Society for Trauma and Emergency Surgery (ESTES).

More info and updates on the EU-HYBNET Future Trends Workshop at:

euhybnet.eu

EU-HYBNET LinkedIn Group

@EuHybnet

EU-HYBNET Project Coordinator Laurea University of Applied Sciences – Päivi Mattila paivi.mattila@laurea.fi

"This workshop should also address expected future manifestation and evolution of hybrid threats so that we look into innovations and solutions for today and tomorrow

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

ANNEX IV: BACKGROUND READING MATERIAL

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Background paper for the 2022 Future Trends Workshop (EU-HYBNET)

Discrediting democratic governance: democracy, populism, and autocracy

One purpose of democracy is to make tyranny impossible by limiting abuses of power. Autocracy works as the exact opposite since it aims to concentrate and maximise power in the hands of a tyrant. Power in democracy is limited by design because it belongs to all citizens. The system avoids the abuse of power at the expense of others. This article characterizes the challenge that democracies can face if hostile external actors would leverage populistic movements and use them against the safeguards of democracy. This article details the logic of populism and refines the dichotomy between democracies and authoritarian systems by suggesting that democracies can derelict into authoritarianism through populism.

Democracy makes several sources of power and legitimacy coexist and check each other. The people are the prime source of power. The executive, legislative and judiciary powers derive from Constitutions established by the sovereignty of the people. Freedom of expression, of the press and of assembly form the last essential power source in a democracy. The constitutional separation of powers[1] together with a free press and free expression are key to avoiding tyranny through checks, balances, oversight and holding power to account. It makes it impossible for sovereignty to be fully confiscated by any constituent part of the body politic at the expense of the whole. Democracy relies on the principle of representative government: channelling the expression of the people's sovereignty in politics makes a form of representation necessary. Elections in democracy fulfil the role of a popular tribunal instead of the direct channel of the people's will. As Karl Popper put it in *The Open Society and its Enemies* (1945): "*Realizing democracy rather implies avoiding the perils of tyranny than putting the People in power*". There can be no deliberation and progress of policy without institutionalising the discussion among the representative parts of the people.

Populism is not a unified ideology, but it is rather a system of claims, sources of resentment, and victimhood. The common denominator of populism is the belief according to which the people is being misrepresented by the existing governance system (the Elites) and deprived of its voice and sovereignty. Populism pits the people against all other forms of power in democracy. The main logic of populist parties and movements is to require a systematic and direct appeal to the people as a mode of governance, abolishing any role to intermediaries identified as "the elite" – the media, the judges, politicians, etc.[2]

This short analysis proposes background to group discussions to be held under the 2nd EU-HYBNET Future Trends Workshop. It highlights a series of considerations along three suggested topics: populism as a growing structural factor of democratic life; digital social networks as accelerators of the kind of information virality model that enable populism; the growing constitution of international groups of actors that can form powerful political movements around populist tenets.

[1] Charles de Montesquieu, *The Spirit of the Laws*, Cambridge Texts in the History of Political Thought, Cambridge University Press, 1989

[2] Collin, Katherine, "Populist and authoritarian referendums: the role of direct democracy in democratic deconsolidation", Report, Brookings Institution, February 2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Hybrid CoE
Unioninkatu 20-22
FIN-00130
Helsinki, Finland

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Future dynamics of populism

Populism contests the legitimacy of the existing representation system in democracy because it would not "adequately" represent the people in its entirety. It contests the formal legitimacy of democracy by pitting the People against institutions and intermediaries. The system of ideas behind populism fuels a series of processes that can frontally contest the tenets of democracy. In this way, populism can be strategically instrumentalised by hybrid threat actors to discredit democratic models of governance. Claude Lefort analyzed totalitarianism as a pathology within democracy's own development path. Lefort's work highlighted how authoritarianism can emerge from democracy as an attempt to negate and overcome divisions within the latter.[3] The populistic challenge consists in a drive for radicalisation of democratic life, which can be a vector towards a more authoritarian practice of power.

Populism considers there is a "gap" between the ideal of representation and the reality of it. Populism seeks to make any power to stem as directly as possible from the People. That's why it considers the principle of separation of powers contrary to that of popular sovereignty. Independent bodies, courts, agencies are against the essence of populism. Populism engenders a concentration of power in those institutions directly stemming from the people. Because power emanates from a unitary people, populism implies the negation of conflict within the people. Negating conflict supposes polarizing the population against an enemy image. The enemy is an amalgamation of figures both external and internal, all directed against the security, safety, tranquillity of the people as an essence.[4]

A key element of the populist platform is the tool of referendum as ordinary practice.[5] The systematic appeal to the referendum would lead to a disappearance of the notion of political responsibility and accountability over the course of policy choices as it extinguishes the relation of responsibility / and structural difference from government to the governed. The possibility of holding government into account over policy offers a space for reflexivity. It makes government oversight possible. As the people would be deciding directly, there would not be a possibility for oversight and sanctioning of harmful policy choices via elections.

The impact of digital social networks

Digital social networks have plugged into this platform to a large degree. They enable and amplify a narrative that flattens hierarchies between individuals and sources of power. It relativizes expertise and established knowledge. Digital social networks have empowered and connected individuals. They have allowed parts of the population to take part in political debates on an equal footing, regardless of expertise, previous standing, or experience. Information virality models of social networks structurally promote emotional and short statements over balanced and reasoned argumentation. Information circulation trends on digital social networks give audience to particularly catchy and short assertions. They account for the eased proliferation of hate speech and polarization because it lessens the space for deliberation and argumentation. Social networks are pushing this process by allowing immediacy to play a role. This also nourishes a strong rejection of "traditional" media.

---

[3] Lefort, Claude, Democracy and Political theory, , Wiley, Polity, 1988, ISBN: 978-0-745-60437-4
[4] Rosanvallon, Pierre, *Le siècle du populisme: histoire, théorie et critique*, Les livres du nouveau monde, Editions du Seuil, Paris, 2020
[5] *Ibid.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Hybrid CoE
Unioninkatu 20-22
FIN-00130
Helsinki, Finland

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Social media favours more radicalisation in democracy. The Election Integrity Partnership in its report about the 2020 US election found that "misleading and false claims and narratives coalesced into the metanarrative of a 'stolen election' which later propelled the January 6 insurrection". The report considers that "the production and spread of misinformation was multidirectional and participatory". "Stop the steal" is emblematic of the populist radicalisation of democracy that social media can amplify. Empowered individuals, on an equal footing, can coalesce a narrative which triggers physical radicalisation, violence online and offline alike. Radicalisation, literally going back to the "root" of democracy – the people – is the result of considering that the People would be the victim of a thief. Power is deemed stolen from the people by the elites of the "system". The radicalisation of democracy fuels authoritarianism because it bypasses the institutions of democracy that are meant to put a check on power. "Stop the steal" shows a coalescence of false and misleading claims with very real feelings of victimhood that translated into a cognitive and physical radicalisation of individuals and groups of protesters.

The constitution of international groups

Individual users are empowered to express their opinion and have a way of connecting with like-minded individuals around the globe. While social networks have always existed, digital social networks offer an unprecedented reach and connection opportunities. Those networks can even constitute international groups around the tenets of populist movements. Digital social networks are a powerful vector in connecting sources of resentment, interest groups and victimhood across borders.

Populism, as a system of ideas, values and victimhood can connect diverse sets of groups, audiences or publics around common causes or metanarratives. This can turn into a powerful political force. The example of the internationalization of the Alt Right highlighted by Weiai Wayne Xu[6] is emblematic of the processes that could play with other audiences connected to populist value systems in the future. International groups can be akin to "counterpublics"[7] as they designate "alternative public spheres in opposition to the dominant public". Counterpublics are useful to understanding the kind of international groups that can form under populist systems of ideas since their identities relate strongly to a feeling of victimhood, marginalization, or discrimination. This is what populism can tap into most efficiently. Social media make "networked connective actions" able to build "counter identities", nurture radicalisation and extremism. [8]

Counterpublics have been associated with positive developments and progresses in rights and inclusion. Counterpublics have been instrumental in feminism, climate change advocacy and militancy for marginalised and discriminated against groups of people. Populist tendencies in democracies logically constitutes counterpublics of a different kind which can be instrumentalised by hybrid threats actors to exploit division or sow even deeper controversy in order to push forward extremism, cognitive and violent radicalisation. The constitution of transnational counterpublics reduces the space for positive sum compromises and debates.[9] The combined effects of populism, digital social networks, and the phenomenon of constitution of

[6] Weiai Wayne Xu, "mapping connective actions in the global alt-right and Antifa counterpublics", International Journal of Communications Vol 14 (2020), UCSC Annenberg School for Communication and Journalism, Los Angeles.
[7] Fraser, Nancy. "Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy." *Social Text*, no. 25/26 (1990): 56–80. https://doi.org/10.2307/466240.
[8] Xu, (Ibid)
[9] Holm, M. 2019. The Rise of Online Counterpublics? The Limits of Inclusion in a Digital Age. 246 pp. Uppsala: Department of Government. ISBN 978-91-506-2778-7.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Hybrid CoE
Unioninkatu 20-22
FIN-00130
Helsinki, Finland

counterpublics online and offline make democracy more polarized and make it easier to leverage extremism and violent radicalisation to cripple decision-making and sound political deliberation.

The dynamics of populism, their amplification with social media and the constitution of international groups can feed metanarratives and coalesce into cognitive and violent radicalisation of individuals and groups. Leveraging radicalisation and extremism is a critical threat surface that hybrid threat actors could seek to exploit in the future. Addressing their root causes and endemic nature is a necessary challenge in order to preserve democracy.

Indicative follow-up questions for the group discussions

1. The future of populism

- Will populism continue to play a role in democracy and for what reasons?
- What is the impact of populism on international relations?
- What are the kinds of victimhood that can fuel the appeal for populist platforms?
- What kind of enemy images are likely to be appealing for populist movements?

2. The impact of digital social networks

- What to expect from the future landscape of digital social networks? More concentration? More diffusion?
- What is the role of hyper-personalized advertising and targeting in the information circulation loops? How are individual data aggregates used?
- Will social media only promote short statements and assertions? Are there other information virality models possible?
- How will the role of individuals evolve in information circulation on digital societal networks?

3. The constitution of international groups

- Which issues are likely to make online communities to coalesce?
- What are the groups and communities that are likely to form into counterpublics?
- What are the ways in which online extremism turns into violent radicalization offline?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Hybrid CoE
Unioninkatu 20-22
FIN-00130
Helsinki, Finland