
# FIRST MID-TERM REPORT ON INNOVATION AND RESEARCH MONITORING

Lead Author: L3CE

Contributors: Laurea, PPHS, RISE, KEMEA, UniBW, Satways

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

# D3.8 FIRST MID-TERM REPORT ON INNOVATION AND RESEARCH MONITORING

| | | |
|---|---|---|
| **Task number** | T3.3 | |
| **Deliverable number** | D3.8 | |
| **Version:** | 1.0 | |
| **Delivery date:** | 17/6/2022 | |
| **Dissemination level:** | Public (PU) | |
| **Classification level:** | Public | |
| **Status** | Ready | |
| **Nature:** | Report | |
| **Main authors:** | Rimantas Zylius | L3CE |
| **Contributors:** | Jarmo Seppälä, Päivi Mattila, Tiina Haapanen | LAU |
| | Bartłomiej Ostrowski | PPHS |
| | Rolf Blom | RISE |
| | Athanasios Kosmopoulos | KEMEA |
| | Son Pham | UniBW |
| | Evaldas Bruze, Edmundas Piesarskas | L3CE |
| | Souzanna Sofou | SATWAYS |

## DOCUMENT CONTROL

| Version | Date | Authors | Changes |
|---|---|---|---|
| 0 | 11-03-2022 | L3CE/ Rimantas Zylius | Table of Contents, structure of the document, descriptions of gaps & needs |
| 0.1 | 12-05-2022 | RISE, LAUREA, PPHS | Contributions from organizations |
| 0.2 | 24-05-2022 | L3CE/ Rimantas Zylius | Structured deliverable with contributions |
| 0.3 | 02-06-2022 | L3CE/ Rimantas Zylius | Prepared for review, two contributions still missing |
| 0.4 | 10-06-2022 | L3CE/ Rimantas Zylius | All contributions incorporated, internal review completed |
| 0.5 | 13-06-2022 | Laurea/ Päivi Mattila | Review and comments for editing |
| 0.6 | 13-06-2022 | Satways/ Souzanna Sofou | Review and comments for editing |
| 0.7 | 15-06-2022 | L3CE/ Rimantas Zylius | Final editing |
| 0.8 | 17-06-2022 | Laurea/ Päivi Mattila | Final review |
| 1.0 | 17-06-2022 | Laurea/ Tiina Haapanen | Final review and submission of the D3.8 to the EC |

## 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.

## CONTENTS

# 1. INTRODUCTION

The Empowering a Pan-European Network to counter Hybrid Threats (EU-HYBNET) project's Description of Action (DoA) Part A document describes this deliverable (D) 3.8 "First mid-term Report Innovation and Research Monitoring" as part of EU-HYBNET Task 3.3 *"Ongoing Research Projects Initiatives Watch*" as follows:

Task focuses on gathering the information of research and innovation projects relevant to EU-HYBNET with a view of delivering material for T3.1 and finally WP4 to compile recommendations for an uptake or industrialization of innovations and standardization. Innovation and Research Projects Monitoring will be performed e.g. with partners information exchange actions and gathering relevant information from available entities, organizations and RTO Networks accessible through the partners networks in the ways of targeted surveys and where possible by exploiting existing solutions for technology driven research and innovation scanning and monitoring. (T3.3) contributes strongly to the GM-01 call medium term impact Nr1 and Nr2. In (T3.3) activities are:

1. Identify and select available techniques and tools to perform the scanning and monitoring.
2. Making an inventory of sources that need to be scanned and monitored: *partner accessible resources; Open sources, Internet, databases, other sources; Recent available technology and horizon scan reports; Closed/Personalized sources and databases like EU SCOPUS.*
3. Using the hybrid threats taxonomy (defined proposal Section1-3) and the selected techniques, methods, tools perform scanning/monitoring: *Run surveys& gathering of the information on the project partners' innovations& researches portfolio; Run surveys& gathering of the information on the extended partners innovations & researches portfolio on the topic; Perform available tools based scanning / monitoring*
4. Align potential innovations and research to the end-users identified Needs & Gaps*: Run initial results reviews; Conduct Innovation potential assessment between experts, academia, practitioners; Produce uptake case descriptions on selected prioritized innovations*
5. Produce a fashionable report or overview of the results, which will be then used by T3.1

The importance of this deliverable in the context of U-HYBNET Work Package (WP) 3 "*Surveys to Technology, Research and Innovations*" for EU-HYBNET and the interactions with other Tasks is depicted in the Figure below.

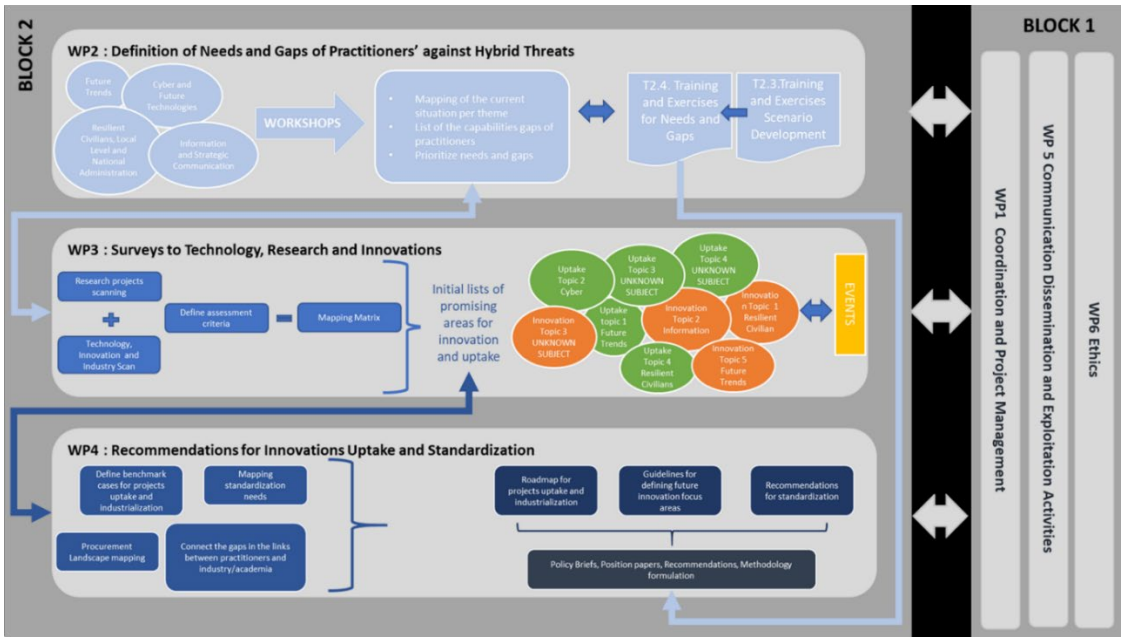



**Figure 1 : EU-HYBNET structure of Work Packages and Main Activities**

## 1.1 OVERVIEW

### OBJECTIVES OF THE DELIVERABLE

EU-HYBNET's Task (T) 3.3 "*Ongoing Research Projects Initiatives Watch*" deliverable (D) "First Report on Innovation and Research project Monitoring" (D3.7) on project month (M) 7 (November 2020) focused on scanning scientific research area, defining the status of the knowledge of the researched phenomena, which were identified in the EU-HYBNET's Gaps and Needs deliverable (D2.9) "Deeper analysis, delivery of short list of gaps and needs" in M5 (September 2020).

This T3.3 document, "First Mid-Term Report on Innovation and Research Monitoring" (D3.8), focuses on identifying relevant EU funded research projects which have relevance to the knowledge areas defined in D2.10 "Deeper Analysis, Delivery of Short List of Gaps and Needs" (further in the text "Gaps and Needs Document") in M22 (February 2022). It aims to build understanding on the activities of EU funded projects related to identified areas, possible cooperation areas with EU-HYBNET.

Innovation scan will discuss state of play in the field, identify concepts, tools, technologies, or solutions which were developed or are under development in EU funded research projects that have potential of addressing identified gaps. Note: focus of this deliverable are the innovations under development or testing. Therefore, only innovations before the widespread adoption in their field would be considered, as otherwise they become a subject matter of EU-HYBNET Task (T) 3.2. "*Technology and Innovations Watch*".

The material that was used in T3.3 is "open access" and generally available, in other words, EU-HYBNET will not use classified or restricted project and research material.

## 1.2 STRUCTURE OF THE DELIVERABLE

This document describes scan results for hybrid threats on the following core areas:

- Section 1: Introduction to the deliverable and work conducted
- Section 2: Core Theme: Resilient Civilians, Local Level and Administration
- Section 3: Core Theme: Cyber and Future Technologies
- Section 4: Core Theme: Information And Strategic Communications
- Section 5: Core Theme: Future Trends of Hybrid Threats
- Section 6: Conclusions

## 1.3 METHODOLOGY

EU-HYBNET "Deeper Analysis, Delivery of Short List of Gaps and Needs" document (D2.10) serves as an input for the scan. D2.10 is structured according to the EU-HYBNET project four Core Themes (Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; Information and Strategic Communications). In D2.10 three areas and dimensions to each of the Core Themes has been identified. These areas and three dimensions are:

- Critical Threats discusses dynamics which lead to the threat.
- Critical Gap discusses what gaps in response exist, which exposes us to the risk associated with the threat
- Critical Need analysis further leads discussion to what needs to be acted upon to close the gap and mitigate the risk.

D2.10/Gaps and Needs document defines overly broad areas, which encompasses a variety of intertwined phenomena, complex dynamics of specialized subject matter and hybrid threats.

Furthermore, D2.10/Gaps and Needs document is restricted, so it cannot be cited in the document, which has classification of “Public”.

Thus the D2.10 defined Gaps and Needs areas for the purposes of this document were redefined in a manner as to narrow down to specific aspects, to which scanning may be further focused.

General process consisted of several steps:

1. As described above, areas defined in gaps and Needs document with by Critical Threat / Critical Gap / Critical Need were redefined in the brief description focusing on some relevant aspect.
2. This redefined subject area was operationalized into relevant searchable keywords.
3. The description keywords were then used to scan EU funded research projects in The Community Research and Development Information Service (CORDIS).
4. Relevant projects were selected, analyzed and relevance to the research area described, linking to the project deliverables or planned deliverables of the project. Recommendations on observations of project development produced.

# 2. INNOVATION AND RESEARCH PROJECTS MONITORING. CORE THEME: RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Focus of this Project Core Theme in the current iteration is on mechanisms of foreign influence on democratic processes of EU countries and aim to harm basic functions of a state e.g. critical infrastructure.

## 2.1 CRITICAL NEED NO.1: EXPLOITATION OF EXISTING POLITICAL CLEAVAGES

### DEFINITION OF THE RESEARCH AREA

A key goal of hybrid operations is to lower trust in the local and country's administration and disrupt trust fabric of the society. In the current digitalized world, people are interconnected through digital social networks that make them susceptible to foreign malicious influence. Often the objective of the malicious influencing is to sow discord between the fellow citizens, which then can exploit and aggravate the existing political cleavages.

At its worst, the purposeful manipulation may lead to harmful societal consequences, such as increasing tensions and ultimately extremism. Although the threat is well-known, Western societies find themselves ill prepared to neutralize foreign influence due to tradition of protecting privacy and freedom of expression.

Freedom of expression is one of strongly protected core values of democratic societies. Thus, it is important to increase citizens' resilience to information attacks, rather than hope to protect them from information attacks as such. There is a need identified to find ways to make citizens better informed about the potential threats and alert when they are exposed to manipulation.

Tools are needed to make citizens more aware of dis-/misinformation and to offer them routes to sources of verified information.

### PROJECTS

We searched projects from the Cordis database by using several terms, including "democracy" and "polarization" (Collection: Projects; Domain of Application: Security/Society; Programme: H2020), yielding several relevant results.

The opportunity for open political discussion is a cornerstone of European democracies. The long tradition of public political debate has in recent years moved increasingly onto virtual platforms as digitalization and technological development have opened new channels for public discussion. These changes have enlivened civic engagement and political discourse. Simultaneously the information load has multiplied, when anyone can post their messages online irrespective of their factual basis. Deliberate (disinformation) and unintentional (misinformation) dissemination of false information have various detrimental consequences, e.g. de-legitimating the justified opinions of experts, losing common ground for discussion in society, sowing distrust in information from officials, and mainstream media, etc.

We identified three pertinent projects that are designed to help individuals' capabilities to discern disinformation from reliable information.

**In the Wider and Enhanced Verification for You (WeVerify)** project (H2020), the aim was "to address the advanced content verification challenges through a participatory verification approach, open-source algorithms, low-overhead human-in-the-loop machine learning and intuitive visualizations."[1] The project has

[1] https://weverify.eu/about/

developed the InVID-WeVerify browser plug-in that will help its user to verify online information[2]. In September 2021, the browser extension was awarded the U.S. State Department's Global Engagement Centers' U.S.-Paris Tech Challenge prize against disinformation and propaganda[3].The award brought additional funding for the project that enables the further development of the plug-in.[4] Furthermore, the WeVerify project assembled a companion to help citizens and fact-checking professionals to take advantage of the features of the plug-in. The companion also includes links for citizens to find online advice concerning disinformation threats. The WeVerify project ended in October 2021.

**Open Distributed Digital Content Verification for Hyper-connected Sociality (SOCIALTRUTH)**[5] project that started 1 December 2018 and closed 30 November 2021 with Grant agreement ID: 825477.

Project tries to investigate alternative path to current mainstream way of entrusting content verification to a single centralized authority which while being expensive approach, has its own share of problems.

SocialTruth's aimed to create an open, democratic, scalable, and completely decentralized environment. The distinctive advantages are: a) avoidance of vendor lock-in through access to configurable combinations of various content analytics and verification services (with support for text, image and video content) via standard Application Programming Interfaces; b) distributed trust and reputation establishment powered by blockchain technology, ensuring immutability and auditability, revealing information cascades and empowering an information veracity observatory; c) integration of lifelong learning approach for detection of new paradigms of fake news; d) easy interaction through a Digital Companion that allows convenient everyday access of individual users to verification services from within their browsers.

SocialTruth developed seemingly promising technologies, still it remains to be seen efficiency of those in real world environments and its sustainability/business model.

**The Co-Creating Misinformation-Resilient Societies (Co-Inform)** project (H2020) aimed at fostering "informed and engaged communities, which constitute the foundations of a healthy democracy and together find a solution to misinformation."[6] More concretely, the project provided tools for citizens, journalists, and policymakers to better identify misinformation, increase their understanding of how misinformation spread and reach verifiably factual information. The main tool is a plug-in to an internet browser to increase citizens' awareness concerning misinformation. The plug-in does this through links to fact-checking articles and corrective information as well as providing other citizens' opinions on specific matters, including comments both for and against. Together with a dashboard targeted at fact-checking journalists and policymakers, the Co-Inform browser plug-in form a misinformation resilience platform. The Co-Inform project has ended in July 2021.

**The Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (COMPROP)** project (ERC Consolidator Grant) complemented previous projects' approaches by implementing research on the use of networks of automated social media accounts. That is, "the use of

[2] https://weverify.eu/verification-plugin/

[3] https://weverify.eu/news/the-invid-weverify-verification-plugin-wins-the-u-s-paris-tech-challenge-against-disinformation/

[4] https://www.safetytechnetwork.org.uk/the-u-s-paris-tech-challenge-hear-from-the-winners/; https://disinfocloud.com/blog/us-paris-techchallenge-summary

[5] https://cordis.europa.eu/project/id/825477

[6] https://coinform.eu/about/the-project/

algorithms, automation, and big data analytics to purposefully disseminate manipulative and misleading messages over these social media networks."[7]

The COMPROP project was able to demonstrate how malicious political actors have been able to utilize computational propaganda in generating a lack of knowledge and unawareness by producing conflicting stories and multiple explanations of specific incidents.

According to the project's findings, the target group of the computational propaganda bot campaigns are "only 10-20 % of the population, typically disaffected, conservative-leaning adults who are politically active."[8] Ability to shape the views of this part of the population in most cases would turn the tide of election/referendum.

The project's findings have been collected into an online resource guide that will help citizens and civil society groups to manage the challenge of disinformation. The platform is called today The Demtech Navigator (originally COMPROP Navigator).[9] The project ended in December 2020. The COMPROP research group have received funding also for a proof-of-concept grant for the Junk News Aggregator[10]. COMPROP project's PI, Professor Philip N. Howard, continues with his team research on computational propaganda in the Oxford Internet Institute at the University of Oxford. The Programme on Democracy & Technology has been active since 2012.[11]

## 2.2 CRITICAL NEED NO.2: EXPLOITATION OF CRITICAL INFRASTRUCTURE WEAKNESSES AND ECONOMIC DEPENDENCIES

### DEFINITION OF THE RESEARCH AREA

Malicious actors employing hybrid tactics aim to utilize and leverage existing weaknesses of a target country. Hybrid threat actors specifically look for targets of attack that have a quality of "cascading effects", usually due to their various dependencies. Increasing complexity has made the management of the potential effects of attacks extremely challenging but also more important than ever. At the same time, the sophistication of attackers rises. More complex attack strategies are employed – they combine multistage action, combine information and cyber-attacks. Very often one step of multistage attack combines actions which do not qualify as high-risk attacks, but in combination they yield significant damaging results.

Critical Infrastructure operators and those responsible for CI protection needs to acquire technologies and skills to identify such complex attacks so that they may respond timely and adequately.

Tools are needed to acquire comprehensive situational awareness spanning across multiple areas of attacks and long periods of time. Comprehensive situational awareness effectively can only be achieved by collaboration of trusted partners in capturing signals, exchanging intelligence, and coordinating action, thus tools are needed for organization of such collaborative situational awareness.

[7] https://cordis.europa.eu/project/id/648311/reporting

[8] https://cordis.europa.eu/article/id/430251-the-secret-robot-armies-fighting-to-undermine-democracy

[9] https://navigator.oii.ox.ac.uk/

[10] https://cordis.europa.eu/article/id/286126-junk-news-aggregator-aims-to-restore-trust-in-media-and-democracy

[11] https://demtech.oii.ox.ac.uk/

PROJECTS

We conducted searches with search terms “critical” AND “infrastructure”, “situational awareness”. Further results directly relevant to the subject of our analysis are discussed.

**Strategic programs for advanced research and technology in Europe (SPARTA)**[12] [13] is one of 4 key pilots dedicated to redefining cybersecurity in EU. Program titled T-Shark is specifically dedicated to Full-spectrum cybersecurity awareness.

One of the important ambitions of T-Shark is effort to extend situational awareness beyond cybersecurity area. SPARTA developed a framework of “Comprehensive Full-Spectrum Cybersecurity Threat Intelligence”. Its aim is to develop technologies and models which allow orchestration of situational awareness processes, identification, intelligence, and counteraction across multiple stakeholders' organizations. SPARTA categorizes addressable threats to (1) full spectrum attacks, (2) high caliber attacks, (3) long term attacks, (4) uniquely designed attacks, (5) multistage attacks, (6) advanced persistent threats (APT) and state of play of different methodological (technological, functional, process or organizational) frameworks of cybersecurity.

T-Shark has developed a model of Comprehensive Full-Spectrum Cybersecurity Threat Intelligence, which, as deliverable concludes, is still in development stage. Further efforts are needed to elaborate and test it in real life situations.

On the other hand, SPARTA T-Shark deliverable D4.3 concludes, that Comprehensive Full-Spectrum Cybersecurity Threat Intelligence is not just theorizing. T-Shark tested existing technologies and developed technologies closing the gap which specifically address requirements of the discussed model. Such as enabling sharing of intelligence, mapping of incidents, etc. These technologies are preselected in the deliverable, tested, and discussed. Maturity level of technologies differ, so further development efforts are needed.

SPARTA started Feb 2019 and ends Aug 2022.

**The Protection of Critical Infrastructures from advanced combined cyber and physical threats (PRAETORIAN)** project aims to produce “a multidimensional (economical, technological, policy, societal) - - toolset”[14] that will benefit CI operators in decision making. The PRAETORIAN will combine the physical situation awareness component and cyber situation awareness component into a hybrid/comprehensive situation awareness system that will ultimately be transformed into a coordinated response system allowing well-coordinated responses to potential emergencies.

The project builds on eight successful critical infrastructure protection projects, which, firstly, allows it to utilize earlier technologies and findings, and, secondly, proves that the partners can produce innovative results. The PRAETORIAN project started in June 2021 and will last until May 2023.

**The Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with a focus on district or regional protection (PRECINCT)** project that started in October 2021, thus at the time of writing of this report it is still in very early stages. The project “aims to connect private and public CI stakeholders in a geographical area to a common cyber-physical security management approach which will yield a protected territory for citizens and infrastructures.”[15]

[12] https://cordis.europa.eu/project/id/830892
[13] https://www.sparta.eu/#SPARTA
[14] https://praetorian-h2020.eu/
[15] https://www.precinct.info/

PRECINCT will develop an ecosystem platform for improving the security and resilience of interdependent critical infrastructures, specifically combining physical and cyber areas for wider situational awareness. It will develop tools and models for collaborative response action to identified threats.

PRECINCT will develop vulnerability assessment tool, based on serious games. It will aim to identify vulnerabilities to cascading effects and to assess measures for enhancing resilience.

From EU-HYBNET's point of view, PRECINCT's approach is noteworthy because of its ambition to integrate private and public stakeholders under the same CI security framework. PRECINCT will bring together prior results from three EU-funded projects and capitalize on legacy structures.

Project started Oct 2021, end Oct 2023

## 2.3 CRITICAL NEED NO.3: EXPLOITATION OR INVESTMENT IN COMPANIES BY FOREIGN ACTORS

### DEFINITION OF THE RESEARCH AREA

Companies are potential channels for hybrid aggressors to extend their leverage to target countries. For example, direct access to corporate decision-making can create opportunities for various kinds of hybrid activities that state-affiliated actors may use in the host countries. The extent of the impact of the action depends on the specific field of operation and the centrality of the given firm in a specific sector.

To watch the development of foreign investments and notice concurrent behavior patterns in several countries, the Member States should be able to exchange relevant intelligence information with each other seamlessly and in a timely manner.

Tools are needed to achieve improved information gathering and sharing practices that will help in the development of more effective investment screening.

### PROJECTS

Searches in the Cordis database concerning projects focusing on investments in general, and foreign direct investments (FDI) in particular, brought dozens of results (Collection: Projects, Domain of Application Security/Society, Programme: H2020, Search term: investment), but none of them was relevant for EU-HYBNET purposes.

Considering how much there has been public discussion about authoritarian states' efforts to use state-affiliated companies and their products as vehicles of intelligence, this must be seen as a surprise.

A potential reason for such a shortage or lack of relevant research projects is most likely the EU's recently adopted investment screening mechanism. The mechanism has been in force only since October 2020 and experiences of its functioning are still preliminary. Yet, based on the initial conclusions from the EU's FDI screening[16], it is clear that EU should make further adjustments to extend the coverage of its screening mechanism to all Member States and to develop mechanisms for advanced cross border risk assessment. This might entail, for example, tools for tracking actions of foreign companies in different Member States or a platform for information sharing between the Member States.

[16] Ghiretti (2021), Screening foreign investment in the EU – the first year (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); First Annual Report on the screening of foreign direct investments into the Union. COM(2021) 714 final.

Recent research has included comparisons of different territorial or national FDI screening mechanisms.[17] These papers have shown the major similarities and differences between the regulatory systems. The findings would be beneficial for at least two different applications. First, they can be used for benchmarking. Alternatively, they provide food for thought for potential cross-border or even globalized risk assessment frameworks.

[17] Chan, Z.T., Meunier, S. (2021). Behind the screen: Understanding national support for a foreign investment screening mechanism in the European Union. The Review of International Organizations.; Ghiretti, F. (2021). Screening foreign investment in the EU – the first year. (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); Jacobs, J. (2019). Tiptoeing the Line Between National Security and Protectionism: A Comparative Approach to Foreign Direct Investment Screening in the United States and European Union. International Journal of Legal Information, 47(2), 105-117; Rajavuori, M., & Huhta, K. (2020). Investment screening: Implications for the energy sector and energy security. Energy Policy, 144, 111646.

# 3. INNOVATION AND RESEARCH PROJECTS MONITORING. CORE THEME: CYBER AND FUTURE TECHNOLOGIES

Disruptive innovations is the name of the game in this iteration of scanning. In the First Iteration of scanning (D3.7) Quantum Computing as a technology capable of significant disruption was analyzed. This iteration focuses on the spectrum of disruptive innovations, and how societies need to be prepared for their effects.

## 3.1 CRITICAL NEED NO.1: SPACE INTERFERENCE AND COUNTERSPACE WEAPONS

### DEFINITION OF THE RESEARCH AREA

The world is increasingly dependent on space systems for economic and military security. Commercial space has opened markets and enabled entirely new industries worldwide. Moreover, the global economy depends on weather data, communications, navigation, timing, remote sensing, and other space systems.

Due to the strategic importance of space, some nations are developing weapons that target space systems, which can destroy space systems and threaten the availability of other regions. However, the strategic importance of space has also inspired new efforts to mitigate conflict and protect the region for peaceful purposes.

Tools and mechanisms are needed to ensure the safety of outer space.

### PROJECTS

A search in the Cordis database has very few projects on the subject.

**Protection and Resilience Of Ground-based infRastructures for European Space Systems** (PROGRESS)[18]. This project was funded under FP7-Security in the period from 01.05.2014 to 31.10.2017.

PROGRESS focused on detecting and mitigating intrusions to GNSS from highly educated attackers whose numbers may increase soon. The goal of the project is to enable expanded intelligence in GNSS architectures to ensure the uninterrupted performance of services. The potential impact of attacks is to be reduced through protective solutions; attacks are to be detected and analyzed for impact, and where necessary, affected elements of the GNSS are to be reconfigured.

**7SHIELD: a holistic framework for European Ground Segment facilities that is able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases[19].** This project was funded under H2020 in the period from 2020 to 2022.

The project focuses to enhance security concerns of ground segments that appear to be potential new targets for complex physical/cyber threats as they receive massive amounts of satellite data. In more detail, the ability to disrupt, inspect, modify or re-route traffic provides an opportunity to conduct cyber/physical attack. Such an attack could have a dramatic impact on the security of European citizens and can initiate cascading effects to other Critical Infrastructures. The 7SHIELD project is also identified to deliver a promising solution to the named gaps & needs in EU-HYBNET Task 3.2 “Technology and Innovations Watch” deliverable 3.4 (submission DL M24/ April 2022), and hence more detailed description of the usability of the 7SHILED solutions in D3.4

[18] https://cordis.europa.eu/project/id/607679

[19] https://www.7shield.eu/project/

### Other Research Findings

A series of "Space Threat Assessments" has been published by Aerospace. They provide a repository of counter space weapons data comprised of tests, technology demonstrations, and unusual behaviors first identified in their annual Space Threat Assessment report series[20].

But for some time, it has been obvious that technical measures are not satisfactory. Outer space technologies became so entrenched and important to various activities, that legally binding mechanisms become necessary to regulate cohabitation and conflict resolution.

Event "2021 Outer Space Security Conference"[21] held in the Palais des Nations, Geneva, under organization of UNIDIR United Nations Institute for Disarmament Research provided forum for the diplomatic community and experts with military, industry, and academic backgrounds to jointly consider challenges related to security in outer space and exchange ideas regarding solutions[22].

To address the challenges of space interference, some experts in space security have called for more robust norms of behavior in outer space. A report published by Jessica West et al. explore the role of norms as a tool for outer space governance and their challenges and limitations[23]. This becomes crucial, as many countries take steps to militarize outer space.

Nina Klimburg-Witjes published an article in 2021 in the journal named "European Security" titled "Shifting articulations of space and security: boundary work in European space policy-making."[24] The paper presents a critical empirical examination of the ongoing changeover in European space policy that significantly affects how we envision a "united Europe in space". And it concludes with a trend, that ultimately EU will have to accept that outer space moves from "security" area of governance to "defense".

## 3.2 CRITICAL NEED NO.2: OFFENSIVE CYBER CAPABILITIES

### DEFINITION OF THE RESEARCH AREA

Secure networks and information systems protect us from cyber-attacks. However, the increasing use and dependency on information and communication technologies produce risks and opportunities for cyber defense. In the emerging digital arms race, the EU is increasingly cooperating on cyber defense to combat cyber attackers.

Offensive Cyber Capability (OCC) combines human, technical, and organizational attributes to support offensive cyber operations: the adversarial manipulation of digital services or networks. The OCC focuses primarily on its (de-escalation) potential in terms of diplomatic tension, instability, or power.

Tools are needed to share the knowledge between different members of the EU to improve and faster develop the offensive cyber capabilities to handle the new challenges, especially in the industry 4.0 evolution.

[20] https://aerospace.csis.org/counterspace-timeline/

[21] https://www.unidir.org/events/2021-outer-space-security-conference

[22] report of the conference https://www.unidir.org/publication/2021-outer-space-security-conference-report

[23] https://www.unidir.org/publication/space_dossier_7_norms_outer_space

[24] https://www.tandfonline.com/doi/full/10.1080/09662839.2021.1890039

### PROJECTS

**Strategic Cultures of Cyber Warfare** (CYBERCULT)[25], which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01.07.2019 to 19.09.2021.

This project studied the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel, and the United States. It also reviewed the cultural, socio-political, historical, and ideological factors involved.

Project put significant focus on cultural aspects and how framing of the cybersecurity overall may be instrumental or detrimental to the global cybersecurity. CYBERCULT discusses, that current global approach where countries frame cybersecurity as "preparation for war" will not lead to any sort of equilibrium. Project authors suggest, that "cyberpeace" is a positive concept which needs to be constructed and protected. CYBERCULT did not aim to create any technologies, but rather to deepen our understanding on strategic thinking and cultural factors which motivates development of offensive cyber capabilities, and framework for achieving less destructive global cyberenvironment.

To promote resilience in international cyberspace, the UNIDIR Security and Technology Programme designated a series of investigation papers summarizing national capabilities to execute international cyber operations and appropriate national principles regulating the behavior of such operations. In the resulting documents, nine scholars and practitioners provide a summary of the capabilities and declarations of 15 countries across different regions: Australia, Brazil, Canada, China, France, Germany, India, the Islamic Republic of Iran, Israel, Japan, the Republic of Korea, the Russian Federation, Saudi Arabia, the United Kingdom of Great Britain and Northern Ireland, and the United States of America[26]

Journal of Global Security Studies by Florian J. Egloff and James Shires under "Offensive Cyber Capabilities and State Violence: Three Logics of Integration." article discusses a re-orientation toward the normatively prior question of their relative violence. It asks: how are OCCs integrated into violent state capacities, and what are the consequences? The article proposes three logics of integration by which OCCs are included in violent state actions in repressive and interstate situations[27].

As discussed above, offensive cyber capabilities do have legal and ideological framing. In hybrid threats domain it is important to discuss ethical and legal aspects of applying hybrid attacks concepts and methods against countries which are engaged in hybrid attacks against EU. This seems to be a field which is not researched and explored.

## 3.3 CRITICAL NEED NO.3: DISRUPTIVE TECHNOLOGIES

### DEFINITION OF THE RESEARCH AREA

Innovations became very important driver of economic and military power, reflecting this most of the countries fund research and development effort as well as innovation uptake. In most cases innovations became necessary part continuous and incremental improvement. This is an effort where country has to invest in order "not to lose".

So disruptive technologies have a potential for "winning" – for the first mover disruptive technologies give asymmetrical advantage against others.

[25] https://cordis.europa.eu/project/id/844129
[26] https://www.unidir.org/cyberdoctrines
[27] https://academic.oup.com/jogss/article/7/1/ogab028/6412386

There is a need to develop framework for coping with emergence of disruptive technologies.

PROJECTS

Disruptive technologies, in this context, will be discussed as new technologies that affect, or rather disrupt normal operation of established market or industry. While most disruptive technologies (e.g. autonomous driving) may change dynamics and power structure of the market, their ascent is gradual over a significant period of time, which sustains the power equilibrium or shifts it in very gradual fashion.

Still there are some cases, where disruption can be very sudden and significant. Such disruptive technologies have power disturb established equilibrium, by changing military or economical balance (consider the change of military balance when first country acquired nuclear arms).

EU-HYBNET D3.7 (M7/ November 2021) discussed one of examples of such potential disruptive technology – development of quantum computer of industrial scale. Such development would be able to break all asymmetric encryption, which is a basis of security of today's electronic communications and thus at a heart of internet.

The subject of disruptive technologies is complex and can be approached from different angles. EU recognizes significant potential disruptive technologies and invests in them to establish leadership (or at least to be among leaders) – subjects of quantum, space technologies, 5G have significant number of hits in Cordis database and EU various policy documents.

For example, **INtelligent Security and PervasIve tRust for 5G and Beyond (INSPIRE-5Gplus)**[28] explores ways to improve control of systems and eliminate vulnerabilities for the infrastructure owners and tenants, employing machine learning, AI, and blockchain technologies. **Isogeny-based Toolbox for Post-quantum Cryptography** (ISOCRYPT)[29] is one of the projects exploring cryptography which would be usable in today's technological context, as well as remain secure when quantum computing capabilities are deployed. Project is exploiting mathematical maps called isogenies in new algorithms for security in a pioneering cryptographic paradigm.

But despite wealth of projects addressing specific technical security aspects, hybrid threat dimension of disruptive technologies is not yet well studied and does not receive attention in EU project funding. While it seems, that "hybrid threats of disruptive technologies" should deserve both conceptualization and practical preparation.

Hybrid CoE paper "**Quantum Sciences – Disruptive Innovation in Hybrid Warfare**"[30] discussed aspects of the disruption related to quantum computing. Paper touches upon the potential to exploit disruptive technologies for hybrid attacks. It concludes with recommendations that should ensure, that EU does not find itself a laggard in this area.

Still, despite investment and efforts it is quite possible, that adversary country will be more successful in the field. In this situation threatening hybrid attacks scenarios become possible.

JRC technical report "**Quantum as a disruptive technology in Hybrid Threats**"[31] published in 2021 is a rare example of trying to illuminate hybrid threat aspects in such technology heavy area. Report finds it necessary to discuss how we should be prepared for the negative outcome of the race. In the report authors discuss

[28] https://cordis.europa.eu/project/id/871808

[29] https://cordis.europa.eu/project/id/101020788

[30] https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-7-quantum-sciences-disruptive-innovation-in-hybrid-warfare/

[31] https://euhybnet.eu/wp-content/uploads/2021/12/Quantum-research-article_final_.pdf

aftermath of adversary country succeeding to develop usable quantum computer first (example of disruptive technology):

> "There may be significant benefits to be attained by an adversarial country, which would provide the greatest opportunities for increased attacks based on innovative technologies, even though these could only be sustained for a brief period.
>
> In the future, we should expect that a post-quantum equilibrium will be reached, as the quantum secure technologies are developed and deployed. Thus, the motivation to leverage this opportunity for the adversary in such a limited time span could be very tempting."[32]

Further research and discussions are needed to conceptualize hybrid threats landscape and response in case of losing disruptive technology race. Quantum computing is important, but nonetheless only one of examples of such disruptive technologies.

[32] ibid

# 4. INNOVATION AND RESEARCH PROJECTS MONITORING. CORE THEME: INFORMATION AND STRATEGIC COMMUNICATIONS

Information and Strategic Communications in this iteration primarily deals with domains of information and intelligence as an element of modern information warfare. This area is strongly interlinked with legal domain, as monitoring criminal and violence inciting activities stay in strictly legal borders.

## 4.1 CRITICAL NEED NO.1: INFORMATION MANIPULATION WITH THE AIM OF DESTABILIZATION

### DEFINITION OF THE RESEARCH AREA

Information attacks became a tool of choice for destabilization activities, employing various levels of information manipulation.

EU, as well as public and private organizations worldwide, invest significant efforts in trying to build human, AI based and mixed systems for fact checking, information verification, deep fakes recognition, there is still much to be done. Such research and initiatives are discussed in this deliverable other chapters, as well as in first iteration of this deliverable (EU-HYBNET D3.7 in November 2020)

Importantly, despite significant public awareness about the proliferation of misinformation and disinformation, the public stays susceptible to such information attacks.

A deeper understanding of the mechanisms behind manipulation of information is needed.

### PROJECTS

**Information and Misinformation Economics: Design, Manipulations and Coutermeasures** (IMEDMC)[33] project that started 1 May 2021 and ends on 30 April 2026 with Grant agreement ID: 101001694.

The discussed project is still in the early stage. It aims to get insight into socially or privately optimal information designs, explaining how they form upstream and downstream decisions, how private interests manipulate them, and how this can be anticipated and countered.

IMEDMC will analyze the unexplored designer-agent-receiver class of games considering fake news production – state falsification, pure agency and state shifting, taking a systems approach.

For simulations, project will employ underutilized designer-agent-receiver class of games, in which the designer picks an information generation system, the agent takes an upstream decision affecting the states of the world, or manipulates the production of information, and receivers choose downstream actions based on realized signals.

This is a rare kind of project trying to employ modeling and experimentation in the area where observation as method is mostly used.

While project results may be useful on their own, for EU-HYBNET the very approach and methods employed in the project may render specific interest. It may be appropriate to observe successes and drawbacks of approach and methods applied and discuss their applicability to model and analysis of hybrid threats.

[33] https://cordis.europa.eu/project/id/101001694

There are a number of interesting technological project focused on fake detection. **Deepfake Detection** (DIGGER)[34] tries to fuse both visual verification and audio forensic technologies to detect both shallow fakes (manipulated audiovisual content (image, audio, video) generated with simple technologies like Cut & Paste or speed adjustments which, despite low investment, may be extremely convincing) as well as deepfakes or synthetic media (these are artificial audiovisual content (image, audio, video) generated with technologies like Machine Learning which is extremely realistic).

**Wider and Enhanced Verification for You** (WeVerify)[35] , project started Dec 2018 to Dec 2021, established opensource, cross modal participatory information verification. Project developed technologies, including browser plugin which had over 57 thousands downloads.

**Open Your Eyes: Fake News for Dummies**[36] is a Erasmus+ project dedicated to improve the digital literacy of adult learners by providing them with tools to identify fake news and fight the spread of disinformation online.

It is important to continue and extend of such project beyond "supply side" verification – how we recognize fakes, to understand more "demand side" of fakes. Research having insight and data access in both spheres have significant potential.

## 4.2 CRITICAL NEED NO.2: FOREIGN INTERFERENCE IN KEY INFORMATION INSTITUTIONS

### DEFINITION OF THE RESEARCH AREA

Foreign interference occurs when activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupt and are aimed to influence outcomes of political processes.

Foreign interferences represent a huge challenge for democratic government and society. The 2016 US Presidential elections, the 2016 referendum on UK membership in the EU, the 2017 French presidential elections are prominent illustrations of a more general and dangerous trend.

While foreign interferences have existed for a long time, the internet and social media have provided new, fertile ground for their pursuit. Social platforms have been used effectively to wage large-scale disinformation campaigns by countries such as China or Russia, particularly ahead of new elections, with social media enabling them to cover their actions behind automated accounts or bots.

There is a need identified to better understand phenomena leading to the receptiveness of democratic societies to foreign influence efforts.

### PROJECTS

We searched projects from the Cordis database by using the term "foreign interference" (Collection: Projects; Domain of Application: Security/Society; Programme: H2020). After an initial analysis of the potential projects, we selected the following two projects that had the best fit with our point of view and thereby offered a notable potential for further development and co-creation.

[34] https://digger-project.com/

[35] https://cordis.europa.eu/project/id/825297

[36] http://dlearn.eu/projects/online-and-offline-security/open-your-eyes/

**The Consequences of the Internet for Russia's Informational Influence Abroad (RUSINFORM)** project - a closer look at Russia's digital disinformation, EU financed H2020, implementation from Nov 2019 to Dec 2024, coordinated by Universitat Passau in Germany.[37]

RUSINFORM aims to deepen the knowledge of the background, model, mechanism of exerting influence and susceptibility to influence, and assess results of such actions. The project is not aiming to develop specific technologies yet. Based on actual examples it aims to use datamining methods together with more traditional research methods, like surveys and interviews.

The expansion of internet technology has enabled digital disinformation attacks on electoral campaigns in the EU states during the last years. Russia has been accused of orchestrating the attacks. The digital interference in elections raised serious concerns about the future of European societies. It will study the role that foreign on-line audience and social media play in the transmission of Russian media content to the Russian speaking media abroad. It will also investigate the role that the Kremlin-controlled search engine Yan-dex plays in foreign influence.

Over the past decade, Russia's ruling elites have massively stepped up their efforts to influence media audiences abroad, in this way limiting exposure of state actor and in many ways escaping scrutiny. Amongst others, Russia has been alleged to have sought to sway votes in Austria, France, Germany, Ukraine, and the US. This project tries to define the role of Internet-based technologies contributed to the emergence of novel resources, techniques, and processes by which influence is exerted.

RUSINFORM scrutinizes three heavily digitally enabled elements of Russia's recent efforts:

- study foreign online audiences who co-create and disseminate Russia-related content.
- research how social media platforms function as key transmission channels that connect Russia's domestic media with Russian-speaking audiences abroad.
- scrutinize the role of the Kremlin-controlled search engine Yan-dex as a resource of foreign influence.

RUSINFORM tries to introduce datamining techniques and automated text analysis in combination with traditional methods (surveys, in-depth interviews, grounded theory). The innovative combination of these techniques hopefully will deepen understanding of the phenomena and build a better methodological basis for further analysis efforts. While RUSINFORM does not plan to produce any specific product because of the project, nonetheless it seems especially important in advancing our knowledge of the mechanisms of foreign influence.

**Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (COMPROP)** EU financed H2020 project, implemented from Jan 2016 to Dec 2020, coordinated by the University of Oxford.[38]

Social media platforms have come to play major roles in shaping politics, culture, and economic lives. COMPRPO researched specific aspects of "computational propaganda" involves the use of algorithms, automation, and big data analytics to purposefully disseminate manipulative and misleading messages over these social media networks. Importantly, computational propaganda method usage is not limited to solely exerting foreign influence. It is constantly used for internal political aims, and increasingly so by lobbyists.

Misinformation on social media has emerged as one of the most serious threats to democratic processes. Political actors with vested interests in interfering with such processes have been attempting to manipulate public opinion. Recent years have also seen the advent of algorithmically derived content systems and bots

[37] https://cordis.europa.eu/project/id/819025
[38] https://cordis.europa.eu/project/id/648311

that deliberately work to amplify hate speech and polarizing misinformation. Democracy itself is under assault from foreign governments and internal threats, such that democratic institutions may not continue to flourish unless social data science is used to put our existing knowledge and theories about politics, public opinion, and political communication to work in their defense.

The project seeks to answer fundamental research questions: How are algorithms and automation used to manipulate public opinion during elections or political crises? What are the technological, social, and psychological mechanisms by which we can encourage political expression but discourage opinion herding or the unnatural spread of extremist, sensationalist, or conspiratorial news? What new scholarly research systems can deliver real time social science about political interference, algorithmic bias, or external threats to democracy?

In this context, COMPROP has been tracking important moments in public life, such as elections and referenda, and more recently the global response to Covid-19, to identify the proportions of misinformation that circulate on social media. To defend the public sphere requires a better understanding of digital citizenship and modern civic engagement. Junk news, and the deliberate spread of misinformation, often generates profitable advertising revenues for technology firms and miscreants. Online hate speech, in particular misogyny and racism, gets aimed at public figures from fake accounts. Personalized political advertising, as used in large-scale data-driven campaigns, delivers targeted interventions with hidden agendas. Political bots and highly automated social media accounts disrupt election campaigns and sow seeds of doubt in the minds of citizens making important decisions around their own health, such as whether to take vaccines. This project advances the social data science, applies it to advance understanding of how contemporary civic engagement operates, and pioneers the social science of fake news production and consumption.

The Computational Propaganda's research has been foundational to the social science of misinformation, having produced the first wave of research on how authoritarian regimes interfere in the elections of democracies using social media. Moreover, the team have used the project's findings to inform and shape policy responses in Canada, the EU, UK, US and other democracies, and the team has been recognized by policymakers on both sides of the Atlantic as pioneers in the field of online disinformation.

## 4.3 CRITICAL NEED NO.3: PROMOTED IDEOLOGICAL EXTREMISM AND VIOLENCE

### DEFINITION OF THE RESEARCH AREA

Proliferation of isolated groups social media and closed groups in messaging platforms facilitate creating of controlled "bubbles", which may lead to extremism via mechanisms of group think, directing and manipulating. End-to-end encrypted messaging platforms are used to incite and coordinate violent actions.

Tools are needed to recognize extremist intentions, without sliding to surveillance and while preserving freedom of expression.

### PROJECTS

Cordis database provides vast landscape of projects which work in the field of "encryption" – developing new algorithms, use cases, approaches.

There very scarce research that would work on the field of accessing end-to-end encrypted communication.

At the time of writing this paper the tendering process is not complete for call **Effective fight against trafficking in human beings** (Fighting Crime and Terrorism 2022 (HORIZON-CL3-2022-FCT-01)[39] which focuses on needs of security practitioners and may fund research in methods and technologies with encrypted end-to-end messaging. Even if these efforts would be dedicated to law enforcement, developments need to be observed as they may provide technologies and methods suitable for broader applications.

**Artificial Intelligence Roadmap for Policing and Law Enforcement** (ALIGNER)[40] a project started Oct 2021 – Oct 2024, is dedicated to broader set of technologies for law enforcement and policing. It aims to jointly identify and discuss how to enhance Europe's security by employing AI and advanced technologies, it will pave the way for an AI research roadmap.

**Functional Encryption Technologies** (FENTEC)[41] started Jan 2018 to Mar 2021 aimed to distance itself from "all or nothing" traditional view on encryption. Functional encryption should in essence allow "functional decryptability". Naturally, one of functional decryption scenarios would be related to law enforcement roles.

This is an interesting approach, though technical feasibility and public acceptance has to be further investigated.

While worldwide there are some noted efforts to make some limited access to encrypted messaging systems[42], their reach and usability seems limited.

Both philosophical, legal and technical research is needed to define approaches to this issue.

[39] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-fct-01-07

[40] https://cordis.europa.eu/project/id/101020574

[41] https://cordis.europa.eu/project/id/780108

[42] Fighting Fake News in Encrypted Messaging with the Fuzzy Anonymous Complaint Tally System (FACTS), https://arxiv.org/abs/2109.04559

# 5. INNOVATION AND RESEARCH PROJECTS MONITORING. CORE THEME: FUTURE TRENDS OF HYBRID THREATS

In this iteration, Future Trends of Hybrid Threats targets its focus on threats related to rise of populism. How this phenomenon impacts political, social/societal and information domains. How to deal with this phenomenon while adhering to liberal principles of democracy.

## 5.1 CRITICAL NEED NO.1: GEOPOLITICAL HEAVYWEIGHT OF DOMESTIC POLICY

### DEFINITION OF THE RESEARCH AREA

Europe's strategic and geopolitical environment is evolving rapidly. It will always be an area of change, and in a manner that increasingly raises concerns. In recent years, violent conflicts have agitated the planet, many of them located in Europe's immediate neighboring regions. These developments take place at a time when global geopolitics is undergoing long-term transformations challenging the traditional predominance of the West, while policies of economic austerity oblige EU Member States to manage scarce resources more effectively. These trends challenge the Union's capacity for guaranteeing its citizens' security while also jeopardizing its aspiration of promoting European values and interests abroad.

In order to evaluate and promote its preparedness for playing its role as an effective security provider, to prevent escalation, to manage and understand risks and mitigation strategies for peace beyond its borders, the EU needs to understand the implications of recent global developments and assess them against its own capacities and willingness to make synergetic use of them. It is a challenge how to improve the EU's effectiveness as a domestic and global security provider.[43]

### PROJECTS

We searched projects from the Cordis database by using the terms “geopolitics” and “domestic policy”. (Collection: Projects; Domain of Application: Security/Society; Programme: H2020. After an initial analysis of the potential projects, we selected the following one project that had the best fit with our point of view and thereby offered a notable potential for further development and co-creation.

**Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (EU-LISTCO)** EU funded H2020 project, coordinated by Freie Universität Berlin, implemented in the period from Mar 2018 to May 2021.[44]

EU-LISTCO set out to analyze when areas of limited statehood (ALS) and contested orders (CO) in the EU’s Southern and Eastern neighborhood turn into threats for EU security. Contested orders refers to situations in which state and non-state actors challenge the norms, principles, and rules according to which societies and political systems are or should be organized. The project aimed to understand 1) under which conditions the situation deteriorates into governance breakdown and violent conflict, and 2) how can the preparedness of the EU and its member states to foster resilience in the neighborhood be strengthened.

EU-LISTCO research objectives were scientific as well as practical policy-oriented:

- Study the conditions for the deterioration into governance breakdown and violent conflict.
- Examine the sources of resilience that may mitigate risks from escalating into threats.
- Analyze the impact of global and diffuse risks on the likelihood of governance breakdown and violent conflict, identifying tipping points at which the latter may occur.

[43] https://cordis.europa.eu/programme/id/H2020_ENG-GLOBALLY-02-2017

[44] https://cordis.europa.eu/project/id/769886/reporting

- Assess the preparedness of the EU and its members to foster resilience
- Elaborate on success and failure cases in the EU's dealings with the challenges and risks

Through close collaboration with its practice partners — the Ministries of Foreign Affairs of France, Germany, and Italy as well as the European External Action Service — EU-LISTCO has ensured that its research has immediate policy relevance and impact.

The project has developed an innovative theoretical framework that lays out how societal resilience can prevent from deteriorating into governance breakdown and violent conflict. Societal resilience is a society's adaptive and transformative capacity to successfully cope with and recover from crises. The project theorizes the concept of societal resilience in an empirically applicable way and avoids the state. EU-LISTCO offers a new perspective for EU foreign and security policy.

The project's main findings overall are that societal resilience is a key mechanism to prevent governance breakdown and violent conflict in the EU's neighborhood.

Three primary sources of resilience were conceptualized:

- Social trust within societies and communities,
- legitimacy of (state and non-state) governance actors,
- effective, fair, and inclusive governance institutions.

These three sources can increase the likelihood that societies are able to deal with diverse risks and are able to peacefully adapt to them. Lastly, external actors seeking to foster resilience need to factor in long-time horizons, in-depth local knowledge, and a clearly designed strategy. Assessing the EU's resilience-building strategies with these criteria, it becomes evident that the EU has a mixed record of success.

The project developed innovative quantitative and qualitative empirical methods for risk-scanning, foresight and forecasting. This included large-scale statistical prediction of conflict as well as development of in-depth qualitative risk scenarios. EU-LISTCO identified six risk clusters: (1) geopolitical rivalry and risks of major armed conflict; (2) unconventional security risks; (3) biological and environmental risks; (4) demography and uncontrolled migration; (5) global financial and other systemic economic risks, and; (6) technology-driven disruption.

The project also studied the EU and select member states' preparedness in anticipating, preventing, and responding to threats of violent conflict and governance breakdown in these countries and evaluated the resilience-building record of their policies. It found that the objective of fostering resilience has been successfully integrated at the level of policy goals and discourse.

The result of the project is new methods of analysis and practical policy guidance. Effectiveness of such policies, should be based on further empirical studies.

## 5.2 CRITICAL NEED NO.2: DIGITAL ESCALATION AND AI-BASED EXPLOITATION

### DEFINITION OF THE RESEARCH AREA

An arms race for dominance in the AI area is ongoing between the dominant high-tech nations. AI is a general-purpose technology which assists in strategic decision-making, in control of critical infrastructures, and almost many other technologically advanced solutions. AI is thus also a key technology in the security and defense sectors where it is of the utmost importance to strengthen cyber defense and enhance attack capabilities. However, AI based systems may be vulnerable to attacks targeting the core AI functionality. Thus, to become a

fully reliable and trusted technology AI must be designed for robustness and resilience against targeted manipulations and attacks.

In his research scan two main aspects are investigated:

- Using AI to detect and respond to cyber security attacks. Here the focus is on using AI for network intrusion detection.
- How to protect AI systems themselves from attacks. Here one area is on attacks using specially crafted input data to corrupt the outcome of AI based analysis and decision-making algorithms. Another area is to understand how AI algorithms can be "hacked" to yield results that are advantageous to the attacker.

### CONTEXT

Following the European Commission's High-Level Expert Group on Artificial Intelligence[45] in defining the AI area it is

> *a scientific discipline includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)*.

AI is a general-purpose technology and is used in strategic decision-making, control of critical infrastructures, and in wide range of other technologically advanced solution. Furthermore, AI is a key technology in the security and defense sectors. Here AI is used to strengthen cyber defense capabilities as well as enhance attack proficiency. However, AI based systems are also vulnerable to attacks targeting the core AI functionality. With proliferation of AI technologies in daily use and in critical infrastructures, risks of hybrid attacks significantly rise.

Thus, to become a fully trusted technology, AI must be designed for robustness and resilience against attacks and manipulations and to be scoped according to the context of the threat landscape.

Research activities in the AI area are abundant in core technologies of AI, in the practical and theoretical application of AI in most technologically advanced countries. An arms race for dominance in the AI area is ongoing between the dominant high-tech nations (US, China and Russia).

### PROJECTS

In the EU, there is a few ongoing networking and coordination activities in the AI area. The European Commission has presented both a proposal for a regulatory framework on AI[46], a (revised) coordination plan on AI[47] and a proposal for a regulation on artificial intelligence[48]. Objectives are to reduce fragmentation in efforts and develop excellence and trust in AI technologies and their application. A public private partnership project, *the AI, Data and Robotics Partnership*[49], has been formed and has published a Strategic Research, Innovation

[45] https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf
[46] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence
[47] https://digital-strategy.ec.europa.eu/en/library/new-coordinated-plan-artificial-intelligence
[48] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence
[49] https://ai-data-robotics-partnership.eu/

and Deployment Agenda[50] which is "*committed to the development of a rich AI, Data and Robotics innovation ecosystem in Europe that is built around a strong skills pipeline, excellent research and effective regulation and standards coupled to best practice in each sector*". The partnership members are different organizations which cover a broad spectrum of users, researchers and organisations. Another community covering AI is the European AI-on-demand platform (AI4EU)[51] which *seeks to bring together the AI community while promoting European values.* The platform's objective is to be a facilitator of knowledge transfer from research to different business domains.

The number of European projects in the AI area is very impressing and a list of recent EU financed projects is maintained by e.g., AI4EU[52]. Another view of the research field can be obtained in the aggregation of AI related calls in Horizon Europe WP 2021-2022[53] by MLIS at the Technion. The calls are presented by following clusters:

- Research Infrastructures;
- Health;
- Culture, creativity and inclusive society;
- Civil Security for Society;
- Digital, Industry and Space;
- Climate, Energy and Mobility;
- Food, Bioeconomy, Natural Resources, Agriculture and Environment; and finally
- Widening participation and strengthening the European Research Area.

The European Defence Fund (EDF) has for some years actively tried to coordinate and drive joint work in the area of AI. The work and the approach are summarized in the news item *Artificial Intelligence: Joint quest for future defence applications*[54]. We also note that the European Defence Fund (EDF) has issued two calls for AI in defence applications. The first call is on Cyber threat intelligence and improved cyber operational capabilities (EDF-2021-CYBER-R)[55] on the topic of Improving cyber defence and incident management with artificial intelligence and the second call is on Artificial intelligence (EDF-2021-DIGIT-R)[56] on the topic of Frugal learning for rapid adaptation of AI systems. These two calls shows that AI is becoming more important in defence applications and the general picture of the AI activities is that the EU targets most aspects of the AI area and invests substantial resources in AI developments.

**AI and security**

When it comes to the efforts of securing AI solutions and the use of AI to secure critical societal functions and in defense applications the picture gets a bit more blurred. The top-level documents do not bring these issues to their front page although trust in AI solutions and explainable AI are mentioned as very important aspects.

[50] https://ai-data-robotics-partnership.eu/wp-content/uploads/2020/09/AI-Data-Robotics-Partnership-SRIDA-V3.0.pdf
[51] https://www.ai4europe.eu/
[52] https://www.ai4europe.eu/ai-community/projects
[53] https://mlis.technion.ac.il/wp-content/uploads/2021/06/HE_All_AI_21-22.pdf
[54] https://eda.europa.eu/news-and-events/news/2020/08/25/artificial-intelligence-joint-quest-for-future-defence-applications#
[55] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2021-cyber-r-cdai
[56] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2021-digit-r-fl

However, ENISA is active in security for AI and has recently published a report on Securing Machine Learning Algorithms[57]. The report provides:

> *… a taxonomy for machine learning algorithms, highlighting core functionalities and critical stages. The report also presents a detailed analysis of threats targeting machine learning systems. Identified threats include inter alia, data poisoning, adversarial attacks and data exfiltration. Finally, the report proposes concrete and actionable security controls described in relevant literature and security frameworks and standards.*

Another recently published report by ENISA is AI Cybersecurity Challenges[58]. The report presents:

> *… the Agency's active mapping of the AI cybersecurity ecosystem and its Threat Landscape, realized with the support of the Ad-Hoc Working Group on Artificial Intelligence Cybersecurity. The ENISA AI Threat Landscape not only lays the foundation for upcoming cybersecurity policy initiatives and technical guidelines, but also stresses relevant challenges. One area of particular significance is that of the supply chain related to AI and accordingly it is important to highlight the need for an EU ecosystem for secure and trustworthy AI, including all elements of the AI supply chain. The EU secure AI ecosystem should place cybersecurity and data protection at the forefront and foster relevant innovation, capacity-building, awareness raising and research and development initiatives.*

From the report on AI Cyber security challenges, we quote the description of the multi-dimensional relationship between Artificial Intelligence and cybersecurity:

1. ***Cybersecurity for AI:*** *lack of robustness and the vulnerabilities of AI models and algorithms, e.g. adversarial model inference and manipulation, attacks against AI-powered cyber-physical systems, manipulation of data used in AI systems, exploitation of computing infrastructure used to power AI systems' functionalities, data poisoning, environment variations which cause variations in the intrinsic nature of the data, credible and reliable training datasets, algorithmic validation/verification (including the integrity of the software supply chain), validation of training and performance evaluation processes, credible and reliable feature identification, data protection/privacy in the context of AI systems, etc.*
2. ***AI to support cybersecurity:*** *AI used as a tool/means to create advanced cybersecurity by developing more effective security controls (e.g. active firewalls, smart antivirus, automated CTI (cyber threat intelligence) operations, AI fuzzing, smart forensics, email scanning, adaptive sandboxing, automated malware analysis, automated cyber defence, etc.) and to facilitate the efforts of the law enforcement and other public authorities to better respond to cybercrime, including the analysis of the exponential growth of Big Data in the context of investigations, as well as the criminal misuse of AI.*
3. ***Malicious use of AI:*** *malicious/adversarial use of AI to create more sophisticated types of attacks, e.g., AI powered malware, advanced social engineering, AI-powered fake social media accounts farming, AI-augmented DDoS attacks, deep generative models to create fake data, AI-supported password cracking, etc. This category includes both AI-targeted attacks (focused on subverting existing AI*

[57] https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms/@@download/fullReport
[58] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges/@@download/fullReport

*systems in order to alter their capabilities), as well as AI-supported attacks (those that include AI-based techniques aimed at improving the efficacy of traditional attacks).*

Guidance on required research can be obtained from the strategic research agendas published by ECSO, the contractual Public Private Partnership projects, and the two EU projects **Concordia** and **Sparta** that are pilots for the establishment of a European Cybersecurity Competence Network and the development a common European Cybersecurity Research & Innovation Roadmap. ECSO, in its Input to the Horizon Europe Programme 2021-2027[59], the section on Basic and Disruptive Technologies: Secure and Trustworthy Artificial Intelligences points out a number of desired developments in the AI security area. In the section on Artificial Intelligence techniques for better security and malicious use of AI research areas mentioned to develop desired abilities are:

- Machine Learning for cybersecurity
- Large-scale, robust threat- and anomaly detection on highly heterogenous and incomplete data to create situational awareness.
- Predictive security and (semi-)autonomous incident mitigation to support active incident response strategies.
- Protect additional attack surface created by new and emerging technologies for interacting with IT Systems.
- Understand and anticipate possible malicious use of artificial intelligence.

In **Concordia'**s Roadmap for Research and Innovation[60] special focus is on Adversarial Artificial Intelligence Attacks and Countermeasures. In the **SPARTA** roadmap for Secure and Fair AI Systems for Citizen[61] the research goals are given as

- Enhanced explainability and better threat understanding in AI context
- Systems using AI more reliable and resilient
- More effective methods and tools for analysis of security threats for AI systems
- A set of techniques and solutions for AI systems protection
- Systems in place to ensure fairness of AI systems
- Defensive and reactive mechanisms geared towards novel cybersecurity threats
- Cybersecurity systems being able to detect stegomalware[62]

As a final observation we note that very recent results in the paper Planting Undetectable Backdoors in Machine Learning Models[63] show that there is a theoretical roadblock to show the non-existence backdoors and thus to certify adversarial robustness. This means that trust in and certification of AI solutions will almost certainly have to be based on a trusted supply chain of solution components and that the components have to be developed using secure software development procedures and tools.

**Observations**

[59] https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf

[60] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-04-Reseach-and-Innovation.pdf

[61] https://www.sparta.eu/roadmap/#timeline

[62] Stegomalware is a type of malware that uses steganography to hinder detection. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, video or network traffic. This type of malware operates by building a steganographic system to hide malicious data within its resources and then extracts and executes them dynamically. It is considered one of the most sophisticated and stealthy ways of obfuscation. https://en.wikipedia.org/wiki/Stegomalware

[63] https://arxiv.org/abs/2204.06974

The AI area is vast and is applied in a large variety of applications, both for good and for malicious purposes, in civil and defence applications. The threats to AI solutions, including cyber security threats are also well understood and studied in many projects.

Within the EU a large number of initiatives have been launched to coordinate, steer and regulate the AI-area. The number of ongoing AI related projects is huge and there are significant efforts invested in AI and cybersecurity. The defence sectors are also involved although it is less open with exactly what its activities are and how they are performed.

From a hybrid threat perspective, the main missing part is an overarching and detailed view of the role AI in hybrid threat countermeasures and mediation. There is also a need to establish a knowledge base on which features AI solutions need to exhibit to make them trusted and secure.

## 5.3 CRITICAL NEED NO.3: RISE OF POPULISM

### DEFINITION OF THE RESEARCH AREA

Populism can be viewed from many angles and interpreted in wildly diverse ways.

We see populism as a divisionary political stance confronting popular sentiment against “elite” or “experts”. Usually this is fueled by the popular feeling that a large part of the population is not represented, their needs are not understood, that there is systematic effort to suppress this part of society.

Part of rise of populism is attributed to nature of current internet/social media, which is increasingly more governed by AI and ever more sophisticated and non-transparent algorithms. It is recognized that the way the news is filtered and presented to the reader has significant potential to influence his/her views, emotional state etc. “Information bubbles” describing this phenomenon became a term of daily use.

There is a need to openly discuss philosophy, logic, and consequences of news filtering/personalization.

### PROJECTS

We searched projects from the Cordis database and selected the following projects for further analysis.

**Profiling and targeting news readers – implications for the democratic role of the digital media, user rights and public information policy** (**PersoNews**)[64] project that 1 August 2015 and ended 31 May 2021 with Grant agreement ID: 638514.

PersoNews project strikes at the core of the discussed issue. It focuses on “recommender systems” – how social media and other platforms algorithms from abundance of material select what will be shown (“recommended” to a particular reader).

Project extensively discusses dynamics of news consumption and news supply. Seemingly “cold blooded” algorithms, which maximize “clicks” of readers and advertisement potential, have far ranging consequences for the readers, their attitudes, actions, and societies.

[64] https://cordis.europa.eu/article/id/434332-algorithms-are-reshaping-our-newsreading-habits-should-we-worry

Project's publications "On the Democratic Role of News Recommenders" [65] consolidates ideas around the ultimate question "how would news recommenders need to be designed to advance values and goals that we consider essential in a democratic society?"

Project work initiated further projects into recommender models.

The project itself focuses on the impact of various recommender models, while not paying specific attention to the aspects of exploitation of them by adversary parties.

EU-HYBNET's should get deeply involved with the recommender models projects and strive to add hybrid threats dimension to them. It might be valuable for readers to transparently know what recommender models are employed on specific platforms, so that they are aware of the content filtering practices.

No specific technologies were developed during this project, as algorithms will remain proprietary technologies of the platforms.

**Collaborative AI Counters Hate (AI4Dignity)** [66] project that started 1 January 2021 and ends on 30 June 2022 with Grant agreement ID: 957442.

The European Commission launched the Code of Conduct in 2016 to respond to the proliferation of hate speech online. AI4Dignity aims to investigate the applicability of artificial intelligence (AI) for hate speech identification in various cultural environments.

While AI can be used to detect (and in turn to decelerate and remove online hate speech), this hinges on the quality, scope, and inclusivity of training data sets. Language barriers and cultural contexts are important, so simple keyword search algorithms either are insensitive, or hit too many false positive results, thus creating systematic bias.

The AI4Dignity aims to merge capabilities of AI technologies with strong human interaction, using community-based classification approach with fact checkers. Project recognizes the necessity for developing procedural guidelines and frameworks.

This is an exceedingly small project working on overly complex "supply side" of internet technologies, where more attention is needed.

[65] https://www.tandfonline.com/doi/full/10.1080/21670811.2019.1623700

[66] https://cordis.europa.eu/project/id/957442

# 6. OBSERVATIONS AND CONCLUSIONS

EU-HYBNET T3.3 "Ongoing Research Projects Initiatives Watch" in the scope of research project and innovation scan completed its first iteration and produced this document, a deliverable D3.8, focusing on the EU Funded projects scan.

We find it relevant to note that EU is dedicating significant resources to research, producing technologies and innovations for a wide spectrum of theoretical and practical issues. All research topics identified in EU-HYBNET D2.10 "Deeper analysis, delivery of short list of gaps and needs" document did produce relevant hits, so even relatively new subjects such as "Hybrid threats" is significantly covered by EU funded research efforts from variety of angles.

Notably, we found AI research area with abundance of the research, development of technologies, methodologies etc. Still, impact of AI vulnerabilities is discussed and researched mostly from purely technological angle. There is no discussion on scale and potential to impact perceptions of population and trust fabric of society, which is a subject of deliberations of hybrid threats community.

Combined area of AI and hybrid threats needs to be better defined, have its objectives set, be coordinated, develop guides on required additional research efforts, and build networks among practitioners and institutions across AI professional network and hybrid threats community.

Researching defined subject areas, we found that several EU funded projects are relevant to the topics of even different EU-HYBNET Project Core Themes. Various aspects of the project may be relevant in the analysis of different Project Core Themes. This we attribute to the very fact, that hybrid threats are multidimensional, crossing boundaries of subject matter perimeters that there is significant interconnectedness between various research areas. For further iteration of scanning, it is advisable to make Gaps and Needs areas much more focused on more specific needs of pan-European security practitioners.

The scanning team analyzed scientific research landscape for the D2.10/gaps and needs identified by practitioners in hybrid threats field. We hope that this document will contribute to deeper understanding of the hybrid threats community of the state of play of the research on the phenomena of interest, and what outcomes could be expected from the scientific research field. Not less importantly, document identified areas, which apparently lack research of the phenomena, which is deeply important for hybrid threats better understanding.

The scanning task proved to be challenging. Gaps and needs, identified by practitioners in EU-HYBNET D2.10. "Deeper Analysis, Delivery of Short List of Gaps and Needs" covered extremely wide areas and interconnected phenomena, thus required significant operationalization effort from T3.3 team.

We find it very relevant to initiate discussion for the next iteration to ensure sharper focus of inputs for the scanning, which would make T3.3 efforts more productive and useful for EU-HYBNET.

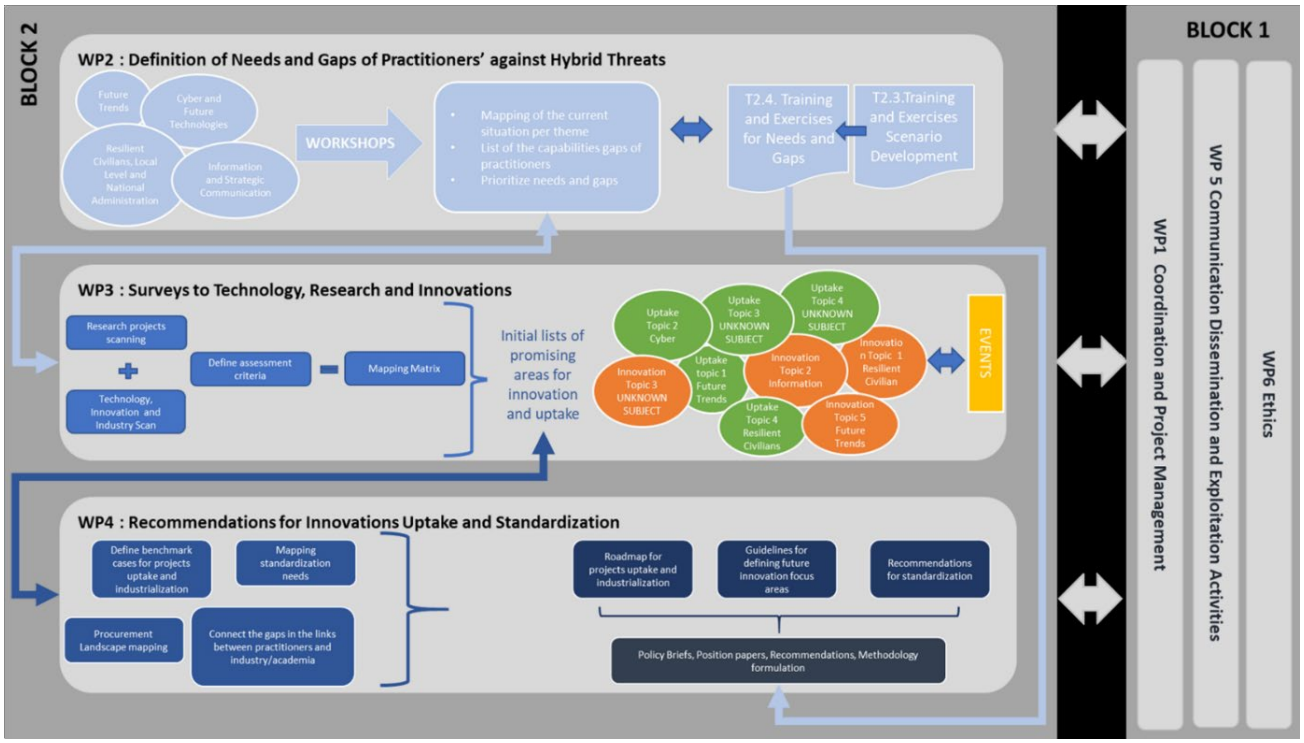
## 6.1 FUTURE WORK

The EU-HYBNET deliverable D3.8 "*Second Mid-Term Report on Innovation and Research Monitoring*" is a part of and Work Package WP3 "*Surveys to Technology, Research and Innovations*"/ Task T3.3 "*Ongoing Research Projects Initiatives Watch*".

Present document (D3.8) has key role to feed information to T3.1 "*Definition of Target Areas for Improvements and Innovations"* and WP2 "*Gaps and Needs of European Actors against Hybrid Threats*"/ T2.3 "*Training and Exercises Scenario Development*" and T2.4 "*Training and Exercises for Needs and Gaps*".

D3.9 will deliver material for T3.1 to aggregate work of several scanning deliverables with the aim to analyze what could the most promising research directions and sound innovations addressing identified EU-HYBNET gaps and needs of pan-European practitioners.

Relationships between EU-HYBNET workpackages and tasks are highlighted in the project WP interdependency picture below:




D3.8 will be instrumental for EU-HYBNET and wider hybrid threats community to better understanding state of play of the fields identified by practitioners regarding the EU funded and thus readily available research. This, we hope will spur better collaboration between projects and exploitations of their results.

The D3.8 has also importance to deliver results to the EU-HYBNET project objective (OB) 3. and its goals and key performance indicators (KPI) as described in DoA Part B, chapter 1.1.

The objective OB.3 to which task T3.3 and deliverable D3.8 provides results is following:

| **OB3: To monitor developments in research and innovation activities as applied to hybrid threats** | | | |
|---|---|---|---|
| **Goal** | | **KPI description** | **KPI target value** |
| 3.1 | To monitor significant developments in research areas and activities in order to define and recommend solutions for European actors | Monitor research initiatives addressing EU actors gaps and needs in relation to knowledge/performance | At least 4 reports every 18 months will be delivered that outline findings from productive research efforts |

## ANNEX I. GLOSSARY AND ACRONYMS

| Term | Definition / Description |
|---|---|
| **AI** | Artificial intelligence |
| **APT** | Advanced persistent threats |
| **BRI** | Belt and Road Initiative-countries |
| **CCE** | Common Configuration Enumeration |
| **CEPS** | Centre for European Policy Studies |
| **CI** | Critical infrastructure(s) |
| **CIS** | Centre for Internet Security |
| **CPS** | Cyber-Physical Systems |
| **CVE** | Common Vulnerabilities and Exposures |
| **CVSS** | Common Vulnerability Scoring System |
| **DoA** | Description of Action of EU-HYBNET |
| **EC** | European Commission |
| **EU** | European Union |
| **EU-HYBNET** | A Pan-European Network to Counter Hybrid Threats project |
| **FDI** | foreign direct investment |
| **FDI RRI** | Foreign Direct Investment Regulatory Restrictiveness Index |
| **FLOSS** | Free and open-source software platform |
| **GDPR** | General Data Protection Regulation |
| **IFCN** | International Fact-Checking Network |
| **IMMERSE** | Integration of Migrants Matcher Service |
| **JRC** | Joint Research Center |
| **KEMEA** | Kentro Meleton Asfaleias |
| **KPI** | Key Performance Indicator |
| **KRSC** | Key Resources Supply Chains |
| **L3CE** | Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras |
| **LAUREA** | Laurea-Ammattikorkeakoulu Oy |
| **MANET** | Mobile Ad-Hoc Networks |
| **ML** | Machine Learning |
| **MS** | Milestone |
| **NAAS** | National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena |
| **NCSC** | National Cyber Security Centrum |
| **OECD** | Organisation for Economic Co-operation and Development |
| **PMT** | Political Micro-Targeting |
| **PPHS** | Polish Platform for Homeland Security |
| **PPP** | Public Private Partnership |

| Term | Definition / Description |
|---|---|
| **RISE** | RISE Research Institutes of Sweden Ab |
| **RTO** | Research & Technology Organization |
| **SCRM** | Supply chain risk management |
| **Hybrid CoE** | The European Centre of Excellence for Countering Hybrid Threats |
| **UniBW** | Universtät der Bundeswehr München |
| **WSN** | Wireless Sensor Networks |