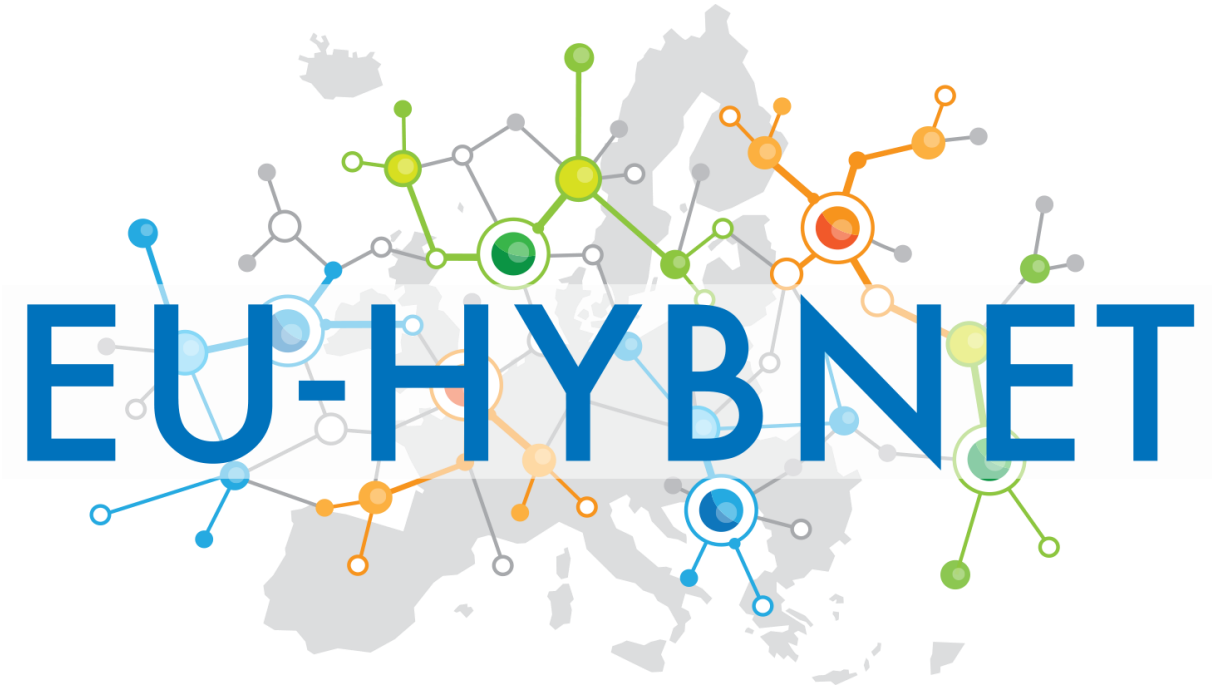


FIRST REPORT ON INNOVATION AND RESEARCH PROJECT MONITORING

Lead Author: L3CE

Contributors: Laurea, PPHS, RISE, KEMEA, COMTESSA, TNO, Hybrid CoE

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

D3.7 FIRST REPORT ON INNOVATION AND RESERCH PROJECT MONITORING

Task number	T3.3	
Deliverable number	D3.7	
Version:	2.2	
Delivery date:	16/12/2020	
Dissemination level:	Public (PU)	
Classification level:	Public	
Status	Ready	
Nature:	Report	
Main authors:	Rimantas Zylius	L3CE
Contributors:	Päivi Mattila, Matti Kropsu, Isto Mattila, Tuomas Tammilehto	LAU
	Steven Ormston	PPHS
	Rolf Blom	RISE
	Maria Kampa	KEMEA
	Son Pham	COMTESSA
	Evaldas Bruze, Edmundas Piesarskas	L3CE
	Hanna Smith	Hybrid CoE

DOCUMENT CONTROL

Version	Date	Authors	Changes
0	14-11-2020	L3CE/ Rimantas Zylius	Table of Contents, structure of the document, descriptions of gaps&needs
0.1	17-11-2020	L3CE/ Rimantas Zylius, Evaldas Bruze, Edmundas Piesarskas	Added scan results of 3.1 and 4.3
0.2	20-11-2020	L3CE/ Rimantas Zylius; Evaldas Bruze, Edmundas Piesarskas	Added scan results for 2.1
0.9	4-12-2020	RISE/ Rolf Blom COMTESSA/ Son Pham KEMEA/ Maria Kampa PPHS/ Steven Ormston Laurea/ Matti Kropsu, Isto Mattila, Päivi Mattila	Added all the sections
1.0	7-12-2020	L3CE/ Rimantas Zylius	Version for review prepared
1.1	9-12-2020	TNO/ Rick Meessen	Review
1.2	10-12-2020	Laurea/ Päivi Mattila	Review and text editing
1.3	10-12-2020	L3CE/ Rimantas Zylius	Text editing and document for submission
1.4	12-12-2020	Laurea/ Päivi Mattila	Final review
1.4	14-12-2020	Hybrid CoE /Hanna Smith	Final review
2	16-12-2020	L3CE/ Rimantas Zylius	Preparation of final version
2.1	17-12-2020	Laurea/ Päivi Mattila, Isto Mattila, Tuomas Tammilehto	Final version review
2.2	17-12-2020	Laurea/ Päivi Mattila	Submitted document

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

1.1 OVERVIEW

DEFINITION OF THE DELIVERABLE IN DESCRIPTION OF ACTION

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) 3.7. "*First Report on Innovation and Research Project Monitoring*" as part of EU-HYBNET Task 3.3 *"Ongoing Research Projects Initiatives Watch*" follows:

DoA Part A document/ Chapter 1.3.3 defines T3.3 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. ~~T3.2.~~ (T3.3) contributes strongly to the GM-01 call medium term impact Nr1 and Nr2. In ~~T3.2~~ (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

SCOPE OF THE DOCUMENT

Further definitions of Research and Innovation are described as well as how they will be used for production of this deliverable.

RESEARCH

For the purposes of EU-HYBNET, the Task 3.3 team focused solely on the Scientific Research subset of works, as discussed above. That is, scientific research aims at discovery and/or analysis of the hybrid threats, their features, working mechanisms, vulnerabilities, countermeasures on various societal, psychological, sociological and technological factors, and their interactions. As there is very limited body of specifically to hybrid threats targeted research, the task looked into broader area, including phenomena relevant to hybrid threat.

With reference to the scientific research principles above EU-HYBNET will prioritize European Union (EU) funded projects where the deliverables, i.e. research findings are approved by the Commission and research articles and journals that include peer review.

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

The publications or the research to be included in the Watch was preferably be peer reviewed.

INNOVATION

During discussion at work package level WP3 and further ones in the Scientific Advisory Group of the EU-HYBNET, the consensus was emerged, that Task T3.3 may include in its scope innovations review, which are developed in the European research projects.

T3.3 research projects Watch includes both technological and non-technological innovations (most likely organizational and social innovations) which are analyzed or developed in research projects and have relevance to the „gaps and needs"[1] list. Priority will be given to projects funded by EU (priority list is provided in DoA Part B/ chapter 1.3). The list is in ANNEX 3.

All references to technological innovations encountered during the task execution was forwarded for analysis to EU-HYBNET T3.2 "*Technology and Innovations Watch*".

OBJECTIVES OF THE DELIVERABLE

This deliverable (D) consolidates results of the scan of Innovations and Research (as described in the chapter "Scope of the Document") from the relevant sources, aiming to discuss underlying phenomena, state-of-play, and early stages innovative solutions to the gaps and needs identified in EU-HYBNET deliverable D2.9 "*Deeper analysis, delivery of short list of gaps and needs* ".

Specifically, scan of scientific research sources will try to define the state of play of the relevant field, describe efforts and the state of the relevant phenomena/technology research, as well as identified problems which are discussed in research community.

Innovation scan will 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 T3.2. "*Technology and Innovations Watch*".

As projects and their solutions refer to variety of areas and address several gaps, it was logical to list them in separate section (Section 6).

1.3 STRUCTURE OF THE DELIVERABLE

This document described 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

[1] EU-HYBNET deliverable D2.9 "Deeper Analysis, Delivery of Short List of Gaps and Needs" (due in M5/ September 2020)

- Section 5: Core Theme: Future Trends of Hybrid Threats
- Section 6: Identified Innovations in EU Research Projects
- Section 7: Conclusions

1.4 METHODOLOGY

Scientific scan was carried out without advanced forms of automation, using "brute force" method of manual research and analysis by experts of the contributing partners. This was a conscious choice hoping to gather most first -hand experience, produce feedback and consider introduction of automation in the next iteration.

Most of the researchers used Harzing Publish or Perish tool for scientific search.

https://harzing.com/resources/publish-or-perish/windows#:~:text=%20Publish%20or%20Perish%20on%20Microsoft%20Windows%20,instructions.%20Start%20the%20PoP7Setup.exe%20installer%20by...%20More%20

SOURCES

Following scan sources are available free of charge (registration may be needed):

- Google Scholar
- PubMed
- Microsoft Academic
- Scopus
- Crossref

SEARCHING

General process consisted of several steps:

1. Operationalization of the Context-gaps-needs text into relevant and searchable keywords. The gaps and needs are deriving from WP2 Task2.2 "*Research to Support Increase of Knowledge and Performance*" D2.9 "*Deeper analysis, delivery of short list of gaps and needs*" that analyzed and listed EU-HYBNET consortium partners and network members main gaps and needs of pan-European practitioners and other relevant actors to counter hybrid threats. D2.9 is defined as "consortium only" not "public" deliverable.
2. The D2.9 description keywords were then used to investigate the research field and calibrate selection of the keywords.
3. Preliminary investigation allowed to develop a concept of the field and define a structure of the specific gaps and needs in deliverable 3.7.
   Note: initially we hoped to have common deliverable structure for all gaps & needs.
   a. Availability of tools (concepts, methods or technological tools) fitting the gap.
   b. Applicability of the tools for new developments
   c. Applicability of tools for legacy structures

   However, in the process of practical analysis we discovered, that some more technical gaps & needs quite finely fall into the predefined structure, while other identified gaps & needs are of a more political / philosophical nature and require their own structuring. Thus, it was decided, that every gap & need analyst would be designing an own structure of analysis.

4. Deep analysis of the research articles is performed afterwards, according to the structure of the deliverable 3.7 and identified keywords sets.

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

2.1 PRIMARY CONTEXT NO.1: DISTRUST AND STRESS IN POLITICAL DECISION-MAKING

The trust in democratic processes and democratic institutions, their efficiency and values are of paramount importance. The gap opens as the traditional social dialogue and communication channels lose their importance, perceptions of population changes.

Need for concepts and solutions to build and sustain trust between institutions and population is identified. It includes changes in habits and processes of participative expression, communication, policy consultations, social dialogue, etc., that would result in increased trust to decision making processes and feeling of decision ownership.

To gather and maintain shared up-to-date situational awareness during the intense periods of crises. To use sensors, platforms, communication channels and system of their aggregation, which enables profiled views to different actors. To standardize exchange of information, common taxonomies and interoperability of technological systems for information sharing and intelligence fusion in a timely manner across all involved partners, considering different nature of crises.

SCANNING RESULTS: DISTRUST AND STRESS IN POLITICAL DECISION-MAKING

ANALYSIS OF KEYWORDS

Initial analysis and structuring of the context-gaps-needs, resulting in the following hierarchical key components for the scan:

“Distrust and stress in political decision-making”

- Social Dialogue and consensus
  - Social dialogue and consensus platforms
  - Habits change
  - New governance models
- Shared and updated situational awareness
  - Sensors and data sources
  - Platforms and communication channels
  - Comprehensive security agencies models
    - Information exchange methods
    - Awareness information exchange platforms
    - Common taxonomies
    - Interoperability of technological systems

AVAILABILITY OF TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

Analysis of the multiple sources revealed that there are several production level developments in the areas related to “Shared and updated situational awareness”. Originated from the military domain, Situation Awareness is proposed with the aim to obtain information superiority through information fusion and thus to achieve decision superiority. It requires not just the perception of the environment, but also the reasoning of the implicit or implicated meaning under the explicit phenomenon. Current research is mostly coming from the areas

of cybercrimes investigation and cyber security. It stands well developed and widely used by different stakeholders' groups.

Methodological part has been strongly progressing during last 5-7 years mostly adopting concepts and methods from defense industry for tackling hybrid operations as well as comprehensive situational awareness and covers such aspects as:

- Formation of awareness process (Massimiliano Albanese and Sushil Jajodia)
- Kinetic and cyber integrated analysis (Alexander Kott , Norbou Buchler , and Kristin E. Schaefer)
- Network-Wide Awareness Development (Nicholas Evancich , Zhuo Lu , Jason Li , Yi Cheng , Joshua Tuttle , and Peng Xie)
- Cognition and Technology (Cleotilde Gonzalez , Noam Ben-Asher , Alessandro Oltramari , and Christian Lebiere)
- Cognitive Process and decision-making process (John Yen , Robert F. Erbacher , Chen Zhong , and Peng Liu)
- Visualization Analytics application in comprehensive situational awareness (Christopher G. Healey , Lihua Hao , and Steve E. Hutchinson)
- Inference and ontologies (Brian E. Ulicny , Jakub J. Moskal , Mieczyslaw M. Kokar , Keith Abe , and John Kei Smith)
- Learning and Semantics (Richard Harang)
- Impact Assessment (Jared Holsopple , Moises Sudit , and Shanchieh Jay Yang)

The area of shared situational awareness is considerably well researched and standardization bodies have entered into the process of standardization of methods and platforms internationally. Successful standardization would make these widely available and would hugely encourage their use. To mention a few recent ongoing developments: SPARTA Pilot project on comprehensive cybersecurity threat prediction.

As shown in the Report "Landscape of Hybrid Threats: A conceptual model" the actor seeks to undermine the target state's capability to develop and maintain situational awareness[2]. Situational awareness is vital for effective detection, countering, and deterrence of hybrid threats particularly for a reason that hybrid threats aim at creating ambiguity, blurring situational awareness and hindering decision-making capabilities at the political level, the ability of public administration to implement policy and at the level of strategic and operational planners.

In "Joint Framework on countering hybrid threats a European Union response"[3] key principles of comprehensive situation awareness were defined. It unites all stakeholder groups representative for joint integrated process and output.

OBSERVATION

Review of the scientific publications and research projects revealed that the field of Governmental trust building, and situational awareness is rather active and productive, but rather fragmented. This finding is highly important, since it show, despite of active level of work in the field of research a clear weakness when it comes to Hybrid Threats. The scientific publications and research projects most of it focus on the certain aspects of it, mainly:

[2] Giannopoulos, G., Smith, H., Theocharidou, M., *The Landscape of Hybrid Threats: A conceptual model*, European Commission, Ispra, 2020, PUBSY No. 117280

[3] *Brussels, 6.4.2016 JOIN(2016) 18 final,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

- General concept of situational awareness, coming from cyber security, and how it can be applied countering wider threats spectrum (directly applicable to hybrid threats).
- Integration of kinetic and cyber environments to improve situational awareness.
- Visual analytics as an instrument to provide comprehensive situational description.
- Teamwork using safe environment to generate unified situational awareness

The least developed part relates to methodological part while addressing recent societal issues, trust building and dynamics of events handling, while it is one of the important subjects identified in gaps & needs short list.

APPLICABILITY OF THE TOOLS FOR SOCIAL DIALOGUE AND CONSENSUS

Review of research articles indicated that the "Social dialogue and consensus" part of the Gap is less explored by different researchers. There are two main aspects to be considered.

Firstly, we find certain attempts to analyze application of social media, mainly in mass emergency events, specifically as a tool for communication and engagement.

Another aspect - environment for social dialog, is less encountered as a research subject. It might be due to the nature of the phenomenon. It seems that "social dialog" is considered more as the policy initiative or a subject of practical success or failure, rather than the object of scientific research. Therefore, most encountered accounts are instrumental, describing scattered initiatives of countries, regions or towns. These are some examples of such activities and different initiatives that can be found around Europe. They vary from rather long-standing history of Switzerland, involving citizens through numerous referendums, to utilization of new possibilities, provided by technologies, such as OpenStand in Amsterdam. Estonia developed electronic platform which enables national internet voting. There are arguments that such technologies are more inclusive than traditional voting, but we did not encounter accounts describing of usage of this platform for more widespread social dialogue.

Even though found accounts lack evidence-based evaluation of their efficiency and effects on society, they might provide insights for further research.

FLOSS (Free and open-source software platform) enabled solutions is one of the areas for discussions and further investigation. They provide centralized/mutual structure for collaboration instead of several collaborative subdivisions. Wider discussion on application of this solution in the area of social dialog and inclusion of society and / or certain groups of society can be found in 15th IFIP WG 2.13 International Conference[4], materials. Those include articles on application of Free Software Platform for Social Participation, Open Source Software Community Inclusion Initiatives to Support Women Participation and other relevant topics.

OBSERVATION

After reviewing over a thousand publications on societal dialogue and consensus, we gather that there is a clear lack of up-to-date concepts, methods and tools with clear guidance and recommendations for regulations, which would serve as a role model for constructive and trust-by-design social dialogue between government and general public leading towards inclusion and consensus.

It can be concluded, that trust building, societal dialogue and consensus building are primary focus areas for further research of phenomena and provision of methods and tools. Citizen involvement tools, such as using FLOSS can be evaluated in more detailed as a provider of new opportunities. Further analysis, benchmarking and

[4] *https://link.springer.com/chapter/10.1007%2F978-3-030-20883-7_3*

evaluation of different initiatives could be useful to understand the efficiency and impact they provide, or challenges they face.

Facilities and processes for multi stakeholder situational awareness, and well-informed, protected from adversary interferences and unified decision making is well advanced and gains significant attention in research and implementation domains.

2.2 PRIMARY CONTEXT NO.2: RELIANCE ON CRITICAL SERVICES AND TECHNOLOGICAL SYSTEMS

In this area, a need is identified to secure supply of critical goods (maybe minimal, albeit sufficient), ensuring availability of critical services and functions. The scope of this need may constitute ways of identification and assessing criticality, assessing resiliency of supply chains, evaluating minimum satisfactory levels of performance, communication platforms, possible PPP or private sector involvement, etc.

SCANNING RESULTS: RELIANCE ON CRITICAL SERVICES AND TECHNOLOGICAL SYSTEMS

Disruption; supply chains and movement of goods and services

Finding 1.1 Technical: Technical systems are aging. Resilience is weak due to outdated data protection. Non-applicable tools for end users.

Finding 1.2 Non-technical: Supply chain risk management.

Distrust (fear) – critical; infrastructure and service and goods

Finding 2.1 Technical: Trust is the key ingredient for sustainable transactions, especially in E-Commerce. The buyer must be able to trust that his purchase will be as agreed. Ensuring network connectivity and the reliability of the supplier of the goods or services is difficult.

Finding 2.2 Non-technical: Educating buyers and exposing unreliable suppliers of goods.

Disruption - critical; infrastructure and service and goods

Finding 3.1: One of the most important critical infrastructures is the information system network. After a disruption, it is important that the network recovers as quickly as possible.

Finding 3.2: The quality of decision making is an important factor in the management of these entities. Critical infrastructure entities aim to provide services necessary to ensure state security and satisfy basic human needs. The quality level is determined by many factors, the key of which are risk management and decision-making process.

AVAILABILITY OF TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

OBSERVATIONS

Observation; Finding 1.1. Cyber-Physical Systems (CPS) represent a fundamental link between information technology (IT) systems and the devices that control industrial production and maintain critical infrastructure services that support our modern world.

This paper reviews the challenges of providing information assurance services for CPS that operate critical infrastructure systems and industrial control systems. These methods are thorough measures to close integrity and confidentiality gaps in CPS and processes to highlight the security risks that remain. This paper also outlines

approaches to reduce the overhead and complexity for security methods, as well as examine novel approaches, including covert communications channels, to increase CPS security[5].

Observation; Finding 1.2. (1) Supply chain risk management (SCRM) approaches suggest that actors in a supply chain network should consider different risk scenarios to address and mitigate supply chain risks in a better way. Overall performance of a supply chain could be severely affected by disruptions that are triggered by failures or service disruptions in the critical infrastructure (CI) systems that the supply chain relies on.

In order to understand such interdependencies and enhance SCRM approaches with a more holistic view, this chapter introduces a multilevel modelling approach. The economic loss impact of disruptions in CI systems and the potential effectiveness of different strategies to improve resilience in Key Resources Supply Chains (KRSC) are modelled and assessed. A combination of Discrete Event Simulation and System Dynamics is used at the different levels of the simulation model[6].

Observation; Finding 1.2. (2) Cyber security is the most critical aspect nowadays of our technologically based lives. The public and private sector each year spend millions of dollars on technologies, security software and hardware devices that will increase the cyber security inside their companies, but they are still vulnerable. The main problem of this situation is that cyber security is still usually treated as a technical aspect or technology, which can be easily implemented inside the organization and this implementation will guarantee cyber security. This attitude must change, because cyber security nowadays is something more than just the technology.

This article presents the taxonomy of the critical infrastructure attacks, analyzes attack vectors and attack methods used to damage critical infrastructure as well as the most common cyber security mistakes, which organizations make in the cyber security field when trying to make themselves safer from vulnerabilities. The main aim of this article is to provide theoretical aspects of the cyber security management model, which can be used to ensure security of critical infrastructure in an organization or company. The cyber security management model that is presented in this article is analyzed from management perspectives and is not concerned with technological aspects and products that are used to protect critical infrastructure from cyber security attacks and vulnerabilities[7].

Observation; Finding 2.1. Trust is the key ingredient for sustainable transactions. In the concept of trust, the trustor trusts the trustees. In e-commerce, the trustor is the buyer and the trustees are the intermediaries and the seller. Intermediaries provide the web-based infrastructure that enables buyers and sellers to make transactions. Trust is the buyer's judgment and comprises two distinct concepts; both *trust* and *distrust* reside in the trustor. The purpose of this study was to examine the complicated effects of trust and distrust on a buyer's purchase intentions[8].

Observation; Finding 2.2. E-commerce is reshaping business practices and education, yet many have expressed concern over the e-commerce education and training provided to students. This study examines the extent to which business schools, particularly accounting programs, are integrating e-commerce education into their curricula[9].

Observation; Finding 3.1. In this paper, the novel study of the multilayered network model for the disrupted infrastructure of the 5G mobile network is introduced. The aim of this study is to present the new way of incorporating different types of networks such as Wireless Sensor Networks (WSN), Mobile Ad-Hoc Networks (MANET), and DRONET Networks into one fully functional multilayered network. The proposed multilayered network model also presents the resilient way to deal with infrastructure disruption due to different reasons, such as disaster scenarios or malicious actions.

[5] https://ieeexplore.ieee.org/abstract/document/8045959
[6] https://link.springer.com/chapter/10.1007/978-981-10-4106-8_18
[7] https://repository.mruni.eu/handle/007/15671
[8] https://www.mdpi.com/2071-1050/10/4/1015
[9] https://www.tandfonline.com/doi/abs/10.1080/06939280600579370

The provided simulations shows that the proposed multilayered network concept is able to perform better than traditional WSN network in term of delivery time, average number of hops and data rate speed, when disruption scenario occurs[10].

Observation; Finding 3.2. Managerial decision -making is an integral process used in public and private organizations. Critical infrastructure entities are a strategically significant group dependent on the quality of decision-making processes. They aim to provide services necessary to ensure state security and to satisfy basic human needs. The quality of decision -making is an important factor in the management of these entities. The quality level is determined by many factors, the key of which is risk management.

This conceptual article introduces an entirely new managerial decision-making process for indicating the resilience of critical infrastructure elements[11].

APPLICABILITY FOR SUPPLY RESILIENCE

Results of the multilevel simulation offers relevant insights toward a better understanding of the strength and dynamics of the interdependence between KRSC and CI, and consequently on resilience improvement efforts. Results help supply chain managers to prioritize resilience strategies, according to their expected benefits, when making decisions on the amount and location of resilience capabilities within a supply chain. The results strongly support the implementation of collaborative and coordinated resilience strategies among supply chain actors to direct efforts where they can be most effective.

Data and the network are critical success factors for many other critical functions of society. Disruptions in the operation of our countries' critical infrastructure may result from many kinds of hazards and physical and/or cyber-attacks on installations and their interconnected systems. Recent events demonstrate the increase of combined physical and cyber-attacks due to their interdependencies. A comprehensive, yet installation-specific, approach is needed to secure existing or future, public or private, connected and interdependent installations, plants and systems.

After preliminary mapping and discussions some ideas for scenarios have been arose. For an example insulin or some other important medicines supply chain are very vulnerable. Another example could be the digital dependence and vulnerability of ports container arrangements.

2.3 PRIMARY CONTEXT NO.3: GLOBALIZATION VS. LOCALISATION

Need to integrate marginalized communities in society is seen as a critical measure in order to prevent that marginalize communities would be used as a tool in hybrid threats to harm society. Methods and tools for communities and administrations of all levels to reach out to marginalized groups, to integrate them, and decrease risks of marginalized communities to form parallel societies is in the core of the counter measures for possible hybrid attacks. Also educational, cultural and social interventions, especially in the case of children, needs to be highlighted as important arenas to minimize the risks of marginalization and use of marginalized communities as tool in hybrid threats.

SCANNING RESULTS: GLOBALIZATION VS. LOCALISATION

Two main gaps in the context of marginalized communities in society were analyzed:

1. Gap in society: polarization, distrust, cultural antagonism, lack of cohesion. These are linked to society's vulnerabilities, such as: ensuring sound communication between citizens, ensuring sound

[10] https://www.mdpi.com/1424-8220/20/19/5491
[11] https://www.mdpi.com/2076-3387/10/3/75

communication and understanding of present situation and flow of event regional and national administration

2. Gap in society: marginalization, destabilization. These are linked to society's vulnerabilities, such as: realization of inclusive society

With reference to the mentioned two gaps and vulnerabilities in the context or marginalized societies, the following keywords were used in the scanning:

- "lack of trust", "distrust", "cohesion", "intolerance", "destabilize", "influence", "interfere", "social", "cultural", "minorities", "region", "inclusive societies".

INTRODUCTION

The present studies have shown that in the context of hybrid threat scenarios integration of marginalized communities is one of the often-used attack vectors. Marginalization here is broadly defined as cultural (minorities, lifestyles, "parallel societies") or economic, or mix of both. The reason why integration of marginalized groups to societies is seen critical is that, if a policy that does not consider the differences between groups and regions, this may lead to a depletion of cohesion and trust towards central authorities not only at the state level, but also at the EU level. This can create frictions when local administration is responsible for a series of core competences and services. This situation engenders a lack of trust and cohesion, which could facilitate attempts to destabilize a society, opening channels for hybrid threat actors to engage in influencing and interference campaigns.

However, according to available research findings there are many concepts and solutions that may enhance societal coherence and connection between citizen to local and national administration - the solutions vary from basic services to citizens to coherence building measures and planning concepts and research findings what concept may empower the citizen-local-national level communication and how to follow possible polarization in society.

CHALLENGES PERTINENT TO THE INCLUSIVENESS

IMPORTANCE TO ENSURE MINORITIES EQUAL POSSIBILITY FOR SOCIETY'S BASIC AND CRITICAL SERVICES

OBSERVATION

Ensuring easy access to health services, especially mental health care services for ethnic minorities is seen critical to ensure that minorities are not forgotten in the societies' basic services. This derives from observation of "longitudinal association between cumulative exposure to racial discrimination and changes in the mental health of ethnic minority people" is severe. The mental health problems among ethnic minorities might lead to unwanted actions against other citizens. In Addition, unequal services in mental health care can be used to increase polarization and lack of trust to government decision making. In general, basic elements of human wellbeing, such as health, security and peace conditions, education that provides possibility for economic growth, ensured human rights, etc., form corner stones to inclusive society.

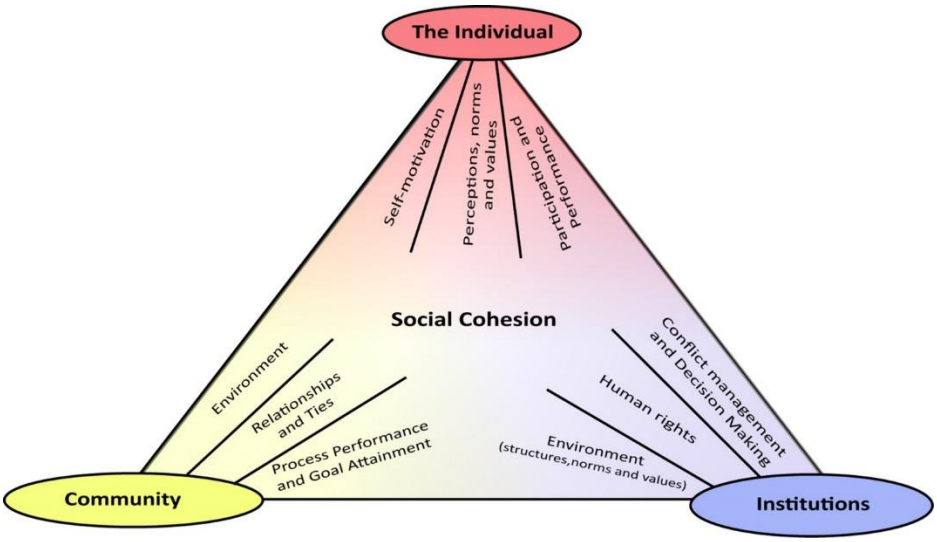
The main concern is that racial discrimination causes mental health problems for ethnic minorities. Therefore, the first action is to decrease racial discrimination and the second action is to ensure that mental health care services are easy to reach and well available to ethnic minorities. This asks for cooperation between local level and national administration in the budged and services planning for mental health care and especially in actions that to reduce racial discrimination and to underline inequality in society.

SOCIAL COHESION FRAMEWORK

OBSERVATION

There is growing evidence that social infrastructure drives social resilience, and resilience can only remain useful as a concept and as progressive practice, if social dimensions are considered. The framework answer is the following: “the social construct of social cohesion in relation to its potential to influence developments within the context of resilient cities and the social systems is responsible for the formation of the resilient societies of the future”.

The main observation is that many initiatives are dedicated to helping cities around the world become more resilient to the physical, social and economic challenges that current societies face. There is growing evidence that social infrastructure, as opposed to physical infrastructure, drives social resilience, and resilience can only remain useful as a concept and as progressive practice, if social dimensions are considered. Fostering social cohesion in cities means creating societies where people can live together with all their differences. A solution to reach this is claimed to be a framework. The framework is to characterize social cohesion and help promote resilient cities, i.e. to help identify levels and possible factors related to cohesion, which need to be taken into account to help design interventions for cities to become more sustainable and resilient. The open framework (picture below) distinguishes three levels that should be considered in future to design and explore the impact of interventions on social cohesion. Note that the framework is not presented with an extensive list of all possible relevant factors, but is designed to be extensible (e.g. new elements, KPIs).



The Framework is seen as a tool for local level and national administration to have general understanding on the basic elements that are seen to be key elements for the social cohesion building. The more there is social cohesion, less aims and actions to cause polarization are expected to be successful.

EFFORTS TO BUILD POSITIVE INTER-GROUP CONTACT IN SOCIETY

OBSERVATION

This is deriving from the observation that changes in people’s attitudes towards out-groups, especially in diverse communities, can go a long way towards reversing declining cohesion in areas. Actions to diminish inter-group contacts may support polarizations and cause distrust between different groups in local level. The local level distrust of certain groups to each other may radiate as distrust or even objection to certain decisions made in national administration level.

It is commonly observed, that diverse communities exhibit lower intra-community cohesion. Little evidence is found that ethnic threat plays a role in this relationship. Therefore, it is argued that perceived threat emerges from other societal processes (such as socio-economic precariousness) and it is when individuals who already

view out-groups as threatening experience diverse neighborhoods that local cohesion declines. In this research it was demonstrated that diversity does not impact all individuals equally and that perceived threat and prejudice play a key role in understanding when and for whom ethnic diversity affects cohesion, at least within communities. Overall, it is observed, that that changes in people's attitudes towards out-groups, especially in diverse communities, can go a long way towards reversing declining cohesion in areas.

More positive inter-group contact in local level has potential increase trust between different actors and decrease intolerance. The cohesion increases resilience of local communities to destabilization attempts. This provides more stable basis for national administration to work as well.

PREVENTION OF CITIZENS TO BE USED AS MAIN TARGETS TO DESTABILIZE SOCIETY; CIVILIAN-MILITARY COOPERATION IN LOCAL AND NATIONAL LEVEL IN SECURITY MEASURES

OBSERVATION

Hybrid threats aim to destabilize society and democracy, and hence civilians, citizens have central role in this context. Therefore, it is seen import to ensure that citizens would not be targeted as main actors to harm society for their own loss. In short, we can and should view from history and have a look at how to protect democracies from within and strengthen both institutions and individual citizens against targeted hybrid threats. Although traditional military strategic thinking emphasizes morality and the will to win as necessary for the civil-military effort, wars cannot be won by military force alone. Therefore, civil-military cooperation in resilience-building is more crucial than ever, given that civil society has become a weaponized battlespace in today's 'like wars' as well as a part of the hybrid threat landscape.

Civil-military cooperation is seen as a key to resilience against hybrid threats; especially in the case to prevent citizens to be targeted as actors who destabilize coherence in society[12]. Resilience has all too often been conceived of as a "target hardening" strategy rather than a larger social challenge. Civil society is a battlespace empowered by information flows, one that military planners, government policymakers and politicians have to take seriously. The more nonlinear and diffuse the distinction between actual war and information or social media war, the more confusing and participatory it gets, as citizens on all sides either wittingly or unwittingly become conscripts. Therefore, civil-military cooperation in resilience-building is seen more crucial than ever, given that civil society has become a weaponized battlespace in today's 'like wars' as well as a part of the hybrid threat landscape.

In the context of the civil-military cooperation, one can also refer to the concept of "total defense" where the citizens are an important actor next to military to provide security in national level. In this case civilians are seen as active actors to provide defense and security to state next to military. For an example in Finland, there is a national volunteer organization called "Finnish reservist association" (FRA)/ "Reserviläisliitto"[13] that has 328 local associations representing approximately 38.000 members. The majority (90 %) of the membership is made up of military reservists of all ranks. In many of the local associations also other Finnish citizens, male as well as female, can participate. The main purpose of FRA is to contribute to the strengthening of the national defense will and maintaining reservist's military skills and fitness for service. However, FRA, as a member of The National Defence Training Association of Finland, also trains and educates citizens to be prepared for and to survive dangerous situations in everyday life and under exceptional conditions.

The focus of civilians as those who maintain and ensure security in society on daily basis and in local level reaching to national level too together with authorities is an issue to highlight in regional as national level in order to have follow-up on adversaries' harmful influence, interference to citizens daily life and perceptions of

[12] https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-25-strategic-citizens-civil-society-as-a-battlespace-in-the-era-of-hybrid-threats/
[13] https://www.reservilaisliitto.fi/en/

society. Accurate information sharing from national and regional administration level to citizens is seen important to ensure that right information is gained by citizens. In addition, information sharing between national and regional level on emerging risks, concerns, accidents among citizens in local level is a key to ensure that citizen who might be targeted by actors to harm society will be prevented well on time in local and national level.

RELEVANT RESEARCH PROJECTS

The following projects are considered to deliver concepts as well as concrete technological tools that may deliver solutions for the above-mentioned challenges.

ICT Enabled Public Services for Migration (MIICT)

The MIICT project the Commission funded project (No. 822380) for years 2019-2021 and from call Horizon2020 Program/ DT-MIGRATION-06-2018-2019. The MIICT has the goal of designing, developing, and deploying tools that address the challenge of migrant integration. In service of this goal, the project undertakes to co-create improved ICT-enabled services with migrants, refugees, public sector services, NGOs (Non-Governmental-Organizations) and other interest groups. By involving research-users at the center of MIICT approach, the project addresses the need to improve and customize the interfaces used to access key public services so that they better address the requirements of migrants and refugees.

The MIICT provides an ICT tool called IMMERSE/ “Integration of Migrants Matcher Service”. The tool supports to customize key public services for migrants so that they are easier to access and use by migrants. This has a strong impact to support migrants to become connected with national and local level services and this will support them to integrate to the society. MIICT supports cohesion and inclusive societies.

The THREAT-DEFUSER project

The THREAT-DEFUSER project is funded by the Research Council of Norway (No. 300002) for year 2020-2026. The THREAT-DEFUSER project explores the role of "soft" information strategies propagated through mass and social media that constitute hybrid warfare by using a case study Norway - Russia. In short, the project investigates Norwegian perceptions of Russia, as well as Russian perceptions of Norway, in the context of Norwegian national security.

Overall, THREAT-DEFUSER is a multi-disciplinary project that combines state-of-the-art methodologies from political science, linguistics, and media studies to forge new methodologies. Whereas academic disciplines tend to be disproportionately focused on the English-speaking world, THREAT-DEFUSER breaks away from that narrow view, focusing instead on Russian and two official languages of Norway: Norwegian and North Saami. Three cultural perspectives are opened: 1) a major international language, since Russian is the second most-used language on the Internet; 2) a majority national language; 3) a minority indigenous language. The tools created by THREAT-DEFUSER are portable to other languages, cultures, and domains, and will be shared open source with the international research community. THREAT-DEFUSER actively disseminates research findings to political authorities (via evidence briefs and closed workshops), to academics (via high-quality open access scholarly journals), and to the public at large through a dedicated, regularly updated website, podcasts, school visits and an app that facilitates rapid response to the dynamic landscape of news and social media. THREAT-DEFUSER assesses Russia's increasingly assertive role in matters of foreign and security policy, particularly in relation to their engagement in hybrid warfare. The same tools are implemented also to analyze Russian attitudes to Europe that have a direct bearing on Norwegian-Russian relation.

Because the project has started in 2020, the tools are not available yet. However, THREAT-DEFUSER project tools are such that are in the interest of EU-HYBNET project in the forthcoming years too.

OBSERVATIONS

All above-mentioned research findings and the technical and non-technical innovations related to them are considered to offer solutions for practitioners in local level and in national administration to counter hybrid threats that may take place in the context of “social out casting and cultural intolerance” (GAP) and “local empowerment and integration of marginalized parts of society” (NEED).

To summarize, the main finding is that different services from society to citizens to engage them to society and to foster inclusive society are important. In addition, support for cohesion between different kinds of groups is needed to encourage cultural understanding and diminish polarization and intolerance. Thirdly, correct information is critical to ensure for citizens not only in local but also in national level in order to avoid citizens to be led by disinformation, fake news and citizens to be used as actors who to destabilize society and cause harm for themselves. In this respect, the information flow between local level and national administration is also crucial to recognize possible hybrid threat on time and to take countermeasures to the situation.

In this research context innovations that can be considered as solutions for the need are more often non-technical/ social science based, policy initiatives and concepts rather than technical. Still the technical solutions may have significant role especially in information sharing, information analysis and delivering services.

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

Cybertechnologies currently one of the most important media for hybrid attacks, both involving cyber-attacks and leveraging social networks for the information attacks. Project investigates future technologies as well analyzing what gaps will be opened with advance of emerging technologies.

3.1 PRIMARY CONTEXT NO.1: GAME CHANGERS: QUANTUM AS A DISRUPTIVE TECHNOLOGY

Quantum computing will make most of the legacy systems vulnerable to attack on encryption level.

The need is identified for "post-quantum" security concepts and tools. They should allow to secure new critical systems with the currently available technologies that would provide level of resiliency to the quantum computing attacks.

On the other hand, tools and methods are needed to secure currently existing legacy systems, which will continue to be used in the foreseeable future and would become highly vulnerable to quantum computing attacks. Concepts and tools of securing, testing, certification, etc., would fall under this need.

SCANNING RESULTS: GAME CHANGERS: QUANTUM AS A DISRUPTIVE TECHNOLOGY

AVAILABILITY OF TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

Analysis of the multiple sources reveal that there is abundant activity in research field aimed at developing quantum-computing resistant cryptography algorithms, both symmetric and asymmetric.

The area of post-quantum cryptography is considerably well researched and internationally standardization bodies have entered the process of standardization of algorithms. Successful standardization would make them widely available and would hugely encourage use.

In July 2020, NIST published "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process" and entered third phase of the selection, with expected completion of selection process within 1-2 years, and further standardization process.

OBSERVATION

Review of the scientific publications and research projects reveal that the field of post quantum cryptography research is very active and productive, international standardization bodies recognize need and considerable maturity of the post quantum cryptography, so standardization efforts are well on the way.

APPLICABILITY OF THE TOOLS FOR NEW DEVELOPMENTS

NIST has published draft of White Paper "Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms"[14]

[14] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.05262020-draft.pdf

The new NIST paper states that *"algorithm selection is expected to be completed in the next year or two, and work on standards and implementation guidelines will proceed expeditiously." However, "experience has shown that, in the best case, 5 to 15 or more years following the publication of cryptographic standards will elapse before a full implementation of those standards is completed."*

Thus, NIST provides expectation, that even though the world is very dependent on cryptography, quantum resistant standards would be implemented only in 5-15 years' timeframe after the completion of standardization process.

Considering, that currently critical systems are being developed and launched which do rely on quantum-vulnerable algorithms – that is currently we still develop systems that will become vulnerable in several years. While current level of knowledge should allow us to build quantum resilient applications or at least applications, which would be "upgradeable by design". "Upgradeability by design" should streamline the process of upgrade of cryptography when the post-quantum algorithms are standardized.

There is an urgency to develop very practical guidelines, which could be recommended or enforced for critical infrastructures at least, which would define "security by design" or "upgradeability by design" blueprints.

OBSERVATION

After reviewing over thousand publications on post quantum security, we gather that there is a clear lack of widely available guidance and regulations, which would govern how to ensure that critical applications built today would-be quantum-safe (or upgrade-ready).

APPLICABILITY OF TOOLS FOR LEGACY STRUCTURES

Review of available research revealed little to none of the research dedicated to securing legacy systems. Considering, that some of the systems were developed decades ago, their upgrade options can be very limited. Other legacy systems may require upgrade of cryptographic algorithms at least.

It is widely recognized that the transition to the post-quantum reality and quantum-safe algorithms will require a decade or more. So, there is clear necessity for the prioritizing and addressing most critical systems of companies and organizations. This is a massive work that will need to be done considering the number of the systems deployed worldwide.

OBSERVATION

Our research and innovation scanning revealed no research on post-quantum protection of the legacy systems. It is a clear necessity to accumulate competence and body knowledge of networks and systems upgrade options and paths to quantum-safe designs. There is a need to develop blueprints for prioritizing criticality of systems.

RELEVANT EU RESEARCH PROJECTS ON THE SUBJECT

EUROPE-WIDE QUANTUM COMMUNICATION TESTING

A test quantum communication infrastructure will be set up in several European countries. Launched by the EU-funded project titled OPENQKD[15]. Its activities will take place in Austria, Czech Republic, France, Germany, Greece Italy, Netherlands, Poland, Spain, Switzerland and the UK. It will boost the security of critical applications in various fields – from telecommunications to electricity supply and healthcare. Bringing together

[15] https://openqkd.eu/

a multidisciplinary team (leading European telecommunication equipment manufacturers, end-users and critical infrastructure providers, network operators, quantum key distribution equipment providers, digital security professionals and scientists) from 13 EU countries, the aim is to bolster Europe's leadership in quantum technologies.

CERTIFIED QUANTUM SECURITY

This project will lay the foundations for the verification of quantum cryptography. We will design logics and software tools for developing and verifying security proofs on the computer, both for classical protocols secure against quantum computer (post-quantum security) and for protocols that use quantum communication.

Our main approach is the design of a logic (quantum relational Hoare logic, qRHL) for reasoning about the relationship between pairs of quantum programs, together with an ecosystem of manual and automated reasoning tools, culminating in fully certified security proofs for real-world quantum protocols.

3.2 PRIMARY CONTEXT NO.2: HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER

Undisclosed vulnerabilities became an important part of development of offensive capabilities of national and private organizations. But stockpiling of vulnerabilities even in the name of national interest may become a threat, which became obvious in the Snowden case.

The need is apparent to develop a framework of governance of undisclosed vulnerabilities among allies. The need exists for the responsible disclosure of vulnerabilities, which would be consistently adopted internationally, as a minimum in countries with common democratic values and interest in mutual security.

Another area is the governance of stockpiling of vulnerabilities. The framework of assessment of the necessity of stockpiling, rules of engagement, assurance of preservation of democratic values and privacy of citizens, governance of stockpiling, checks and balances is of great interest.

SCANNING RESULTS: HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER

INTRODUCTION

Software nowadays is embedded almost everywhere: in smartphones, cars, offices even homes. This fact in addition to hyperconnectivity reveals that most products are exposed to vulnerabilities. It has been estimated that the average software program has at least 14 separate points of vulnerability. Each of those vulnerabilities can allow an attacker to compromise the integrity of the program and exploit it for personal gain. Hence, software vulnerabilities and their timely patching have become a crucial concern for everyone. Security vulnerabilities in software are one of the fundamental reasons for security breaches; and a critical challenge from knowledge management perspective is to establish an efficient method for the knowledge disclosure of those vulnerabilities. In an ENISA research from 2016, it is clearly demonstrated that it is urgent to bring different stakeholders together to discuss the challenges associated with vulnerability disclosure and the ways such challenges can be addressed. The development of a core set of principles upon which different stakeholders can agree, and to which they can adhere, can go a long way towards reconciling the existence of distinct and at times conflicting interests. Thus, it can be characterized as a crucial requirement in future research, to identify the key cyber security vulnerabilities, targeted/victimized applications, mitigation techniques and infrastructures, so that researchers and practitioners could get a better insight into it.

Zero-day vulnerabilities, which are software vulnerabilities for which no patch or fix has been publicly released, and their handling is useful in cyber operations — whether by criminals, militaries, or governments — as well as in defensive and academic settings. The question of whether the government should stockpile or publicly disclose zero-days is challenging, and a precise answer cannot be given. The RAND Corporation's report, "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits[16]" finds that “zero-day exploits and their underlying vulnerabilities have a 6.9-year life expectancy, on average. That is 2,521 days after the initial discovery, with 25% of those zero-days surviving for more than 9.5 years”.

However, according to available research findings there is still no simple answer to the question of whether governments should stockpile or publicly disclose zero-day vulnerabilities.

AVAILABILITY OF TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

Vulnerability management programs have long been a part of reasonable information security programs. Best practices, tools, methods and resources are broadly available to assist organizations build robust programs, including:

[16] https://www.rand.org/pubs/research_reports/RR1751.html

- The **NIST Cybersecurity Framework[17],** which is a risk-based methodology for building a comprehensive information security program, including vulnerability management.
- The **CIS™ (Center for Internet Security)[18]** Critical Security Controls, provides an informative reference for the NIST Framework and detail 20 key information security controls, including: *Control #1:* inventory and control of hardware assets; *Control #2:* inventory and control of software assets; *Control #3*: continuous vulnerability management; *Control #5:* secure configuration for hardware and software on mobile devices, laptops, workstations, and servers; *Control #9:* limitation and control of network ports, protocols, and services; and *Control #11*: secure configuration for network devices, such as firewalls, routers, and switches.
- Detailed guidance on secure configurations for common devices and systems, which are available from most vendors and independent sources, such as**: NIST's Common Configuration Enumeration (CCE) resources;** and the **Center for Internet Security's CIS Benchmarks™.**
- **The Common Vulnerability Scoring System[19] (CVSS)** defines a standardized approach for describing and scoring vulnerabilities, according to risk and severity levels.
- **The Common Vulnerabilities and Exposures[20] (CVE)** list, which provides an internationally recognized standard for naming and cataloging known cybersecurity vulnerabilities, with a maintained list of many publicly released advisories.
- **The National Cyber Security Centrum (NCSC)** in the Netherlands has published a general guideline for responsible disclosure[21], which can serve as a useful model that EU member states can follow in drafting their own responsible disclosure policy. In addition, it gives security researchers guidance on how to act in finding and reporting a vulnerability.

The CEPS Task Force on Software Vulnerability Disclosure in Europe attempted to collectively draft with EC and MS a European-level framework complemented by national legislation in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111 in order to provide legal clarity for software vulnerability discovery and disclosure. However, as was mentioned before only the NCSC in Netherlands created and published a guideline for responsible disclosure. These guidelines include principles, definitions and organizational measures, vital for responsible disclosure policy as a state policy. Many vendors already have introduced responsible disclosure policies or "bug bounty" programs.

The RAND report investigates the issue of stockpiling and hypothesizes that if zero-day vulnerabilities are difficult to find and hence the possibility of stumbling across the same vulnerability that was identified by the other association is moderate then itis logical to stockpile. The research predicts that only 5.7% of zero-day vulnerabilities are identified by another entity per year. Hence, the "collision" rate, or the possibility of the same vulnerability being discovered independently by multiple parties, is limited. Thus, stockpiling rather than disclosing may be advantageous for offensively focused entities.

The argument in favor of stockpiling is that the identification of zero-days is a costly process, but when successful, provides the government with an asymmetric advantage against the adversaries, allowing for practically undetectable intelligence gathering and even the ability to disable or sabotage opponents' infrastructure."

[17] https://www.nist.gov/cyberframework
[18] https://www.cisecurity.org/
[19] https://www.first.org/cvss/
[20] https://cve.mitre.org/
[21] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

OBSERVATION

In this orientation, development of a European framework for EU cross country cooperation in the case of cybersecurity crisis is a work in progress. The NIS Directive does not address this. Current EU's abilities to act at the operational and political level in large-scale cybersecurity crisis has been characterized as "limited". Partly due to a fact that cybersecurity is not yet integrated into existing EU-level crisis response coordination mechanisms.

APPLICABILITY OF THE TOOLS FOR NEW DEVELOPMENTS

Creating an effective response to cyberattacks is crucial to stopping them in their tracks as soon as possible. It is vital that critical sectors, Member States and EU institutions are capable to respond in a swift and coordinated way. Crucial to this is early detection.

Scanning of the available sources revealed that the applicability of each tool depends on the country and the type of the organization, as well as the type of the vulnerability. For example, in the EU there are already some available implemented tools for the management of cyber vulnerabilities. However, each vulnerability requires different handling.

Popular cyber detection tools assist defeats a large scale of attacks daily. However, digital systems have become so complicated that preventing each attack is almost impossible. Their sophistication means attacks often evade detection for extended periods. Experts claim that attention should be on rapid detection and defense. However, some detection tools such as automation, machine learning and behavioral analytics, which look at reducing risks, and analyzing and learning from system behavior – suffer from low adoption rates by businesses. That is implemented because of the generation of false positives; whereby non-threatening activities are mistaken as malicious. Concerning this, network defenders face a disadvantage against attackers, since the defenders must protect against zero-day vulnerabilities of which they are not yet aware. They would be highly favored from a capability to predict the number and severity of zero-day vulnerabilities that will be identified soon. Based on research papers, researchers focus primarily on developing Vulnerability Discovery Models that can be used to generate these forecasts.

OBSERVATION

From the academia side, models are analyzed to foresee zero-day vulnerabilities. These models are formulated into three noticeable forecast model suites, and they are currently being applied at the global and category (web browser, operating system, and video player) levels. The accomplishment of some of these forecast models have been assessed and the outcomes display promise for future use of these models. Future development of these models will include a consensus forecast model that integrates the individual models into a larger model with better long-term accuracy. These models should also be extended and adapted to forecast vulnerabilities at the software application and be applied also to level multi-version software.

APPLICABILITY OF TOOLS FOR LEGACY STRUCTURES

Available studies conclude that cybersecurity governance can be strengthened to boost the global community's ability to respond to cyberattacks and incidents. At the same time, preventing all attacks is impossible. Therefore, rapid detection and response, together with better Information exchange and coordination between the public and private sectors are key challenges to be addressed. Finally, the growing global cybersecurity skills shortfall means that raising skills and awareness across all sectors and levels of society is also a vital challenge.

3.3 PRIMARY CONTEXT NO.3: THE INDIVIDUAL AS A DIGITAL ENTITY

Democratization of content creation and the proliferation and accessibility of tools used for "deep fake" production is a severe challenge in distinguishing genuine content from doctored one.

The needs identified are technologies for identification of "deep fakes" and methods and technologies for determination and verification of the source of content and its integrity.

SCANNING RESULTS: THE INDIVIDUAL AS A DIGITAL ENTITY

Deep fakes can be based on modification and transformations of available media content or they could be completely synthetic products. Based on this we define three different problem areas. The first is to detect if media content has been modified or transformed or if it is completely synthetic. The second is to be able to relate non synthetic deep fake content to the original media content. The third and final area is to be able to attribute the original media content to its source of origin.

Technologies and methods for detecting deep fakes has become a well-established research area. The production of deep fakes relies heavily on AI based tools and techniques and so does most of the methods and technologies for detection. Published research show that different AI approaches and different distinguishing features are studied and tested. However, we have not found any recent comprehensive comparison of weak and strong points and detection rate of the different techniques used. The area of "improving" deep fakes in the sense that they become more difficult to detect is also developing. Thus, there is an arms race between making new production tools available and new and better technologies for detection.

To be able to perform content source attribution, it is necessary to first link a deep fake to the original media content. The methods used to achieve such linking are mostly based on comparing media meta data (if it exists) and different media and content features. The research scan performed has produced few hits in the area and is judged as more immature.

Finally, the problem of attributing media to its original source of origin is an exercise in searching media content. Bing (Microsoft), Google and Yandex (Russia based) offer free reverse image search. There are also commercial offerings that perform searches, which are more advanced and e.g. can handle and identify the original of images that have gone through different kinds of transformations such as resizing, cropping, edits, occlusions and color changes. Image search tools are already being used today to detect e.g. copyright infringements.

The EU Directive on Copyright in the Digital Single Market includes requirements on online content-sharing service providers to perform "upload filtering" of content to detect upload of copyright protected content. The filtering will in general be performed against content registered by copyright owners. These requirements will most certainly drive the development of new advanced and innovative methods and technologies to identify the original content source. A remaining problem is to collect and annotate all of the original content.

An interesting initiative here is the "Content Authenticity Initiative"[22] introduced by Adobe. The Content Authenticity Initiative aims at developing an industry standard for digital content attribution and is "designing components and drafting standards specifications for a simple, extensible and distributed media provenance solution". Media carrying such attribution information would not have to be upload filtered as the required information is available together with the media.

OBSERVATION

To conclude, the problem of detecting a deep fake is an active research area, but as deep fake technologies evolve so must the detection methods. Working methods have been developed and are used in practice but

[22] https://contentauthenticity.org/

there are no published standards or generic services. The problem of relating a deep fake to its original media is an area where less information has been found, but this problem may be of less importance in a fake news context as trust will gone if it becomes known that the content is doctored.

The content attribution problem is however of great importance in a fake news context as it should help to verify that the claimed origin of media is the genuine one. This area will certainly get a lot of attention from online content-sharing service providers leading to the development of new media search solutions as well as attribution schemes. But there is a strong need to design and implement these solutions in a way which the public can trust and hence would use.

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

4.1 PRIMARY CONTEXT NO.1: GOING VIRAL

There is a need for concepts, methods, and tools to increase the population's resilience to manipulated information. From a broad perspective, this encompasses increasing skills and motivation to judge critically content they consume, increasing media literacy, developing tools for validating content's integrity and trust ability of sources, etc.

SCANNING RESULTS: Going Viral

KEYWORDS ANALYSIS AND DEFINITION OF TERMS

Basic keywords and definition of terms in the field of manipulated information:

Keywords (used for scanning):

- Media manipulation
    - Fake news on social media
        - Internet manipulation
        - Distraction
        - Photo manipulation
        - Video manipulation
    - Hoax
    - Propaganda
    - Satir/ Parody
    - Rumors
    - Click-bait
    - Junk news

Counter measurements

- Detection methods
- Tools
- Concepts

Definitions:

- Fake news: fabricated news articles that could potentially or intentionally mislead the readers, as they mimic traditional news content in form but not in the intent or the organizational process.
- Hoax: a fiction intentionally fabricated to masquerade the truth.
- Propaganda: news stories created to influence the emotions, opinions, and actions of the target audiences using deception in selectively omitting or providing wrong messages for political, ideological, or religious purposes.
- Satire/Parody: a form of news written to entertain or criticize the readers, and it could mimic genuine news; this is harmful when shared out of context.
- Rumors: originated from a Latin word that means noise and has been identified by some scholars as a subset of propaganda. An unverified claim that did not originate from news events could spread from one user to another.
- Click-bait: low-quality journalism that is intended to attract traffic and benefit from advertising revenue.
- Junk news: more generic and aggregates several types of information; it usually refers to the overall content that pertains to a publisher rather than a single article

- Deep fake: Deepfakes are fake videos or audio recordings that look and sound just like the real. Usually deepfakes leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content with a high potential to deceive. Together with fast spreading of information it has huge potential for hybrid threat scenarios.
-

Type of information:

- Textual
  - Unstructured information
  - Semi-Structured information
  - Structured information
- Multimedia
  - Images
  - Video
  - Audio
  - Graphic

TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

Most studies have so far focused on three main themes:

- The definition and the scope of the problem,
- The potential causes and impacts and
- The proposed solutions

Research on the impact of manipulated information

- Manipulated information has primarily drawn recent attention in a political context, but it also has been documented in information promulgated about topics such as vaccination, nutrition, and stock values. It is particularly pernicious in that it is parasitic on standard news outlets, simultaneously benefiting from and undermining their credibility.

Research on concepts/methods/tools to counter the problem of manipulated information

- A very well-known research problem with the most advanced techniques. The literature on manipulated information is still expanding.
- A lot of publications focused on social network.
- Manipulated information detection and protection is a very challenging problem because of two reasons:
  - Big Data: The problem with big data is that they are becoming larger and larger; organizations can often not understand the opportunities and extract usable information. Organizations often do not recognize where to deploy their resources. This lack of resources is since the information is not fully utilized.
  - Unstructured information: As described above, information on the internet is represented in many forms, e.g., text, audio, image, or video. Each information provider has a different structure for their interface or a different way to describe the information, making the information extremely unstructured. The analytics of unstructured information is a very difficult research problem.
- Platform-based detection and intervention: Algorithms and bots
  - The detection approach using machine/deep learning is widely applied and shows a huge potential for fully automatic detection and protection.

OBSERVATION

Some of the papers are not always comparable (and often not comparable) to each other, although they appear as academic exercises. The main problem with most of the papers is that, while they perform well when applied to specific input datasets, they do not generalize to unseen data. In our analysis, the content-based approach seems to work only to a limited extent, whereas contextual analysis is more easily applied to general behaviors (e.g. comments, reviews, dissemination, etc.).
Here are the observations based on our review in this field:

- Missing of a general concept to reduce the spread of manipulated information
    - Fundamental questions: how do we create the news ecosystem and culture that values and promotes truth?
        - Need for an international action rather than a national action
- Future research should further explore the various impacts of manipulated information. The negative impact is currently assumed, rightly so, but a closer examination of the various negative effects of manipulated information can better guide initiatives to combat it. For example, while manipulated information derives part of its ability to fool individuals by mimicking the look and feel of real information, no systematic analysis of its effect on real information perceptions has been conducted.

4.2 PRIMARY CONTEXT NO.2: DIGITAL MONOPOLIES AND MASSIFICATION OF DATA

The extensive collection and aggregation of data with respect to individual user actions on the net and in social media enables unprecedented consolidation of data. The collected data can be mined to infer persons' preferences and behaviors, which in turn can be used for micro-targeting in influence operations. Data and or mined target groups are tradeable commodities.

The needs identified are to investigate regulatory and technical means for limiting the data collection and incur stricter usage control and explore means and potential for having aggregated personal data about large population groups designated as a critical commodity.

SCANNING RESULTS: DIGITAL MONOPOLIES AND MASSIFICATION OF DATA

Published research discuss the pros and cons of the massive collection of data on user behavior on the Internet and in real life. Data driven research and analysis benefit from using Big Data and in general it is true that the bigger the data the better the results. In essence, it is agreed that future advantageous developments would be hampered if the use of Big Data would be severely restricted. There is an ongoing current discussion if the paradigm should shift from restricting the collection of data to how it is allowed to be used.

One important aspect of big data is the collection and use of personal information, which should be protected and not openly disclosed. In the EU we have GDPR which incurs strict requirements on the handling and use of personal information. To allow analysis of big data based on personal information different methods for anonymization or pseudonymization can and are used. But today, it has been observed that when more and more data is collected, and more and more computing power is available, anonymized data sets can often be deanonymized using complementing information from other data sets. This is another reason that regulations for use of big data will become important.

Furthermore, it has been observed that user behavior as e.g. instantiated in browsing habits may be uniquely tied to an individual. This means that personal data is not only what we are in our daily life consider as personal information but in the context of big data is much more. Collected traces of what we do on the Internet can be easily recorded and analyzed into descriptors that can be used as identities for tracking and microtargeting.

The slogan that the bigger data the better the results from analysis has also opened a market for data brokering. Here data about users and user groups can be sold and bought. Such third-party data can together with data provided by users on (service-)platform and data on users' browsing behavior be used to profile users and user groups for launch of microtargeting influence operations or micro phishing.

The research scan did not find evidence of an ongoing discussion about making aggregated personal data about large population groups designated as a critical commodity. This deserves deeper analysis, because such data is a basis for microtargeting, and may be an object for well measured policy action.

OBSERVATIONS

The problem of controlling the collection and use of big data must be seen as a regulatory problem rather than a technical one. Possible means to limit which data is collected, how it is used, for what purpose, and how it is traded should be researched.

4.3 PRIMARY CONTEXT NO.3: DETERIORATION OF THE QUALITY OF CONTENT

It is observed, that increased usage of social networks and internet resources traditional media increasingly loses its revenue streams and is less able to fund creation of quality journalistic content, so the "gatekeeper" role of traditional media is decreasing.

Need is identified to label quality journalistic content. Models of direct or indirect subsidies to quality content may be explored, recognizing critical role of journalistic content for the public information.

There is a need for new models of journalistic content distribution via digital platforms, to ensure fairer revenue distribution.

SCANNING RESULTS: DETERIORATION OF THE QUALITY OF CONTENT

Scanned keywords: "journalistic content" AND labeling

Fact AND checking

AVAILABILITY OF TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

Reviewed research has demonstrated, that despite all the changes in media delivery, proliferation of social media and increasing efforts of traditional media to work via social media, consumers still attribute higher degree of trust to the "journalistic content", though it seems that there is agreement, that this degree of trust is generally decreasing.

In the context of hybrid threats, "degree of credibility" attributed to the traditional media is a very valuable asset. In order to use this "degree of credibility" significant effort was dedicated to build somewhat trustable sources as instruments for fake news. Whole spectrum of such "media" outlets are functioning, starting from government funded propaganda outlets (e.g. RT), to traditional media like websites, specialist websites, etc.

It is well established, that countries which strongly protect freedom of speech, are very slow in restricting propaganda outlets, as it is extremely difficult to have clear-cut difference between "opinion" and propaganda / one sided information. Our scan did not discover any relevant efforts to classify and label quality of journalistic content or its compliance to the standards. Apparently, traditional media relies on ethical standards and quality enforcement by editorial staff and self-governing professional bodies. Many articles point out that while ethical standards in traditional media outlets in countries are more or less enforced, this enforcement is far from ideal. It mainly relies on the media outlet's internal ethical standards, while non-media influencers are not bound to them at all.

It is worth to note, that political bias of the media outlets is considered appropriate. In this area, there are efforts to evaluate journalistic content using proxies. One of interesting examples can be evaluating political "bias" in US media[23]. The project uses elaborated methodology and strives for objectivity. As the project analyses content, it is highly labor intensive, and naturally can be done only in large countries where significant funding would be available for such projects. It will be highly interesting to see the evolution of this project, analysis of construct validity by researchers and leveraging more of the automation to lower the costs of operation and increasing an applicability.

While evaluating journalistic content is only marginally conceptualized, there is huge ongoing research in the tools methods and techniques to assessing the truthfulness of a claims.

[23] https://www.adfontesmedia.com/static-mbc/

Vast research efforts are focused on automated fact checking, using natural language processing, machine learning and artificial intelligence, knowledge representation, etc. Fact checking became household term, social media giants increasingly use fact-checking and flag misleading content, countries have numerous organizations (media and non-media) operating as fact-checkers.

OBSERVATION

The research scan revealed that main efforts in the journalistic content evaluation is dedicated to fact-checking claims. A number of organizational and technical solutions were deployed and are functioning, using mix of technical solutions (e.g. natural language processing, artificial intelligence, machine learning, etc.) and human intervention. At the present time it is a quite mature field both organizationally and technologically.

Still the impact of fact-checking to public opinion remains the object of discussion. Some studies indicate that fact-checks can reduce misperceptions, but most often fact-checking has no significant impact on vote choice or candidate selection. So more of the research and practical testing is needed to:

- further elaborate techniques for automated fact-checking, approaching near-real-time fact-checking,
- ensure unbiased result of fact-checking,
- tracing real source of the claim,
- understand better how fact-checking impacts or fails to impact consumers' perceptions.

APPLICABILITY OF THE TOOLS FOR NEW DEVELOPMENTS

The International Fact-Checking Network (https://www.poynter.org/about-the-international-fact-checking-network/) is one of important forums bringing fact-checking organizations together, enables best practice sharing and establishing "code of principles". The IFCN currently has over 80 signatories' organizations from variety of countries. Partners of fact-checking community are both traditional media outlets, as well as other organizations.

APPLICABILITY OF TOOLS FOR LEGACY STRUCTURES

Traditional media outlets, being "legacy" structures themselves are considered to be the most resilient to the fact-bias due to the established editorial process. Note, that traditional media outlets quite often are systematically politically biased. This is rather positive feature, when the preference is openly declared, like in the case of CNN and Fox New in US . While outlets with hidden agenda and hidden preferences can be destructive.

Traditional media base is struggling to find new revenue sources and retain the significant share of attention. Our scan did not reveal any significant efforts to conceptualize new models which would ensure necessary revenues for the media for quality content development and ensuring that this content be labelled accordingly (via the sorts of journalistic content labelling).

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

5.1 PRIMARY CONTEXT NO.1: TREND: OFFICIAL STRATEGIC COMMUNICATION LOSING POWER - HOW TODAY'S INFORMATION ENVIRONMENT EFFECTS KNOWLEDGE?

The challenge is the tendency to distrust official information.

Concepts, models, tools of official communication that would create and maintain trust levels with the public are needed. This should be considered in widest context – including for authorities how to communicate uncertainties without losing authority, how to communicate highly negative news of forecasts without creating panic, how to leverage existing channels, deal with multitude of sources and attempts of disinformation, etc.

SCANNING RESULTS: OFFICIAL STRATEGIC COMMUNICATION LOSING POWER - HOW TODAY'S INFORMATION ENVIRONMENT AFFECTS KNOWLEDGE?

Our review of the research materials did not demonstrate relevant hits, while this subject is extremely popular in the strategic communications, public relations, and political sciences. Thus, tendency of official communication losing its power is rather addressed in advisory ("know-how") level, analysis of experience or philosophical considerations, rather than scientific research. It might be that the analysis of the phenomena is yet to mature, to become suitable fall under scientific research microscope. On the other hand, there is no lack of professional discussion (not scientific per se) on the modalities and efficiency of the communication under the stress (e.g. flood of bad news).

An area which attracts visible research efforts is relation between transparency (in case of bad news) and efficiency of decision making. While there is solid body knowledge, that organizations which practice transparency tend to be more efficient (mostly by means of facilitating channeling of efforts and attention to most pressing issues), instincts of organizations and leadership work contrary to that.

While in corporate situations disclosure is very much regulated, level of disclosure and transparency in the state governance is usually much more subject to the established practices and instincts of politicians. Some projects are investigating opportunities to develop blueprints for political communication, with the hope that it could make transparent communication of risks and bad news a default strategy.

OBSERVATION

Overall, the subject as described is very complex, built on numerous phenomena and influencing factors. Therefore, the research is not addressing the phenomena as such, but rather focusing into specific areas (like relationship between transparency and efficiency of organization). Application of research in the political communication is even less common.

So the subject overall is observed to be practical models, "know-how" and subject of philosophical consideration much more than scientific research.

5.2 PRIMARY CONTEXT NO.2: TREND; BIG DATA AS A NEW POWER SOURCE

Proliferation of micro targeting practices and possible use in hybrid attacks creates need for the state actors to be aware of such attempts. Concepts, models and tools are needed for situation awareness, where the challenge is that micro targeting is difficult to spot (due to "micro" targeting).

Regulatory measures need to be explored and conceptualized to regulate the use of micro targeting both in political campaigns and in other areas.

SCANNING RESULTS: TREND; BIG DATA AS A NEW POWER SOURCE

AVAILABILITY OF TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

'Data is the new oil', 'Information is Digital Gold', and similar terms are becoming commonplace within the media and technology domain. Organizations are dependent on data to maintain pace in the digital world and are seeking innovative ways to leverage the information. As technology and computing power improves, the data can be mined and processed much quicker. The current focus is on big data and the scale it brings.

The term 'big data' refers to the aggregation of numerous raw-data points (the more, the better). Next, the data is synthesized into one database of reference. Following refinement and cleansing, the data is used to inform or create insights on a specific target. It is worth noting that 'big data' has many use cases and can be leveraged for 'good' or for 'bad'.

The 'micro-targeting' is essentially utilizing the data in the most efficient and impactful way. Micro-targeting is widely used across Industry and brings convenience to many - in all areas of life. For example, the TV programs recommended, the songs suggested, the restaurants proposed, etc.

Political micro-targeting has been described as a "technique of political communication based on the use of data and analytics to tailor messages to a subgroup or individuals via different channels" with views to foster relationships with prospective voters and supporters (Bodó et al., 2017).

'Micro-targeting' and 'data-driven' political campaigning has gained significant attention in the wake of the Cambridge Analytical campaign linked to the US Presidential Elections of 2016 and similar connections related to the Brexit referendum in the same year. Research shows a plethora of content connected to the topics and associated subjects.

OBSERVATION

As a discussion point, the matter of data-driven micro-targeting, especially connected to political campaigning has gained prominence in recent years, both academically and in the wider public domain. The criticism of Social Media and tech giants; namely Facebook, Twitter and Google are central to the dialogue. Papers and research have been growing since the aforementioned elections of 2016, but the release of The Social Dilemma[24] and The Great Hack[25] has pushed the topic higher on the agenda of public issues and concerns.

Social Media was scrutinized following the Trump election for allowing political advertisements on their platforms. Facebook, specifically, was subject to close media attention for their role and lapse legislation allowing private firms to exploit the platform and its users. Twitter was the first Social Media provider to announce a blanket ban on political advertisements, and both Google and Facebook have committed themselves to using stricter measures to reduce the spread of misinformation. Interestingly, during most recent 2020 US elections,

[24] https://www.netflix.com/gb/title/81254224
[25] https://en.wikipedia.org/wiki/The_Great_Hack

Facebook introduced a temporary ban on adverts relating to social issues [26]. Conversely, Facebook also threatened legal action against New York University[27] for the use of 'Ad Observer', a data scrapping browser-plugin, used by researchers to determine which groups of citizens have received certain adverts.

Ad Observer [28] allows the researchers to collect ads targeting data from users and feed the anonymized information into a public database. The webpage for the plugin states:

> "Online ads are usually seen only by the audience the advertiser wants to target, and then they disappear. This makes it difficult for the public to monitor them and hold advertisers, including political groups, accountable. While platforms have developed some transparency libraries for political ads, these libraries are missing many political ads and often do not include vital information like ad targeting. This is not a partisan issue. We think it's important for our democracy to check what politicians of all stripes are saying."

An article by Vice[29] states that 'Ad Observer' is not the only plugin used to capture such data, and at the time of writing this, Facebook, after receiving public criticism, has signaled that the ad-tracking project can continue.

Although less talked about - or even overlooked is the use of micro-targeting by central and left-leaning political campaigns, such as the first presidential campaign of Obama in 2008. Therefore, one should avoid making assumptions that only certain parties are using micro-targeting as a strategy and that its use is always negative. Thus, one should consider what the purpose of the campaign is and how the big data is gathered and used.

There is a dialogue on the best way to prevent micro-targeting for political campaigning; one argument is to ban the advertisements of a social/political nature. However, there are also comments that this will not change the underlying issue and will add additional risk.

> "*By acknowledging a willingness to moderate online content — be it through Germany's online hate speech rules, upcoming EU and U.S. changes to so-called content liability rules or the companies' own political ad restrictions — Facebook, Google and Twitter have started a process that will only end in one way: taking more and more responsibility for what is shared on their networks.*
>
> *That may not be what they want — or something that any of us should clamor for if it means private companies, not elected officials, setting the standards for what can be said online*." (*Mark Scott, Politico 2019)*

From the initial analysis, there does not appear to be many tools aimed at countering micro-targeting. Although, as we have seen, there are efforts to counter malicious content, misinformation, fake news, etc. However, there is no direct correlation between microtargeting and the former threats, although micro-targeting, viral content and advertising exacerbate their impact.

Review of the scientific publications and research projects reveal that most of the publications concern the political micro-targeting which is threatening media pluralism and democracy at a global level.

[26] https://en-gb.facebook.com/business/help/167836590566506?id=288762101909005
[27] https://apnews.com/article/media-social-media-76247e67b19ca0cd77f2732f84f489d5
[28] https://adobserver.org/
[29] https://www.vice.com/en/article/n7vegw/facebook-decides-to-let-research-project-collecting-ad-targeting-data-continuefor-now

POSSIBLE STEPS FORWARD

Considering this is an issue when the tactic of micro-targeting is used inappropriately, the most common demand is for legislative and legal requirements to govern the use of micro-targeting. The Utrecht Law Review suggest policymakers enhance the transparency of all micro-targeted advertisements used by political parties. However, there is a caveat that they should remain vigilant to freedom of expression when imposing regulations. The law review also states that it would likely be harder for extensive political micro-targeting in Europe when comparing to the U.S, because of existing frameworks covering personal data and privacy.

Throughout research, there are calls for algorithmic transparency and reporting and increased general transparency amongst social media platforms. There have been recent changes that provide the public access to information related to who funded certain political advertisements and how the desired audience was selected. Thus, internet users have methods to avoid political manipulation of their data – however, researchers argue that the data does not provide enough information, and it is not clear how many people will check this and what the efficacy of the approach is[30].

Although steps are being made and social media platforms are increasing transparency regarding their advertising policies, internet users are still vulnerable. The responsibility lies in the hands of policymakers, social media platforms and media outlets, which, as Dennis G Wilson from the University of Toulouse has argued, can themselves employ AI to combat its malicious use by others[31].

The use of AI, algorithms, big data and targeted content can be seen to manipulate voters and influence their opinions – but the underlying approach is nothing new. Politicians have always tried to sway voters and conjure support. The actual content, the funding sources and rationale behind the campaigning is key to stabilizing democracy.

Furthermore, micro-targeting is not a symptom that needs to be dealt with in isolation. It forms a part of a growing list of vulnerabilities and risks related to the spread of misinformation and disinformation. Thus, fact-checking, transparency and credible sources are required. Moreover, education and awareness of the risks is needed. Users of Social Media should be aware of the 1-dimensional content they are exposed too. Likewise, other media outlets have a duty to share more objective perspectives, rather than the polarized opinions that are often broadcast to their respective audiences.

POLICY RECOMMENDATIONS

As stated in the report from International IDEA, legislation related to micro-targeting differs from country to country. Moreover, the rapid changes in technology result in the regulation becoming quickly outdated[32]. A standardized model with a central body for keeping policy and regulations updated could be effective. Moreover, the leverage of a central organization could have more influence on technology companies. Realistically, it is challenging for individual researchers or small states to tackle the tech giants alone – especially when one considers their financial might and base of users. Therefore, a collective method with a unified goal appears to be the most sensible and practical short-term solution. This argument is reinforced in the wake of the disagreement between Facebook and New York University mentioned above.

However, additional complications can arise as the judgement on what is and what is not appropriate, is rather subjective. Thus, it could be challenging for political actors to agree on a unified approach.

[30] https://www.ivir.nl/publicaties/download/UtrechtLawReview.pdf
[31] https://sigai.acm.org/static/aimatters/3-3/AIMatters-3-3-12-Wilson.pdf
[32] https://www.idea.int/sites/default/files/publications/digital-microtargeting.pdf

Nevertheless, research stresses the importance of transparency covering the data used in microtargeting, especially when the data is meant to determine an individual's political persuasion or personality traits and online behavior.

As this research shows[33], the current GDPR has some efficacy in the EU, but it is not enough.

> *It is common that using apps and online platforms, people voluntarily provide their personal data and allow their further usage as a by-product of the service. It is important for users to become aware of what they are agreeing on, and what consequences their actions have. In this direction, certain normative and legal imperatives have already been formulated: transparency of data collection, processing and application (Barocas et al., 2017[34]), autonomy of the subject on having control of their own personal data (McDermott, 2017[35]), and (in)visibility: the right of the subject to choose if and to know how personal data might be collected and used (Taylor, 2017[36]), are stated as necessary for supporting someone's privacy. The EU General Data Protection Regulation makes also steps towards this direction, by explicitly incorporating transparency and consent in its regulatory claims.*
>
> *Despite the regulatory efforts, the act of a user opting in, given a very long document of terms and conditions, where how personal data might be used is outlined in a short and general manner does not signify transparency, or actual consent (Strandburg, 2014[37]). Especially regarding personal data for microtargeting, the information that should be presented to the subject in order to give their consent should clarify exactly what information is going to be collected, how, by whom and for what purpose. This is a prerequisite for the subjects' expectations about the collected data to coincide with the actual data usage (Barocas and Nissenbaum, 2014[38]). At the same time, the individuals should be emancipated, by both getting to know through access to the history of their personal data used by services (Kennedy and Moss, 2015[39]), and realizing how datafication has pragmatically altered the contemporary social structure.*

Simplifying and prioritizing the terms and privacy statements could also assist in educating users on what they are reading and viewing online. The exemplary examples of the modified Cookie Policies on websites following the introduction of GDPR could be used for inspiration, especially the use of clear 'opt-in' choices and straightforward explanations of the use of data. Likewise, clear signaling on media platforms who is funding the adverts could also be helpful.

RESEARCH

Unlike transactional micro-targeting where a company can review the conversion rates from the money invested on advertising to the volume of transactions and/or conversions – the political sphere is more complex; as it is difficult to determine how a voter's decision was influenced. However, research does show that politically charged adverts are effective and persuasive, especially when targeted at a user's specific personality traits - using psychometric data[40]. This only reinforces the claims made by Cambridge Analytica when they used personality profiling to model the voting preferences of American citizens.

This form of micro-targeting is also complex from an ethical perspective as the ability to show content that is better suited to an individual can provide value by informing them about information and knowledge that is most

[33] https://journals.sagepub.com/doi/full/10.1177/2053951718811844
[34] https://journals.sagepub.com/doi/full/10.1177/2053951718811844
[35] https://journals.sagepub.com/doi/full/10.1177/2053951718811844
[36] https://journals.sagepub.com/doi/full/10.1177/2053951718811844
[37] https://journals.sagepub.com/doi/full/10.1177/2053951718811844
[38] https://journals.sagepub.com/doi/full/10.1177/2053951718811844
[39] https://journals.sagepub.com/doi/full/10.1177/2053951718811844
[40] https://journals.sagepub.com/doi/full/10.1177/0093650220961965

appropriate and suitable. In contrast, it can be used for devious purposes to shift someone's political vote by showing emotionallycharged content that best resonates with their personality.

This is reflected in the conclusion of the above research paper:

"It is therefore of crucial importance to investigate the potential risks and threats of PMT (Political Micro-Targeting) in a broad sense. This will lead to valuable insights regarding how PMT might undermine our democratic values, while at the same time, offer answers on how to use PMT in a responsible manner to maximize its mobilizing potential."

5.3 PRIMARY CONTEXT NO.3: TREND; INCREASING STRATEGIC DEPENDENCY OF CRITICAL SERVICES

SCANNING RESULTS: TREND; INCREASING STRATEGIC DEPENDENCY OF CRITICAL SERVICES

A foreign direct investment (FDI)[41] is an investment in the form of a controlling ownership in a business in one country by an entity based in another country. Stephen Hymer wrote about FDI back in the 1960s, emphasizing that FDI differs from other forms of investment, such as portfolio investment, as FDI is not necessarily a movement of funds from a home country to a host country; rather it is concentrated on particular industries within many countries and refers to the investor remaining control of operational activities[42].

FDI is commonplace, money from around the world circulates – stimulating and driving global economies. Quality FDI that helps the integration of indigenous firms in developing countries into the world-wide supply chain-network has proven a promising tool for advancing these countries, as has been evidenced in numerous scientific studies. Thus in 2017, in their aim of setting up a strategy with Africa, the G20 countries, together with international organizations, were urged to review measures of turning FDI into 'quality FDI'[43].

However, with the rising amounts of Chinese investment in the EU from the beginning of the decade, there were concerns raised over the imbalance of reciprocity of market access for Chinese investors comparing to their EU counterparts. According to the OECD FDI regulatory restrictiveness index[44], China is one of the most restrictive economies with respect to inward FDI.

Although not specifically directed at China, a joint letter from France, Germany and Italy highlighted some of these concerns back in 2017[45].

This letter followed a year where China's global outbound foreign direct investment soared to record levels in 2016, jumping to almost 200 billion US dollars. This marked the peak, and the figures have been in decline since. The European Union was a preferred choice for Chinese investors. Chinese FDI in the EU totaled more than EUR 35 billion in 2016, an increase of 77 per cent from 2015. With 11 billion Euro of completed deals, Germany was the largest recipient, accounting for 31 per cent of total Chinese investment in Europe[46].

From its peak in 2016, the downward trend of China's outbound FDI can be linked directly to a more restrictive overseas investment landscape, as well as to shifts in political stance and priorities, prompting Chinese firms to reconsider their engagement strategies – according to this article from Ernst Young (EY)[47].

EY postulate that deglobalization and protectionism are the reasons behind the decline, emphasized by more stringent investment controls. For example, EY highlights that between 2017 and 2018, 49 restrictions or regulations related to FDI were introduced in 28 countries, 40% of which deriving from national security concerns about foreign ownership of infrastructure, technology, real estate, and elements of the defense sector. Perhaps the most public disagreement is the US-China trade war and accusations made by the 2016 – 2020 US president, Donald Trump[48].

[41] https://en.wikipedia.org/wiki/Foreign_direct_investment
[42] https://www.jstor.org/stable/1805601?seq=1
[43] https://www.g20-insights.org/wp-content/uploads/2018/05/attract-quality-fdi-1525857438.pdf
[44] https://goingdigital.oecd.org/en/indicator/74/
[45] https://www.reuters.com/article/uk-eu-trade-france-idUKKBN15T1ND?il=0
[46] https://merics.org/en/report/record-flows-and-growing-imbalances-chinese-investment-europe-2016
[47] https://www.ey.com/en_cn/china-opportunities/how-do-chinese-firms-navigate-the-new-global-trade-landscape
[48] https://www.theguardian.com/us-news/2019/aug/23/trump-china-economic-war-why-reasons

With a decline of FDI and mergers and acquisitions in Europe and the US, unsurprisingly, Chinese investors have diversified their reach, looking at Asia and South America. Also, beneficiaries include the Belt and Road Initiative-countries (BRI)[49].

> "China's overall ODI (Outward Direct Investment) volume has been decreasing from their most recent peak in 2016, when it amounted to US$196.2 billion. Fast forward to 2019, and overall ODI amounted to US$117.1 billion, a 9.8% drop YoY. Of this, non-financial ODI accounted for US$110.6 billion, down 8.2% YoY. Although these figures represent clear decreases, the structure of Chinese investment is also becoming more balanced, suggesting diversification in industry targets."[50]

Of course, FDI does not only concern China, and security concerns extend to other regions too. In general, potential national security threats from foreign ownership fall into three categories: (i) the transfer of (military) sensitive technology; (ii) the denial or manipulation of access to a critical input by a foreign-controlled supplier; and (iii) the infiltration, surveillance or sabotage of production systems crucial for the functioning of economy (e.g. critical infrastructures in energy or transportation, or telecommunications and cyber networks) – Three Threat Framework, Moran 2017[51].

In contrast, FDI is commonly considered for having a positive influence on global development. Studies find evidence[52] that it can positively impact countries – reducing political risk and promoting political stability.

EU POLICY OBSERVATION

FDI has been a discussion point for many years[53] but has gained increased attention in recent times.

Typically, countries will have thresholds related to FDI that are triggered because of risks to National & Public Security, Media plurality maintaining stability in financial systems. The EU has stated:

Even though half of the Member States already screen investment at national level, a strong EU-wide approach to foreign investment screening is necessary in a time of public health crisis and related economic vulnerability.

Therefore, in October 2020 the EU introduced a new framework for screening FDI. The EU is seen as one of the most open regions and is keen to continue engaging foreign investors, but under certain provisions:

> *'The EU is and will remain open to foreign investment. But this openness is not unconditional. To respond to today's economic challenges, safeguard key European assets and protect collective security, EU Member States and the Commission need to be working closely together. If we want to achieve an open strategic autonomy, having an efficient EU-wide investment screening cooperation is essential. We are now well equipped for that.' European Commission Executive Vice-President Valdis Dombrovskis, 2020*

Similarly, the UK has amended its approach, reducing the threshold for Military or dual-use goods subject to export, computer processing unit's quantum technology. The 2020 Queen's speech highlighted an entirely new and much broader regime to be introduced, which will cover share sales, asset sales and land acquisitions. It can look at any market that could pose a national security risk. There is a focus on core infrastructure - Energy, Transport, Defense - and advanced technologies, as well as critical supplies to government and emergency services. No safe harbors or thresholds. The changes will give the UK power to block deals and impose fines.

[49] https://en.wikipedia.org/wiki/Belt_and_Road_Initiative
[50] https://www.ey.com/en_cn/china-opportunities/what-was-the-state-of-chinese-outbound-investment-in-2019
[51] https://www.piie.com/system/files/documents/moran201702draft-c.pdf
[52] https://jbrmr.com/cdn/article_file/i-25_c-241.pdf
[53] https://www.oecd.org/mena/competitiveness/35275189.pdf

Other countries, such as Germany, have also introduced stricter more onerous measures from 2018 preventing critical industries to be triggered at acquisitions of just 10% of the voting rights of the target. It is worth noting that 'critical industries 'is a very broad domain; including software, cloud computing, utilities, health, transport, media, etc.

The World Investment Report 2019[54] outlines all the changes and summarizes the reasoning behind the increase in additional policy instruments and screening procedures.

> *It is each country's sovereign right to design and apply those policy tools that it deems most fit for the entry of inward investment. This is also the case for the increasing number of FDI screening mechanisms to protect national interests.*
>
> *This investment policy instrument has evolved significantly over the years. Originally, governments used FDI screening procedures for defense and other sectors strictly related to security. With the progress of technology and modern warfare, host countries added dual-use products and sophisticated cryptology systems as well as technologies and communication equipment.*
>
> *In a second phase, the concept of national security advanced from countering military threats to also protecting strategic industries and critical infrastructure. The reasoning behind this move is that the protection of core domestic economic assets may be as important for a country's well-being as the absence of military threats.*
>
> *A further explanation may be that governments considered some sort of FDI screening in this area as a necessary counterweight to earlier privatization of State-owned companies and infrastructure facilities. Extending the scope of screening was in part also a reaction to the increasing investment activities of foreign State-owned enterprises.*
>
> *The latest phase in FDI screening emanates from the unprecedented acceleration in technological development across industries with the new industrial and digital revolutions. Advanced countries that compete in this technological race may wish to protect domestic cutting-edge technologies that are considered key assets in the global competition against foreign takeovers.*

BASED ON THE LATEST GUIDELINES, EU MEMBER STATES ARE ADVISED

1. Member States may maintain their existing screening mechanisms, adopt new ones or remain without such national mechanisms.
2. In its Guidance issued in March 2020 the Commission has called upon all Member States to make full use of their FDI screening mechanisms and those Member States that currently do not have a screening mechanism, or whose screening mechanisms do not cover all relevant transactions, should set up a full-fledged screening mechanism.
3. 14 EU Member States currently have national investment screening mechanisms. Several are in the course of updating them, or adopting new ones.
4. The Regulation establishes some key requirements for national screening mechanisms:
    - Transparency of rules and procedures
    - non-discrimination among foreign investors
    - confidentiality of information exchanged
    - The possibility of recourse against screening decisions, and prevent circumvention by foreign investors

AVAILABILITY OF TOOLS (CONCEPTS, METHODS OR TECHNOLOGICAL TOOLS) FITTING THE GAP

[54] World Investment Report 2019

FDI is of significant interest from an economic perspective. Research, Business and Politics are all interested in the links and trends of FDI and the impacts on economic markets. World Investment Report 2018[55], 2019[56]. However, research did not provide a wide array of tools for assessing the risk of FDI within a specific market. Below is a selection of common tools and platforms that can be used to monitor and assess FDI and related restrictions.

Investment Map database - The Investment Map[57] database collects yearly FDI statistics for about 200 countries and detailed FDI sectoral and/or country breakdown for about 115 countries. The Investment Map helps Investment Promotion Agencies identify priority sectors and competing countries for foreign investments, as well as existing and potential foreign investors. Moreover, it helps companies identify potential locations for investment abroad.

Together with the other ITC Market Analysis Tools, Investment Map aims at enhancing information transparency in international trade and helping actors in developing countries taking the right decisions in a globalized and changing world.

FDI Markets[58] - a service from the Financial Times, is comprehensive online database of cross border greenfield investments available, covering all countries and sectors worldwide. It provides access to real-time monitoring of investment projects, capital investment, created jobs. There are tools to track and profile companies investing overseas, as well as conduct in-depth analysis to uncover broader trends.

The Foreign Direct Investment Regulatory Restrictiveness Index (FDI RRI)[59], developed by OECD, is consolidated index to measure restrictions of the countries applied to FDI. Index measures four types of statutory restrictions on foreign direct investment: (i) foreign equity restrictions, (ii) screening and prior approval requirements, (iii) rules for key personnel, and (iv) other restrictions on the operation of foreign enterprises.

OBSERVATION

From the initial research, there are no clear tools that support the ongoing analysis of the risks associated with FDI. Much of the discussion around FDI relates to the need for reciprocal relations and the avoidance of market imbalances. Also, with the increased scrutiny of foreign investments; better transparency and awareness of events related to the three risk framework (Moran) mentioned above, could be useful to conceptualize the changing landscape.

[55] https://unctad.org/system/files/official-document/wir2018_en.pdf
[56] https://unctad.org/system/files/official-document/wir2019_en.pdf
[57] https://www.investmentmap.org/home
[58] https://www.fdimarkets.com/
[59] https://goingdigital.oecd.org/en/indicator/74/

6. IDENTIFIED INNOVATIONS IN EU REASEARCH PROJECTS

Identified project (MI-ICT https://www.miict.eu/) is an ambitious example to develop a collaborative platform (IMMERSE) to address one of the most non-technical problems as integration of migrants/refugees. All such projects are at risk of being "just another system" which only partly fulfills hopes of the project owners. On the other hand, project developers seems to give special focus to the beneficiaries of the system, which gives hope for successful achievement of results.

6.1 ONLINE SYSTEM FOR FACILITATING EFFICIENT MIGRANT INTEGRATION

<table>
<tr><td colspan="2">Online system for facilitating efficient migrant integration
By developing a database system named "IMMERSE", the project plans to improve and customize the interfaces used to access key public services (Integration of Migrants MatchER SErvice) to better address the requirements of migrants and refugees. IMMERSE will capture the specific socio-cultural, economic and legal contexts of migrants that is shared with public authorities.</td></tr>
<tr><td>REFERENCE TO CAPABILITY GAP/NEED
- To facilitate migrant integration, to mitigate risks of social and cultural outcasting
- Applicable JRC domains as stated by the gaps/needs social/ societal; administration; information; culture; political
Applicable core theme(s) as stated by the gap/need
- CT3: Resilient Civilians, Local Level and National Administration</td><td>TYPE OF SOLUTION
- Technical: a software tool
- Social/human: to be used for efficient information collection and sharing, to enable better, in time quality decisions
- Organizational/process: cross departmental</td></tr>
<tr><td colspan="2">PRACTITIONERS
- Provide disciplines for which the solution is valuable:
Targeted to administration at local and central levels
- Provide the level of practitioners in the same discipline:
○ Ministry level (administration): departments engaged with the services provision and migrants' integration
○ Local level (cities and regions): departments engaged with the services provision and migrants' integration
○ Support functions to ministry and local levels (incl. Europe's third sector): n/a</td></tr>
<tr><td colspan="2">STATE OF THE ART
- Indication of Technology Readiness Level (TRL 1-9 index):n/a
- In which stage is the solution (research, technology, available innovation, proven innovation): early stage, project just started
- Expected time to TRL-9. n/a
- Expected time to market. 2-3 years</td></tr>
<tr><td colspan="2">DESCRIPTION OF THE USE CASE(S)
An ICT system that will facilitate integration of migrants by grasping large spectrum of information and providing them relevant information and services.</td></tr>
<tr><td colspan="2">IMPACT ON COUNTERING HYBRID THREATS
- Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.
Efficient integration mitigates risks of social or cultural outcasting
- Resilience/defensive/offensive. Increase resilience of migrants</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the solution?
ICT</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.? n/a</td></tr>
<tr><td>COSTS
- Indication of costs
Differentiate if possible in development, procurement and exploitation</td><td>COUNTERMEASURES
- Are there any foreseen / potential countermeasures that could degrade the effectiveness of the solution?</td></tr>
</table>

No information	no - **How durable is the idea (how long the idea is expected to be effective/useful?)** Efficient integration of migrants seems to be systematic need, long term

6.2 NATIONAL ECOSYSTEM FOR THE RECOGNITION AND ANALYSIS OF THE INFORMATION EFFECT PHENOMENA (NAAS)

Hereby selected project (NAAS http://www.lka.lt/en/research/research-projects/naas_1480.html) is an effort to bring academia, training and practitioners together by means of newly developed IT platform with the hope, that this collaboration will be instrumental for all stakeholders in achieving their aims, and will produce better results that otherwise would be possible.

Though the to-be-developed platform will be specifically designed to accommodate needs of hybrid threats analysis, we consider the main innovation to be a non-technical part. Developing collaboration model, including processes, use cases and alignment of motivations, aims to develop sustainable mechanism. This mechanism would be able to dedicate resources and attention to the longer term problems, which practitioners cannot afford. Additionally this would lead to better innovation uptake.

Academia would receive opportunity to work on relevant problems, with the pooled data and accessible spectrum of instruments.

At the same time, this collaboration platform will be instrumental in training of hybrid threats students and practitioners, integrating them to wider community.

<table>
<tr><td colspan="2">National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena (NAAS)
Hybrid threats is a new phenomenon which changes constantly, so the knowledge on it should be constantly updated, new experts trained, etc. NAAS aims to create an efficient and modern ecosystem of science and studies enabling higher education institutions to train public security specialists and carry out research activities, including information security, information and hybrid threat analyses, integrated (Internet and kinetic) information space monitoring and analysis of potentially criminal content. The newly developed ecosystem integrating technological, software and methodological instruments is intended for training the specialists of integrated electronic and physical space analysis and scientific research. The ecosystem will contribute greatly to more effective mitigation of the impact of hybrid threats at the national and international levels and ensuring public security.</td></tr>
<tr><td>REFERENCE TO CAPABILITY GAP/NEED
- Official strategic communication losing power - how today’s information environment effects knowledge?
- Distrust and stress in political decision-making
Applicable JRC domains as stated by the gaps/needs
social/ societal; administration; information; culture; political
Applicable core theme(s) as stated by the gap/need
- CT3: Resilient Civilians, Local Level and National Administration
- Future Trends of Hybrid Threats</td><td>TYPE OF SOLUTION
- Technical: this is a software enabled platform
- Social/human: to be used for data analysis, research, training and education
- Organizational/process: cross departmental – academia and hybrid threats practitioners (via representative organizations)</td></tr>
<tr><td colspan="2">PRACTITIONERS
- Provide disciplines for which the solution is valuable:
Targeted to academia and administration at local and central levels
- Provide the level of practitioners in the same discipline:
○ Ministry level (administration): departments directly responsible or related to hybrid threat mitigation</td></tr>
</table>

○ ***Local level* (cities and regions):** departments related to hybrid threat exposure ○ ***Support functions to ministry and local levels* (incl. Europe's third sector):** academia
STATE OF THE ART - **Indication of Technology Readiness Level (TRL 1-9 index)**: project just started, very early stage - **In which stage is the solution (research, technology, available innovation, proven innovation):** concept development stage - **Expected time to TRL-9. n/a** - **Expected time to market.** 2-3 years
DESCRIPTION OF THE USE CASE(S) Software platform will enable pool resources of academia and practitioners to share data, access and test tools, share know-how and pool resources for analysis of specific tasks. Strategic communication methodologies will be developed, tested and monitored on this collaborative platform.
IMPACT ON COUNTERING HYBRID THREATS - **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.** Development of hybrid threats analysis capability, development of strategic communications and other methodologies - **Resilience/defensive/offensive.** Increase analytical capabilities, increase efficiency of communication

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the solution?** ICT Cross departmental collaboration	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** n/a
COSTS	**COUNTERMEASURES**
- **Indication of costs** **Differentiate if possible in development, procurement and exploitation** This project is a pre-commercial procurement	- **Are there any foreseen / potential countermeasures that could degrade the effectiveness of the solution**? no - **How durable is the idea (how long the idea is expected to be effective/useful?)** Platform for knowledge sharing, data sharing, research facilitation and training should be viable long term

6.3 CYBERSECURITY SKILLS ALLIANCE - A NEW VISION FOR EUROPE (REWIRE)

This is a non-technical innovation in the field of cybersecurity skills (REWIRE https://www.efvet.org/portfolio-items/rewire/). Significant number of hybrid threats identified by practitioners are leveraging cyber-weaknesses as a vector for attacks. Overall, with the digitization of industries, infrastructures and personal life, cyber weaknesses will be increasingly more exploited for both non-hybrid and hybrid attacks. Closing the gaps in cybersecurity area overall will remain challenge for years to come in EU, as the need for cybersecurity professionals is increasing every year.

REWIRE project was selected as a just started endeavor to bring together pieces of scattered efforts in members states and EU, with the aim to develop European cybersecurity skills framework which would allow various stakeholders to talk to each other, to develop synchronized actions and to monitor progress in the whole area.

Cybersecurity Skills Alliance - A New Vision For Europe (Rewire)
REWIRE Skills Alliance is aiming to develop sustainable organization which would own and develop European Cybersecurity Skills Framework. This frameworks is aspired to become common dictionary for

academia, industry and policy makers to analyze situation with cybersecurity skills and take synchronized actions

REFERENCE TO CAPABILITY GAP/NEED	TYPE OF SOLUTION
- Weak level of digital security: digital security architecture, numerical technologies and encryption protocols - **Applicable JRC domains as stated by the gaps/needs** administration; cyber, infrastructure **Applicable core theme(s) as stated by the gap/need** - Cyber and Future Technologies	- **Social/human**: this is a multi-stakeholder organization that should enable concerted action in the field of cybersecurity skills development - **Organizational/process**: multi-stakeholder process facilitating update of the common body of knowledge (Framework) and its application across the various fields in academia, industry

PRACTITIONERS

- **Provide disciplines for which the solution is valuable:**
  For academia (to understand demand and design education for purpose), for industry (do understand skills gaps in their cybersecurity organization, plan and implement upskilling), for policymakers (to understand situation and take relevant policy decisions)
- **Provide the level of practitioners in the same discipline:**
  - ***Ministry level*** **(administration):** departments directly responsible or related to hybrid threat mitigation
  - ***Local level*** **(cities and regions):** departments related to hybrid threat exposure
  - ***Support functions to ministry and local levels*** **(incl. Europe's third sector):** academia, industry

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: project just started, very early stage, though relevant examples exists
- **In which stage is the solution (research, technology, available innovation, proven innovation):** concept development stage
- **Expected time to TRL-9. n/a**
- **Expected time to market.** 2-4 years for implementation

DESCRIPTION OF THE USE CASE(S)

European Cybersecurity Framework will act as a common dictionary for various stakeholders to communicate their needs, design services, recognize skills across the borders and take policy cations.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**

Successful project should facilitate development of cybersecurity skills, attraction of talent to cybersecurity profession and strategically enhance cybersecurity situation in EU.

- **Resilience/defensive/offensive.** Increase defensive and offensive cyber related skills and capabilities

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the solution?** Multi-stakeholder collaboration	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** n/a

COSTS	COUNTERMEASURES
- **Indication of costs** **Differentiate if possible in development, procurement and exploitation** n/a	- **Are there any foreseen / potential countermeasures that could degrade the effectiveness of the solution**? no - **How durable is the idea (how long the idea is expected to be effective/useful?)** REWIRE aspiration is to develop sustainable organization which would be relevant long term

7. CONCLUSIONS

EU-HYBNET Research Project and Innovation scan completed its first iteration and produced this document, a deliverable D3.7.

The scanning team analyzed scientific research landscape for the 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.

Furthermore, scanning did identify some of the EU research and other projects, which would contribute, if successful, in filling the identified gaps.

During the execution of the task, EU-HYBNET reached out to a number of EU funded projects. It is observed that communication with other project requires significant effort and time, so the work will have to continue through all EU-HYBNET project. Although even early encounters demonstrated that cross-disciplinary nature of hybrid threats is a very important factor that EU-HYBNET can bring to the table discussing collaboration with very subject focused projects. The discussion and strong aim to collaboration with the EC funded project INCLUDING (No. 833573) https://including-cluster.eu/ is an important demonstration.

The scanning task appeared to be very challenging, due to the very limited resources allocated and the vast gaps and needs, identified by practitioners in EU-HYBNET Task 2.1 "*Needs and Gaps Analysis in Knowledge and Performance*". On the task and work package level, the experience of scanning task execution will be discussed and evaluated, so that the lessons learned will be used for next iteration to do the work that is more efficient and produces results that are even more relevant.

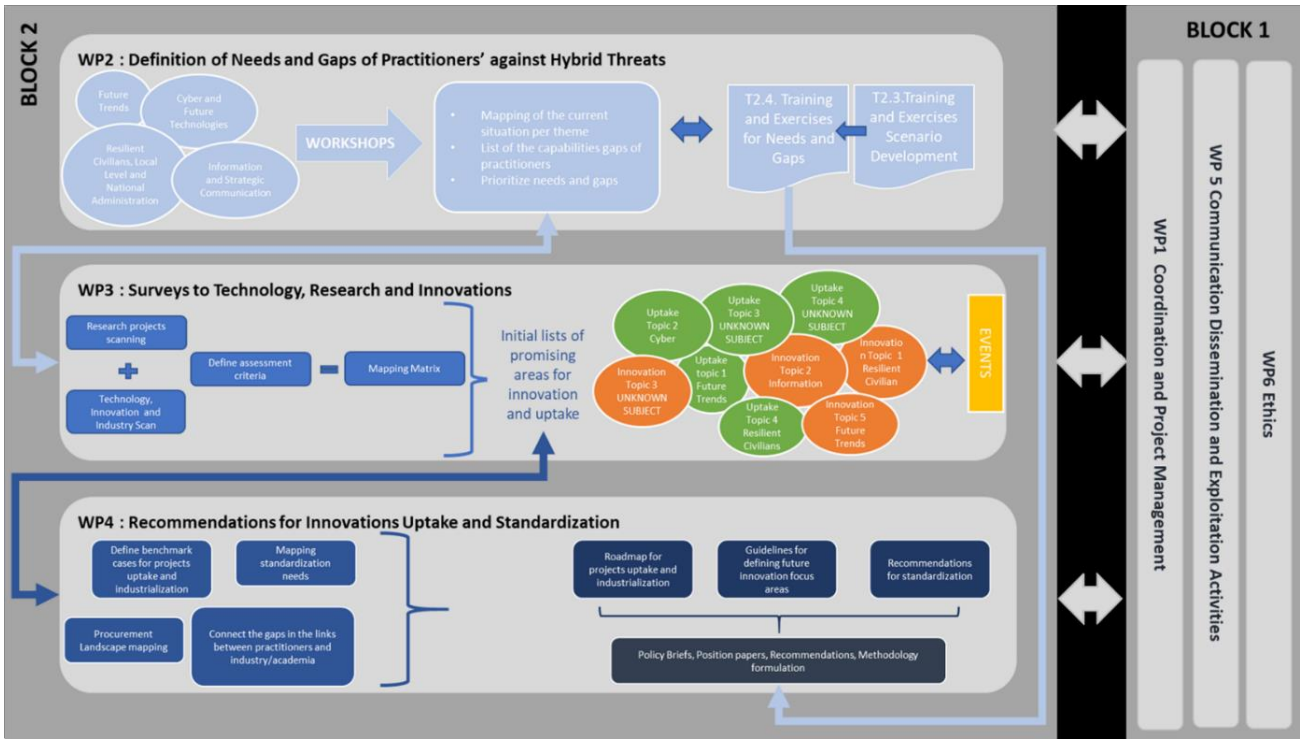
7.1 FUTURE WORK

The EU-HYBNET deliverable D3.7 "*First Report on Innovation and Research Project 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 (D3.7) has important 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*".

D3.7 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:



Not less importantly, D3.7 tried to analyze areas which lack research efforts, so that prioritization of research areas could be considered.

For overall EU-HYBNET project D3.7 will be instrumental for better understanding state of play of the fields identified by practitioners. This is extremely important because hybrid threats are a crosscutting domain.

D3.7 results demonstrate that clearly some of the areas call rethinking of hybrid threats dimension and overall relationships of hybrid threats community with other professional communities. This deliverable will serve as a basis for discussion in EU-HYBNET project how to reach out to other communities, how to develop relevant relationships

The D3.7 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 D3.7 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

Lastly, the importance of D3.7 to the future is that T3.3 will repeat the research and research projects scan to identified pan-European practitioners' and other relevant actors gaps and needs to counter hybrid threats, and hence the D3.7 works as example how to proceed in the work and what to change or improve, if seen necessary.

ANNEX I. GLOSSARY AND ACRONYMS

Term	Definition / Description
AI	Artificial intelligence
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
COMTESSA	Universitaet der Bundeswehr München
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
MIICT	ICT Enabled Public Services for Migration
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

Term	Definition / Description
PPP	Public Private Partnership
RISE	RISE Research Institutes of Sweden Ab
RTO	Research & Technology Organization
SCRM	Supply chain risk management
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
Hybrid CoE	The European Centre of Excellence for Countering Hybrid Threats
WSN	Wireless Sensor Networks

ANNEX II. REFERENCES

[1] European Commission Decision C (2014)4995 of 22 July 2014.

[2] Communicating EU Research & Innovation (A guide for project participants), European Commission, Directorate-General for Research and Innovation, Directorate A, Unit A.1 — External & Internal Communication, 2012, ISBN 978-92-79-25639-4, doi:10.2777/7985.

ANNEX III. EU RESEARCH PROJECTS

Project
MEDEA – Mediterranean practitioners' network capacity building for effective response to emerging security challenges https://cordis.europa.eu/project/id/787111 (iii) Push for the "co-creation" of security technology and capabilities innovations between practitioners and innovation suppliers, which is based upon their evaluation and prioritization on multi-criteria analysis (technology, operational and cost-benefit, etc.) and also linked to Human Development, Policy Making and Organizational Improvements in-terms of facilitating its use by the practitioners (iv) Establish and annually update the Mediterranean Security Research and Innovation Agenda (MSRIA), that identifies areas where security & defence research is needed and the establishment of recommendations for European Security & Defence technology investments.
I-LEAD – Innovation - Law Enforcement Agencies Dialogue https://cordis.europa.eu/project/id/740685 I-LEAD's focus is on the incapability of groups of operational Law Enforcement Agencies (LEA) practitioners defining their needs for innovation. This will be done in a methodological way, also with the help of the research & industrial partners supplemented by a broad range of committed stakeholders. I-LEAD will build the capacity to monitor the security research and technology market in order to ensure a better matching and uptake of innovations by law enforcement agencies with the overarching aim to make it a sustainable Pan-Europan LEA network. Earlier funded European research with a high technology readiness level as well as pipeline technologies will be closely monitored and assessed on its usefulness. Where possible a direct uptake from this research will be facilitated and implemented in the ENLETS and ENFSI networks supporting the action. I-LEAD will indicate priorities in five practitioner groups as well as aspects that needs (more) standardization and formulate recommendations how to incorporate these in procedures. As a final step, I-LEAD will advise the Member States through the existing EDBP-ESTP procurement group about how the outcomes of this project could be used in Pre-Commercial Procurement and Public Procurement of Innovation activities.
ARCSAR – Arctic and North Atlantic Security and Emergency Preparedness Network https://cordis.europa.eu/project/id/786571 The ARCSAR project will establish international best practice and propose innovation platforms for the professional security and emergency response institutions in the Arctic and the North-Atlantic. The focus is on increased interaction in targeted networks between the professional institutions, academia and the innovators in the preparedness service and equipment industry. The ARCSAR project will monitor research and innovation projects and recommend the uptake and the industrialization of results, express common requirements as regards innovations that could fill in capability and other gaps and improve their performance in the future, and indicate priorities as regards common capabilities, or interfaces among capabilities, requiring more standardization. The project will look into the need for enhanced measures to respond to composite challenges including surveillance of and mobilization

in case of threat situations, and emergency response capability related to search and rescue (SAR), environmental protection, fire fighting, and actions against terror or other forms of destructive action.

SAYSO – Standardisation of situational Awareness sYstems to Strengthen Operations in civil protection

https://cordis.europa.eu/project/id/740872

Handling the crises faced by modern societies often requires the coordination of multiple types of stakeholders from different countries. One of the key requirements to manage crisis is to have access to situational awareness (SA). However, current SA solutions (SAS) are not adapted to operate in cross-border contexts and present several shortcomings related to interoperability, data anagement/processing, decision making, standardisation and procurement. This hinders a reliable sharing of SA information. SAYSO will address these shortcomings and pave the way for the development of innovative European cost-effective Multi-Stakeholders SA Systems (MSSAS) which will provide practitioners with user-friendly solutions, providing a clear picture of the situation at hand with relevant advices. Addressing both the technical and human aspects of technology implementation, SAYSO will define the specifications of future MSSAS on the basis of practitioners' requirements and specify the corresponding Reference Architecture to support the integration of various data into a common operational picture. This architecture will support interoperability and allow the integration of legacy and future SAS. It will also be customisable to practitioners' needs and safeguard adequate privacy protection and data security levels. SAYSO will pursue the agreement and sustainable involvement of a community of practitioners, relevant suppliers and potential procurers, institutions and policy makers to obtain widely accepted results and prepare future procurement actions at EU level. SAYSO will develop a toolkit for MSSAS procurers, which will include tender documentation for SAYSO-compliant MSSAS and a SAYSO Procurers Handbook (with tools to evaluate MSSAS tenders and assess their compliance with the SAYSO specifications and existing standards). A registry of potential suppliers and procurers of MSSAS will be set up. Finally, SAYSO will deliver roadmaps for future MSSAS and standardisation.

FIRE-IN – The first European Fire and Rescue Innovation Network

https://fire-in.eu/en

alternative title SAYSO

Whether you are a Fire & Rescue expert, a technology provider or a researcher, register to engage with other experts through this collaborative platform. Here practitioners can find latest technologies and innovators can promote their solutions.

INCLUDING – Innovative cluster for radiological and nuclear emergencies

https://including-cluster.eu/

INCLUDING is seek to provide a full-fledged and comprehensive training in the Radioactive-Nuclear security sector at European level. Starting from the existing training resources of the Partners in the Consortium, in most cases developed in the framework of EC projects, INCLUDING aims to enhance practical know-how and to boost a European sustainable training and development framework for practitioners in the RN Security sector. Far from being a simple aggregation of entities separated geographically and with complementary expertise, INCLUDING is intended to be a cluster of facilities and resources pursuing a Federated Model in which individual components will cooperate together to provide a common framework for optimizing the exploitation of all the potentialities available in the Cluster.

NO-FEAR – Network Of practitioners For Emergency medicAl systems and cRitical care

https://cordis.europa.eu/project/id/786670

The emergency medical care in the EU is a fragmented chain including population, emergency medical services, volunteers, hospitals and cooperation with fire services, police and authorities. It needs to prepare to respond to new threats and assist casualties after security incidents. In response to this challenge, NO-FEAR proposes to bring together a pan-European network of practitioners, decision and policy makers in the medical and security fields. They will collaborate to achieve a common understanding of needs, as well as - in collaboration with academia and industries – increase the EU innovation potential that could better fill the operational gaps and recommend areas for future innovations.
NO-FEAR main objectives are to:
- create a long-lasting community of practitioners, interacting with a network of suppliers and academia,
- elaborate an innovation roadmap, with practical recommendations for uptake,
- advise relevant Research and Innovation projects,
- support market uptake of EU research results,
- issue policy and regulatory recommendations enabling collective procurement,
- indicate priorities for standardisation;
- support quick wins and practical short term results,
- implement a transactional dynamic portal providing fora, a catalogue, market place and flexibility to address new threats.
The project will be conducted by a consortium of 18 partners, of which 11 and the coordinator are practitioners, under the advice of the EC Community of Users. It aggregates the various dimensions of the project (acute care, operations and training), supported by the already large networks. To disseminate and exploit the NO-FEAR recommendations, an ambitious strategy will be implemented, including workshops, demonstrations and communication events every 6 months. This will enable knowledge sharing, build a common understanding and promote innovation uptake by organising technology showcases and demonstrations in a real practitioner environment.

ECHO – European network of Cybersecurity centres and competence Hub for innovation and Operations

https://cordis.europa.eu/project/id/830943

Cyber defence is vital for prosperity and security. The project ECHO aims to deliver an organised and coordinated approach to improve proactive cyber defence of the European Union, allowing the bloc to act in anticipation, defending against an attack on computers and networks. ECHO is developing a network through which the EU's Cybersecurity and Competence Centres can be best coordinated and optimised. This can help contribute to a lasting and sustainable development of cybersecurity skills, including increased research and experimentation for certified security products such as early warning systems and inter-sector technology roadmaps.

SPARTA – Strategic programs for advanced research and technology in Europe

https://cordis.europa.eu/project/id/830892

In the domain of Cybersecurity Research and innovation, European scientists hold pioneering positions in fields such as cryptography, formal methods, or secure components. Yet this excellence on focused domains does not translate into larger-scale, system-level advantages. Too often, scattered and small teams fall short of critical mass capabilities, despite demonstrating world-class talent and results. Europe’s strength is in its diversity, but that strength is only materialised if we cooperate, combine, and develop common lines of research. Given today’s societal challenges, this has become more than an advantage – an urgent necessity. Various approaches are being developed to enhance collaboration at many levels. Europe’s framework programs have sprung projects in cybersecurity over the past thirty years, encouraging international cooperation and funding support actions. More recently, the Cybersecurity PPP has brought together public

institutions and industrial actors around common roadmaps and projects. While encouraging, these efforts have highlighted the need to break the mould, to step up investments and intensify coordination. The SPARTA proposal brings together a unique set of actors at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity. Strongly guided by concrete and risky challenges, it will setup unique collaboration means, leading the way in building transformative capabilities and forming world-leading expertise centres. Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

CONCORDIA – Cyber security cOmpeteNce fOr Research anD Innovation

https://cordis.europa.eu/project/id/830927

Europe needs to step up its efforts and strengthen its very own security capacities to secure its digital society, economy, and democracy. It is time to reconquer Europe's digital sovereignty. The vision for Europe can only be to join forces across Europe's research, industry and public sector and to include all talents not just those that have representation in the EU mainstream or are within big organizations. Diversity and inclusion are keys for success. Europe has incredible coverage and talent in the area of IT and cybersecurity. The area of cybersecurity is geographically fragmented across Europe for competences, and often also technically fragmented with problem-specific development of security solutions. There is no doubt that excellent research exists in Europe. Nevertheless, it is a fact that this research does not result in IT products and solutions that contribute to the European Single Digital Market. On contrary, a lot of research, also financed by EU ERC grants, is tested on real data in large US companies that cooperate with them. Europe has to and is already rethinking this strategy. CONCORDIA addresses the current fragmentation of security competence by networking diverse competences into a leadership role via a synergistic agglomeration of a pan-European Cybersecurity Center. The vision of CONCORDIA is to build a community a strong cooperation between all stakeholders, understanding that all stakeholders have their KPIs, bridging among them, and fostering the development of IT products and solutions along the whole supply chain. Technologically, it projects a broad and evolvable data-driven and cognitive E2E Security approach for the ever-complex ever-interconnected compositions of emergent data-driven cloud, IoT and edge-assisted ICT ecosystems.

5G-ENSURE – 5G Enablers for Network and System Security and Resilience

31 October 2017

https://cordis.europa.eu/project/id/671562

5G-ENSURE will define and deliver a 5G Security Architecture, shared and agreed by the various 5G stakeholders. It will specify, develop and release an initial set of useful and usable security enablers for 5G. These enablers will be selected for their relevance in addressing some of the foremost security concerns in order to generate the trust and confidence necessary for 5G to be widely adopted and to deliver its promises through innovative business applications. The 5G-ENSURE project will also initiate a 5G Security testbed vision and initial set-up in which the security enablers will be made available. Moreover, the potential of the developed 5G Security enablers will be showcased and demonstrated in the context of carefully selected 5G security use cases (e.g. use cases related to cybersecurity and aerospace).

Coupled with this, 5G-ENSURE will be closely linked to the overall 5G PPP programme through active participation in common activities and fora. Specifically, 5G-ENSURE will be the project that creates and animates a dedicated 5G PPP Security Working Group to coordinate the various security-related activities.

5G-ENSURE is led by a strong consortium bringing together the appropriate and complementary skills, including standards involvement and deep telco understanding, along with an extensive network of

interested parties, and have a proven track-record in coordination. 5G-ENSURE will avail itself of the support of a group of international opinion leaders.

CIVIL NEXT –

https://www.civilnext.eu/

The European Union Global Strategy on Foreign and Security Policy (EUGS) has highlighted the need for the EU to further improve its civilian missions, by pursuing better communication, information-sharing, joint reporting, analysis and response planning between member state embassies, EU delegations, Commission services, EU Special Representatives and Common Security and Defence Policy (CSDP) missions.
The CIVILnEXt project supports the development of a solution addressing existing "fragmentation" and closing "gaps", to provide civilian CSDP missions with the next generation of secure and cost-effective information systems. Fully informed of contributing initiatives in civilian CSDP and EU external action, the project will aim to develop solutions leveraging on the results extracted from projects funded by the EU. The common challenge in CIVILnEXt is to develop, test and validate a cost-effective and interoperable operation control platform (OCP) that will support the conduct of civilian CSDP missions. The OCP will improve coordination in EU external action through better information exchange, situational awareness and operation control in diverse theaters of operation.
CIVILnEXt is a Pre-Commercial Procurement EU-funded project that teams up a group of 5 buyers and 9 technical and institutional organizations with significant experience in EU external policies.

MARISA – Maritime Integrated Surveillance Awareness

End date 29 February 2020

https://cordis.europa.eu/project/id/740698

Combating irregular migration, human smuggling, terrorism at sea, piracy, as well as arms and drug trafficking has become a high priority on Europe's security agenda. Securing the sea requires a day-to-day collaboration activities among European actors of maritime surveillance, Member States' administrations and European agencies principally, and a significant number of initiatives are being taken at EU level to address this challenge. The large amount of 'raw data' available today are not usable by systems supporting maritime security since they are not accessible at the same time and, often, they are not interoperable. Therefore, the overarching goal of MARISA project is to provide the security communities operating at sea with a data fusion toolkit, which makes available a suite of methods, techniques and modules to correlate and fuse various heterogeneous and homogeneous data and information from different sources, including Internet and social networks, with the aim to improve information exchange, situational awareness, decision-making and reaction capabilities. The proposed solution will provide mechanisms to get insights from any big data source, perform analysis of a variety of data based on geographical and spatial representation, use techniques to search for typical and new patterns that identify possible connections between events, explore predictive analysis models to represent the effect of relationships of observed object at sea. Enterprise and ad-hoc reporting and services, within the CISE context, will be provided to support users and operational systems in their daily activities, as well as presentation tools for navigating and visualizing results of data fusion processing. The involvement of 5 practitioners as full partners will allow on the one hand to align innovation to user needs, on the other hand to validate the toolkit through a number of trials addressing cross country/cross domain applications.

ANDROMEDA – An EnhaNceD Common InfoRmatiOn Sharing EnvironMent for BordEr CommanD, Control and CoordinAtion Systems

https://cordis.europa.eu/project/id/833881

Sharing data can make surveillance cheaper and more effective. Under the European Union's Common Information Sharing Environment (CISE), information may be shared seamlessly with a range of third actors, including police agencies and defence forces. It is making different systems interoperable so that data and other information can be exchanged easily via modern technologies. Already an important building block of the EU's overall maritime surveillance framework, CISE can also be extended to help secure land borders. The EU-funded ANDROMEDA project aims to extend the scope of CISE for land borders. The project will leverage on the developments, results and experience of the consortium from current and previous research projects (PERSEUS, CloseEye, MARISA, RANGER).

CARISMAND – Culture And RISkmanagement in Man-made And Natural Disasters

End date 30 September 2018

https://cordis.europa.eu/project/id/653748

As risks are not "objective" but socially and culturally constructed, disaster management which is aware, respects, and makes use of local cultural aspects will be not only more effective but, at the same time, also improve the community's disaster coping capacities. CARISMAND is setting out to identify these factors, to explore existing gaps and opportunities for improvement of disaster policies and procedures, and to develop a comprehensive toolkit which will allow professional as well as voluntary disaster managers to adopt culturally-aware everyday practices. This goal will be achieved by approaching the links, and gaps, between disaster management, culture and risk perception from the broadest possible multi-disciplinary perspective and, simultaneously, developing a feedback-loop between disaster management stakeholders and citizens to establish, test, and refine proposed solutions for culturally-informed best practices in disaster management. Whilst experts from a variety of fields (in particular legal, IT, cognitive science, anthropology, psychology, sociology) will undertake a comprehensive collation of existing knowledge and structures, a number of Citizen Summits and Stakeholder Assemblies will be organised. Systematically, CARISMAND will use an approach that examines natural, man-made and technical disasters, placing at the centre of attention specific aspects that affect culturally informed risk perceptions, eg whether disasters are caused intentionally or not, the different "visibility" of hazards, and various time scales of disasters such as slow/fast onset and short- and long-term effects. By organising six Citizen Summits (two per disaster category per year in two separate locations) where such disaster risks are prevalent , and three Stakeholder Assemblies (one per year) where the results are discussed through a wide cross-sectional knowledge transfer between disaster managers from different locations as well as from different cultural backgrounds.

IN-PREP – An INtegrated next generation PREParedness programme for improving effective inter-organisational response capacity in complex environments of disasters and causes of crises

https://cordis.europa.eu/project/id/740627

An INtegrated next generation PREParedness programme for improving effective inter-organisational response capacity in complex environments of disasters and causes of crises.

BE-AWARE – Enhancing decision support and management services in extreme weather climate events

https://cordis.europa.eu/project/id/700475

"In every disaster and crisis, incident time is the enemy, and getting accurate information about the scope, extent, and impact of the disaster is critical to creating and orchestrating an effective disaster response and recovery effort. The main goal of beAWARE is to provide support in all the phases of an emergency incident. More specifically, we propose an integrated solution to support forecasting, early warnings, transmission and routing of the emergency data, aggregated analysis of multimodal data and management the

coordination between the first responders and the authorities. Our intention is to rely on platforms, theories and methodologies that are already used for disaster forecasting and management and add the elements that are necessary to make them working efficiently and in harm under the same objective. The overall context for beAWARE lies in the domain of situational awareness and command and control (C2). The first phase concerns the forecast of the extreme condition and the relevant preparations. Once a disaster occurs, an initial assessment needs to be conducted as soon as possible to determine the scope, geographical distribution, and scale of the incident. Situational awareness means being able to accurately determine what has happened, what is happening now, and what will come next, all in order to plan and coordinate the most effective response possible with the resources available. This observation phase will lead to an orientation phase suggesting both an individual as well as collective “cognition” orientation to data that is sensed and communicated. Once orientation to the data (or the lack of it) occurs then a decision is made, ultimately resulting is the final step, which is “act”. The crisis management center is always striving or struggling to gain a sense of what is reality to be able to feel that he or she can make a decision that is the ""best possible"" given the circumstances."

PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people

https://cordis.europa.eu/project/id/826293

PANACEA will deliver people-centric cybersecurity solutions in healthcare. The Partners will execute on a leanly-orchestrated research workplan, which envisages continuous involvement of the end-user Partners at three European health care centres, including also devices utilised in remote care & homecare settings. Ultimately, PANACEA delivers two toolkits for cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices: the Solution Toolkit and the Delivery Toolkit. The first one comprisesfour technological tools (for dynamic risk assessment & mitigation, secure information sharing, security-by-design & certification, identification & authentication) and three organisational tools (for training & education, resilience governance, secure behaviours nudging). The second one, specifically supporting adoption of the solution toolkit, comprises two tools (methodology to evaluate the ROI of cybersecurity interventions, guidelines to adopt the solution toolkit and implement other ex-ante mitigation actions). The toolkit will benefit from ninePANACEA ambitious research goals, achieved by moving beyond the current state of the art in the strategic areas of dynamic risk assessment & mitigation (threat modelling, attack modelling, response management, visual analytics), blockchain for secure information sharing, identification/authentication (cryptographic authentication protocols, biometric recognition/digital identity, IoMT identification), secure behaviours decision models and influencers. Impact creation will be supported by designing and executing on an effective communication, dissemination and exploitation strategy involving all partners, from project onset. The PANACEA Consortium is committed, competent and complementary. The Consortium is led by a private hospital, supported by 3 research organisations, 3 large enterprises, 5 SMEs. Severalend-user scenarios, developed in Italy, Crete and Ireland, will provide a solid test-bed.

CITYCoP – Citizen Interaction Technologies Yield Community Policing

https://cordis.europa.eu/project/id/653811

End date 31 May 2018

Theories underlying community policing received new impetus with the recent advent of smartphones and social media and especially user-generated content (UGC) where citizens engage in closer interaction with their local community and law enforcement agency (LEA). The years 2010-2014 have seen a rapid upsurge of smartphone apps aimed at improving crime reporting and other forms of UGC and interaction associated with community policing. Yet these apps are characterised by a predominantly Anglo-Saxon approach with the largest number originating in the USA, a few in Canada, Australia and with the UK apparently the only major EU state where there has been some take-up of these technologies. CITYCoP sets out to find out why

the EU appears to be lagging behind although Community Policing is nominally a policy which has been put into action in a number of EU countries. It then goes on to develop a solution including a new smartphone app and on-line portal which are capable of being deployed in any European city while still retaining "local flavour" and diversity. These ICT solutions will also be designed from scratch to be fully compliant with strict privacy and data protection laws. A training scheme, including use of serious games, will be developed to assist training of officers and citizens in use of the app and portal. CITYCoP will benefit from a multi-disciplinary approach that will include the sociology of community policing as well as cognitive science perspectives of the citizen's interaction with community and LEAs through technology. The partners in CITYCoP build on long years of successful collaboration in EU projects dealing with UGC, smart surveillance and privacy (CONSENT, SMART, RESPECT) positioning CITYCoP solutions to achieve integration into smart city eco-systems. CITYCoP will pilot deployments of multi-lingual smartphone apps, portals and serious games training packages in Bucharest (Romania), Lisbon (Portugal), Florence (Italy), Sheffield (UK).

MEDI@4SEC – The emerging role of new social media in enhancing public security

https://cordis.europa.eu/project/id/700281

End date 31 December 2018

MEDI@4SEC focuses upon enhancing understanding of the opportunities, challenges and ethical consideration of social media use for public security: the good, the bad and the ugly. The good comprises using social media for problem solving, fighting crime, decreasing fear of crime and increasing the quality of life. The bad is the increase of digitised criminality and terrorism with new phenomena emerging through the use of social media. The ugly comprises the grey areas where trolling, cyberbullying, threats, or live video-sharing of tactical security operations are phenomena to deal with during incidents. Making use of the possibilities that social media offer, including smart 'work-arounds' is key, while respecting privacy, legislation, and ethics. This changing situation raises a series of challenges and possibilities for public security planners. MEDI@4SEC will explore this through a series of communication and dissemination activities that engage extensively with a range of end-users to better understand the usage of social media for security activities. MEDI@4SEC will seek a better understanding of how social media can, and how social media cannot be used for public security purposes and highlight ethical, legal and data-protection-related issues and implications. Activities centre around six relevant themes: DIY Policing; Everyday security; Riots and mass gatherings: The dark web; Trolling; and Innovative market solutions. MEDI@4SEC will feed into, support and influence changes in policy-making and policy implementation in public security that can be used by end-users to improve their decision making. By structuring our understanding of the impact of social media on public security approaches in a user-friendly way MEDI@4SEC will provide an evidence-base and roadmap for better policymaking including: best practice reports; a catalogue of social media technologies; recommendations for EU standards; future training options; and, ethical awareness raising.

TAKEDOWN – Understand the Dimensions of Organised Crime and Terrorist Networks for Developing Effective and Efficient Security Solutions for First-line-practitioners and Professionals

https://cordis.europa.eu/project/id/700688

End date 31 August 2019

Organized Crime and Terrorist Networks (OC/TN) are a major challenge for the European Union and many different stakeholder groups are involved in creating awareness, preventing, identifying and intervene in case of risk or threat. But in order to develop better strategies and instruments, we still need a deeper understanding of these phenomena.

TAKEDOWN therefore aims at generating such novel insights on OC/TN. In order to meet this challenge and to investigate this complex field of research a multidimensional modelling approach is used. The resulting, proprietary TAKEDOWN Model describes social, psychological, economic aspects as well as further

dimensions, activities and response approaches. A comprehensive empirical research combined with European and international expert knowledge ensures a valid and intuitive model.

The TAKEDOWN Open Information Hub targets first-line-practitioners and provides modular solutions and inductive materials. The public web platform helps individuals to navigate to the right third party reporting and help lines including an innovative crowd reporting application to report digital OC/TN cases.

The TAKEDOWN OC/TN Professional Solution Platform consists of various modules for law enforcement and homeland security departments. Designed with a flexible Platform as a Service (PaaS) architecture it combines knowledge materials and digital security solutions. Via the TAKEDOWN Security Dashboard information streams of native and third party applications are combined in an identification and issue management cockpit. The TAKEDOWN Professional Advisor supports experts on the selection of relevant approaches and security solutions to tackle OC/TN.

With this multi-level approach, TAKEDOWN will force a better understanding of OC/TN, develop modern approaches and solutions, and will finally lead to a more efficient and effective response on OC/TN and strengthen social cohesion at pan-European level.

INSPEC2T – Inspiring CitizeNS Participation for Enhanced Community PoliCing AcTions

https://cordis.europa.eu/project/id/653749

End date 30 April 2018

INSPEC2T projects' scope is to develop a sustainable framework for Community Policing that effectively addresses and promotes seamless collaboration between the police and the community. INSPEC2T approach bases its conceptual foundations on EU crime prevention and Member States specific Internal Security Policies, validated research results and best practices from cooperation between police and local, regional and national communities. This is perceived as an origin to apprehend special characteristics, particularities and determinants for trust between all stakeholders. INSPEC2T is focusing on a user-centric design and development approach, and has already mobilized and engaged a critical user group mass, in EU and abroad. With special emphasis on social media, it consolidates and modernizes bidirectional communication of stakeholders, using multi-level anonymity flags and having a clear understanding of acceptability issues. Driven from accommodated transnational and multicultural best practices, it adheres to an approach where social, cultural, legal and ethical dimensions are embedded into core user centric design specifications and implementation procedures. INSPEC2T will be demonstrated and validated in 5 EU cities by a wide range of relevant stakeholders. INSPEC2T engagement and active participation is stimulated through fully dynamic, interactive and immersive training Serious Game applications that empower players to familiarize themselves with the system, gain an intuitive understanding of its functionalities and motivate their engagement in Community Policing activities. Special focus will be given to Community Policing awareness raising activities for both police and citizens. The above activities and associated results, will provide a solid foundation for the evolution of the Next Generation Community Policing roadmap in Europe.

ESSENTIAL – Evolving Security SciencE through Networked Technologies, Information policy And Law

https://cordis.europa.eu/project/id/722482

End date 31 December 2020

Though security is a field of study capable of diverse applications in daily life, security science is a young discipline requiring larger inter-disciplinary effort. ESSENTIAL seeks to develop security science by addressing two of its main problems: the ad-hoc approach to security research and the growing complexity of the security environment. To do so, ESSENTIAL has set itself two main goals: a) to train inter-disciplinary security experts and professionals, to tackle security threats in a systematic manner and b) to increase societal

resilience and security by addressing in an interdisciplinary manner 15 research topics, each associated with long-standing problems in the field of security science ranging from modeling security perception and democratizing intelligence to improving security and privacy in data ecosystems.
ESSENTIAL will be the first programme of its kind that aims to jointly educate the next generation of interdisciplinary experts in security science, by uniquely exposing the 15 ESRs to: (1) theoretical knowledge and practical expertise in such areas as: (a) the policing and regulation of information-security technology, and (b) the implementation of policies and legal standards within computing and communication systems; (2) real-world environments in law enforcement, intelligence and industry; (3) strong academic guidance offered by highly qualified supervisors and mentors; (4) high tech research infrastructures; and (5) a diversity of interdisciplinary research events, such as workshops, conferences, summer/winter schools.
The ESSENTIAL consortium is built upon long-lasting cooperation relations among leading organizations coming from academia, international and national stakeholders and the private sector, many of whom have over 25 years of experience in contributing directly to national, European and UN technology-related policy making.

CF SEDSS II – Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) Phase II

https://cordis.europa.eu/project/id/789231

End date 15 August 2019

The objective of this proposal is to explore through the engagement of experts from the energy and defence sectors, the benefits that could be enabled in support of the European Commission's implementation of the Energy Efficiency Directive (EED), Renewable Energy Directive (RED), and Energy Performance of Buildings Directive (EPBD). Moreover the objective is further enhanced by its orientation to support the EU efforts for sustainability in line with prevailing policy and regulatory framework.
This proposal is highly relevant to the work programme given that the focus of the work will be on:
i. Energy Management,
ii. Energy Efficiency,
iii. Renewable Energy Resources, and
iv. the Protection of Critical Energy Infrastructure.
The deliverables of CF SEDSS II will also have the potential to generate relevant projects that could be possibly funded by the EC's related and applicable funding instruments according to the legislative and administrative rules in force at that time.
EDA will build on its experience in capability development, research and innovation, project management and consensus building with specific regard to the two core themes of the Consultation Forum. The work will be conducted under the umbrella of EDA's Energy and Environment programme, using, where possible, existing studies and networks to deliver quality products in the shortest possible time. The concrete multi-stakeholder work to be implemented, becomes increasingly relevant given that the scope of work will include identification, relation with and impact on wider EU policies, identifications of existing or missing relevant innovative funding instruments in the context of energy in the defence and security sector.

DRIVER+ - DRiving InnoVation in crisis management for European Resilience

https://cordis.europa.eu/project/id/607798

End date 30 April 2020

DRIVER+ starts from the experience that neither successful R&D nor strong end-user demand always lead to innovation in the Crisis Management (CM) domain. This is a problem since as societies become more complex, increasing scope and unpredictability of potential crises and faster dynamics of major incidents put increasingly stringent demands on CM. European CM capabilities already constitute a mature System of Systems; hence wholesale redesign would often be too costly and might critically destabilise existing CM

capabilities. Therefore DRIVER+ focuses on augmenting rather than replacing existing capabilities. DRIVER+ has three main objectives: 1) Develop a pan-European Test-bed for crisis management capability development; 2) Develop a well-balanced comprehensive portfolio of crisis management solutions, and 3) Facilitate a shared understanding of crisis management across Europe.

MINDb4ACT – Mapping, IdentifyiNg and Developing skills and opportunities in operating environments to co-create innovative, ethical and effective ACTions to tackle radicalization leading to violent extremism

https://cordis.europa.eu/project/id/740543

End date 31 August 2020

"MINDb4ACT is a collaborative project participated by 7 LEAs, think-tanks, reserach centres, universities, industry associations and NGO based in 10 Member States (Austria, Belgium, Denmark, Finland, France, Germany, Italy, Poland, Spain and United Kingdom). The project will align its research priorities with some of the most relevant issues already identified by the European Commission:
Priority 1. Systematizing the available knowledge and expertise to support strategic decision-making
Priority 2. Enhancing interdisciplinary fieldwork on terrorists' recruiting grounds, socialisation and techniques
Priority 3. Using big data in order to analyse the information related to the communication practices of violent radicalisation
Priority 4.Improving existing links between academia including non-EU researchers, policy-makers and other stakeholders
MINDb4ACT will contribute to such priorities for the improvement of current counter-violent extremism policies (CVEs) in the countries represented in the consortium (Austria, Belgium Denmark, Finland, France, Germany, Italy Poland, Spain and United Kingdom) and the generation of new ones connecting through collaboration ecosystems (innovative, open, participatory, user-centred environments) to co-design interventions such as research actions, exchanges, strategic-policy exercises, training courses and pilot projects based on social innovation and civic engagement schemes (a community of practice of 1,500 people). All actions will be developed in 5 specific domains: prisons and judiciary system; migration hotspots and asylum centres, schools, cities (peri-urban contexts) and the Internet and media. A special contribution of the project will be the integration of technology based practical solutions with the contribution of the industry.
As mentioned in the call, MINDb4ACT will NOT be “focused on studying the phenomenon of radicalization" but focused on “developing policy recommendations and practical solutions for end-users".

SENTER – Strengthening European Network Centres of Excellence in Cybercrime

https://www.senternetwork.eu/

The project “Strengthening European Network Centres of Excellence in Cybercrime“ (hereinafter – SENTER project, Reference No HOME/2014/ISFP/AG/7170) is funded by the European Commission under Internal Security Fund-Police 2014-2020 (ISFP).

The main goal of the project is to create a single point of Reference for EU national Cybercrime Centres of Excellence (hereinafter – CoE) and develop further the Network of national CoE into well-defined and well-functioning community. Project target groups are:

- LEA organizations: police, prosecutors, judges,

- Relevant NGO and mediation institutions,

- Education – police colleges, universities, competence

- Certification and qualification control bodies

- Science – Universities, hubs, clusters, R&D institutions or departments

- International – EUROPOL, INTERPOL, EC3

- Intersecting domains networks - InSafe, FIU.NET

ARMOuR – Large-Scale Experiments of IoT Security Trust

https://cordis.europa.eu/project/id/688237

End date 31 January 2018

The Internet-of-Things (IoT) is rapidly heading for large scale meaning that all mechanisms and features for the future IoT need to be especially designed and duly tested/certified for large-scale conditions. Also, Security, Privacy and Trust are critical elements of the IoT where inadequacy of these is a barrier to the deployment of IoT systems and to broad adoption of IoT technologies. Suitable duly tested solutions are then needed to cope with security, privacy and safety in the large scale IoT.
Interestingly, world-class European research on IoT Security & Trust exists in European companies (especially SME) and academia where even there are available technologies that were proven to work adequately in the lab and/or small-scale pilots. More, unique experimental IoT facilities exist in the EU FIRE initiative that make possible large-scale experimentally-driven research but that are not well equipped to support IoT Security & Trust experiments. But notably, Europe is a leader in IoT Security & Trust testing solutions (e.g. RASEN toolbox, ETSI Security TC, etc.) that can be extended to large-scale testing environments and be integrated in FIRE IoT testbeds for supporting experimentations.
The ARMOUR project is aimed at providing duly tested, benchmarked and certified Security & Trust technological solutions for large-scale IoT using upgraded FIRE large-scale IoT/Cloud testbeds properly-equipped for Security & Trust experimentations. To this, ARMOUR will: (1) Enhance two outstanding FIRE testbeds (> 2700nodes; ~500users) with the ARMOUR experimentation toolbox for enabling large-scale IoT Security & Trust experiments; (2) Deliver six properly experimented, suitably validated and duly benchmarked methods and technologies for enabling Security & Trust in the large-scale IoT; and (3) Define a framework to support the design of Secure & Trusted IoT applications as well as establishing a certification scheme for setting confidence on Security & Trust IoT solutions.

SAFFRON – Semantic Analysis against Foreign Fighters Recruitment Online Network

http://www.saffron-project.eu/en/home/

The aim of SAFFRON is to build a system able to support early detection of foreign fighters recruitment by terrorist groups in Europe, with a focus on ISIS and Al-Qaeda. It consists in studying recruitment communication strategies on social media (e.g. narrations, argumentative tropes and myths used), and their evolution in time, as well as identification of needs, values, cultural and social contexts of the target.

A specific “social media guide” will be developed in order to give detailed guidelines to the social media team for managing different communicative situations, user generated contributions and reactions. Furthermore, a “social media crisis protocol” will be identified in order to identify critical communicative situations and design correct interactions.

The main objectives of SAFFRON are:

Objective 1 : Deliver and test a tool to be used by all relevant players (which are also part of the consortium) to identify in a timely fashion both all internet activities of direct and indirect recruitment of Foreign Fighters and all signals (weak or strong) pointing at radicalization of single individuals

Objective 2 : Analyze the recent trends about recruitment of young European people by terrorist groups

Objective 3 : Analyze the online communication strategy of terrorist groups and develop a social media campaign to contrast their propaganda

EU-ECSEL

https://www.ecsel.eu/

The ECSEL Joint Undertaking - the Public-Private Partnership for Electronic Components and Systems – funds Research, Development and Innovation projects for world-class expertise in these key enabling technologies, essential for Europe's competitive leadership in the era of the digital economy.

Through the ECSEL JU, the European industry, SMEs and Research and Technology Organisations are supported and co-financed by 30 ECSEL Participating States and the European Union.

ECSEL JU launches annual Calls for Proposals for research, development and innovation projects. You can find information about open Calls, and about projects that were selected from previous Calls, on the respective pages.

SECREDAS – Cyber Security for Cross Domain Reliable Dependable Automated Systems

https://cordis.europa.eu/project/id/783119

Goal : SECREDAS aims to develop and validate multi-domain architecting methodologies, reference architectures & components for autonomous systems, combining high security and privacy protection while preserving functional-safety and operational performance.

Internal Security Fund - Police

https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police_en

The Internal Security Fund (ISF) was set up for the period 2014-20, with a total of EUR 3.8 billion for the seven years. The Fund will promote the implementation of the Internal Security Strategy, law enforcement cooperation and the management of the Union's external borders. The ISF is composed of two instruments, ISF Borders and Visa and ISF Police.

Achieving the key objectives

The ISF Police component of the Internal Security Fund will contribute to ensuring a high level of security in the EU. Within this general objective, the Funds' activities will focus on achieving two specific objectives:

Fight against crime: combating cross-border, serious and organised crime including terrorism, and reinforcing coordination and cooperation between law enforcement authorities and other national

authorities of EU States, including with EUROPOL and other relevant EU bodies, and with relevant non-EU and international organisations;

Managing risk and crisis: enhancing the capacity of EU States and the Union for managing effectively security-related risk and crisis, and preparing for protecting people and critical infrastructure against terrorist attacks and other security related incidents.

For the 2014-20 period, slightly over EUR 1 billion is available for funding actions under the ISF Police instrument, of which EUR 662 million will be channeled through shared management and EUR 342 million through direct management.

Concrete actions to be funded through this instrument can include a wide range of initiatives, such as setting up and running IT systems, acquisition of operational equipment, promoting and developing training schemes and ensuring administrative and operational coordination and cooperation.