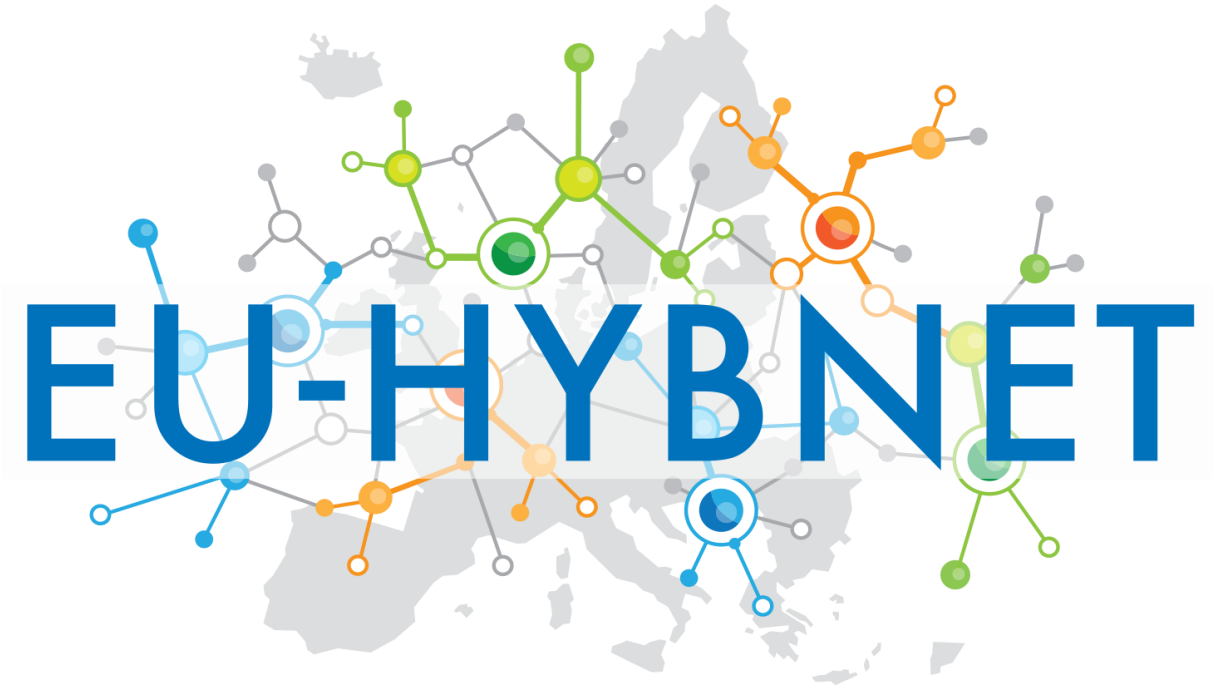


FUTURE TRENDS WORKSHOP REPORT

DELIVERABLE 3.14

Lead Author: Hybrid CoE

Contributors: TNO, Laurea
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

D3.14 FUTURE TRENDS WORKSHOP REPORT

Deliverable number	**3.14**	
Version:	**0.7**	
Delivery date:	**1/6/2021**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public (PU)**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	**Paul Dickson, Emma Lappalainen, Maxime Lebrun**	**Hybrid CoE**
Contributors:	**Okke Lucassen** **Päivi Mattila, Tuomas Tammilehto**	**TNO** **Laurea**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	11 May 2021	Paul Dickson, Emma Lappalainen, Maxime Lebrun / Hybrid CoE	First draft, text to all chapters
0.2	25 May 2021	Okke Lucassen / TNO	Review
0.3	31 May 2021	Emma Lappalainen / Hybrid CoE	Editing
0.4	31 May 2021	Päivi Mattila / Laurea	Review
0.5	31 May 2021	Emma Lappalainen / Hybrid CoE	Final editing
0.6	1 June 2021	Tuomas Tammilehto/ Laurea	Ethics Review
0.7	1 June 2021	Päivi Mattila / Laurea	Submission

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

The Future Trends Workshop 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. It is one of the event arranged under EU-HYBNET Task (T) 3.4 "*Innovation and knowledge exchange events*".

The first EU-HYBNET Future Trends Workshop was organized by the Hybrid CoE, and it took place as a virtual event on 31st March, 2021. 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.

Chapther 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 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 up new possibilities in countering hybrid threats.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is the organiser of the first workshop, and 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 – government practitioners, local administration, non-governmental organisations, academia and private sector – to learn from each other.

Due to the central role of the 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 Gaps and Needs Events in EU-HYBNET WP2 "Gaps and Needs of European Actors against Hybrid Threats" include an element of anticipation, but the Future Trends Workshops specifically concern perspectives relevant for the next two decades. The Future Trends Workshop contributes especially to one of the project objectives (OB.7), 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. The participants learned how megatrends could affect European security, from high-level keynote and panellist speakers. In the second part of the workshop, they got to share from their own perspective in smaller groups, which were fuelled with diverse input they 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 think are the most relevant trends affecting future of hybrid threats. The event was virtual and public, and therefore accessible to any interested stakeholder.

3. METHOD

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

3.1 TERMS AND DEFINITIONS

Trend – The general development of the phenomenon in question over a long period of time can be called a trend. A trend is a feature of the present that may continue in the future in such a way that it is easy to trace or predict. There is always a time aspect involved in understanding a trend because the trend is time dependent. Trends guide decision-making by influencing choices, tastes, values, etc. Trends can also be part of megatrends. A trend can be a factor of disruption or stability.

Megatrend – A megatrend is a general direction of development, consisting of several phenomena, or a wide-ranging process of change. They are often considered to occur at the global level and development is often believed to continue in the same direction. Megatrends are familiar things, changes that are already happening today and highly likely to continue in the future. [1] Examples of megatrends are ageing population, urbanization, and technology being embedded in every aspect of life. A megatrend can be a factor of disruption or stability. Megatrend may include multiple trends.

Mid-term future – Trends are time dependent, and it is important to define the time horizon in which the future is observed. In this context, the horizon was the mid-term future, in 2030-2040. Mid-term future allows to look beyond the rule of current governments for example, but is still relatively easy to comprehend.

3.2 OBJECTIVE AND FOCUS

The main objective of the event was to gather information from participants on what they think were the most important elements that could impact the future context in which hybrid threats will manifest, twenty years on. These reflections 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 abled 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 (OB.5), 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.

[1] Dufva, Mikko 2020: What are megatrends? Published on the website of Finnish innovation fund Sitra. https://www.sitra.fi/en/articles/what-are-megatrends/

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 of the EU-HYBNET core theme leaders: Hybrid CoE, UiT, L3CE, and URJC. In a core theme leader meeting, it was decided that there would be three breakout sessions with the following topics:

Group 1: Intelligent infrastructures – New IT and Smart Cities

Group 2: New Geography – Changing Identities and Power Relations

Group 3: New Drivers of the Information Domain – Platforms Ownership, Flows and Influence

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 core themes. The group themes also reflected more tentative ideas by the core theme leaders which were then taken on board as a means of exploration.

3.3 WORKSHOP STRUCTURE

The event organisers chose to arrange a full-day virtual workshop, consisting of two parts: the first part would entail a keynote and a panel of high-level experts. Participation was open to anyone, and there were no requirements for previous experience in future-oriented thinking. The keynote and panel served the purpose of inspiring and introducing everybody to the approach. The topics of the keynote and panel were megatrends and European security, and included foresight specialists from the Finnish Innovation Fund *Sitra*, the Finnish Prime Minister's office, the EU and the NATO, in pursuit of comprehensive geographical and institutional scope.

The second, more interactive part consisted of 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 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 participant registered in one of three breakout session groups. Participants received background reading per group and were requested to answer a questionnaire before the event. Background reading material was produced by the experts at the Hybrid CoE, and reviewed by the otherEU-HYBNET core theme leaders. The purpose of the pre-reading material was to provide food for thought, a

context for emerging threats, and an introduction to the questionnaire. Pre-reading texts are in the annexes of this deliverable.

QUESTIONNAIRE

Questions to the participants were following:

Group 1: Intelligent infrastructures – New IT and Smart Cities 1. What are the main (for example technical, social, or environmental) things that you see changing in your city or cities close to you, in the coming 10-20 years? 2. What kind of technological solutions would this change require or bring? 3. What kind of changes in your city or cities do you anticipate, that will affect your daily work? 4. Name one topic that should be discussed, but is not discussed enough, when it comes to city development and security
Group 2: New Geography - Changing Identities and Power Relations 1. What are the main issues that are likely to be the object of large-scale transnational mobilization in the future (both online and in the physical world)? 2. Which issues, identities or problems may develop in the future which would have a particularly "insurgent" character? 3. How do you see the evolution of liberal democratic systems in the future? 4. What do you think should be discussed that you feel is not paid enough attention?
Group 3: New Drivers of the Information Domain - Platforms Ownership, Flows and Influence 1. From your point of view, what challenges and opportunities will come with an increasingly fractured information domain? 2. From your point of view, what challenges and opportunities will come with an unified information domain? 3. Which events or developments could shift the development significantly into one direction? 4. Through which domestic and/or transnational policies could governments resist or impact this development? 5. What societal impact will the increased division into filter bubbles have?

Altogether 44 participants sent their responses to the questionnaire before the event. Altogether 68 participants from 44 organisations participated the event.

DISCUSSION ON DRIVERS OF CHANGE AND DISRUPTIVE EVENTS

Breakout sessions built on the results of the questionnaire by highlighting a series of themes and ideas that were present in the responses. Discussions in breakout sessions focused on what drivers of change, undercurrents or disruptive events might shape the future of the topic of the session.

Discussion session was followed by an "inject" in form of video or radio play, depicting a future in which hybrid threats in the given contexts were emerging. The purpose of the inject was to steer the discussion towards most obvious dystopic scenarios, and challenge participants to think about the plausibility of these scenarios.

CONNECTING CHANGES

Participants worked on a table representing three spheres of transformation to connect the changes, drivers, undercurrents and disruptive events identified in the previous steps. Working with different levels allowed the connection of observations and findings to personal (values and paradigms), political (systems and structures) and practical (processes and technology) levels. The aim was to deepen the understanding on connections between personal and global change, and on the relevant actors. The idea of reaching a more comprehensive outlook on change via these three levels originates from the concept of *three spheres of transformation*, used by CChange and Finnish Innovation Fund Sitra, among others.

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

The workshop collected input in form of the pre-questionnaire results, discussion notes, and tables that were collectively filled during the last part of the breakout session. Hybrid CoE clustered the information based on the phenomena that the participants deemed as relevant for the context, and possibly affecting a change in the future. These phenomena or sub-trends were then looked from the point of view of changing and preserving factors, and how plausible the workshop participants considered them. Implications to hybrid threats were derived from the phenomena and factors indicating change or stability. The table depicting the analysis sequence is in annex II.

The identified phenomena formed three technology-enhanced megatrends, considered having most relevant hybrid threat implications in the mid-term future: levelling of the networks of human interaction, expansion of the availability of personal data, and increasing transparency of social, societal and political vulnerabilities.

TREND 1 – LEVELLING OF THE NETWORKS OF HUMAN INTERACTION

Communication flows, business and trade exchanges, relations between and among institutions (global corporations and global governance network) will continue to follow patterns of distributed network. Those patterns enable central nodes to connect more with distant extremities. As a consequence, extremities of the networks will gain as much systemic influence as the nodes of the network by exploiting the distributed architecture of the networks. In terms of hybrid threats, this implies a further complexification and unpredictability of risk and attack vectors. The factors listed below emerged from participants' discussions and fed into the definition of the mega-trend above.

- **The sources of interests, agendas and motivations undergo diffusion and dispersion**. There is a process of diffusion of the knots of power and influence on local, national and international contexts. The networks that form the backbone of interactions among individuals such as social media and internet-based communication tend to connect at all levels. In terms of hybrid threats, it implies an increased set of opportunities for proxying, dissimulation and escaping detection of actions.

- **The processes of information production, validation and dissemination escape traditional hierarchies and structures**. The fragmentation of producers, sources and circulation patterns induce a fluidity of information. This environment can foster the emergence of sub-cultures of content producers and influencers, new "gatekeepers" marking a decline of established experts, and dissemination entrepreneurs. In a hybrid threat perspective, it implies a very fluid environment in which manipulated information can be propagated in a distributed manner.

- **The means to create large scale impacts are increasingly available to a wider array of users**. This induces a democratization of the means to inflict harm, damage and violence. It also generally empowers individuals' agency and capacity to influence the system. It is a practical avenue for network extremities to gain importance and flatten and/or distribute power within the network, for example by influencing populations even overseas via social media. In terms of hybrid threats, this spells the disproportion between effort and impact that actors can expect.

TREND 2 – EXPANSION OF THE AVAILABILITY OF PERSONAL DATA

Individuals in their daily online activities leave a wide spectrum of traces and signals about their expectations and preferences in many domains such as business, consumption, and politics, among other examples. This trend implies a centre-stage role for individuals in the digital economy and networks of interaction. This will make them empowered actors, targets for communication as well as economic resources on a systemic scale. The factors listed below emerged from participants' discussions and fed into the definition of the mega-trend above.

- **Progresses in deep machine learning and algorithms make statistical predictions based on individual variables increasingly powerful**. This technological progress upends the traditional paradigm of statistical methods: instead of focusing on social categories for prediction, those progresses split the data to ever-more granular levels while algorithms are able to integrate this into calculations. It is a process of atomization of the data exploited for prediction at individual levels, which enables a continuously more effective micro-targeting of individuals by hostile actors.

- **The standards, infrastructure and ethics frameworks of data ownership will be the focus of reforms and changes**. Necessities to adapt the data ownership regime in order to include individuals into the data market can become an essential point of contention. The challenge of data ownership regimes is to seek and reduce the disruptive effects of individual data aggregation and exploitation.

- **The internet of things shows a trend of dissemination of critical individual data among objects that can be breached.** This is likely to suggest a trend of deconcentrating the architecture of cyber security in order to have an increased redundancy of digital infrastructures down to most private and daily devices. The dissemination of data enabling the use of everyday objects bears the risk to obscure individuals' understanding of the value of their data. In terms of hybrid threats, this suggests that hacking and data gathering from multiple connected objects increases the computability of societal vulnerabilities based on individual choices, traces and signals.

- **Social media may undergo a fringe platforms phenomenon**. This relates to the possible fragmentation and complexification of echo chambers because of an especially flattened architecture of networks. The multiplication of fringe platforms may diminish the relative importance and power of previous platforms and their outreach. In terms of hybrid threat implications, this may give rise to attempts at leveraging the fragmented circuits via fringe platforms, in particular those that connect and intersect with mainstream and other platforms.

TREND 3 – INCREASING TRANSPARENCY OF SOCIAL AND POLITICAL VULNERABILITIES

This trend assumes that the increasing availability of individual and personal data and its aggregation and the ongoing development of algorithmic driven neural networks machine learning will result in deep learning, to **identify vulnerabilities and fault lines at systemic level**. The capacity to connect

increasingly granular aggregates enables a deeper, more individualized thus more destabilizing exploitation. The factors listed below emerged from participants' discussions and fed into the definition of the mega-trend above.

- **Possibilities to leverage individuals' thought processes on a systemic scale**: beliefs, desires, preferences and past behavior can become actionable in the framework of attempts at destabilizing a society. Combined with the widespread availability of individual data, computing tools become increasingly democratic with a capacity to leverage more and more individuals' predicted behaviour, progressing data analytics capabilities from diagnosis to prediction, and perhaps even to anticipatory predictive targeting.

- **Identity politics that are both exclusionary and inclusive**. Identity politics can be an aspiration for exclusion, differentiation and separation such as anti-immigrant or nativist sentiments. Identity politics can also be a way to demand rights and recognition as a group and its inclusion into a larger community. Feminism is for instance a type of identity politics that claims inclusion in the form of equal standing to the population. Identity politics in terms of hybrid threats, and associated with the algorithmic computation capabilities, may enable the leveraging of complex feelings and resentments that relate to the fabric of societies. This is a cross trends factor.

- **The energy transition and ecological imperatives can be important sources of political polarization.** It pertains to fundamental transformations in labour, structure of production chains, political agenda pitting economic freedoms against ecological imperatives. This process of creation of new customer expectations, political discourses and normality will also generate violent oppositions. This can allow the leveraging of potential violent protest movements for or against ecological standards.

- **Political movements could stem from digital literacy, awareness and data privacy concerns**. Anti-digitals generation movement and counter cultures to digitalization could form a bedrock of contestation and identity politics in societies increasingly reliant on digital means. In terms of hybrid threat implications, this also offers a series of exploitable fault lines: questioning the premises and foundations of systems relying extensively on digital data from individuals, leveraging the issue of digital pre-eminence as a political focal point in order to stir divisions and accentuate potential gaps.

- **The capacity of algorithms to concentrate or diversify exposure will likely remain as a leverage for societal polarization**. In terms of hybrid threats, this spells a regulation problem so that content exposure would get more diverse and not deepen systemic echo chambers. Leveraging the structure of echo chambers and exploiting the process for creating or reinforcing them can be a significant vulnerability and attack vector.

- **The crisis of liberal democratic representative systems may constitute a key decision-making vulnerability.** Rampant discontent as to the quality of representation in liberal democracies has for instance contributed to Brexit, and the election of Donald Trump. Deterioration of trust and confidence in institutions, and consequent populist politics pits the people against all other forms of legitimacies (judiciary and courts, Parliaments, Press, etc.), calling for direct forms of democracy and referenda to improve representation, and to overhaul alliances. This

undermines the principle of political responsibility and reversibility of decisions and policies: elected governments and majorities take decisions and can be voted out of office, the people cannot. The absence of reversibility and responsibility over decisions can lead to a deeper crisis of trust and undermine the essence of liberal democracy and its attractiveness as a model. This precise lever has a high stake in a hybrid threats context for external actors as fostering populist politics contributes to discrediting decision-making in liberal democracies.

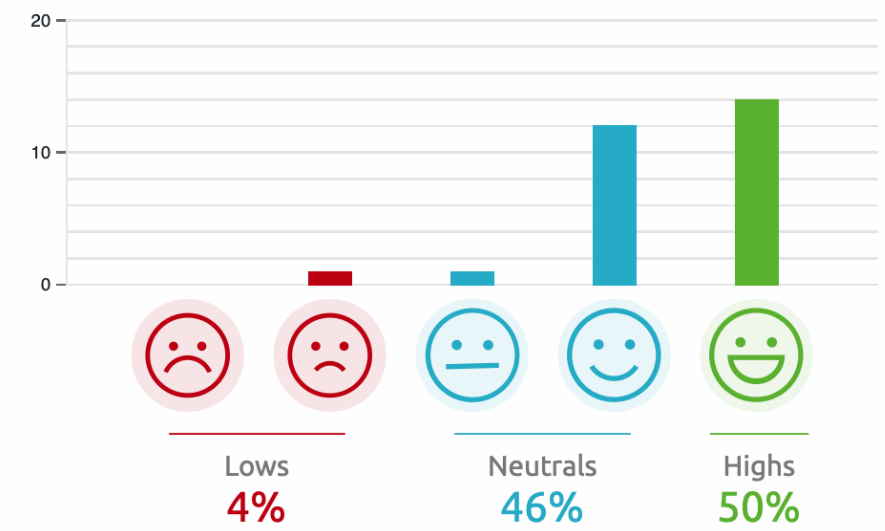
- **Institutional stress in the face of increasingly complex and wicked problems contains a risk of undermining rule-of-law based liberal governance**. Facing seemingly intractable problems, governments under public pressure to deliver could take decisions that can undermine the rule of law and liberal standards of governance. The fight against terrorism has shown this bias. In particular, states of emergency tend to confuse the roles of the different branches of government, and even shift entire judicial systems gradually towards new standards and benchmarks. Judicial systems' reaction to terrorism have for instance put a gradually stronger emphasis on intention rather than on action of individuals, warranting increasingly preemptive decisions than *a posteriori* judgements. This continues to pose essential challenges in terms of the fundamentals of judicial systems.

5. PARTICIPANTS, FEEDBACK AND LESSONS LEARNED

The event was arranged as a virtual meeting taking place on BlueJeans platform. The event was public, and it was announced open for all interested participants from EU and Associated Countries. It was advertised on EU-HYBNET website (https://euhybnet.eu) and social media from January 2021 on. 68 participants from 44 organisations took part in the event. The list of participant organisations is in annex I.

Feedback was collected immediately after the event via anonymous questionnaire link, and out of 68 participants, 28 responded.

Distribution of responses were the following:



Best value for the event was given by 14 respondents, neutral value by 13 respondents, and bad value by 1 respondent.

Those who considered the event excellent were especially thanking the high quality of speakers, the unconventional choice of topics, and opportunity to discuss in small groups.

Examples of positive feedback:

The topics on smart cities and changing identities are seldom addressed in the field of hybrid threats so far. So therefore it was quite interesting and raised some new ideas and think-abouts. In addition, the workshop was well organised with good high-level speakers and much variety in the programme

The event was well organized, hosted and prepared for, the keynote speakers and panelists provided excellent discussion and thought provoking content and the breakout rooms process was well thought out and flowed well minus the unforeseen technical issues with BuleJeans. The contributions of participants was of very high quality and I think that more events like this could bring the project next level results. I wish our normal telcos were as efficient and expertly guided to allow for partners to freely contribute their expertise to the critical areas of the project.

Those who gave neutral value gave the same positive feedback, but considered technical problems that occurred during the event too disturbing.

Examples of neutral feedback:

The program, the participants, the discussion were all excellent! Unfortunately, the technical hassles during the event prevented me from giving a higher rating.

The event was great with a good concept and way of working. It might be better to be shorter in time due to the fact that most of us have additional work to do. The only negative where the technical issues. Maybe a short in time with more often exchahge of feedback sessions could be better. Many thanks!

The platform was chosen to its quality to filter only registered participants to the workshop. This was done in order to limit participation of uninvited participants. The platform however was not fully compatible with certain devices or browsers, which led to some participants having difficulties with video or audio settings in the beginning of the workshop. Moreover, the platform does not allow adding unregistered participants after the meeting has opened, and some essential people had not registered. When they were added to the meeting, notifications were sent to everybody via e-mail. In the future, this can be avoided by double-checking that the list of registered participants is comprehensive. Moreover, the platform did not allow breakout rooms for the type of meeting that was chosen, which was not anticipated, and creation of new meeting rooms took time from the event. In the future, organisers are advised to use another platform.

One who gave neutral value and the one who ended up giving bad value score, criticized the approach for being too top-down. In the future, it is important to manage expectations and emphasise to participants, that the event is primarily about enabling interaction and gathering out of the box ideas on possible futures in different contexts of hybrid threats. It is also important to highlight the findings of the small groups already during the event, for example by including a reporting panel to the end of the event.

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 recognise important trends. 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. Feedback confirmed that it was possible to achieve the goals in a virtual environment, despite technical difficulties and limitations in interaction. Since the event was public and accessible to anyone who wanted to participate, this resulted in a high number of participants. Result was that the discussion between the participants was sometimes restricted, as the discussion time per person became smaller as the group size grew.

The identified phenomena formed three technology-enhanced megatrends, considered having most relevant hybrid threat implications in the mid-term future:

1) Levelling the networks of human interaction

Communication flows, business and trade exchanges and relations between and among institutions (global corporations and global governance network) will continue to diffuse. Information production will continue to develop further away from traditional hierarchies and structure. Use of social media and internet-based communication are the source and will enhance the development. This will result in potentially disproportionate role of extremities of the network. In terms of hybrid threats, it means an increased set of opportunities for proxying, dissimulation and escaping detection of actions and that creation of large-scale impacts is available for wider array of users.

2) Expansion of the availability of personal data

Individuals in their daily online activities leave a wide spectrum of traces and signals about their expectations and preferences in many domains. This trend implies a centre-stage role for individuals in the digital economy and networks of interaction and brings serious vulnerabilities down to the individuals. As the deep machine learning and algorithms develop and people gravitate towards fringe platforms, it is easier to derive individual's preferences and target them. Critical individual data is increasingly fed also to devices that can be breached. Assumption of liberal distribution of individual data to different platforms and devices also bears the risk to obscure individuals' understanding of the value of their data. Standards and ethics frameworks will become the focus of change.

3) Increasing transparency of social and political vulnerabilities

This trend is closely connected to the above. It directly concerns the vulnerability surfaces susceptible to hybrid threats actions. This trend suggests that the availability of the personal data and the development in machine learning will result in deep learning, and machine-based ability to identify vulnerabilities on a systemic level. It will make possible leveraging individuals' thought processes and decision-making. This increases opportunities to polarize discourses and movements, and affect decision-making institutions by calling for direct forms of democracy. It postulates that hybrid threat actors will have an ever greater ability to compute systemic vulnerabilities for exploitation.

The main purpose of identifying these 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 (Task 3.1, Definition of target areas for improvement and innovations), as an additional cluster for identified gaps and needs. The relevance of 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.

BIBLIOGRAPHY

Dufva, Mikko 2020: What are megatrends? Published on the website of Finnish innovation fund Sitra. https://www.sitra.fi/en/articles/what-are-megatrends/

Lahti, Vesamatti, 2020: Aukkoja sivistyskäsityksessä. Published on the website of Finnish innovation fund Sitra, https://www.sitra.fi/julkaisut/aukkoja-sivistyskasityksessa/

CChange: Three spheres of transformation https://cchange.no/about/the-three-spheres-of-transformation/

ANNEX I: LIST OF PARTICIPANT ORGANISATIONS

Alanya Alaaddin Keykubat University, Turkey
Belgian Defence Forces
German Council on Foreign Relations, DGAP Technology Programme
European Commission
European Organization for Security, EOS
European Parliament
Expert System SpA, Italy
Finance Finland
Finland Futures Research Center
Finnish Innovation Fund Sitra
Geostrategic Intelligence Group (GIG), Finland
GLOBSEC, Slovakia
Institut Euclid, France
KEMEA, Greece
Kosciuszko Institute, Poland
Laurea University of Applied Science, Finland
Lithuanian Cybercrime Centre of Excellence, L3CE
Luxembourg Foreign Ministry
Mihai Viteazul National Intelligence Academy, Romania
Ministry for Economic Transition of France
Ministry of Finance, Estonia
Ministry of Foreign Affairs, Poland
Ministry of Infrastructure, Poland
Ministry of Interior, Republic of Latvia
Ministry of National Defence, Turkey
Ministry of the Interior and Administration, Poland
Multinational Peace Support Operations Training Center, Greece
National Cyber Security Centre, Poland
NATO CCDCOE
NATO Joint Force Development, ACT
NORSECON, Sweden
Polish Government Centre for Security
Polish Internal Security Agency, ABW
Polish National Research Institute
Polish Platform for Homeland Security
Prime Minister's Office, Finland
RISE AB, Sweden

Santander, Poland
SATWAYS, Greece
Smartlink, Romania
TNO, the Netherlands
UiT, The Arctic University of Norway
UK Ministry of Defence, Development, Concepts and Doctrine Centre (DCDC)
Uni Bw Munich, Germany

ANNEX II: ANALYSIS TABLE

Trend 1	Levelling of the networks of human interaction			
Context	Phenomenon deemed relevant for the context	Factors indicating change	Factors indicating contiunity	Hybrid threats / hybrid threat implications
Geography	Relational power, power of networks more prominent: diffusion and dispersion of the knots of power and influence	Diffusion of the sources of interests, agendas and motivations. Dispersion of the determinants of international relations to increasingly individual levels	Idea of equilibrium among the different knots and centres, connectors of the networks. Unlikely.	Using decoys: Opportunities for proxying, dissimulation and escaping attribution to detected movements. Deniability opportunities increasing.
Information	Relativity of information production, validation and dissemination processes	Atomization of actors and sources of information circulation. Fluidity of the models of information circulation.	Emergence of sub-cultures on content producers, "gatekeepers" and dissemination entrepreneurs. Organizing logics per reputation, giving a dynamic order logic to information sphere.	Fluidity of the environment in which manipulated information with hostile intent can be propagated. Difficulty to stop the manipulted information if it follows own network logic of diffusion.
Information	Decentralization and deconcentration of disinformation	Atomization of actors and sources, fragmentation of circuits, sources, responsibilities	Maket competition for attention, emergence of regulations and practices to ensure free and fair competition in information market	Possibility for hybrid threat actors to multiply the vectors of informational influence, increasing opportunities to use decoys and hide true intent within the noise of information

New IT	Availability and democratisation of technological devices and solutions	Diffusion of the capabilities to have a large scale impact (diffusion of content, speech, focalisation power)	Improvements in individual follow up of labour intensive sectors such as healthcare.	Democratisation increased of the means to inflict harm, damage and violence. Opportunity to exploit the trend of disproportionate importance given to cyber attacks and disruptions. Paradox of perceptions vs actual impact is paramount in trust undermining activities.
Trend 2	Expantion of the availability of personal data			
Context	Phenomenon deemed relevant for the context	Factors indicating change	Factors indicating contiunity	Hybrid threats / hybrid threat implications
New IT	Progresses in AI and deep maching learning processes	Individualisation of predictions and atomization of categories of statistical representation induce intense actionability of levers deemed too individual or microscopical to be relevant	Increasing precision of prediction of individual behaviours online and in the physical world by the interpretative capacities of neural networks fed by massive individual data flows	Leveraging individual horizons: levels / beliefs / interactions can be actionable in the framework of attempts at destabilizing a society. Disruptive potential of a tool that becomes more and more available and democratic: capacity to leverage every single individual's predictive behavior.
Information	Increasing quantity, rapidity and precision of information flows	Neural networks deep machine learning		Vulnerabilities of neural networks to hacking and disruption. Capacity to use them for improving predicting of individual behavior and

				increasing individual representation levels for prediction.
Information	"Fighting disinformation" vs freedom of expression?	Political momentum for countering disinformation if not appropriately defined and circumscribed can have excessive reach and effectively tend to curb free speech per the standards of fact correctness		Possibility to immunize disinformation from fact checking by ostensibly presenting it as political expression representing the views of a large part of society. Generally relativizing any form of "fact" or "truth" based narrative.
Information	Data ownership infrastructure in democratic and ethical standards	Necessity for adaptation of data regime of ownership, alternative model of data	Potential to build a solid data regime that would induce a sense of stability, predictability and reduce the disruptive character of data aggregates exploitation processes.	Individual data as a high value commodity
New IT	Internet of everything, including of people / loss of privacy	Dissemination of information critical to the individual among breachable objects	Arriviing at a cyber security architecture that would be decentralised and deconcentrated in order to have an increased redundancy of the digital infrastructures. Security by design and by device.	Hacking and data gathering from multiple connected objects increases the computability of societal vulnerabilities based on individual choices traces and signals.
Geography	Polarization and increased salience of narratives	Weaponization of narratives conducive to conflict	Instruments of social, group or national cohesion and nation building.	Multiplication of identity narratives working at increasingly individual levels.

			Reinforcement to the institution of the State in world politics	
Information	Fringe platforms phenomenon	Fragmentation and complexification of the phenomenon of echo chamber. Flattened architecture of the network.	relativization of the power and reach of each platforms	Power to leverage the atomized and relativied circuits of the fringe platforms. Leverage the connections and passages from them towards the bigger platforms and mainstream media circulation channels.
Trend 3	Increasing transparency of social and political vulnerabilities			
Context	Phenomenon deemed relevant for the context	Factors indicating change	Factors indicating contiunity	Hybrid threats / hybrid threat implications
Geography	Identity politics both exclusionary and inclusive	Aspiration for exclusion, differentiation and separation	Aspiration for inclusion and recognition.	Opportunities to leverage complex feelings and resentments that relate to the fabric of societies.
New IT / Geography	Energy transition / ecological agenda	Transformations in labour, structure of production chains, political agenda pitting economic freedoms against ecological imperatives as a source of polarization in politics	creation of new customer expectations, political discourses and normality.	Leveraging potential violent protest movements for or against ecological standards.
Information	Digital literacy, awareness and data privacy as political movements -	Questionning the premises and foundations of systems relying extensively on	Potential for better regulations and principles that can increase societal	Leveraging the issue of digital preeminence as a political focal point in order to stirr

	Native anti-digitals generation movement / counter culture	digital data from individuals	acceptability of digital systems reliance.	divisions and accentuate potential gaps.
Geography	Technological processes and automation of work making labour forces redundant / changing structure of employment	Massive waves of unaccompanied unemployed workers made redundant - social and political consequences. Impact of out of job market utility	Adjustement towards a less labour intensive value production system for developped economies, gradual transition and reconversion of skills. Systems and webs of social support palliating for labour immobiity.	Economic discontent with social and political consequences can be leveraged in many domains.
Information	Algorithms capacity to concentrate or diversify exposure to select content	Maintenance of echo chambers or social media bubbles increasing societal polarization upon issues ranging from health to politics	regulation of algorithms on social media for diversifying content presentation and exposure	Leveraging the structure of echo chambers and exploiting the process for creating or reinforcing them.
Geography	Crisis of liberal democratic constitutional representation	calls for reforms in order to improve the experience of representation in its form and substance		Undermining the principle of political responsibility. Political responsibility of elected governments gives also the principle of reversibility: decisions taken by the people via more direct decision making (i.e. referendum) are difficulty reversible and engender deeper crisis of trust if decision is faulty.

				No reversibility / no responsibility. Discredit to the essence of liberal democracy.
Geography	institutional stress	Decisions that tend to undermine the rule of law and liberal standards of governance (i.e. anti terrorism legislation judging cases baased on intention not commission of acts)		Merging of powers, confusion of mandates, encroachment of intention anticipation over rule of law frameworks.

ANNEX III: WORKSHOP AGENDA

EU-HYBNET

EU-HYBNET 1st Future Trends Workshop Online #FTW

31 MAR

BlueJeans call
Link will be sent to registered participants

08.00-15.15 CET

The purpose of the **Future Trends Workshop** is to support the practitioners' and stakeholders' everyday work by providing a future outlook for **strategic planning** and consider consequences of today's policy choices in long-term.

This workshop builds on the EU-HYBNET project findings and provides a **platform of interaction for various stakeholders**. Since the landscape of hybrid threats is continuously evolving, foresight and creative thinking is central for understanding, detecting and responding to emerging threats. It focuses on a more anticipatory and prospective outlook, highlighting the weak signals and outliers **of disruptive and paradigmatic change to the European security environment.**

To who? EU-HYBNET Partners, stakeholders, EAB members, network members, and interested innovation providers, industry, SMEs and NGOS, according to registration check.

When? 31st of March 2021 at 08.00-15.15 CET / 09.00-16.15 EET

More information: Event organizer, Project coordinator in the European Centre of Excellence for Countering Hybrid Threats, Emma Lappalainen emma.lappalainen@hybridcoe.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

EU-HYBNET

Agenda

Time (CET)	Topic	Speaker(s)
08.00	Introduction	**Teija Tiilikainen**, Director of the European Centre of Excellence for Countering Hybrid Threats.
08.15	Keynote speech and Q&A from the audience	**Jyrki Katainen**, President of The Finnish Innovation Fund Sitra
09.00	**Coffee Break**	
09.15	Panel discussion: Megatrends and European security	**Jaana Tapanainen-Thiess** Secretary General, Government Report on the Future and Government Foresight Group Prime Minister's Office, Finland **Ilmars A. Lejins** Brigadier General Assistant Chief of Staff NATO Joint Force Development, ACT **Dimitri Lorenzani** Member of Cabinet of Maroš Šefčovič, Vice-President for Inter-institutional Relations and Foresight - European Commission
10.45	**Coffee Break**	
11.00	Breakout sessions (including 10-minute break)	1.Intelligent infrastructures – new IT and smart cities 2.New geography – changing identities and power relations 3.New drivers of the information domain – platforms ownership, flows and influence
13.00	**Lunch**	
14.00	Closing panel (inputs from the breakout sessions)	**Gunhild Hoogensen-Gjørv**, Professor, Critical Peace and Conflict Studies, Centre for Peace Studies, UiT The Arctic University of Norway **Ruben Arcos**, Lecturer and researcher in Communication sciences, Rey Juan Carlos University in Spain **Hanna Smith**, Director of Research and Analysis, European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE **Evaldas Bruze**, Lithuanian Cybercrime Center of Excellence for Training Research and Education
15.00	Closing remarks	
15.15	**End of the day**	

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

EU-HYBNET

House Rules

- The event is held under **Chatham House rule**, so that none of the discussion substance can be attributed to any panelist or workshop participant.
- It is important to maintain an atmosphere of trust and respect that encourages interaction and innovative thinking.
- During breakout sessions, **please keep your camera open, but mic muted when you are not talking.** It is acceptable to comment also in chat.

Photo by Miikka Pirinen

Keynote: Jyrki Katainen

Jyrki Katainen's career has focused on analysing societal change, finding solutions and decision-making. Before his appointment as the President of Sitra, Katainen was the European Commission Vice-President for Jobs, Growth, Investment and Competitiveness.

Prior to the Commission, he has held the positions of Prime Minister and Minister of Finance. During his 15 years as a Member of the Finnish Parliament he has chaired the Committee for the Future among other appointments.

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

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

GROUP 1: INTELLIGENT INFRASTRUCTURES – NEW IT AND SMART CITIES

The smart city concept represents a certain kind of utopia, where citizens' needs find a perfect match in advanced technology. In a smart city, intelligent solutions can be found everywhere, from cars to fridges to decision-making systems, and these technologies calculate and respond to citizens' needs, improving their quality of life, safety, and businesses. This would entail freeing people from having to adapt to the constraints of the city, such as traffic jams and inaccessibility, and enabling the city to adapt to people's needs in the face of increasing urbanization, an aging population, and climate change. However, it also means increasing dependency on intelligent infrastructures, technology providers, and surveillance, creating a new unfamiliar environment. The benefits, possibilities, risks and vulnerabilities are still unknown.

EU developing a smarter urban culture

The smart city concept is attractive to the EU, with the harmonization of people and technology being actively pursued in a number of initiatives to address city-related challenge.[2] The European Commission (EC) characterizes key functions of smart cities as smarter urban transport networks, upgraded water supply and waste disposal facilities and more efficient ways to light and heat buildings, a more interactive and responsive city administration, safer public spaces and meeting the needs of an ageing population.[3]

One of the initiatives to build smart cities in Europe is the "Join, Boost and Sustain" movement, driven by EUROCITIES, a network of large cities in Europe, the European Network of Living Labs (ENoLL), and Open & Agile Smart Cities (OASC). Their declaration from 2019 calls for a digital Europe, developed with and for people[4] People-centrism is an important value in developing this idea: the future technology must be aimed at enhancing quality of life.

Urbanization and hybrid threats

In a security environment where hybrid threats have become one of the major challenges for democratic societies, the new smart city environment creates new possibilities for hostile action. Hybrid threat actors aim to undermine public trust in democratic institutions, deepen unhealthy polarization both nationally and internationally, challenge the core values of democratic societies, gain geopolitical influence and power through harming and undermining others, and affect the decision-making capability of the target.[5] A city could be a target of a hybrid campaign, either during a conflict or below the threshold of an open conflict. Forms of hybrid influencing in the context of cities are explored, for example, in the report on Helsinki in the Era of Hybrid Threats.[6]

[2] See https://ec.europa.eu/digital-single-market/en/smart-cities-smart-living.
[3] See https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.
[4] See https://www.living-in.eu/declaration.
[5] Giannopoulos, G., Smith, H., Theocharidou, M., *The Landscape of Hybrid Threats: A conceptual model*, EUR 30585 EN (Publications Office of the European Union, Luxembourg, 2021).
[6] See https://www.hybridcoe.fi/publications/helsinki-in-the-era-of-hybrid-threats-hybrid-influencing-and-the-city/.

The ideal smart city implies the ability to gather, store and analyze a vast amount of data, which would be ethically and safely used. In a less idealistic scenario, the safety of the data gathered might be compromised, it might fall into the wrong hands, or the initially right hands might use it for unethical purposes. Who are the parties to the checks and balances for the management of the smart city and the data it needs to function?

The smart city concept presupposes "smart citizenship", the ability of people to constantly interact with technology in a way that optimizes it to benefit all inhabitants equally. It will still take some time before all ages/generations are digitally native, meaning that the smart city concept might end up dividing people and excluding some groups from society. What will this mean for societal trust? Will it face challenges or become stronger in the face of such responsibility to "educate" the city? How high will the tolerance of dysfunction be in the smart services? Might it affect people's interaction with the city when this trust is challenged, as a result of an external influencing campaign, for example? How would the development of an urban population in Europe define the development of smart solutions in cities? And what would the role of rural areas be?

Some devices that smart cities require include sensors, cameras, drones and satellites, which would utilize algorithms and AI solutions in decision-making. An example of this functionality could be detecting a traffic jam via GPS signals or drones, and optimizing the routes of automated vehicles accordingly. We are constantly presented with increasingly sophisticated technologies, one of which with high importance for smart city development is undoubtedly 5G technology.[7]

The 5G era will bring network and service capabilities that have not been available previously, enabling the real internet of things (IoT). With 5G, more and more devices can be connected to the network, and they will be able to maintain connectivity at any time in any place. With cloud computing and big data technology solutions, we are one step closer to smart city reality, where devices communicate with each other in real time, based on a vast amount of processed and speedily analyzed data. This can be exemplified in the idea of fully autonomous vehicles, which could communicate with each other and other objects on the road even at high speed.

The devices would need to gather a vast amount of data and share it in the cloud, and there would very likely be applications to help increase public safety through crime detection and monitoring.

This development also has the potential to blur cultural understandings, since even algorithms and AI solutions have their cultural codes embedded in them. This allows developers to code in a way that benefits them, effectively deconstructing and reshaping the culture and identity of the users.[8]

[7] Guevara, L., Auat Cheein, F. 'The role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems'. Sustainability 2020, 12(16). https://www.mdpi.com/2071-1050/12/16/6469.
[8] See https://thereader.mitpress.mit.edu/algorithms-are-redrawing-the-space-for-cultural-imagination/.

GROUP 2: NEW GEOGRAPHY – CHANGING IDENTITIES AND POWER RELATIONS

This background paper describes elements of a developing geography of identities and power relations. 'Identities' in this context refers to the ways in which individuals in democratic systems express their rights, values, opinions and sense of belonging. These identities are manifested across digital communication spaces in particular. They have the potential to connect individuals and build communities. However, they can also deepen the rifts between governments and their citizens, and within groups in society. The new geography that results from these identities crosses traditional borders and creates new networks of people, ideas, communities and interests.

This paper interprets the new geography of identities and power relations in connection to the issue of populism in democratic societies, which may expose vulnerabilities for hybrid threat actors seeking to exploit the seams of such societies. Indeed, populism has become a destabilizing trend in democratic societies. It builds a discourse that pits technical expertise and scientific knowledge, rule of law safeguards such as constitutional courts, or any type of representative institution against popular sovereignty. This populist discourse may result in the increasing radicality of social mobilization and the political debate.[9]

In a democracy, power is considered to belong to the people as a whole. However, it is the elected majority that visibly manifests this power. Herein lies a core dynamic of democracy: popular sovereignty materializes via counting votes, giving the majority the right to implement its agenda; but the majority does not represent the full extent of the power of the people. This tension between popular sovereignty and its concrete manifestation has an unsettling effect on the democratic regime: the majority rule must take account of minority views. This tension deepens when democratic societies become polarized.

The legacy of the structural economic crisis that occurred at the end of the 2000s, as well as the most recent impacts of the COVID-19 pandemic, may lead to a deepening of the tensions at the core of the majority-minority rule in democracies. Populism stems in part from this tension: it attempts to offer reassuring fictions to citizens in search of a more satisfactory experience of representation. In effect, it directly corresponds to an authoritarian tendency since it portrays popular sovereignty as the sole and radical source of power, regardless of the liberal systems in place to safeguard the interests of the minority.

Populist discourses can exploit the current phenomenon of transnational changes in identities. Information and communication technologies have opened up a horizontal, level and global socialization space. Individuals are fully empowered to immediately and directly formulate and share their opinions on a global scale. Like-minded individuals and groups can connect and integrate to an unprecedented extent. This phenomenon transcends obstacles in group constitution, producing immediate and horizontal forms of socialization. It generates identities that have a strong influence on an individual's choice of information source, the constitution of its political opinion, and its social self-identity.

[9] Pierre Rosanvallon, *Le siècle du populisme: histoire, théorie, critique*, Les Livres du Nouveau Monde, Editions du Seuil, 2020, ISBN 978-2-02-140192-9

The transcendental aspect of this global socialization space coupled with the changing identities deepens the crisis of liberal democratic representation: it makes identities prevail over other forms of opinion constitution such as facts, reasoned argumentation, or respect for minorities. Identities can rest on a sense of systematic defiance towards representative institutions. As identities are diverse and conflicting, they are a vector of political polarization among segments of society. The crisis of democratic representation has concrete manifestations, for example in the Yellow Vests movements of 2018–2019 in France, depicting a fragmented movement radically refusing to be represented in any form.

The spaces in which changing identities take shape have an impact on power relations precisely due to their global scale. Changing identities are transnational phenomena. They connect issues such as the social and political polarization of societies, and cultural intolerance in the face of migratory challenges, which are common to many countries in Europe. Identities can also serve to integrate centre-periphery issues at regional and local levels, making them connect with a wide range of similar problems and narratives. Largely privately owned, digital communication spaces are effective tools to level the political playing field down to individuals. The viral spread of disinformation and conspiracy theories is to a large extent the result of individuals seeking empowerment and tools to take part in political debates. The circulation of pieces of disinformation creates a sense of belonging for groups around a shared notion of identity.

The formation of transnational identities has an impact on power relations as they may plug into and resonate with alternative geopolitical narratives. Economic and social progress in globalization is an iterative, non-linear and adaptive process that leaves a potential space for models other than those of liberal democracies to prove attractive. The intersection between the transnational character of changing identities, and systems of representation that offer an alternative to democracy, establishes power relations of a different sort. The Chinese example demonstrates a combination of trade openness closely regulated by the state and without political liberalism. The vaccine diplomacy and the showcasing of a success story in curbing COVID-19, associated with a series of pressures on multilateral fora, provides an insight into the type of geopolitical narrative that can connect with the transnational formation of those identities that are associated with the crisis of democratic political representation. The geopolitical narratives plugging into changing identities can provide destabilization levers that exploit the seams of democratic societies.[10]

Transnational identity and socialization processes, made possible on an unprecedented scale by digital technologies, may create changes in power relations globally. These phenomena will likely develop from and amplify the main dynamics and seams of democratic systems. Populism has thus become a transnational destabilizing force that exploits economic, social and political crises. Digital communication spaces, within which changing identities develop, allow for constituting, levelling up and empowering networks of shared interests, identities and communities that contest traditional models of governance, international borders and other norms. Changing identities can connect with alternative geopolitical narratives to those of democratic systems. The interplay between changing

[10] Kreps, S. (2020). *Social Media and International Relations* (Elements in International Relations). Cambridge: Cambridge University Press. doi:10.1017/9781108920377

identities and power relations uncovers a range of destabilizing opportunities that could weaken the decision-making and societal resilience of European democratic states.

GROUP 3: NEW DRIVERS OF THE INFORMATION DOMAIN – PLATFORMS OWNERSHIP, FLOWS AND INFLUENCE

Introduction – hybrid threats and the information domain

The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target the vulnerabilities of democratic states and institutions. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.[11]

Hybrid threats can undermine both elections and free speech. Using the information domain is a cost-effective way, for example, for adversaries to interfere in elections by changing sentiments, or to limit free speech by spamming and interfering in online conversations. These tools are not limited to states alone – non-state actors can also use the information domain to further their aims. Cost-efficiency and the ability to obscure their identity make trying to impact or control the information environment an attractive goal for adversaries. For individual users, this can be seen in increased ambiguity regarding the truthfulness of material posted on platforms, and an increased risk relating to voicing opinions online.

While changes in the information environment will impact traditional news outlets as well, this paper will focus on the possible developments occurring in and on social media platforms. It is, however, worth considering how developments regarding social media will, in turn, impact more traditional news outlets.

Current developments

During the 21st century, the emergence of social media platforms has not only changed our way of communicating, but also the security environment. The monopoly of traditional news outlets, such as printed news, radio and TV, has decreased, and fringe news outlets have risen in popularity by using social media platforms to amplify their messages. This has led to the creation of echo chambers – individual beliefs are amplified within filter bubbles on social media, filtering out differing or opposing views. In time, this can lead to increased polarization and fragmentation as it limits and restricts debate with individuals presenting opposing views.

The emergence of social media platforms, combined with the decreased power of traditional news outlets, has a range of effects on free speech and the integrity of democratic processes. Platforms have provided an arena for all users to voice their opinions, enabling an open exchange of views. At the same time, a range of issues, such as the emergence of hate speech on platforms and the possibility of outside interference in societal discussions, have raised concerns.

[11] See https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

The information environment is currently at risk of becoming increasingly fractured. The rise of the alt-right, among other movements, has impacted social media platforms, and forced mainstream platforms such as Facebook and Twitter to censor users (by blocking accounts and restricting posting, among other measures). These actions can also be seen as restricting free speech on platforms, while the same actions are considered by some to safeguard platforms against the spread of hateful rhetoric. Actions such as banning users have, in turn, accelerated the rise of fringe platforms[12] as some disgruntled users have switched to new and less regulated platforms. This enables users to interact with like-minded peers,[13] but at the same time entails the risk that different societal groups will become increasingly disconnected from each other as what can be considered 'neutral platforms' disappear.

Several efforts, such as the EU Democracy Action Plan[14] and EU Digital Services Act,[15] are regulatory attempts to ensure the transparency and accountability of big social media platforms. While this will resolve a set of issues, both the division of users into 'filter bubbles' and the operational challenges of day-to-day cooperation with social media platforms will likely remain.

Possible developments

Two different future scenarios relating to the development of social media present new challenges for governments. What currently appears to be developing is a hybrid model, where fringe groups move to fringe platforms, but 'core' users remain on the mainstream platforms. This may increase pressure on legislation, regulation and resources, as governments and institutions will need to keep track of emerging platforms with ambiguous ownership.

One course of development is that social media will become increasingly fragmented – fringe platforms will rise in popularity, and most users will transfer to them. In this scenario, it is possible that social division will determine the choice of platform, strengthening existing echo chambers even more. This will present governments with a unique set of challenges. It is also possible that fringe platforms will have foreign ownership, creating further challenges for regulation and securing democratic processes. In the future, the rise in the popularity of fringe platforms could be accelerated by existing privacy concerns regarding mainstream platforms, further prompting users to explore other options.

Unification, where several large social media companies dominate the field, is also a possibility. In this scenario, regulation might play a bigger role, and governments will have the opportunity to establish working relations, enabling cooperation with platforms to safeguard democratic processes, for example. In this scenario, will filter bubbles and echo chambers still exist? It is possible that platforms will need to navigate foreign policy? Will it be possible for them to establish working relations with authoritarian states, and what will this mean, in turn, for freedom of speech globally?

[12] See https://www.politico.com/news/2020/11/13/extremists-fringe-social-media-election-fraud-436369.
[13] See https://cyber.fsi.stanford.edu/io/news/sio-parler-contours.
[14] See https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250.
[15] See https://ec.europa.eu/digital-single-market/en/digital-services-act-package.