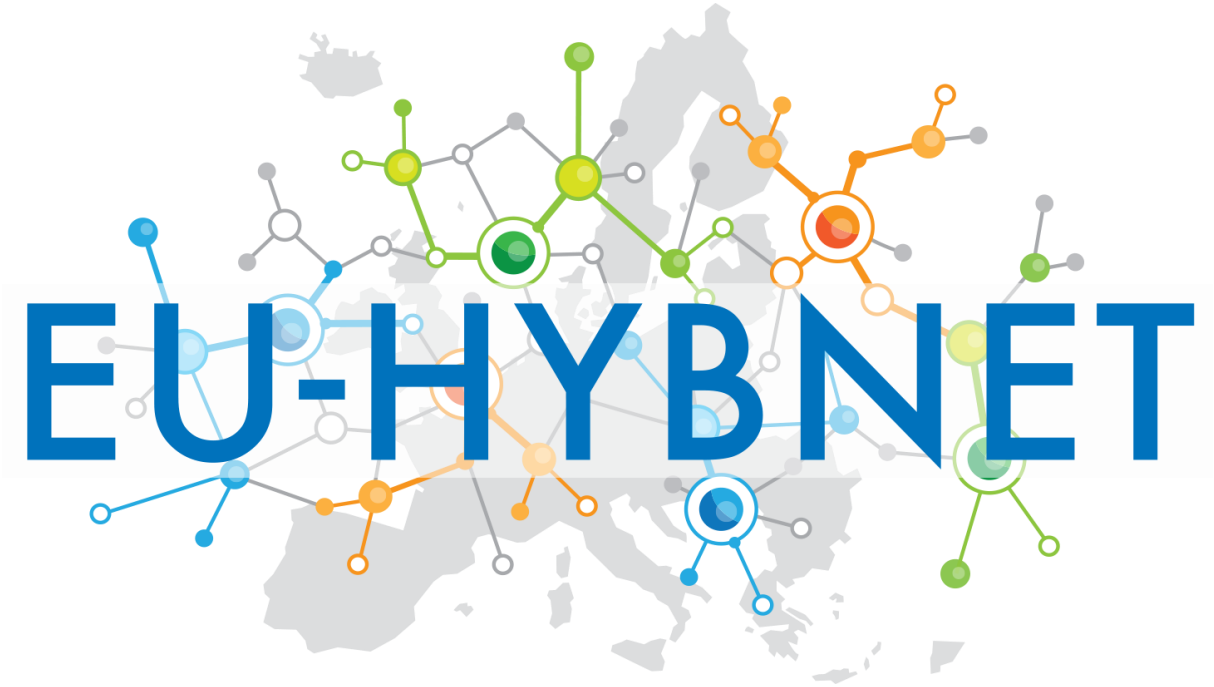

TRAINING AND EXERCICE, SCENARIO DELIVERY

DELIVERABLE 2.17

Lead Author: KEMEA

Contributors: HybridCoE,LAUREA, TNO,NL MoD, ZiTiS

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

D2.17 TRAINING AND EXERCISE, SCENARIO DELIVERY

Deliverable number	**D2.17**	
Version:	**1.0**	
Delivery date:	**31/3/2021**	
Dissemination level:	**Public**	
Classification level:	**n/a**	
Status	**Final Version**	
Nature:	**Public Report**	
Main author(s):	**Athanasios Kosmopoulos**	**KEMEA**
Contributor(s):	**Maria Kampa**	**KEMEA**
	Mirela Rosgova	**KEMEA**
	Athanasios Grigoriadis	**KEMEA**
	Päivi Mattila	**LAUREA**
	Gunhild Hoogensen Gjørv	**UiT**
	Edmundas Piesarskas	**L3CE**
	Rubén Arcos	**URJC**
	Anja van der Hulst	**TNO**
	Okke Lucassen	**TNO**
	Emma Lappalainen	**HCoE**
	Maxime Lebrun	**HCoE**
	Margriet Drent	**NLD MoD**
	Michael Meisinger	**ZITIS**

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	11-12-2020	KEMEA	Table of Contents
0.2	11-1-2021	KEMEA	Scenario outline
0.3	27-1-2021	KEMEA, LAUREA, HCOE, TNO	Vignettes outline, Deliverable first draft
0.4	30-1-2021	KEMEA	Update on document based on discussions
0.5	2-2-2021	HCOE	Update on structure
0.6	10-2-2021	KEMEA, LAUREA, HCOE, TNO, MoD	Update on vignettes based on new outline
0.62	19-2-2021	KEMEA, LAUREA, TNO, ZITIS, UiT, MoD	Update of vignettes
0.7	25-2-2021	KEMEA	Updated version based on comments received & write the deliverable introductory and final section
0.8	2-3-2021	KEMEA, L3CE, TNO	Ready for internal and external review
0.81	5-3-2021	RISE	Comments sent to KEMEA
0.82	8-3-2021	EOS	Comments sent to KEMEA
0.9	9-3/2021	KEMEA	Update based on comments received by external and internal reviewers
0.95	24-3-2021	EU-HYBNET Security Advisory Board review (Hybrid CoE, Laurea, PPHS, KEMEA)	EU-HYBNET Security Advisory Board review (Hybrid CoE, Laurea, PPHS, KEMEA)
0.96	31-3-2020	KEMEA	Update based on comments received by Innovation Manager & Project Coordinator
1.0	31-3-2020	Laurea	Final review

DISCLAIMER

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

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

TABLE OF CONTENTS

FIGURES

1. INTRODUCTION

1.1 DELIVERABLE OVERVIEW

This deliverable aims to present the work carried out in the frame of the preparation of the training activities of the H2020 EU-HYBNET project.

The aim of the current document is to prepare the exercise/training material that will be used to test the most promising innovations (technical and non-technical) to identified gaps and needs under each one of four core themes. The D3.3-*First Report on Improvements and Innovation* and D3.7- *First Report on Innovation and Research Project Monitoring* deliverables have provided the innovations that address the short list of the gaps and needs for the EU-HYBNET practitioners, available from D2.9 – *Deeper Analysis, delivery of short list of Gaps and Needs*, and in this regard should be tested. The scenario preparation and the training structure are two important aspects that will be fed to T2.4 – *Training and Exercises for Needs and Solutions for Gaps* so as to arrange the actual training and to start planning the evaluation of the innovations and the training itself. The evaluation of the innovations will serve as the basis for WP4 in order to know what will be stated as innovation uptake recommendations. All the aforementioned aspects are depicted in the image below:

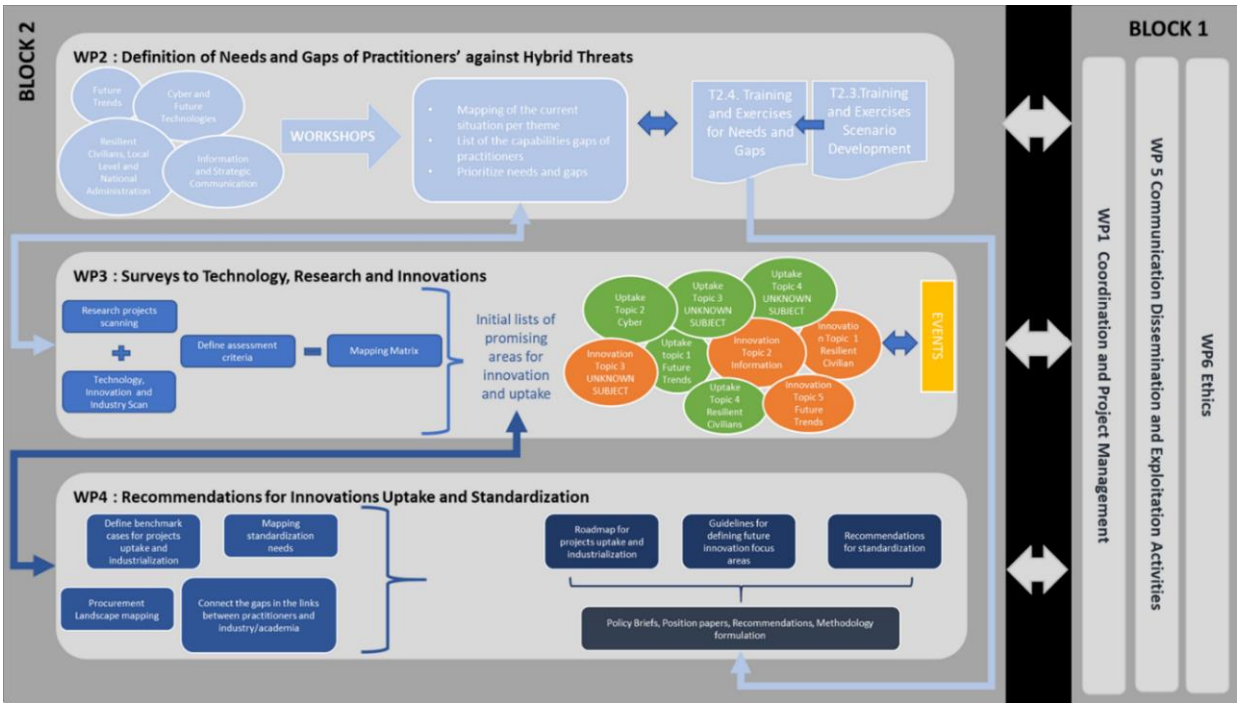

Figure 1: EU-HYBNET structure of Work Packages and Main Activities

In more detail, following the relevant work in identifying the short list of the gaps and needs in countering hybrid threats, as well the analysis of the available technological and non-technological solutions under T2.2 and WP3 respectively, D2.17 will serve as the basis in order to:

1. build the objectives of learning and training that will be performed under Task 2.4;
2. develop the scenarios that will be used for the training and exercise delivery taking into account all four Core Themes: [1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication] and select the innovations to be tested during the training.
3. set the tools to be used to achieve the objectives as well as the evaluation methodology framework.

Nonetheless D2.17 does not directly deliver results to certain EU-HYBNET project objectives (OB), still D2.17 strongly supports other EU-HYBNET Task to deliver results especially to:

- OB 6.4 : To empower European practitioners, industry, SME and academic actors' capacity to counter hybrid threats by offering relevant trainings and materials
- OB 7.1 : To share information on EU-HYBNET activities and training possibilities among European stakeholders
- OB 2.2 : To define innovations that can overcome the identified gaps and needs in certain focus areas in order to enhance practitioners (priority), industry, SME and academic actors capabilities
- OB 2.4 : To develop a roadmap of the requirements for on-going research and innovation necessary to build the preferred system of the future for confronting hybrid threats

The named Objectives are following and closely related to training arrangements and innovation testing and selection.

1.2 DEFINITIONS

Hybrid threats: Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties." [1] Hybrid threats can be characterised as coordinated and synchronised actions that deliberately target democratic vulnerabilities of states and institutions through a wide range of means. The aim is to influence different forms of decision making at institutional, local, regional and state levels to favour and/or achieve strategic goals while undermining and/or hurting the target. To effectively respond to hybrid threats, improvements in information exchange, along with breakthroughs in relevant research, and promotion of intelligence-sharing across sectors, and between the EU and its MS and partners, are crucial[2].

According to the joint framework on countering hybrid threats[1], while definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept of the framework aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. Diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

Practitioners at different levels: The EU-HYBNET H2020 project follows the European Commission definition of practitioners which states that "a practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection." In addition, practitioners in the hybrid threat context are expected to have a legal mandate to plan and take measures, or to provide support to authorities countering hybrid threats[3].

Therefore, EU-HYBNET practitioners are categorized as follows: i) ministry level (administration), ii) local level (cities and regions), iii) support functions to ministry and local levels (incl. Europe's third sector). EU-HYBNET includes practitioner partners from all these levels and its primary focus is on civilian security issues.

Training: is teaching, or developing in oneself or others, any skills and knowledge or fitness that relate to specific useful competencies. Training has specific goals of improving one's capability, capacity, productivity, and performance.

Table-top Exercise: A tabletop exercise is an activity in which key personnel assigned emergency management roles and responsibilities are gathered to discuss, in a non-threatening environment, various simulated emergency situations.

Scenario: a coherent, internally consistent, and plausible description of a potential future trajectory of a system to assess current practice, screen new opportunities, and improve the design and implementation of policy responses[4]. Within a training, a scenario builds on different assumptions about future developments and the effects of measures. The purpose of a scenario creation is to understand the future trajectories' impact on the system, when no action is taken or when alternative options are considered, and uncertainties associated with complex dynamic systems. One scenario can serve different purposes and it can be constructed from multiple sources, even multiple other scenarios (e.g., external inputs, narratives, or model simulations).

[1] Joint Framework on Countering Hybrid Threats, Join (2016) 18 Final, European Commission
[2] EU-Hybnet Description of Action, Coordination and Support Action, Grant Agreement No 883054
[3] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/3156
[4] Gómez et al. 2017

Vignettes are brief stories or scenarios that describe hypothetical characters or situations. Stories must be believable and appear as realistic as possible to participants. This means that the vignette needs to be relatable for the participant. Vignettes need to contain sufficient context for respondents to have an understanding about the situation being described but be vague enough to for participants to provide additional factors which influence their decisions. It is important that the stories presented in the vignettes are easily understood, internally consistent and not too complex.

1.3 STRUCTURE OF THE DELIVERABLE

This document includes the following chapters:

Section 1 includes the objectives of this report, some important definitions and the deliverable structure description.

Section 2 introduces the aim of the exercise and the exercise methodology in order to give the reader a better overview of the rational of the training.

Section 3 presents the EU-HYBNET exercise details, i.e. the aim, the tool to be used and the necessary concepts.

Section 4 provides the background scenario as well as information regarding the actors and organisations that are involved.

Section 5 presents the four vignettes that will be used for the training event.

Section 6 outlines the proposed methodology for measuring the impact of the EU-HYBNET training and how this will be achieved.

Section 7 provides the conclusion of the current document while **section 8 recommends** the future work that needs to be done until the actual implementation of the training.

2. TRAINING METHODOLOGY

In the context of EU-HYBNET training, the wargaming approach was chosen. A wargame is a type of strategy game that realistically simulates warfare, as opposed to abstract strategy games such as chess. Wargaming may be played for recreation, to train military officers in the art of strategic thinking, or to study the nature of potential conflicts. Many wargames recreate specific historic battles, and can cover either whole wars, or any campaigns, battles, or lower-level engagements within them. Many simulate land combat, but there are wargames for naval and air combat as well.

Wargaming in its modern form originated in Germany in the 1820's. Over the next two centuries, the armed forces of most nations employed various forms of wargaming for training and planning purposes, and wargaming was generally accepted across the military by the mid-twentieth century.

However, up to now there is no single, commonly accepted, definition of 'wargaming'. NATO defines a war game as: a simulation of a military operation, by whatever means, using specific rules, data, methods and procedures[5]. The importance placed on the decisions of the wargame players, not contained in the NATO definition, leads to the working definition of wargaming contained in the Red Teaming Guide[6]: A scenario-based warfare model in which the outcome and sequence of events affect, and are affected by, the decisions made by the players.

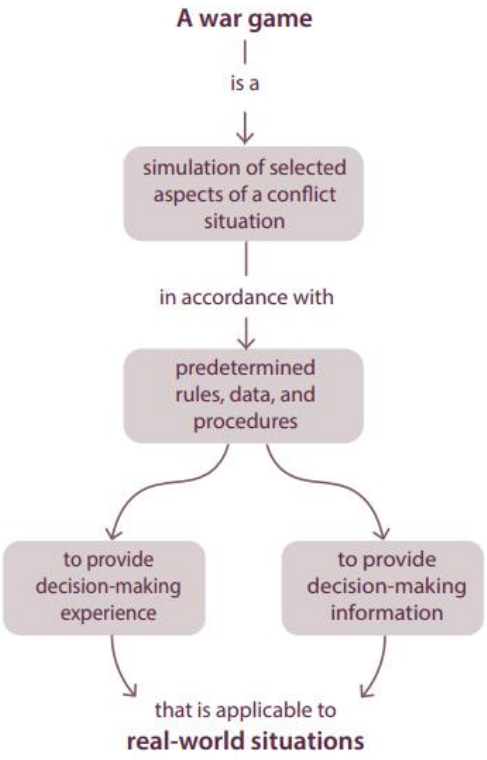

Figure 2 The general purposes of wargames[7]

In this context, a wargame, which is a recognized red teaming tool, serves as a process of adversarial challenge and creativity, delivered in a structured format and usually umpired or adjudicated. Wargames are dynamic

[5] https://nso.nato.int/natoterm/Web.mvc
[6] Development, Concepts and Doctrine Centre (DCDC), Red Teaming Guide, 2nd Edition, 2013, Lexicon.
[7]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

events driven by player decision making. As well as hostile actors, they should include all 'oppositional' factors that resist a plan. At the core of wargames are:

- the players;
- the decisions they take;
- the narrative they create;
- their shared experiences; and
- the lessons they take away.

In this regard, training ('learning') wargames are a 'fitness programme for thinking', enabling practice in the conceptual elements of command and control. In common with all training methods, a wargame is best considered in terms of a holistic life cycle, as shown in Figure 3.

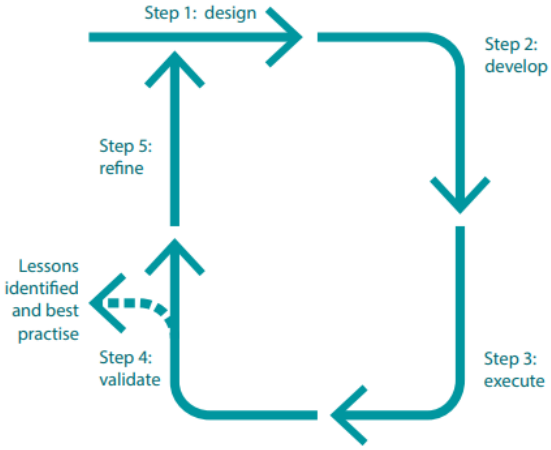

Figure 3 Wargame training process[8]

The stepwise approach that needs to be followed for the implementation of the first step i.e. the design of the wargame training, which is the purpose of the current document, is described below:

1. Specify the aim and training objectives. (section 3)

2. Identify how the outputs will be used and integrated. (section 3)

3. Identify the people to be trained, their roles and the decisions they will be expected to make. (see section 5)

4. Determine the desired effects on the players, and the exercise activities required to create these. (section 3)

5. Determine the scenario, and any specific vignettes, required to enable the training execution. (section 4,5)

6. Identify the tool needed to enable these structures and processes. (section 3)

8. Create an evaluation methodology of the training (section 6)

All the aforementioned are analysed in the context of the EU-HYBNET training in the upcoming sections.

[8]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

3. EU-HYBNET EXERCISE OVERVIEW

3.1. AIM OF THE EXERCISE & OBJECTIVES

The aim of the exercise is to face participants, acting at various levels of responsibility and decision making in a given state / multinational context with a series of disruptions (accidents and threats) in order to make apparent the different policy, strategic, operational and tactical dilemmas that arise for the organisation or system in crisis. In this content wargaming was considered the appropriate training approach. **The exercise depicts a system whose essential means are affected by the threats to such a degree that the resilience of the system does not suffice to manage the system in crisis.**

This setting utilizes and operationalizes the main **gaps and needs** in countering hybrid threats that were identified throughout WP2, and the EU-HYBNET training event is expected to discover new gaps and needs through practice. The scenario depicts various organisations that form a system in crisis confronted to a set of external actors. In this context, the participants will be requested to test a series of innovation solution possibilities (identified under WP3), whether technical, social, material and immaterial, in order to assess their opportunity, fitness, utility and readiness to help organisations manage the crisis and solve the dilemma they face.

3.2. DTAG

A DTAG is a seminar type wargame, used to assess potential innovations and their impact on hybrid campaigns and the operating environment. A Disruptive Technology Assessment Game (DTAG) will be used to test the innovations identified in WP3 in a realistic setting. The DTAG essentially allows the deployment of innovations (available in D3.3 and D3.7), or so-called Ideas of Systems (IoSs) as described in WP3 (Deliverables D3.3 and D3.7) within a realistic operational context. That is, to understand the operationalization of the innovation, its impact on the operational environment, the potential vulnerabilities adversaries might exploit and thus allow countering of the innovative measure and finally, how to anticipate such countering. The DTAG format was originally developed by an international team of researchers from NATO countries through NATO's Science and Technology Organisation in 2010. The overall method is described in the DTAG handbook [5] as supplied by NATO's Allied Command Transformation.

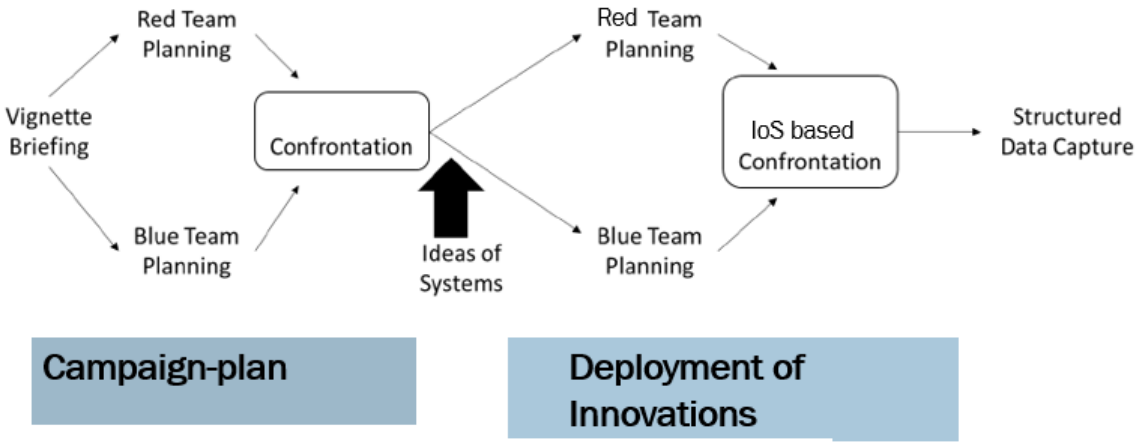

Figure 4: DTAG concept

A DTAG uses a scenario and one or more vignettes (see section 4,5) to sketch hybrid challenges within a realistic future operational environment.

With reference to Figure 4, a DTAG assumes a BLUE (friendly or allied forces) and a RED (adversarial) team that both are asked to create a campaign plan a series of challenges. A confrontation follows which helps to inform the teams on the BLUE Course of Action (CoA) and the possible countering by RED. This process aims to help participants understand the vignette, its challenges, the teams' objectives and the potential CoAs, it creates a baseline from which to work. Then cards with the Ideas of Systems (the Innovations) are being introduced. Now the BLUE teams select the relevant Innovations and aims to implement the Innovations in their campaign plan. They describe 1) how they implement those IoSs, 2) why, 3) what the implications are for their campaign plan and finally 4) the possible counter measures by RED they would anticipate. The RED team attempts to undermine the BLUE campaign by countering it, if possible, by exploiting possible vulnerabilities within the IoSs applied.

There will be structured data capture by analysts taking notes during the discussion, by means of forms that participants will fill out during the operationalization of the IoS and by means of a structure's discussion during the validation phase.

3.3. CONCEPTS

Organisations in crisis - organisations in crisis are defined by their mission and values that they are founded upon. The main objective of organisations is to defend these respective values. The objectives of organisations are allocated per their fields of competence: the objectives aim at fulfilling these values. In other words, **organisations in crisis defend their values by pursuing objectives that are responding to the dilemma they face**. *The implementation of those objectives is hampered by sources of risk that lie in accidents or threats.* Organisations to this end, make use of tangible and intangible means.

Objectives of organisations - participants following the scenario and each of the vignettes must respond to a series of objectives, related to the organisation / system in crisis that they represent. The **main objective is to maintain and safeguard the organisation / system's core values and interests while facing dilemmas caused by the unanticipated nature of events.** Participants have at their disposal the IoSs cards of the DTAG that present innovation solution possibilities (tangible and intangible means) in order to achieve their objectives while balancing their values and interests within the specific crisis management needs. DTAG cards are perceived as those means that enable organisations to preserve their objectives.

Risk mitigation as means to pursue the following objectives:

- impact reduction
- occurrence probability reduction
- reduction of destructive / lethal force
- reduction of attractiveness and feasibility.

In this context, each organisation / system that its participants use the vignettes has the objective to assess the specific needs of the situation and has specific requirements for situational awareness. The cards at their disposal are given to balance their objectives**.**

Translating the methodological framework of people-processes –technology into the EU-HYBNET exercise we can define the following:

People = participants; processes = objectives / values / interests assessed; technology = technical and non-technical innovation solution possibilities.

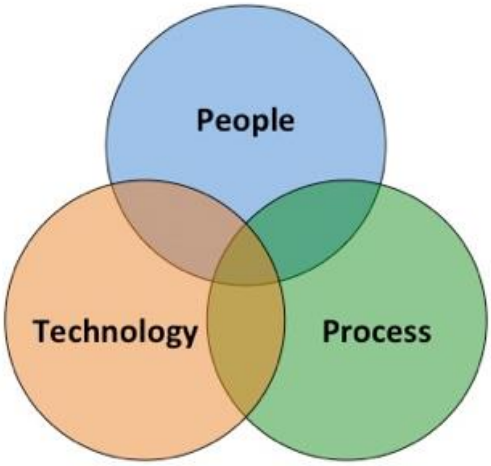

Figure 5 Methodological Framework of people-processes- technology

4. EU-HYBNET SCENARIO

The ultimate goal of building scenarios, whether they originate from models, stakeholder participation, or as it is often the case both, is to assess outcomes from alternative future trajectories, through model analysis and planning with stakeholders, to inform decision making. A more specific goal is to assess the response of the involved practitioners to alternative future trajectories, based on model analysis or expert knowledge. The scenarios should include the different views of the stakeholders on possible alternative future developments that are hard to predict and the assumptions behind the scenarios must be made transparent. The scenarios need to represent different kind of challenges and alternatives to deal with them.

The EU-HYBNET scenario and vignettes portray a crisis situation, giving opportunities to hybrid threat actors in leveraging societal and other vulnerabilities in order to further their strategic objectives while acting under the threshold of detection and circumventing political attribution, using a variety of means that have the characteristic to offset and upend anticipations and predictions of policymaking, crisis management and contingency management.

More specifically, the scenario simulates an outbreak of an influenza-like illness transmitted from bats to pigs to people that eventually efficiently transmits from person to person, leading to a severe pandemic. The pathogen and the disease it cause, are modelled largely on SARS, but it is more transmissible in the community by people with mild or no symptoms.

Below the chronological sequence of the events until the pandemic outbreak in M0 is outlined.

M-1,5month: reports of mystery killer disease in Vosechia.

During the last two weeks, in the small town of Scenariotown approximately 5 kilometres from the capital Scenariocity there have been five unconfirmed reports for several cases of severe, influenza-like illness. It was reported that the majority of the people who have fallen ill, have developed very serious symptoms, and two patients have already died.

At the same time, a local blog was running a front-page article reporting that a bus driver witnessed a family with three children travelling from Scenariotown to Scenariocity mainly because, as they told him, "children were getting ill and are dying" in their town. Rumours spread via local medical association representatives that several staff members of the main town hospital, to which the ill people have been transferred for treatment, have refused to get into close contact with the patients because they were afraid of catching the disease themselves. The disease appears to have developed quickly and infected a number of family members and friends in a matter of a few days.

M-1month: virus spreads outside of the established containment zones in Vosechia.

Following the aforementioned reports and the increasing number of patients, citizens started to panic. Some went into isolation voluntarily, while others refuse even to accept that the virus actually exists. The mayor of Scenariotown decided to establish a containment zone around the town. At the same time, the government of Vosechia has confirmed reports of two additional incidents in the suburbs of the capital Scenariocity.

The government has reassured citizens that the containment operation was successful in preventing the spread of the virus and that the new clusters in the Scenariocity occurred before the start of the establishment of the contamination zone. Moreover, it was decided that the containment zone will be expanded to include the two new clusters. There have been no reported cases in any other countries. Since the start of the outbreak in Scenariotown two weeks ago, more than 800 people have been hospitalized and more than 60 of those have died.

Rumours via local TV stations are spreading information that a number of neighbouring countries are in the process of closing their borders with Vosechia. Initial surveillance and screening measures are in place at regional and international airports as well as major border crossings.

Following a request from the Vosechia government, the WHO (World Health Organisation) and CDC (center for disease control) have mobilized a team from Geneva and Atlanta, which has been deployed to the containment zones to assist the Vosechia government in monitoring the situation.

M-0,5month: virus spreads outside of Vosechia.

The disease has started spreading outside of Vosechia. The WHO has officially reported that the disease started in pig farms in Vosechia, quietly and slowly at first, but then started spreading rapidly from person to person in the low-income, densely packed neighbourhoods. The WHO warned of the possibility for the situation to escalate into a pandemic.

M0: WHO declares pandemic phase 6

40 days after the first confirmed cases of the novel influenza virus in Vosechia, the virus has spread in more than 80 countries, with most countries affected to some degree or another. As a result of the current situation, the WHO have officially declared pandemic phase 6.

M+ 0,5month: pandemic initial phase

The numbers of people showing serious symptoms due to infection increases rapidly, something that has alarmed medical experts throughout the globe. Although not official, media report that the virus has an infection rate of about 40-45% and the case-fatality rate is approximately 10%. In an attempt to limit the spread of the virus, many governments have taken preventive measures such as the closure of schools, minor curfews, a ban on gatherings and obligatory usage of face masks by citizens. Restrictive measures are met with increasing opposition by populations as the memory of the COVID19 pandemic is still vivid with its economic and social consequences. Citizens appear to be anxious about the adequacy of supplies.

Some citizens have started opposing any potential general lockdowns. Since the whole human population is susceptible, during this initial phase, the cumulative number of cases increases exponentially, doubling every day. And as the cases and deaths accumulate, the economic and societal consequences become increasingly severe.

4.1. ACTORS AND ORGANISATIONS

Vosechia is a Member State (MS) of **X** Union. The global pandemic is putting a strain on the Member States' governments of X Union. X Union decision making is based on a delicate balance between intergovernmental and supranational processes, with deep integration in all matters societal and political. X union constitutive treaties entrust the directorate of the union to watch and safeguard the interests of the union as such, through legislative and non-legislative means. The role of the directorate of the union is to make proposals and gather consensus for decision-making among the members of X union. Calls for a greater strategic role of X union in its environment and the region have intensified in recent years because of severely deteriorated relations with **federation Y**.

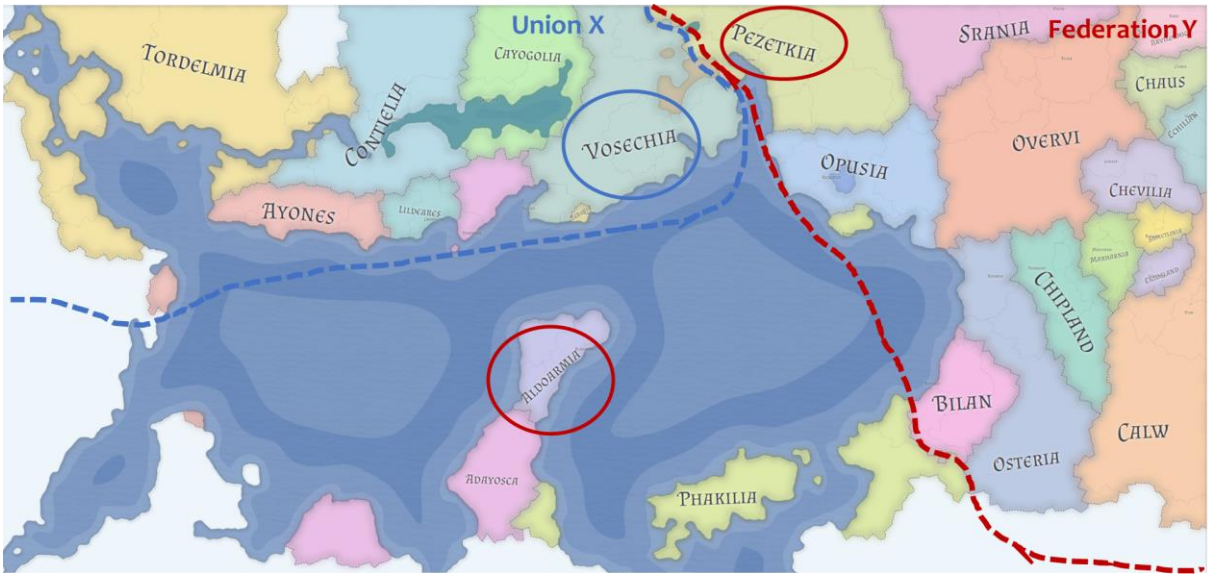

Figure 6 Actors' map

Federation Y has recently been suspected to have temporarily encroached the territory of an X Union member state during a naval exercise, claiming mistaken coordinates usage. On the other hand, Aldoarmia (another adversarial nation) has revived an old maritime delimitation dispute with an X Union member state. Aldoarmia tries to take advantage of the immigration issue that puts further pressure in X Union in order to gain leverage. X Union council made up of its members' heads of state and governments adopted conclusions calling the directorate of the union to devise and implement measures to streamline a strategic attitude to X Union crisis management in order to enhance situational awareness, coherence of national measures, communication among X Union member states and contributing to closing gaps and vulnerabilities for destabilization and coercion throughout X Union. In consequence, the directorate of the union has taken the decision to set up a dedicated task force "strategic union."

Pezetkia is a member state of federation Y. Federation Y pursues a global agenda to present itself as an essential stakeholder in any security crisis, hoping to gain additional international influence. Interests of federation Y mix diplomatic, economic, political and military concerns as well as social and societal stability imperative to consolidate the regime at home. It relies on a delicate balance of revisionism abroad in order to serve the domestic agenda while managing margin of manoeuvre and credibility as powerbroker. The chief strategic objective of federation Y is to consolidate its own authoritarian style of government by relativizing liberal democratic counter-examples in the eyes of its population. It is of primary importance for federation Y to portray the X union negatively, underlining or staging its failures, problems and contradictions. The degree of polarization of public opinion in X Union and the fragmentation of the media landscape present a series of opportunities in order to distribute information that feeds into Y's narrative.

The political impacts of the pandemic crisis are being felt. Several X union member states have integrated far right and far left populist political parties and movements in government, either as part of or heading government coalitions. The social and economic effects of the pandemic crisis have increased unemployment rates, social exclusion, and territorial fragmentation between urban and rural areas. The continued migratory pressure on the external borders of X union is putting an additional strain on public finances of the majority of X union member states while it accentuates cultural clashes, fear and intolerance in many X Union member states and severe social fabric cleavages are being observed. This constitutes a series of factors that explain a widespread political distrust towards governments and expertise, which runs as a continuous thread in elections throughout X union member states. While far rights and lefts populists occupy junior coalition partner roles,

politics tend to be more polarized and fuelled with multifactorial grievances, characterized by more regular outbreaks of violence.

Regarding the political scene of the MS Vosechia during the global pandemic period, one of the main parties of Vosechia is the right-wing populist Party X, with close ties to Pezetkia, which advocates harder border control during this pandemic, and gradual separation from the X Union. Party X has even surpassed the ruling Party Y, which currently heads the governing coalition of Vosechia. Apart from the aforementioned parties of Vosechia, there is also a small anti-refugee political party W which claims that refugees are not welcome to Vosechia. Vosechias statistical bureau has shown that citizens trust in government has fallen to an all-time low.

While the new pandemic deepens a climate of populistic distrust, ambiguity and institutional stress, security tensions in X union neighbourhood with strategic intimidation, destabilization and coercion attempts, global economic trade disputes and retaliation measures put to test X union strategic autonomy for the first time.

5. VIGNETTES

The exercise is divided into four vignettes that depict variations enabling to deepen situational settings, arrange different levels of decision making and dilemma solving, thereby distributing a series of technical innovations and social / policy ideas per relevance. Importantly, each vignette features a specific organisation engaged in a defensive situation to manage the crisis.

The following chapters, each one addressing one core theme, are composed by a short introduction followed by a table where the core theme addressed is mentioned as well as the targeted needs, linking this way each vignette with the outcomes of D2.9. "DEEPER ANALYSIS, DELIVERY OF SHORT LIST OF GAPS AND NEEDS". On the same table, the indicative targeted audience, involving organisations from the EU-HYBNET Consortium and the Stakeholders' Group, is introduced. Finally, the prior knowledge needed for the exercise participants is described.

Following the above, the reader can find the background information for each vignette, the three injects and the vignette's specific information (risk, objectives, organisations). At the end of each chapter the innovations that will be used as DTAG play cards are described in detail involving potential events that could arise from their usage as well as possible RED counteractions.

5.1. VIGNETTE 1: STRATEGIC INTER-AGENCY COORDINATION – NEED FOR DAMAGE ASSESSMENT AND CONTINGENCY MANAGEMENT AT STRATEGIC LEVEL.

This vignette depicts a situation in which critical infrastructure and critical supply chains would be targeted by a state or non-state threat actor. The scale effect of disruption is dire.

The participants are manning an inter-agency strategic coordination body with an operational role: the mission of the Inter agency strategic coordination body is to respond to the disruptions, manage ensuing contingencies, communicate efficiently to the civilian population in order to maintain coherence among agencies, responders and create the conditions for crisis management and resilience of society.

The vignette sets **infrastructure and supply chains disruptions suspectedly caused by a hostile/threat actor, with domino and scale effects in a context of elections and extremely polarized politics.** The participants / actors in this scenario are expected to apply the tools / innovations suggested at the end of the vignette, at their respective level of competence and within their fields of competence.

The expected outcome of the use of these solutions is better **situational awareness, sharing tools and specific cooperation** procedures to access specific instructions on what to do. Better management of contingencies and **containment** of scale and domino effects, of the disruption (how to avoid spill over effects as driving goal of contingency management). This is mainly an operational level vignette, in which practitioners will be requested to respond to guidelines (prior knowledge) given by strategic level.

Context of extreme polarization of society hampers any communication based on unknowns, puts stress on the governments of X union. Postulate that the innovations proposed had not yet been utilized by X union in a real time crisis.

Core theme	Targeted Context(s)
CT1: Future trends of hybrid threats	1. Official strategic communication losing power. 2. Big data and high connectivity as a new "power" source. 3. Increasing strategic dependency of critical services and assets.

Target audience	Prior knowledge
Select the target audience from the following: (1) Practitioners I) ministry level (administration),	Communication and sharing information procedures from governments to citizens.

II) local level (cities and regions), III) support functions to ministry and local levels (2) academic representatives (3) industry high level representatives ***N.B.*** *all training participants are coming from the EU-HYBNET consortium and Stakeholder Group.* Here is suggestion of the participants: **<u>Consortium</u>** Practitioners (**all**) Industry, SME (**all**) RTO, research association, organisations (**all**) • Finish Border Guard • Ministry of Justice and Security in the Netherlands • Tromso Police District Tromso, Norway • Ministry of the Interior Finland • Systematic • Expertsystem • Ardanti • Soprasteria • Fraunhofer-IVI • SafeCluster • Tecnoalimenti • CeSI - Centro Studi Internazionali • European Security and Defence College (ESDC) • European Health Management Association (EHMA) • CSIC - Spanish National Research Council, Research group on Cryptology and Information Security (GiCSI) • Ukrainian Association of Scholars and Experts in Field of Criminal Intelligence	Understanding of horizontal communication needs in state administration and with citizens and regions Dependency of critical infrastructures and critical strategic level assets Data aggregates and micro targeting in politics.

The outbreak of pandemic occurs when Vosechia is preparing for elections. The X Union MS Vosechia is about to hold parliamentary elections in three months. One of the main parties is a right-wing populist Party X, which advocates for harder border control during this pandemic, and gradual separation from the X Union. The right-wingers have so far been in opposition but have throughout the pandemic gained a strong position according to recent polls. Party X has even surpassed the ruling Party Y, which heads the governing coalition.

Pezetkia would benefit from the success of the Party X. The Party X shares many fundamental value presuppositions with Pezetkia and Federation Y in general. Most importantly, it actively questions international commitments besides the ones with Federation Y.

The actor is not especially skilful in manipulating the information environment of Vosechia. Vosechia has been aware of Federation Y information operations for many years and has consolidated the media environment. However, the pandemic has hit the country hard, and people's sentiments are increasingly negative towards the government led by Party Y. The economic downturn has caused crushing unemployment and business bankruptcy. Unprecedented levels of distrust among the population towards the government are fuelling an election campaign marred by a concerning increase in violence against journalists, politicians, and scientists. The pandemic provides an exceptional **opportunity** for the actor to disturb the Vosechia information environment ahead of elections by spreading disinformation through various channels. It aims primarily for deepening confusion and dissatisfaction towards the sitting government, to make Party X look better in comparison. The

underlying message tends to reinforce the idea that Party X would be the only political alternative when all other parties and political authority figures would have let Vosechia be hit harder than it should have been by the pandemic. The campaign builds on a powerful narrative that some of the decisions to curb the virus spreading have disproportionately hurt businesses and livelihoods.

INJECT 1: COORDINATED ATTACK ON HOSPITAL AND ARSON ON MIGRANT CAMP, CONFUSING GOVERNMENTAL COMMUNICATION.

The Vosechia's hospitals are reaching the limit of their capacity to provide intensive care for seriously affected patients. The hospital staff is overworked and under significant stress. Their capability to take care of the basic IT security is compromised: the sense of urgency and pronounced need to know the latest news and instructions leads healthcare workers to not follow basic security precautions when browsing through e-mails. Ransomwares infects hospitals' IT systems, and often the ransoms are paid.

The main university hospital in the capital of Vosechia has been hit with an exceptionally serious attack that encrypts the hospital computers and diagnostic equipment. As a result, thousands of appointments are cancelled, and patient safety is endangered. The healthcare staff are not able to access their devices, access patient medical records or share MRIs, X-rays or blood tests. Vosechia's road traffic operator simultaneously reports a critical fault in its monitoring and control systems for road traffic, rendering traffic lights on a default orange mode. Rescue call standards are quickly overwhelmed with intervention requests on road traffic accidents, and hospitals are hampered by massive bottlenecks and delays for incoming Emergency Response admissions. Media reports indicate that a massive migrant camp on the outskirts of the capital has been set on fire by arson. Members of a prominent right-wing violent extremist groups have been spotted near the camp before the outbreak of the fire.
The combination of road traffic disruption as well as the concomitant fire on the migrant camp fuel suspicions of a coordinated campaign. The facts point to the involvement and incitement of a specific adversary state actor that has benefited from the destabilization of Vosechia. It is not known who is behind the massive attack on hospital systems, but its sophistication and magnitude point towards a state actor. The country in question is speculated to be Aldoarmia.

Tools (more in subchapters below):

- Resilient democracy infrastructure platform
- Smart message routing and notification service (SMRNS)

INJECT 2: SUPPLY-CHAIN DISRUPTION FOLLOWING ATTACK ON AUTOMATED POWER GRID TIME MANAGEMENT DEVICES.

Two days into the disruptions at the hospital during which the backlog of patients keeps weighing heavier, as its systems are still not restored to their full operational capacity. The main cities of X Union start experiencing a series of repeated blackouts due to a persistent attack on the time measurement devices of automated power grids. Some key data centres upon which transnational critical supply chains rely, are also affected by the repeated power outages – it causes a substantial disruption in the provision of goods in supermarkets for consumers. The decision from abroad independent company X to halt supply to X Union because of those disruptions fuels a strong reprobative sentiment among population which further opens criticism on the ruling party Y and its agenda on the generalization of quantum computing in services throughout X Union.

The time device power grid disruption might cause other cascading effects.

Tools (more in subchapters below):

- Early / Rapid Damage Assessment System

- Critical Infrastructure Resilience platform
- Resilient democracy infrastructure platform

INJECT 3: POLITICAL HYPER-PERSONALIZED ADVERTISEMENT.

Several communication campaigns, advertisements, jokes, conspiracy theories, which mostly take the form of memes seem to follow a series of precise target patterns to a diversity of audiences. Various social media platforms are filled with content that in creative and humoristic ways undermines government communication. Social media users report the ads to be extremely targeted, corresponding to their searches and appealing to very specific details. Social media platforms remain deaf to calls for exposing the financing sources of those ads in order to trace the origins of a coordinated campaign. Three months till the elections, those micro targeted messages effectively misbalance the political campaigning fairness but as they are not openly political and most often strike a humoristic note, social media platforms reject calls to take down those contents. Opinion polls suggest however that party X has taken a decisive lead over all other political parties, while forecast for voter turnout is keeping heading lower and lower.

Tools (more in subchapters below):

- Countering disinformation with strategic personalized advertising (by government actors)

VIGNETTE SPECIFICS

ORGANISATION

Interagency coordination in governmental and regional level with executive competences and focus to follow government - citizens communication procedures, knowledge of critical infrastructure supply chain and cyber security situational awareness and sharing posture context.

RISKS

- Poor management and implementation of existing procedures and consequently their misuse at the requested time.
- Citizens' dissatisfaction with decisions leading them to ignore restrictions and recommendations, as these be explained and perceived in a confusing and ambiguous manner.
- Problems between organisations in sharing information and risk management cooperation at strategic level.
- Additional burden to governments and administrations as to address additional expenses and clarification needs.
- Political issues and diplomatic pitfalls may delay the communication that is needed.
- Intricate communications and cybernetic strategies may emerge not only in governmental level but also at hospitals and immigrant camps.
- Various issues among MSs may trigger several uncontrolled situations (e.g. over-power of media companies to share information that is propaganda like e.g. humoristic images of certain political parties that is to lead the party to loose respect among citizens).

OBJECTIVES

- Set the conditions for comprehensive damage assessment and building solid and flexible situational picture.
- Making hospital IT systems working back to normal.
- Alleviating the immediate pressure / backlog of cases.
- Develop communication elements to the population in order to divert and alleviate the pressure.

- Develop communication to signify that the government is in control of the situation, reassuring messaging to solve initial communication hiccups.
- Countering hyper personalized political campaign.
- Identify critical assets and infrastructures.
- Develop plans and procedures from top (X Union – Governments) to bottom (organisations, industry and citizens).

MEANS – INNOVATIONS AS PLAYCARDS IN DTAG

INNOVATION 1 - RESILIENT DEMOCRACY INFRASTRUCTURE PLATFORM (OFFICIAL COMMUNICATION TO MITIGATE INFRASTRUCTURE AND CRITICAL SUPPLY CHAINS DISRUPTIONS)

Possible uses of innovation 1

The scope of the platform is to provide expert advice on how to behave during emergency and crises situations informing target audiences. It can also be used to provide online official announcements to the public by the government agencies and information on the availability of essential public services.

This IoS card can be used in inject 1 and 2 as an app and citizens are requested to download it into their cell phones in order to ensure accurate information sharing between government and citizens regarding the coordinated attack which has taken place in hospitals, traffic lights and power grids and the fact that government agencies are working in order to restore them. Moreover, guidelines will be circulated in order to avoid moving around in the city with the exception of an emergency until the aforementioned issues have been resolved. This card will facilitate the Vosechia citizens to have access to real information from a trusted source. A challenge for this card will be that media will not cooperate with this.

Possible events

- Citizens are suspicious about the information received through this platform and turn to other sources in order to verify them.
- Media start questioning the usage of this platform and the pure intention of Vosechia's Government.
- Conspiracy theories start to spread about the Government's initiative to deploy the aforementioned platform.

Possible RED counteractions:

- Fake news starts to spread that the Government cannot handle the situation and the country undergo a severe crisis.
- Hack the resilient democracy infrastructure platform system in order to stop general public information

INNOVATION 2 – EARLY / RAPID DAMAGE ASSESSMENT SYSTEM

"Rapid damage assessment" enables first responders and the responsible organisations to assess in real-time the expected structural damage and identify possible expected impacts. The algorithms for an automated rapid damage assessment system can automatize the reaction process during a severe event i.e., Propose automated reaction, optimize response (areas in green can continue to operate, areas in yellow integrity can be assessed automatically, whereas the red areas should be investigated in detail before entering operational mode). When fed with real time now casting or forecasting data instead of a scenario hazard, the platform is an early or rapid damage assessment system respectively, thus providing the unique capability to initiate efficient response actions, right after (in case of now-cast data) or even before (in case of forecast data) the occurrence of catastrophic events.

Possible uses of innovation 2

This card can be used during inject 2 by Vosechia authorities to evaluate the damage caused in their infrastructures and respond timely (right after the event) and efficiently. This IoS card could provide rapid identification of the damage sources, optimal response to emergency, reduced reaction time, more efficient organisation of assistance and rehabilitation, increased reliability of damage and loss estimates and information from diverse data sources in common formats standardized across the Union X. A major challenge with card is that end users of Vosechia may be reluctant to share information using this tool.

Possible events

- The response to the incidents may not be successful due to the severity of the attack. The citizens in view of inability of the Government to respond to this major crisis start losing their trust. Party X takes advantage of this destabilization, to promote Pezetkia's political agenda within Vosechia.
- Citizens start questioning the purpose of such tools and translate them to a way of abusing the freedom of society.

Possible RED counteractions:

- Pezetkia actors hack the system in order to obtain the operational picture and gain valuable information about the vulnerabilities of the power grid supply chain and the hospital in the view of another attack.
- Pezetkia actors start flood social media with fake news to point out that Vosechia uses resilient democracy infrastructure platform to control the citizens while the system has cost over a million euros and has proven its inability to protect the country from similar incidents.

INNOVATION 3 - SMART MESSAGE ROUTING AND NOTIFICATION SERVICE FOR SHARING THE OPERATIONAL PICTURE TO EVERY AGENCY INVOLVED IN THE RESPONSE AT EVERY LEVEL OF COORDINATION. (A SMART INFORMATION SHARING MECHANISM)

The service enables the sharing of the information among involved actors at every level of coordination enabling collaborative response and the proper alerting of personnel/ practitioners/ stakeholders. Based on the EMCR, responding teams will be capable of sharing the operational picture (information related to the management and response to an emergency) by routing messages. This way relevant information will reach the appropriate persons at every level of coordination in a timely manner. It can be evolved and integrated to share the operational picture to every agency involved in the response at every level of coordination.

Possible uses of innovation 3

This IoS card can be used in inject 1. This card can assist the authorities who are responsible for road traffic operations, hospitals and migration camps in governmental and regional level, and ensure that they are able to share information about their incidents and coordinate their response. The tool will allow them to take the appropriate actions and initiate strategically planned operations and responses. A major challenge with card is that end users of Vosechia may be reluctant to share information using this tool.

Possible events

- End users are reluctant to share the operational picture through this service.

Possible RED counteractions:

- Adversarial actors hack the system in order to avoid the coordinated response of Vosechia to the incidents.
- The same actors start spreading fake news that the country is close to a chaotic situation and promote as the only solution the election of Party X.

INNOVATION 4 - COUNTERING DISINFORMATION WITH STRATEGIC PERSONALIZED ADVERTISING (BY GOVERNMENT ACTORS)

The intended use is to influence the behaviour of citizens in a positive way by leading them with personalized advertisement to the right information provided by a trustworthy source. Concerning disinformation, it is expected that the delivery of related information on the right point can help stabilize the social comprehension. As can be seen, personalized advertisement can be used both in an offensive or defensive manner.

By using this tool, the relative statement will be given by a trustworthy organisation about the topic the user was interested in, and this way disinformation could be weakened. In fact, as a trustworthy channel provides the user with the requested information, the user will not search for other sources.

Possible uses of innovation 4

A social media firm working closely with the government operating in Vosechia, used such strategies on social media platforms to contrast social discontent during the election campaign. They create personalized messages in order to counter the targeted disinformation campaigns. This IoS could be used in inject 3 to strategically target populations within *Vosechia* who are caught within certain bubbles of disinformation. This IoS could be used to facilitate real news to the public through trusted sources. Essential to this IoS is that the specific 'trusted source' in question would need to be trusted by other media, government and the end-user. Blowback risk for establishing trusted sources is that it could be perceived to a state monopolization of the truth. Collaborating with local community leaders and digital influencers could aid in establishing mutually trusted sources within intended communities. In essence this IoS aims at reversing the path the end-user followed when it went "down the rabbit hole" of disinformation in the first place.

A major challenge is the potential blowback risk of government-supported trusted news sources. Consumers might perceive this initiative as censorship of free speech, infringement upon the independence of (social) media organisations, or even the emergence of state propaganda.

Possible events

- Other social media companies refuse to cooperate with the aforementioned supported strategic personalized advertising towards government supported news sources. They cite their responsibility to remain independent.
- Social media users are leaving traditional social media and move towards social media platforms that market themselves as beacons of free speech and free of any kind of content moderation. This could turn into a whack-a-mole game between social media users and content moderators, security organisations trying to mitigate the spread of disinformation, fake news and deep fakes.

Possible RED counter actions

- Social media company affiliated to Pezetkia government releases fake documents indicating the collection and use of citizen personal data in election campaigns.
- Pezetkia infiltrates (or hacks into) the organisations' algorithms that are nudging consumers towards government-supported trusted news sources. They use the same data to redirect consumers on platforms with ties to Pezetkia towards more disinformation.

INNOVATION 5 – EFFICIENT CYBER THREAT INFORMATION SHARING THROUGH HYPER CONNECTIVITY NETWORKS

Possible use of Innovation 5

This IoS card can be used in inject 2 so that Member States of Union X can share information related to the power grid time management devices. The benefits of information sharing through hyper connectivity, are numerous. High speed sharing enables organisations or even governments to enhance their cyber defences by leveraging the capabilities, knowledge, and experience of a broader community. It can provide better situational awareness of the threat landscape, including a deeper understanding of threat actors and their tactics, techniques, and procedures (TTPs), and greater agility to defend against evolving threats. In this context, MSs of Union X by using this IoS card can improve coordination for a collective response to the new threat and reduce the likelihood of cascading effects across an entire system, industry, sector, or across sectors. Moreover, Internet of Things consortia formulation will enhance the cyber information sharing associated with the intersection of device security and safety (e.g., medical devices, autonomous vehicles, on-board avionics, zero-day network attacks). Sharing will increasingly occur as machine-to-machine transactions that are managed by trust contracts and chronicled as transactions on blockchain infrastructures.

Possible events

- Several MS refuse to share classified information about the aforementioned attack. In this regard, the response could not be coordinated and be as efficient as possible.
- Shared information using hyper connectivity networks incorporate adversary behaviour elements and behavioural analytics, which are designed to detect real-time behavioural patterns of an unfolding cyber-attack (zero-day indicators). In this context, MSs of Union X will be prepared for next attacks.

Possible RED counter actions

- Pezetkia actors having a more in-depth research and knowledge in quantum technology manage to hack the community information gaining valuable information on the vulnerabilities of several MSs' power grid systems.

5.2. VIGNETTE 2: ATTACKS ON FINANCIAL SECTOR, VACCINE CHAIN AND INDIVIDUAL DATA – NEED FOR RESPONSES.

Developments in the domain of quantum computing are fast and many patents and technological solutions are currently under development and it is expected that this technology will revolutionize the field in cybersecurity. This will affect many everyday activities such as e-commerce. The inherent capability of quantum computers to perform calculations, unlike traditional computers, enables them to break (some) existing cryptographic systems.

At the same time the actors who will have access to quantum computing will also be in a position to harness enormous computational power which will change the landscape of applications varying from chemistry to defence systems thus potentially changing the world order and giving an unprecedented advantage to the pioneers of this technology.

On the other hand, in recent decades, infrastructures, services and economic sectors have become highly interconnected and this interconnectedness is poised to continue. This has led to unprecedented levels of increased efficiency in certain sectors (technological and economic) such as logistics, however, at the same time this has led to systemic risks and much higher potential for cascade effects. One of the most important systemic risks is of course, related to cyber. All infrastructures, services and economic sectors rely heavily on IT systems. This is also to be applied for communication between governmental institutions at national and international levels. Furthermore, any disruption in the cyber sector may have consequences in a number of sectors. These cascade effects exhibit an emerging behaviour due to the inherent complexity of the global economy and underlying technological systems such as critical infrastructures.

In this context, cybercriminals take advantage of the pandemic to target and exploit vulnerabilities to the financial digital transactions system, augmented by the observed increase in online markets due mainly to the extensive lockdown policies.

The country of Vosechia is preparing to receive in collaboration with other neighbouring countries large quantities of medical supplies and vaccines. Simultaneously the main actor "Pezetkia" is planning to recruit hackers as to interfere with the supply logistics chain in order to create disruptions and shortages in Vosechia's stock of medical supplies.

At the same time Pezetkia is deploying an extensive dis/misinformation campaign, diffusing fake news regarding both the cybercriminals activities on the financial system as well as the shortages observed on the medical supplies of Vosechia.

Pezetkia actions aim to create ambiguity and doubt on Vosechia's population, increase fear for the future and anger for the present, amplify distrust to the current rule of law system and influence Vosechia's decision making process and the government efficiency in general.

Core theme	Targeted Context(s)
CT2: Cyber and future technologies	1. Game changers: quantum as a disruptive technology 2. hyper connectivity as an impact multiplier of cyber 3. The individual as a digital entity

Target audience	Prior knowledge
Select the target audience from the following: **Practitioners** I) *ministry level* (administration), Ii) *local level* (cities and regions), Iii) *support functions to ministry and local levels* (incl. Europe's third sector) Industry, sme Academic actors # of participants Here is suggestion of the participants: **-Consortium, e.g.** ***Practitioners*** • KEMEA, MTES, Espoo, JRC, Hybrid CoE, MoD NL, PLV, ABW, DSB, RIA, ZITIS, COMTESSA ***Industry, SME*** • Satways ***RTO, research association, organisations*** • Laurea, PPHS, RISE, L3CE, MVNIA, ICDS **-Stakeholder group, e.g.** ***Practitioners (* priority)*** • *Ministry of Justice and Security – **Law and justice** (NL) • *Ministry of the Interior Finland, Department for Rescue Services - **Internal security, CBRN, Civil Protection and emergency response** (FI) • Tromso Police District – **Law enforcement** (NO) ***Industry, SME*** • *Systematic - **Critical infrastructure** (FR)	Quantum Technology Fake news IT – Network security Regulatory Legal Journal-news handling

• Ardanti Defense (FR) • *Expertsystem - **Critical infrastructure** (FR) ***RTO, research association, organisations*** • *Fraunhofer-IVI - **Critical infrastructure, electricity grids** (DE) • *CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI) • *CE.S.I. Istituto di Analisi di Politica Internazionale - **International Politics** (IT) • *European Security and Defence College - **Crises management** (EU, BE) • SafeCluster - **Security technology** (FR) **Role/position:** Experience level: *mid-ranking to senior officials or experts on* the above-mentioned participants	

The pandemic rages on. Allied states have experienced several changes or challenges in their daily routine:

- Economies are weakened due to continuous lock-down of traditional business. Structural changes are taking place, moving traditional sectors to new environments of remote trade and service provision. In parallel significant financial resources are streamed to health and pandemic management sectors. Thus, governments are not able to support investment and social care activities at the level expected.
- Most activities, that are not related to the physical presence at a workplace, have moved to remote mode. Work moved from offices that had significant cybersecurity measures to protect institutional cyber perimeter, to home, where cybersecurity capabilities of public infrastructure are much weaker.
- All communication between different institutions, involved in pandemic management and beyond moved to remote mode. This also includes cross-country or joint regional communication. Thus, such communication requires digital infrastructures and becomes vulnerable. Main consideration becomes trust – is the source of information received trusted and how fast this can be verified.

In such circumstances, the unexpected cyber-attack on two major entities, was made. It included Vosechia's Central Bank and the destruction of supply chain, by taking over supply chain management platforms.

INJECT 1: FINANCIAL SECTOR ATTACK AND MASSIVE BANK AND INDIVIDUAL DATA BREACH.

At an alarming rate, transnational organized crime groups are leveraging specialist providers of cybercrime tools and services to conduct a wide range of crimes against financial institutions, including ransomware campaigns, distributed denial of service (DDOS) attacks and business email compromise scams (Social Engineering attacks). Banks not only store money but also gather network activities and personal information of the customers, including names, phone numbers, addresses, email addresses, and dates of birth. This data has essential value and can be used for other malicious activities such as **identity theft**, which can often lead to more disastrous and significant consequences.

As investigation of the incident showed, Quantum decryptors were applied for the execution of the attack. In parallel one of the countries, being considered as "competitor" (or even an "enemy") to the allies, announces that they have launched Quantum technology-based capabilities. As the investigation goes on, it becomes clear, that the attack was more of the testing nature and main goal was to generate fear and feelings of helplessness.

Post Quantum Security capabilities of allies are rather weak. There are some solutions which are in the final TRL levels, but are still not available for mass application. Some organisations, especially those handling secret and very sensitive data, have set up closed infrastructures that are resilient to Quantum decryptors. Combined with

a steady growth of the usage of mobile devices, cloud-based data storage and services, and digital payment systems, cybercriminals have exploited an ever-expanding host of attack vectors.

Under this scope, Vosechia's central bank has been targeted, although they were vigilant in the face of this evolving threat, they nonetheless suffered a successful destructive data breach where the end goal was to transfer funds and exfiltrate sensitive data. Adversaries got information about running processes on bank's system. Information obtained could be used to gain an understanding of common software running on systems within the Union X's financial network. Adversaries may use the information to shape follow-on behaviours, including other financial institutions in member states or even in the Union X's central bank which seem to be resilient and attempt to execute specific malignant actions.

Tools (more in subchapters below):

- OPENQKD
- Future proofing the connected world: Quantum Resistant Trusted Platform
- A blockchain based real-time information management and monitoring system
- Vulnerabilities Stockpiling
- Efficient cyber threat information sharing through hyper connectivity networks.
- Public-private (pp) information-sharing groups developing collaborative investigations and collective action

INJECT 2: VACCINATION SUPPLY CHAIN ATTACK THROUGH PHISHING OF SUPPLIES.

At the same time, hackers are targeting Union X's companies critical to the production and distribution of vaccines as well as the logistics chain of pharmaceutical and medical material across Union X MSs, a sign that digital spies are turning their attention to the complex work involved in inoculating the Union X's population against the pandemic. An innovative pan-Union X phishing campaign is deployed focused on organisations associated with the vaccine "cold chain" - the process needed to keep vaccine doses at extremely cold temperatures as they travel from manufacturers to people's arms. Understanding how to build a secure cold chain is fundamental to distributing vaccines, because the shots need to be stored at minus 70 degrees Celsius or below to avoid damage. An advanced group of hackers from Pezetkia working to gather information about different aspects of the cold chain, using precisely crafted booby-trapped emails sent in the names of executives with many biomedical companies in Union X. Quantum technology based malignant software has been alleged on many occasions since decryption was successful in an unreasonably short period of time.

It is evident that without a clear path to a cash-out, cyber criminals are unlikely to devote the time and resources required to execute a calculated quantum-based operation with so many interlinked and globally distributed targets. Advanced insight into the purchase and movement of a vaccine and medical material that can impact life and the global economy is likely a high-value and high-priority nation-state target. The hackers went through an exceptional amount of effort, emails were sent to around 10 different organisations in Union X with the purpose to harvest credentials, possibly to gain future unauthorized access to corporate networks and sensitive information relating to the pandemic vaccine distribution.

Tools (more in subchapters below):

- Efficient cyber threat information sharing through hyper connectivity network
- Public-private (pp) information-sharing groups developing collaborative investigations and collective action
- Vulnerabilities Stockpiling

INJECT 3: FAKE NEWS / DISINFORMATION.

The aforementioned data breaches and hacking events in the financial and medical sectors are getting amplified by an extensive mis/disinformation campaign in Vosechia, via probes in mainstream media and Think Tanks that underline central government's inability to handle the situation being presented as losing control. Many different actors diffuse fake news in social media and mainstream channels which are whitewashing trending and viral social media views, increasing the level of uncertainty and ambiguity regarding the real dimensions of the situation in hand. Fear and doubt are instilled regarding the ability of local governments to handle the crisis and manage operationally the proper responses. The central claim is that the government is not sufficiently equipped to secure the cold chain for the vaccines and therefore renders them inefficient at best, or harmful at worst depending on cases. Data breached through the central bank attack and also through the phishing attempts, is used for identity theft having the objective of overburdening the online platform for vaccine time appointments.

- Fake news exposer
- Fact checkers community
- EU Directive on copyright in the digital single market

VIGNETTE SPECIFICS

An operational coordination body will be asked to provide input to the strategic level decision making regarding the situational awareness, the incident response and the public communication policy concerning the three specific injects. To this purpose the aforementioned body has available in its arsenal a set of techno innovations described hereinafter.

1. Applying Quantum Technology in the context of hybrid threats
2. Intra institutional coordination for incidence response and situational awareness
3. Debunking fake news and diffusing valid information for public communication purposes

ORGANISATION

Representatives of main ministries involved, agencies and institutions working in a coordinated manner to produce "one voice" suggestions for the strategic level decision makers. More specifically, banking sector, cyber security agencies and offices in EU MSs and EU level.

RISKS

Lack of operational coordination, silo approach, inability of successful collaboration between the operational and strategic levels.

OBJECTIVES

- Regain normal operational status for the central banking system.
- Safeguard personal and sensitive data.
- Protect from disruption of the vaccination chain.
- Reduce the ambiguity and doubt environment which is being cultivated by the fake news campaign.
- Ministries level needs to focus on communication to reduce the fear, aiming to avoid cascading effects, leading to further impact on economy and possible riots.
- Local level needs to handle particular flashpoints, related to fear.
- Transition is secure infrastructure requires full (end-to-end) transformation. The most vulnerable points are connected secondary, small actors. If one segment of supply chain is compromised, the whole outcome is at loss of trust on entire chain.

MEANS –INNOVATIONS AS PLAYCARDS FOR DTAG

The practitioners will use the IoSs provided in the DTAG playcards.

INNOVATION 1 - EFFICIENT CYBER THREAT INFORMATION SHARING THROUGH HYPER CONNECTIVITY NETWORKS.

Possible use of Innovation 1

This IoS card can be used in inject 1 and 2 having a dual organisational/ technical nature and refers to information sharing and collaboration platforms as for CSIRTs (Computer Security Incident Response Teams) network, information sharing and analysis centers (ISACs), etc. Information sharing provides a way for members to cooperate, exchange information and build trust.

By implementing this card, MS will be able to improve the handling of this cross-border incidents and even discuss how to respond in a coordinated manner. In this context, they could benefit from the high-speed sharing to enhance their cyber defences by leveraging the capabilities, knowledge, and experience of a broader community of users. Moreover, they could share and acquire information about the attacks that have taken place in all MS of Union X.

By using this tool, MS of Union X will have better situational awareness picture, enhanced incident response capabilities and recovery procedures regarding the cyber threat landscape, including a deeper understanding of actors behind the attack and their tactics, techniques, and procedures (TTPs), and a greater agility to defend against evolving threats.

In this regard, by using this innovation MSs of Union X will manage to improve their coordination for a collective response to the new threats and reduce the likelihood of cascading effects across an entire system, industry, sector, or across sectors.

A challenge of using this IoS card could be the fact that MS could be reluctant to share their vulnerabilities with any other organisation.

Possible events

- MSs display an attitude of Informational and Intelligence ownership, not willing to share and exchange what they consider to be important for their own national security
- Agencies within MSs present a silo approach as well, reducing the effectiveness of a comprehensive and coordinated approach

Possible RED counter actions

- Pezetkia actors infiltrate and hack the network obtaining critical information about MSs cyberdefense plans and policy

INNOVATION 2 - PUBLIC-PRIVATE (PP) INFORMATION-SHARING GROUPS DEVELOPING COLLABORATIVE INVESTIGATIONS AND COLLECTIVE ACTION

Possible use of Innovation 2

This IoS card can be used in inject 1 and 2. Cybercrime cannot be addressed without creating a more effective deterrence model by confronting the source of cybercriminal activity, reducing the return on investment and making the risk of prosecution real. Nevertheless, the skills, data and capabilities to detect and disrupt cybercrime often reside within the private sector. This innovation card has to do with leveraging existing and future info sharing mechanisms as for European cybercrime Centre (ec3), the national cyber-forensics and training alliance, Microsoft digital crime unit (DCU), cyber defense alliance (CDA) etc. In this context, MS of Union X, by using this card could cooperate with private entities in order to address the attack in their supply chains and financial sector. They can improve their resilience for common attacks and zero-day vulnerabilities.

A challenge of using this IoS card could be that Public-Private information sharing is hampered by fears about giving competitors an advantage, as well as concerns about sharing sensitive internal data. Geopolitical drivers and fragmentation in international co-operation can affect public-sector enthusiasm for data exchange programmes. The private sector is often reluctant to share information with governments for fear of regulatory impact, to avoid complicity in any privacy and rights violations and because they often see no benefit to doing so.

Possible events

- Private sector corporations are reluctant to share information trying to avoid any jeopardy to their marketing reputation and brand name.

Possible RED counter actions

- Pezetkia actors recruit C-level (e.g., CEO, CFO, COO, CSO) and middle staff of certain corporations thus obtaining direct access to all information shared between public and private sectors in MSs of Union X.

INNOVATION 3 - FAKE NEWS EXPOSER

Possible use of Innovation 3

This IoS card will be used to inject 3. This innovation card gives insights that makes it easy to follow, analyse, and report on what's happening with public content on social media posts and assists users to identify fake news and disinformation. To do this, these tools analyse both content and metadata and some tools also have the ability to classify the article as fake or not by evaluating the article based on predefined external and internal indicators.

By implementing this IoS card, Vosechia authorities can inform the public to hold back from the disinformation campaigns that have been identified. Vosechia could improve societal resilience against adversarial actors that try to use disinformation campaigns as a way of gaining leverage. A potential challenge could be that a group of people is needed to analyse the results of this software tool.

Possible events

- Citizens are unwilling and hesitant to follow government's fake news debunking efforts and are more inclined into accepting fake news.
- Social media platforms accuse government's authorities of attempting to manipulate news feed.

Possible RED counter actions

- Pezetkia actors hack the algorithms of the fake news exposer in order to wrongly classify news as fake. Information is spread throughout the internet that news is accidentally identified as fake by the Vosechia's Government. This led to legal issues and claims.
- Pezetkia spread a huge amount of fake news over the social media and the group of people responsible for analysing the results cannot cope with the workload.

INNOVATION 4 – OPENQKD

Possible use of Innovation 4

This IoS card can be used for Vosechia as well as other Union X MSs to gain the necessary competences related to the Quantum communication capabilities. By using this IoS, Union X MSs and more specifically Vosechia authorities could be trained and get involved in an innovation ecosystem that will grow the technology and

solution supply chain for quantum communication technologies and services. In this context, Vosechia authorities could understand better their vulnerabilities and the potential impact.

This IoS card should be used in conjunction with the training of the consumers in order to create awareness in relation to emerging risks related to the Quantum Computers. With the aforementioned capabilities society as a whole will be resilient in similar attacks.

Possible events

- Basic stakeholders are not attracted to this training activity based on the assumption that this issue is too futuristic and does not constitute a present and imminent threat.

Possible RED counter actions

- Red actors via probes in academic institutions and other research entities in X Union MS diffuse fake news that Quantum Computing risks are very distant, so the probability of their occurrence is very hard to come by.

INNOVATION 5 – A BLOCKCHAIN BASED REAL-TIME INFORMATION MANAGEMENT AND MONITORING SYSTEM

Possible use of Innovation 5

This IoS card can be used to prevent the identity loss in the financial system in inject 1. By using this IoS card, Vosechia central bank as well as the Union X central bank, could verify the transaction in the system based on blockchain technology. The information used in the transaction will be partly anonymized. Only verified transactions are allowed to be executed. The verification can be done by Vosechia Government.

A challenge of this card could be the ethical and human rights violation concerns that exist on the implementation of such technologies.

Possible events

- Financial institutions may not be so attracted into adopting blockchain mechanisms to monitor transactions, mainly because they will lose the central command and control power they already have.

Possible RED counter actions

- Red actors could spread information about how insecure and problematic it is implementing blockchain philosophy and mechanisms in financial transactions, derailing the current banking system.

INNOVATION 6 – FACTCHECKER'S COMMUNITY

Possible use of Innovation 6

This IoS card can be used in inject 3. This IoS can be used in conjunction with IoS card No 3. The most prominent approach to combating misinformation is the use of professional fact-checkers. However, Vosechia Government will use this innovation by capitalizing on crowds of regular people at moderating fake news as professional fact-checkers which is considered as a good alternative. Unlike professional fact-checkers, who are in short supply, it is easy (and inexpensive) to recruit large numbers of laypeople to rate headlines – thereby allowing scalability. By creating fact checkers communities, best practices and exchanges in this field can be further promoted.

A challenge of this IoS card is that personal opinions may influence the quality of results.

Possible events

- Public authorities may face difficulties in organizing regular people in communities with the specific task to moderate fake news.
- Citizens may accuse the government of attempting to manipulate information flow under the cover of community fact checking

Possible RED counter actions

- Red actors may diffuse fake news alleging that a government manipulation campaign is on the go, with specific target to utilize unsuspecting citizens.
- Red actors could infiltrate the fact checking communities. This way they could deteriorate the quality of results and report real news as fake ones.

INNOVATION 7- FUTURE PROOFING THE CONNECTED WORLD: QUANTUM RESISTANT TRUSTED PLATFORM

Possible use of Innovation 7

This IoS card can be used in inject 1 to provide to Vosechia a new generation of TPM (Techniques- Processes-Methodologies) based solutions, incorporating robust and formally verified QR cryptographic primitives. By using this card, Vosechia Government could be able to perform their smooth transition from current TPM environment, based on existing widely used and standardized cryptographic techniques, to systems providing enhanced security through QR cryptographic functions, including secure authentication, encryption and signing functions. This innovation, since it is tested in several use cases, will be fit for purpose for addressing the financial sector attack in inject 1. Moreover, for the implementation of this IoS successfully the training of the public officials will be a prerequisite to be made independent on advice and allow them to make fundamental decisions faster.

Possible events

- Not easy to complete the training of public officials since a very high level of expertise is required
- Technological solutions may not be ready to be applied on the spot as to support already up and running systems

Possible RED counter actions

- Red actors try to publicly support that this solution is not feasible from the technical and financial viewpoint

INNOVATION 8 - EU DIRECTIVE ON COPYRIGHT IN THE DIGITAL SINGLE MARKET

Possible use of Innovation 8

This IoS card can be used in inject 3. It includes requirements on online content-sharing service providers to perform “upload filtering” of content to detect upload of copyright protected content. By using this innovation Vosechia authorities can filter against content registered by copyright owners. It will assist the Vosechia Government into countering disinformation campaigns and fake news spread over social media platforms.

A remaining challenge of this IoS card is to collect and annotate all the original content.

Possible events

- The Government may be accused that is imposing a heavy control mechanism on the content over the Internet.

- Providers as well are not willing to comply to this initiative since it will considerably decrease their expected turnover.

Possible RED counter actions

- Red actors could support voices objecting to the "manipulation" attempts by the Government regarding the online content and accuse Union X for strict and undemocratic regulatory approach.

INNOVATION 9 – VULNERABILITIES STOCKPILING

Possible use of Innovation 9

This IoS card can be used in inject 1 and 2. By using this IoS card, MS of Union X can stockpile software vulnerabilities, providing the government with an asymmetric advantage against adversaries, allowing for practically undetectable intelligence gathering and even the ability to disable or sabotage opponents' infrastructure.

Stockpiling is based on the hypothesis 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 it is 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 can be advantageous for the offensively focused entities of inject 1 and 2.

A challenge of this IoS card is that stockpiling is an extremely costly process.

Possible events

- There might be the case for a boomerang effect on critical infrastructure mainly because a stockpiling approach challenges the ability to patch and effectively address any existing vulnerability in a system since the latter is not disclosed and remains stockpiled for future offensive exploitation.

Possible RED counter actions

- Red actors may offensively exploit any existing vulnerability whilst known exploits remains stockpiled and is not patched properly.

5.3. VIGNETTE 3: SANITARY RESTRICTIONS AND REGIONALIZED PROTEST AND MOVEMENT – NEED FOR INTEGRATION

Core theme	Targeted Context(s)
CT3: resilient civilians, local level and administration	1. Distrust and stress in political decision-making 2. Reliance on critical services and technological systems 3. Globalization vs. Localization

Target audience	Prior knowledge
Select the target audience from the following: (1) Practitioners I) *ministry level* (administration), II) *local level* (cities and regions),	Communication means and processes and procedures between government to local administration and to citizens.

III) *support functions to ministry and local levels* (incl. Europe's third sector) & (2) academics (3) industry (4) NGO representatives. ***N.B.** all training participants are coming from the EU-HYBNET consortium and Stakeholder Group* Here is suggestion of the participants: **-Consortium, e.g.** ***Practitioners*** • KEMEA, MTES, Espoo, JRC, Hybrid CoE, MoD NL, PLV, ABW, DSB, RIA, ZITIS, COMTESSA ***Industry, SME*** • Satways ***RTO, research association, organisations*** • Laurea, PPHS, UiT, EOS, MVNIA, ICDS **-Stakeholdergroup, e.g.** ***Practitioners (* priority)*** • *Ministry of Justice and Security – **Law and justice** (NL) • Finnish Border Guard - **Border and maritime security, internal and external security** (FI) • *Ministry of the Interior Finland, Department for Rescue Services - **Internal security, CBRN, Civil Protection and emergency response** (FI) • Tromso Police District – **Law enforcement** (NO) ***Industry, SME*** • *Systematic - **Critical infrastructure** (FR) • *Expertsystem - **Critical infrastructure** (FR) ***RTO, research association, organisations*** • European Health Management Association - **Health care** (EU, BE) • *Fraunhofer-IVI - **Critical infrastructure, electricity grids** (DE) • *Institute for Public Goods and Policies; Spanish National Research Council - **Fake news and strategic communication** (ES) • *Ukrainian Association of Scholars and Experts in Field of Criminal Intelligence - **Law enforcement** (UA) • *CE.S.I. Istituto di Analisi di Politica Internazionale - **International Politics** (IT) • *European Security and Defence College - **Crises management** (EU, BE) SafeCluster - **Security technology** (FR) **Role/position:** Experience level: *mid-ranking to senior officials or experts on* the above mentioned participants	Understanding of horizontal communication needs in state administration and with citizens and regions Understanding of supply chains importance to the stability of the state Understanding of importance of disinformation and fake news follow-up and counter measures

As the pandemic took hold, most epidemiologists have had clear proscriptions in fighting it: No students in classrooms, no in-person religious services, no visits to sick relatives in hospitals, no large public gatherings. On the other hand, hundreds of opponents of the night-time curfews in many X Union MSs have clashed with police

resulting in scores of arrests. The situation offers an attractive attack surface for Pezetkia to deploy hybrid influence operations (OPS).

INJECT 1: GOVERNMENTAL TRUST BUILDIN

Vosechia's government needs to take preventive measures and to set new temporary restrictions regarding general population movement, retain obligatory usage of face masks by citizens and to restrict the opening of shops and restaurants and schools and public spaces to prevent the virus from spreading. The government restrictions are followed by citizens in all regions and cities. Pezetkia hires actors to feed comments into general discussion in social media (SOME) channels to foster doubt and the questioning of government's decisions. Local newspapers state that some regions of the country are subjected to unequal treatment due to their remoteness and smaller populations in comparison to the more heavily populated, and more heavily affected, center regions. At the same time, the more remote locations are more vulnerable even the lowest infection rates due to the more limited healthcare facilities which are few and far apart, as well as a less developed transport/transit infrastructure to get to health facilities, or for goods to be effectively transported to their regions during a pandemic. Preferential treatment for some services is inadequately explained by the government communication services, raising questions as to why, for example, some citizens are allowed to keep their businesses going and thereby avoid financial hardship (e.g. some restaurants) while others are not. Pezetkia actors have been able to establish a trusted relationship with an influential region Yellowzone. The region's authorities claim that the government's regulations are not equal and fair to all regions, esp. for the Yellowzone region and its' close neighbouring regions. The guidance of Pezetkia actors to region Yellowzone encourages the local authorities to openly challenge national government policy making and to state that the government restrictions are ineffective and harmful, especially to their region and locals. Locals follow the debate in news and provide similar comments in SOME channels. Yellowzone's authorities clearly imply that pubs could be well opened.

These events generate the development of a protest movement in the regions concerned, against the government decisions. Several other claims get incorporated in the protest movement (revolt against sanitary restrictions, blatant opening of restaurants and public spaces without authorization, defiance towards police and authority's intent on applying sanitary measures). Pezetkia actors imply in SOME channels as well as social media platforms that police harshly forced the closure of pubs and restaurants which had been opened without permission. The movement sees the emergence of a group of radicalized protesters led by a charismatic figure, a restaurant owner that went bankrupt because of government restrictions (narrative). This group oftentimes uses the example of Pezetkia, which is perceived to have maintained restaurants open. The "open restaurants" protest movement gains pace and transforms gradually into a political movement that gains momentum and national significance ahead of the elections, threatening government instability. The "open restaurants" ideas and narratives gains a suspiciously systematic and important volume of sharing, visibility and content production on social media. Individuals are targeted throughout the country by very personalized advertisements that seem to rely on social media data.

Tools (more in subchapters below):

- Floss platform or Propastop
- Resilient Democracy Infrastructure Platform (RDIP)

INJECT 2: MARGINALIZED GROUPS USED AS A TOOL TO HARM STABILITY IN SOCIETY

Vosechia's government needs to change some regulations at the state and local level, and to set further restrictions and limitations establishing a new "everyday" way of living (obligation to stay at home and only grocery visits are allowed, gatherings are banned, obligatory usage of face masks by all citizens). Some citizens begin to question the measures and wonder if the restrictions are effective and if they are being implemented fairly. The situation is fuelled by Aldoarmia actors who spread rumours in SOME channels that illegal refugees

that live in hosting facilities and are originated from a neighbouring do not follow the given restrictions and that therefore they are the reason for the ineffectiveness of the measures taken. In the same rumours, it is stated that the local administration does not invest enough in refugee hosting infrastructure and do not provide the necessary guidance to refugees on the virus and protection against it. In addition, it is stated that the local administration takes care of the necessary actions but the refugees, due to their different cultural background, do not follow Vosechia restrictions that well. Moreover, it is stated that the refugees are the ones spreading the virus in the Vosechia regions where they are located.

Since rumours have gained much attention, Vosechia's government states in the media that refugees, already living in the country since 5 years ago are not spreading the virus more than any other citizens are, and that refugee services are well covered. Simultaneously more refugees start to appear on the border of Vosechia. The border authority's IT based surveillance systems, which monitors illegal crossings, failed. This failure is speculated to be driven by Aldoarmia actor's hack. This event is leaked to media by Aldoarmia actors, whom stress that many infected refugees have managed to find their way into Vosechia territory. Mistrust of citizens to government and security authorities have flourished.

While more refugees arrive in Vosechia, the long-lasting issue that government should do more for refugees in integrating them into society rises again. Simultaneously, Aldoarmia actors begin to influence members of a small anti-refugee political party W who loudly claims that refugees are not welcome to Vosechia due to their behaviour. The government and local administration do not consider the refugees to be a high enough risk towards the whole of Vosechia virus situation. The integration of marginalized groups into society becomes a hot topic of debate in the middle of the crisis just a few months before regional elections in the Vosechia. This makes citizens either anti- or pro-refugees and the polarization in society is seen to risk the peace of coming elections.

Public opinion is further influenced by media outlets historically close to Aldoarmia positions, depicting Aldoarmia as a "success story" in combating the virus by closing borders strictly while keeping society seemingly open. Aldoarmia has a habit of lying about public figures and the Vosechia's government and Union X in general are aware of data manipulation in Aldoarmia to picture a better situation.

Tools (more in subchapters below):

- Tool with the capability to detect/analyse emojis in order to improve the understanding of user's perceptions, sentiment, and emotion.
- Civil-military cooperation –concept
- Online system for facilitating efficient migrant integration
- Automated detection of hate speech

INJECT 3: CRITICAL SUPPLY CHAIN AUTHORITY NOTICES FAILURE IN ITS CRITICAL SUPPLY CHAIN(S)

Vosechia has started to get vaccines for the virus and the vaccination campaign has begun. The vaccines are spread throughout Vosechia regions and their hospitals. The arrival of vaccines is mastered by governmental medical supply chain IT-system. Pezetkia actors are able to hack into Vosechia's governmental medicine supply chain IT-systems and infect a computer virus to it – the computer virus starts to show a reduced number of vaccines available than there are in reality; it also falsely claims delays in the vaccine delivery to regional hospitals. The Vosechia IT-system's malware and cyber protection programs do not discover the computer virus in the IT-system, and hence the government and local administration are alarmed by the situation and fear that the vaccination campaign will have delays.

As such, citizens criticize Vosechia government and local health care actors on their unrealistic vaccination planning. This is spread by Pezetkia actors in SOME. Citizens' mistrust towards government increases while Pezetkia claims that they had offered their vaccine to Vosechia many months earlier with 100% delivery guarantee but that Vosechia government had not made an agreement with them even though Vosechia could

have in this way secured their need for the vaccination. The anti-government party X, which has close ties to Pezetkia, claims that Vosechia's government and local level medical administration are willing to risk human lives instead of trusting the vaccine produced in Pezetkia. Pezetkia narratives claim that this is simply policy grandstanding on behalf of Vosechia, rather than focusing on saving lives and getting a vaccine, no matter which provider. The spread of this narrative inspires some citizens to demonstrate in major cities and the support to party X increases. Furthermore, Pezetkia actors have leaked information about the computer virus which has recently affected the Vosechia's governmental medical supply chain IT-systems to several social media platforms – furthermore an "unidentified individual" has also sent information on the issue to the Vosechia's news channels via a secured email address. The posts state that the "unidentified individual" has revealed that Vosechia has "no clue about the vaccination progress because of a computer virus that has affected their IT system". It is also stated that the IT systems are reporting low vaccines availability when in fact there are enough vaccines in the country at the moment. The Vosechia intelligence service have confirmed claims for the computer virus in the governmental medical supply chain, but also states that there are enough vaccines for the vaccination campaign.

At the same time, Pezetkia actors have started to gather and distribute Vosechia yellow journalism / press scientific articles, in part written by some leading Pezetkia medical scientists as well as by minor, relatively unpublished and mediocre international scientists, who together claim that asthma medicine would help people to recover from the virus, if one gets infected. The articles also encourage people to buy asthma medicine while waiting to be vaccinated. This leads a large number of citizens to buy asthma medicine in such an enormous amount that individuals who actually have asthma claim that they have difficulties in buying their medicine. At the same time international cargo companies state that they cannot deliver all necessary cargo containers and hence there can be delays even in the critical supply delivery incl. medicine and especially asthma medication. This causes people to hoard even more asthma medication and local pharmacies and hospitals start to report a lack of asthma medication in their supply storages. Government and local administrators requests people not to buy the asthma medicine, but citizens claim that the government has not been able to guarantee the safety of its critical medical supply even though it should have been fairly easy to do so as asthma medicine is sold by many international medicine companies. Under citizens pressure the government and regional medical authorities start to make new, expensive contracts on asthma medicine delivery to Vosechia in order to calm the citizens' minds and most of all to ensure the availability of the asthma medication. Soon after this, Pezetkia actors start to publish scientific articles in SOME that asthma medicine does not help against the virus. In addition, there is news that the cargo containers to vessels are readily available and that Pezetkia and its like-minded countries may deliver them as soon as possible to the international companies and countries. The various cases of supply chain challenges in Vosechia makes party X more popular than ever before in many of the affected regions of Vosechia. Party X claims that it would be best to focus on the timely delivery of vaccines and that can only happen though the cooperation with Pezetkia. This is not supported by Vosechia government who relies on wide international cooperation in supply chain issues. The critical supply chain and supplies related issues become the most central, hot topic in the forthcoming election debates between parties favouring the party X.

Tools (more in subchapters below):

- Smart message routing and notification service (SMRNS)
- Supply chain risk management (SCRM)
- Cyber security management

VIGNETTE SPECIFICS

ORGANISATION

Interagency coordination in governmental and regional level with executive competences and focus to follow citizens reactions, knowledge of critical supply chain and cyber security management in the supply chain storage

follow-up. Third sector organizations who have status of practitioners due to their delivery of tools, products and services necessary for the state security and basic functions.

RISKS

- Emerging thoughts and feelings of unequal treatment based on education and/or profession
- Dissatisfaction with decisions and ignoring restrictions and recommendations, as these may be explained and perceived in a confusing and ambiguous manner
- Fear of infection from visitors from neighbouring countries or regions
- Demonstrations make access to hospitals more difficult
- Misinterpretation of facts, spread of them in social media platforms and using the big influence-> Multiplier effect with sharing these modified, incorrect, or wrong messages
- Governments and administrations are busy with reactive power actions because of clarifications and additional expenses
- Lowering trust in governments, medical system, and services plus security forces
- Lowering acceptance and empathy for refugees' motivation and needs
- Increasing violence against refugees, security forces and rescue services; Additional disputes between pro and con groups
- Exploitation of technologies, e.g., web-links to infected pages, to infect poorly secured PCs with malware
- Missing vaccine may lead to a parallel vaccination campaign, perhaps even abroad, by criminal organisations; Promise the costs would be covered by health insurance companies. Useless or dangerous 'vaccine' getting used

OBJECTIVES

- Set conditions for comprehensive situational awareness in the development of public opinion and supply chains
- Capability to build media strategy to counter disinformation
- Develop communication elements to the population in order to divert and alleviate the pressure
- Develop communication to signify that the government and regional admin and other relevant regional authorities in different field (e.g. health care/ hospitals) are in control of the situation, reassuring messaging to solve initial communication hiccups.
- Counter measures and follow up of possible polarization and political, economic and health care challenges in society
- Enhancing supply chain management in unexpected crises and under pressure from media and citizens

MEANS- INNOVATIONS – PLAYCARDS FOR DTAG

INNOVATION 1 - RESILIENT DEMOCRACY INFRA PLATFORM

"Resilient Democracy Infrastructure Platform" (RDIP). RDIP does not fit in the present format to vignette 3 and hence it is updated to include following: RPID could include a channel where government could provide information to citizens on propaganda actions, actions to influence locals' opinions in order to harm the present stability. So-called media monitoring and propaganda & disinformation alert function both to government and local administration authorities and to citizens.

Possible use of RDIP (including the suggested new features)

This IoS card can be used in inject 1 "Governmental Trust building". RDIP functions as an app and citizens are requested to load it into their cell phones in order to ensure accurate information sharing between government and citizens and to prevent severe disinformation to spread.

Possible events

- RDIP provides information that protest movement is to harm society in general and pubs are not allowed to be open even though this is claimed in SOME and implied by Yellowzone.
- Yellowzone shares information to its locals on the fact that they had been fooled into trap of a propaganda of Pezetkia and hence the Yellow zone had given misleading information on Governments decisions that they would have been bias although they were not.

Possible RED counter actions

- Pezetkia actors claim that RDIP is a propaganda tool of government and targets to control citizens far more than needed.

INNOVATION 2 – FLOSS AND/OR PROPASTOP

Possible use of Propastop

To be used in inject 1 "Governmental Trust building". Floss platform to engage public debate, crowdsource opinion formation, trigger discussion or because Floss does not exist yet Propastop https://www.propastop.org/eng/2019/01/25/online-media-small-form-manual/ Propastop is a blog aimed at cleaning Estonia from propaganda, false information and media lie. The blog is run by volunteers. By implementing this IoS, disinformation and fake news can be minimized on various media platforms. The card can be used to mitigate the cascading effects of the spread of fake news in the society. A challenge would be that such initiatives should be originated by a trusted source.

Possible events

- Propastop provides information that shows that the Yellowzone is guided by Pezetkia actor, and Yellowzone authorities' claims seem to be mistaken and misleading. Propastop shows that police have not been using too harsh actions in closing pubs but the news on police's exaggerated use of power is fake. Furthermore, Propastop shows that protest movement often takes example on Pezetkia and the information the movement claims are often biased e.g., certain actions in Pezetkia (e.g., opening pubs) have not improved the situation, vice versa.

Possible RED counter actions

- Pezetkia actors feed media with disinformation stressing that Propastop is not a trusted source and is affiliated to the Government promoting their agenda.
- Adversarial actors hack the platform feeding fake news in it, reducing its trustworthiness.

INNOVATION 3 - TOOL WITH THE CAPABILITY TO DETECT/ANALYSE EMOJIS IN ORDER TO IMPROVE THE UNDERSTANDING OF USER'S PERCEPTIONS, SENTIMENT, AND EMOTION

Possible use of Innovation 3

This IoS card will be in inject 2 Marginalized Groups used as a Tool to Harm Stability in Society. This tool provides the capability to detect/analyse emojis to improve the understanding of user's perceptions, sentiment, and emotion. The solution can be used to grasp the citizen's response to the outreach strategies to capture responses and evaluate the success of the communication campaign. The solution can be used to capture the society's response to outreach strategies designed to fight social inequality and injustice and can help in the society's resilience to hybrid threats.

Possible events

- Government and local administration will be kept updated by SOME with the help of this IoS card regarding the attitude of citizens and locals towards refugees in general and especially in the border areas where the refugee flow is most acute. The tool shows that the negative emojis (e.g. angry mood

and fist icons) are used a lot especially in the border areas and the capital of Vosechia where the new, small anti-refugee party W has many supporters.

- In addition, just before the elections it is noticed from the tool that capital emojis that have explosive and weapon icons are increasing. This leads government intelligence to follow more of party W's actions and gatherings. In addition, government intelligence announces to police located in border regions and in the cities where refugees are located to be prepared for attacks against refugees. Some regions where no negative emojis exist, a yellow arrow has been identified and is connected with very severe attacks against refugees, and refugee premises. This leads governmental intelligence to learn that party W has a certain type of icon language that means alert to attack and to a certain type of attack. The challenge is that the icon language changes periodically but there is much intelligence on it. The government wishes to know where the intelligence in the icons is coming from and are similar parties to W, in other countries using similar icons.
- Moreover, the tool shows smiley faces and positive icons in the discussion on refugees in some regions and hence also the other regions wish to learn from this region how they have been able to avoid the polarization that is taking place elsewhere. This leads regions to share their best practices in regards to the question of refugees.

Possible RED counter actions

- Pezetkia actors could hack the algorithms used in this tool in order to provide a fake societal picture to Vosechia Government.

INNOVATION 4 – CIVIL-MILITARY CONCEPT

Possible Use of Innovation 4

Civil-military cooperation is seen as a key to resilience against hybrid threats; especially in the case where it is needed to prevent citizens from being targeted as actors who destabilize social coherence.

Government and local administration arrange media campaigns in order to tell citizens and locals, especially in the border areas where the refugee question is a hot topic, how citizens and locals can be manipulated to change their behaviour in such a way that eventually it becomes harmful for society due to increasing polarization. The concept where citizens and locals can be used as those who harm their own society due to manipulation, needs to be stated clearly. In addition, government and regions need to state how citizens and locals can act as preventive actors against harming society and building it stronger and more united, as a safe and good place for all to live together.

Possible events

- Local citizens remain strongly opposed and polarized against refugees flows and irregular immigration.
- Government loses credibility and is accused of being incompetent to handle properly the situation

Possible RED counter actions

- Red actors may support populist voices of the "pro" or "anti" immigrant rhetoric attempting to destabilize society by exploiting the existing cleavages.

INNOVATION 5: SMART MESSAGE ROUTING NOTIFICATION SERVICE

Possible Use of Innovation 5

Smart message routing and notification service (SMRNS) for sharing the operational picture to every agency involved in the response at every level of coordination. This IoS card enables the sharing of information among involved actors at every level of coordination enabling collaborative response and the proper alerting of personnel/practitioners/stakeholders. Based on the Emergency Message Content Router (EMCR) that will be capable of sharing the operational picture (information related to the management and response to an emergency situation) among involved responding teams by routing messages. This way relevant information will

reach the appropriate persons at every level of coordination in a timely manner. It can be improved and integrated to share the operational picture to every agency involved in the response at every level of coordination.

Possible events

- The authorities who are responsible for medical supplies and supply chains in governmental and regional level, as well as hospitals, are able to share information on their vaccine amounts during the vaccination campaign. When the sudden loss of vaccination available is noticed the actors can record and make a follow up among themselves on the situation.
- The SMRNS can also be used to gather information on the asthma medicine availability in regions and local pharmacies, pharmacy companies are given access to report on their situation in the tool. When it is noticed that there really is lack of asthma medicine in many of the Vosechia regions then the government can start to plan together with the region's contracts of asthma medicine with new companies. In addition, the situation on the availability of the cargo containers in vessel and especially in the case of medicine supplies can be updated in SMRNS by government to regional level medical actors, such as pharmacies, in order to share information on future prospects.

Possible RED counter actions

- Adversarial actors hack the system in order to gain information about the vaccination supply chain
- Rumours can be spread that SMRNS is such a platform that local pharmacies should not have access to while they do not have authority status and the information is sensitive; in addition, some pharmacies use the information on their own advantage.

INNOVATION 6: SUPPLY CHAIN RISK MANAGEMENT

Possible Use of approach

This IoS card 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, it 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[9].

Possible events

- The governmental and regional health care administrations will use the approach to consider what may follow if they do not start doing contracts with new asthma medicine delivery companies.
- In addition, the governmental and regional health care administrations will use the approach to consider if there would be any other way to get the asthma medicine to the Vosechia than using cargo containers/ vessels?

Possible RED counter actions

[9] https://link.springer.com/chapter/10.1007/978-981-10-4106-8_18

- Adversarial actors by providing fake documents to social media inform that the used approach is insufficient because it does not give accurate situation picture and hence it leads to delayed and risky decision making in such a critical situation.

INNOVATION 7: CYBER SECURITY MANAGEMENT

Possible Use of Innovation 7

Cyber security is the most critical aspect nowadays of our technologically based lives. The public and private sectors 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 organisation and this implementation will guarantee cyber security. This attitude must change because cyber security nowadays is something more than just the technology. By using this IoS card, a taxonomy of the critical infrastructure attacks is provided, analysing attack vectors and attack methods used to damage critical infrastructure as well as the most common cyber security mistakes, which organisations make in the cyber security field when trying to make themselves safer from vulnerabilities.

By implementing this card, theoretical aspects of the cyber security management model will be provided, which can be used to ensure security of critical infrastructure in a country, an organisation or a company.

With this IoS card, Vosechia Government and local actors think what kind of cyber security management they should have taken in order to avoid the situation where the IT-virus to governmental medicine supply chain IT-systems could have been detected on time and this would not happen again.

Possible events

- Vosechia Government officials remain attached to an obsolete and outdated cybersecurity perception that focuses solely on technical aspects ignoring the new cyber threat landscape.

Possible RED counter actions

- Pezetkia may support non state (nonetheless state supported) actors to conduct highly sophisticated cyber operations as to achieve not a destructive attack on Vosechia but rather a gradual weakening of its ability to protect effectively its national infrastructure.

INNOVATION 8: ONLINE SYSTEM FOR FACILITATING EFFICIENT MIGRANT INTEGRATION

Possible Use of Innovation 8

With this IoS card, Vosechia Government could better address the requirements of the migrants and refugees. This tool plans to improve and customize the interfaces used to access key public services by developing a database system named IMMERSE. By using this card, Vosechia Government could facilitate the migrant integration and health management.

Possible events

- Vosechia Government could use this tool for migrants and refugees in order to provide them all relevant information and instructions for the pandemic.
- Moreover, this tool could be used to handle the overall vaccination status in relation to this population.

Possible RED counter actions

- Adversarial actors can hack the system and gain medical information for the migrants and refugees that could be spread in the media. Party W will take advantage of this information in order to increase their anti-refugee agenda based on the claims that the majority of the refugees are sick from the virus.
- Fake news could be spread that the vaccination in refugees' camps is well ahead of plan while the rest of the Vosechia population is not vaccinated in the right pace.

INNOVATION 9: AUTOMATED DETECTION OF HATE SPEECH

Possible Use of Innovation 9

This IoS card can be used by the Vosechia Government to identify hate speech in an extreme form that can lead to hate criminality. To prevent and prosecute crimes connected to that and avoid distrust in society and state this card can be used as an efficient tool to identify hate speech on the internet especially on social media. By implementing this card, Vosechia government could identify hate speech in social media, against refugees and different parties preparing themselves to the elections in order to prevent potential attacks by supporters of Party W to refugee camps and clashes between different parties.

Possible events

- Vosechia Government can use this tool and will be able to prevent and stop coordinated potential attacks on migrants and refugees.
- Moreover, this tool could be used to identify the reasons for the negative attitude towards migration. The possible reason behind this attitude could be disinformation campaigns or discriminatory content of Pezetkia actors supported by party W. By rectifying this information, the conflict to the wider public can be weakened. Overall, by using this tool, Vosechia can improve societal resilience.

Possible RED counter actions

- Adversarial actors can spread over the media that Government is using this tool in order not to let the citizens widely express their opinion. The same rumours present current government as a dictatorship that does not support free speech. In addition, information will be shared that by using this tool, the privacy of the persons that express their opinions in social media is not protected.

5.4. VIGNETTE N 4: STRATCOM AND STATE-CITIZEN-MEDIA TRUST

Core theme	Targeted Context(s)
Ct4: information and strategic communications	1. Going viral 2. Digital monopolies and massification of data 3. Deterioration of the quality of content

Target audience	Prior knowledge
Select the target audience from the following: Practitioners I) *ministry level* (administration), Ii) *local level* (cities and regions), Iii) *support functions to ministry and local levels* (incl. Europe's third sector) Suggested participants: **Consortium, e.g.** ***Practitioners***	**Government (Strategic) Communications** **State-citizen trust (building)** **Fake news, deep fakes** **Data ownership** **Public security and policing**

• Analytical and policy entities: MoD NL, DSB, MTES, MVNIA • Executive security entities: PPHS, Espoo, PLV, ABW, RIA, ZITIS • Information and cybersecurity entities: RIA, ZITIS, MVNIA ***Industry, SME*** To be determined ***RTO, research association, organisations*** • Maldita • URJC **<u>Stakeholder group, e.g.</u>** ***Practitioners (* priority)*** • *Ministry of Justice and Security – **Law and justice** (NL) • Finnish Border Guard - **Border and maritime security, internal and external security** (FI) • Ministry of the Interior Finland, Department for Rescue Services - **Internal security, CBRN, Civil Protection and emergency response** (FI) • *Tromso Police District – **Law enforcement** (NO) ***Industry, SME*** • *Ardanti!Defence- Information technology, digital services (FR) ***RTO, research association, organisations*** • *Institute for Public Goods and Policies; Spanish National Research Council - **Fake news and strategic communication** (ES) • *Ukrainian Association of Scholars and Experts in Field of Criminal Intelligence - **Law enforcement** (UA) • European Security and Defence College - **Crises management** (EU, BE) **Role/position:** Experience level: *Junior to senior officials or subject-matter experts on governmental communications, STRATCOM or state-citizen trust.*	

Disinformation is flourishing and citizen trust in government is decreasing. This decrease of trust in governance is making it harder for governments to communicate effectively to its populaces and is hampering the effectiveness of policies intended in mitigating the pandemic. Even the measures that governments have taken to combat the epidemic in hard-hit regions of *Vosechia* are affected in their effectiveness due to a lack of compliance by the citizenry. As the **Union X expects the crisis to worsen before it gets better, the member states are looking for effective solutions to increase trust in governance, to enhance STRATCOM capabilities, and to regain the compliance of the population to collectively solve the crisis**. Various hostile countries are abusing the crisis in the Union X as an opportunity to further undermine the unity and strength of the Union X by spreading disinformation, especially targeting minority populations in ethnically diverse communities with little to no comprehension of their country of residence's language. *Pezetkia* has taken an active role in such undermining efforts. The local population in *Greyzone* overall consumes a mix of locally produced social media,

national and local mainstream media, but also *Pezetkia* affiliated media that push anti-*Vosechia* and anti-*Union X* messaging, including fake news.

INJECT 1: REGIONAL CRISIS

The region *Greyzone* in the country *Vosechia*, consisting of a mixed population of native Vosechia*ers*, and *Pezetkiaers,* is especially problematic as *Pezetkiaers* are strongly anti-Union X and pro-*Pezetkia*. Trust in the *Vosechia* government and the Union X has always been low in Greyzone, particularly among pro-Pezetkia citizens and is falling further as the government measures to reduce the spread of the virus heavily affects local businesses. What makes things worse: unemployment that was already relatively high in this region is rising to levels previously unknown. Language is becoming more hostile towards other ethnic groups, towards government institutions and the Union X. Conspiracy theories that propagate the idea that *Vosechia* government and Union X measures to address the crisis are merely fronts to subdue the people and have become a normalized interpretation of events. As media organisations continue to report on government policies and guidelines, media and journalists have become targets of the public's outrage. Media organisations' offices have been vandalized with paint and graffiti, and calls are spreading on social media to heckle and attack journalists when spotted in the streets. National police organisations have expressed concerns that the vandalizations and threats are mere preludes for attacks to come. Their greatest concerns lie with the minority population of *Pezetkiaers* who lack the language skills to read government and traditional media communication and rely on social media posts in their multiple native languages. To make matters worse, a video has surfaced on social media showing police officers brutally beating a young *Pezetkiaer* who was caught vandalizing one of the media buildings. The video itself is being widely shared amongst *Pezetkiaer* social media users and has become one of the most watched videos in the *Pezetkiaer* community.

INJECT 2: DEEP FAKES IN SOCIAL MEDIA

Social media have become rife with AI-generated deep fake content, in visual, audio and text formats. The social media platforms have seen in their analyses that user engagement with the deep fake disinformation content is very high. Even more problematic is that after video emerged of police officers beating a *Pezetkiaer*, deep fake videos of other police officers have appeared online. These fake videos do not only show police officers beating up victims, but also allegedly the chief of police caught on camera commenting "Just spit in their faces and let the virus do the rest". Furthermore, deep fake audio has emerged in which the minister of health is reportedly in a confidential discussion stating that the virus was first discovered in *Vosechia* before being reported to the WHO by *Pezetkia*, continuing the myth and falsehood that the virus originated from *Vosechia* instead of *Pezetkia*. Finally, a satirical newspaper has released clearly fake documents allegedly showing how the 'deep state' is responsible for the creation of the virus in a biochemical lab, which studied the effects of viruses on pigs and bats. Nonetheless, unsuspecting users mistook the headline as truth and have begun circulating these documents on social media as well; since the satirical content went viral, new deep fake images of the supposed biochemical lab have emerged. This has led to further protests and unrest. This is only a pick of the vast amount of various deep fakes that are circulating amongst users in *Vosechia* in general and *Greyzone* in specific. Preliminary results indicated that there has been an exponential increase in deep fake content on social media since the start of the crisis and have only amplified the regional crisis.

A private company known as 'Peace Data', which has been linked to election rigging in various countries including Pezetkia, has come under scrutiny. Intelligence reports by *Vosechia* agencies as well as open-source investigative journalism have indicated that this company has been hired by *Pezetkia* officials to buy up data from social media companies, targeting populations within *Greyzone* that are most susceptible to anti-*Vosechia* and anti-Union X disinformation. According to these reports *Pezetkia* has used Peace Data micro targeting analyses to target anti-*Vosechia* groups within *Greyzone* to amplify the effectiveness of *Pezetkia* disinformation efforts.

Whilst social media companies do crack down on outright hateful expression and violent content, their own algorithms cannot keep up with the flood of deep fakes being disseminated on their platform. Simultaneously, their user-engagement algorithms keep feeding users with more related deep fake and disinformation content, as it maintains user engagement and thus increases ad revenue. As a result, social media companies, police the most problematic content, but continue to play an active role in the dissemination of disinformation that is actively undermining the citizenry's trust in the *Vosechia* government and its response to the epidemic. To add insult to injury, social media companies are accused by *Pezetkiaers* of censorship and trying to silence those protesting the *Vosechia* government.

INJECT 3: REGIONAL NEGLECT

In the region of *Greyzone* problems have arisen as a result of a lack of medicine, healthcare capacity, and oxygen supplies that are vital to treat the worst affected. Neither *Vosechia* nor the Union X can spare any additional resources to help dealing with this immense shortage of supplies. Local community leaders have spread conspiracy theories on social media in a mix of the various native languages of the *Vosechiaers* and *Pezetkiaers*. These conspiracy theories allege that the central *Vosechia* government is intentionally neglecting the *Greyzone* region as an experiment to see what will happen if the disease is allowed to rage freely. *Greyzone* was supposedly chosen since it has traditionally been a difficult, anti-*Vosechia,* anti-Union X, and pro-*Pezetkia* region. *Greyzone* has been hit hard by the epidemic, which the central *Vosechia* government has attributed to lower rates of compliance to the measures and a higher rate of scepticism towards the disease in general. The central and local authorities blame each other, whilst an immediate solution to the lack of resources remains side-lined due to a wider shortage of these resources across the country. Meanwhile an ambassador of *Pezetkia* who has in the past tweeted a number of fake conspiracy theories and is notorious for further enflaming tensions between *Pezetkia* and *Vosechia* has retweeted the deep fake audio in which the minister of health states that the virus was first discovered in *Vosechia*. "This once again shows that *Pezetkia* is not responsible for what is happening around the world! It is time for leaders to take their responsibility and stop blaming us for the chaos which they have sowed." the tweet states. *Pezetkia* has simultaneously started a vast PR campaign with videos showcasing trucks filled with medicine and supplies at the *Vosechia-Pezetkia* border. The *Pezetkia* ambassador sent out a second tweet "*Pezetkia* is offering the people of *Greyzone* medicine, doctors and necessary supplies, if only the government of *Vosechia* would allow us to help. But no, they would rather let *Pezetkiaers* in their own country suffer!"

Frustration is rising amongst the local population and during the past two weeks conspiracy theories and disinformation are rife, and a sense of dissent is growing in the streets. Social and local media point to local authorities stating that they are only trying to find out who is to blame within the central government instead of taking ownership of and solving the problems at hand. Furthermore, calls are growing louder to accept the aid of *Pezetkia* citing their ability to control the virus within their own country's borders. Some social media reports are circulating indicating that both the local and central authorities were made aware of the risk of these problems arising by healthcare professionals, but politicians refused to act. *Greyzone* locals and *Pezetkia* officials are quick to point to messaging over the last years by central authorities portraying *Greyzone* as a problematic region, rife with "scum whose norms and values deviate from true *Vosechiaish* norms".

VIGNETTE SPECIFICS

ORGANISATION

The syndicate represents the Department for Regional Security and Safety for the region of *Greyzone* inside the country of *Vosechia* , media companies play a significant role as well.

RISKS

- Rampant disinformation, including (audio, visual, and textual) deep fakes
- Disorder, riots and violence in the streets, particularly targeting media and security forces

- A breakdown in state-citizen-media trust and a vast decrease of confidence in public security and policing
- Social media platforms functioning as information bubbles and echo chambers amplifying the spread and impact of disinformation and conspiracy theories

OBJECTIVES

- Regaining citizen trust in regional and state governance
- Regaining safety and security in the streets
- Protection of media and journalists
- Debunking and limiting impact of disinformation, conspiracy theories and deep fakes
- Limiting the effect of external interference in regional affairs, gaining regional coherence between different groups

MEANS- INNOVATIONS – PLAYCARDS FOR DTAG

INNOVATION 1: JOURNALISM TRUST INITIATIVE

Possible uses of innovation 1

This IoS could help promote trustworthy journalism, reduce disinformation and sets standards of transparency, journalistic methods and ethics. As such it may contribute to regaining the public's trust in media and their reporting. By regaining this trust, (threats of) violence against media should decrease. A major challenge in the use of this IoS is that audiences that are vulnerable to disinformation (such as *Pezetkiaers* in *Greyzone*), tend to not consume the (types of) media that would be a member of the Journalism Trust Initiative. *Pezetkiaers* are likely to read and watch *Pezetkia* media that targets the diaspora of *Pezetkia*, rather than media from their country of residence. As a consequence, *Pezetkiaers* are likely to stay in their own information bubble where an anti-Vosechia narrative is fed to them by *Pezetkia*. Any Journalism Trust initiative that is linked to *Vosechia* authorities can backfire as it is likely to become a target for *Pezetkia* media to forward the narrative that *Vosechia* is actively influencing and feeding the population with biased information.

To overcome such challenges, the Journalism Trust Initiative could target specific sub-populations. Such sub-populations could include groups such as younger people that have less ties to *Pezetkia*, local community leaders, digital influencers, celebrities, and higher educated groups that do speak the language of the Journalism Trust Initiative media members. By targeting influential members of the community, the Journalism Trust Initiative could create a trickle-down effect to reach a wider audience.

In addition, the Journalism Trust Initiative could consider options to include cooperation with central or local authorities on the implementation of oversight on the quality of and adherence to the Journalism Trust Initiative standardization. This also poses blowback risk where such oversight could be perceived as censure of non-adhering media outlets, or even the censoring of free speech. Adversarial actors (like *Pezetkia*) could exploit such blowback by alleging *Vosechia* repression through censorship.

Adversarial actors could also try to infiltrate (media organisations affiliated with) the Journalism Trust Initiative and undermine the IoS from inside out; for example, by undermining the activities and efforts directly; or by leaking internal documents to the public or adversarial actors.

Language barriers that vulnerable populations face is another obstacle that would need to be overcome for the effective exploitation of this IoS.

Overall, the Journalism Trust Initiative is an IoS that works best in circumstances with a strong state-citizen-media relationship. As such, this IoS requires a baseline level of trust in government and is less effective in situations where the disinformation-prone groups consume media inside disinformation bubbles. The Journalism Trust Initiative as such is an IoS best implemented pre-emptively and in the long term.

Possible RED counter-actions:

- Media organisations become a target of an adversarial actor's slanderous disinformation campaign alleging collaboration with a nefarious *Vosechia* state agenda.
- Some media organisations break (for example due to *Pezetkia* pressures) with the Journalism Trust Initiative and allege corruption of the Initiative and/or media landscape and/or the state of Vosechia.
- Targeted sub-populations hijack the message and/or initially cooperate but at a later stage contradict the intended messaging.

INNOVATION 2: DEBUNKING OF FAKE NEWS

Possible uses of innovation 2

Near real time debunking of fake news, using AI and crowdsourced local experts could help battle the rampant disinformation and deep fakes on various social media platforms. By implementing this IoS, disinformation and deep fakes can be stopped in their tracks before they reach their audiences and would have been able to gain a critical mass.

This IoS could be used as a way of mitigating the viral spread of fake news and deep fakes in inject 2. A challenge in the use of this IoS could lie in the (un)willingness of social media platforms to cooperate. Regulators (Union X or *Vosechia*) may want to mandate content moderation, or the elimination of viral fake news, but social media companies could use public opinion against the infringement of free speech to pushback on such efforts.

A major challenge in the use of this IoS is that organisations putting out products debunking fake news need to be trusted. This could be the social media companies themselves, the state, independent oversight entities, (citizen) journalists, or other entities within society. Within the scenario and vignette, there is a clear lack of state-citizen-media trust which complicates the delegation of the execution of debunking to any specific party. Given the financial interests of social media companies to maximize advertisement and user engagement, some parties (like social media companies) are incentivized to counteract the implementation of this IoS.

Possible events

- Social media users are leaving traditional social media and move towards social media platforms that market themselves as beacons of free speech and free of any kind of content moderation. This could turn into a whack-a-mole game between social media users and content moderators, security organisations trying to mitigate the spread of disinformation, fake news and deep fakes.
- Detecting and producing Generative Adversarial Networks (GAN) are constantly outpacing each other's' accuracy and speed to detect/produce deep fakes, leading to a continuous arms race with switching 'winners' between the detecting and producing entities. Citizens no longer trust anything they see, as anything could be a deep fake, or not. Given the low levels of community-media-state trust, any further investments in trying to debunk fake news is only counter-productive. Efforts are slowed down or stopped entirely.
- Social media companies start a widespread lobby campaign to counteract legislators' efforts to mandate the elimination of viral fake news.
- The Union X/Vosechia bans Pezetkia-affiliated media in the *Union X/Vosechia in* an effort to counteract malicious disinformation campaigns. The public becomes outraged at the ban perceived as censorship.

Possible RED counter actions

- Adversarial actors 'flood' (social) media with fake news to the point that AI and crowdsourced local experts cannot keep up with moderating and/or fact-checking the vast amount of material that is being produced. Whilst the IoS works as intended, it is not sufficient in counteracting the vast proliferation and effectiveness of fake news.
- Adversarial actors target the crowdsourced experts as nefarious *Vosechia* actors, alleging corruption and an evil agenda.
- Adversarial actors infiltrate/hack the (organisations running) the detection algorithms, hijacking the IoS and repurposing them to either I) become useless; or II) target real news as fake news.

- When the algorithms/statistical patterns are known and identify content as fake, any generation of deep fakes by Pezetkia actors could be modified to escape such patterns. Interestingly this would in the end screw up the patterns Vosechia Government is using for detection subsequently this might generate a lot of false positives/negatives- and that might enrage the companies and users alike. Hence, they might stop using the filters.

INNOVATION 3: NON-PARTISAN NATIVE-LANGUAGE NEWS CHANNELS FOR MOST INTERDEPENDENT ABROAD REGIONS

Possible uses of innovation 3

This IoS could aid the *Vosechia* government to reach the local minority communities who have not been able to access regular government and media communications channels due to language barriers.

A major challenge for the use of this IoS is that the intended audience is the community that is vulnerable to disinformation, who are already trapped inside a disinformation bubble on alternative and social media. Lack of state-citizen-media trust is hard to breakthrough or regain by the establishment of new news channels when these news channels are supported by government initiatives, since the intended audience is distrustful of *Vosechia* government, Union X, and mainstream media. Collaboration with local community leaders, digital influencers, and other locally trusted, embedded and influential entities could benefit this IoS. Integrating such individuals and/or subgroups could help improve engagement with the newly established news channels. This is however also a blowback risk, as these entities could disproportionally steer the content of these news channels into an alternative direction.

Possible events

- Local community leaders condemn the news channels as propaganda and counterproductive efforts to distract from the very real problems of neglect inside *Greyzone*.
- Mainstream media companies perceive the newly established news channels as (unfair) competition and start their own campaigns to prevent engagement with the new news channels.
- The wider public becomes concerned with the media landscape becoming coopted by the *Vosechia* state and the Union X. Nationwide resistance emerges, organizing demonstrations against the demise of independent media.

Possible RED counter actions

- Adversarial actors like *Pezetkia* target the news channels and start a campaign alleging a nefarious *Vosechia* and/or Union X agenda.

INNOVATION 4: FAIR TRADE DATA PROGRAM

Possible uses of innovation 4

A central problem of how social media companies operate is their monopoly on the data of its users. Through their analyses and algorithms, they keep feeding their users content that is highly engaging, thus retaining consumer engagement and driving advertisement revenue. Humans tend to stay engaged and get addicted reading controversial, upsetting and shocking content. The fair-trade data program would put the users' data back into the users' hands instead of the social media companies. As a result, social media companies would need to ask permissions or even pay for the users' data, which would make it harder for companies like Peace Data to obtain and analyse user behaviour for malign purposes as exemplified by *Pezetkia*. This type of power relations reversal could both i) diminish the amount of micro targeting of users leading to radicalizing disinformation echo-chambers and ii) could impact social media companies' business models and their focus on optimizing user engagement.

A major challenge in implementing this IoS is that (social) media companies have a vested interest to prevent the enactment of such legislation. (Social) Media lobbying efforts to dilute or prevent the implementation of this IoS pose a real threat to the viability of this IoS.

The intended effect of the fair-trade data program is to enable consumers the rights to their (advertisement) data. Yet consumers might not use this empowerment in their best interests. Consumers might still decide to give away or sell their all their data to (a select few or all) entities. Given the financial upside of selling their personal advertisement data might perpetuate the problem the fair-trade data program is intended to mitigate. In such a case, the only real change of the implementation of this IoS would be that the consumers are financially benefitting from the collected data. Social media companies, that generally rely on data collection and targeted advertising for their revenue, would in turn need to reinvent their business models. Here the *Vosechia* government and Union X would need to think of incentives to make the fair-trade data program within the interests of the social media companies, for example by providing support in finding alternative means of revenue.

Possible events

- Consumers proceed with business as usual, enabling the sharing of all their collected data which in turn is still enabling adversarial actors to target vulnerable communities with disinformation.
- Social media companies' lobby succeeds in preventing the enactment of the fair-trade data program.

Possible RED counter actions

- Adversarial actors, like *Pezetkia*, provide alternative free-of-charge free-of-moderation (social) media platforms.

INNOVATION 5: TRAINING APPLICATION FOR MEDIA LITERACY

This IoS intends to empower citizens and making them more critical consumers of media content. Improving citizen resilience through critical media consumption would circumvent problems of distrust towards the *Vosechia* government and the Union X.

Possible uses of innovation 5

In inject 3 we see a typical pattern of hybrid behaviour emerging, the combination of good actor propaganda in combination with putting blame the hybrid actor (promises to) help solve a problem, while in the meantime it puts the blame for the crisis on others. In a training application for media literacy such repeating patterns should be subject to training, so that participants will be more aware of such hybrid behaviour and will be able to recognize it themselves.

However, making citizens more media literate is a long and arduous process, one that is best achieved by implementing such media literacy courses as mandatory education in primary and secondary schools (Finland model). This IoS requires a baseline level of state-citizen-media trust, which might not be present in the most vulnerable populations. Cooperation with local community leaders and digital influencers might improve the

engagement with such training initiatives. Decoupling this training initiative from active problems might further drive community uptake. Including examples of bad government communications could even be a helpful driver to facilitate engagement by disinformation-prone communities. This would simultaneously pose a blowback risk to government credibility and might not be politically expedient.

This IoS would be more effective as a long-term application, ideally in combination with other trust-building initiatives aimed at media institutions. This way all parties to the state-citizen-media relationship would be targeted in the effort to improve mutual trust. This IoS would be best utilized in inject 1, where the focus is on disinformation and hate/violent groups targeting media.

Possible events

- The government enacts mandatory media literacy training as part of school curricula. The public becomes outraged and alleges that the *Vosechia* state and Union X are starting propaganda initiatives.
- Vulnerable communities take up the media literacy trainings, but they are unsuccessful. Consumers still trust fake news (channels) more than actual facts.

Possible RED counter actions

- Adversarial actors, like *Pezetkia*, offer their own media literacy trainings, mitigating the intended effect of the government-supported initiative leading to even more polarization in society.

INNOVATION 6: AUTOMATED FACT CHECKER

Fact-checking is time-consuming. Problematic with the wide proliferation of disinformation and deep fakes is that the time to fact-check and debunk false information/fake news is vastly more time consuming than the time needed to produce it. In addition, by the time viral fake news is being debunked it has often already reached its target audience and done its harm in undermining trust in media and governance.

Possible uses of innovation 6

This innovation can be used by media organisations and fact-checkers to speed up cross-checking the veracity of information. Combined with other trust-building initiatives this could further improve the state-citizen-media trust relationship. This IoS could be used to mitigate the effect of Wolf Warrior diplomacy and false claims made by malign actors (e.g., on the origin of the virus) in inject 3. The automated fact checker could in real-time fact-check and debunk the false information that is propagated as part of Wolf Warrior diplomacy engagement. Since the implementation is intended at the media organisations themselves, the practical use of this IoS poses a challenge for non-compliant media organisations, for example those affiliated with *Pezetkia*. Independent media organisations, oversight bodies, citizen(-journalists) could also make use of the IoS and apply it on fake news disseminating organisations, including *Pezetkia* media; yet the efficacy of the debunked information remains conditional on the trust towards the debunking party.

A major challenge in the use of this IoS is that organisations putting out products debunking fake news need to be trusted. This could be social media companies themselves, the state, independent oversight entities, (citizen) journalists, or other entities within society. Within the scenario and vignette, there is a clear lack of state-citizen-media trust which complicates the delegation of the execution of debunking to any specific party. Given the financial interests of social media companies to maximize advertisement and user engagement, some parties (like social media companies) are incentivized to counteract the implementation of this IoS.

Possible events

- Social media users are leaving traditional social media and move towards social media platforms that market themselves as beacons of free speech and free of any kind of content moderation. This could turn into a whack-a-mole game between social media users and content moderators, security organisations trying to mitigate the spread of disinformation, fake news and deep fakes.
- Detecting and producing Generative Adversarial Networks (GAN) are constantly outpacing each other's' accuracy and speed to detect/produce deep fakes, leading to a continuous arms race with switching 'winners' between the detecting and producing entities. Citizens no longer trust anything they see, as anything could be a deep fake, or not. Given the low levels of community-media-state trust, any further investment in trying to debunk fake news is only counter-productive. Efforts are slowed down or stopped entirely.
- Social media companies start a widespread lobby campaign to counteract legislators' efforts to mandate the elimination of viral fake news.
- The Union X/*Vosechia* bans *Pezetkia*-affiliated media in the Union X/*Vosechia* in an effort to counteract malicious disinformation campaigns. The public becomes outraged at the ban perceived as censorship.

Possible RED counter actions

- Adversarial actors 'flood' (social) media with fake news to the point that AI and crowdsourced local experts cannot keep up with moderating and/or fact-checking the vast amount of material that is being produced.
- Adversarial actors target the crowdsourced experts as nefarious *Vosechia* actors, alleging corruption and an evil agenda.
- Adversarial actors infiltrate/hack the (organisations running) the detection algorithms, hijacking the IoS and repurposing them to either I) become useless; or II) target real news as fake news.

INNOVATION 7: COUNTERING DISINFORMATION WITH STRATEGIC PERSONALIZED ADVERTISING

Possible uses of innovation 7

This IoS could be used in inject 2 and 3 to strategically target populations within *Greyzone* who are caught within certain bubbles of disinformation. Utilizing the same underlying data as 'Peace Data', this IoS could be used in similar fashion to facilitate real news to the public through trusted sources. Essential to this IoS is that the specific 'trusted source' in question would need to be trusted by media, government and the end-user. Blowback risk for establishing trusted sources is that it could be perceived to a state monopolization of the truth. Collaborating with local community leaders and digital influencers could aid in establishing mutually trusted sources within intended communities. In essence this IoS aims at reversing the path the end-user followed when it went "down the rabbit hole" of disinformation in the first place. Discussion within the syndicate on the benefits and risks of using this IoS versus using Innovation 4 (Fair Trade Data Program) might be interesting for the DTAG as a whole.

A major challenge is the potential blowback risk of government-supported trusted news sources. Consumers might perceive this initiative as censorship of free speech, infringement upon the independence of (social) media organisations, or even the emergence of state propaganda.

Possible events

- Social media companies refuse to cooperate with *Vosechia* government supported strategic personalized advertising towards government supported news sources. They cite their responsibility to remain independent and are only willing to engage in advertisement campaigns with private entities.
- Social media users are leaving traditional social media and move towards social media platforms that market themselves as beacons of free speech and free of any kind of content moderation. This could

turn into a whack-a-mole game between social media users and content moderators, security organisations trying to mitigate the spread of disinformation, fake news and deep fakes.

Possible RED counter actions

- Adversarial actors, like *Pezetkia*, obtain (or release fake) documents indicating the collection and use of citizen data to steer consumers' behaviour towards government-supported trusted news sources. *Vosechia* society becomes outraged at what it calls a PSYOPS on its own population. *Pezetkia* seizes the opportunity to allege *Vosechia* and the Union X as nefarious actors engaging in psychological warfare with its own citizens. Polarization and anti-*Vosechia* and anti-EU sentiments skyrocket.
- *Pezetkia* infiltrates (or hacks into) the organisations' algorithms that are nudging consumers towards government-supported trusted news sources. They use the same data to redirect consumers on platforms with ties to *Pezetkia* towards more disinformation. *Greyzone* media consumption splinters into completely disjunct pro-*Vosechia* and anti-*Vosechia* media infospheres.
- *Pezetkia* releases a large media campaign alleging *Vosechia* of 'Orwellian' intentions, policing content, censoring critical thought, monopolizing the truth and endangering *Pezetkiaers* inside *Greyzone* by only allowing falsehoods regarding the *Vosechia* neglect in the region, and the dangers of the virus.

6. PROPOSED TRAINING APPROACH

The training under EU-HYBNET project is composed of a virtual exercise, is addressed to different levels of practitioners, and keeps an inclusive set up to researchers, academics, civil society and the business community in articulating dilemmas, innovations and responses to counter hybrid threats. The focus of the training will be composed by the following aspects:

- Crisis: disruption in management and inability of usual processes to fix the situation. Disruption caused by rupture in management chain, rupture of communications or essential services, damages to fundamental information sensors, blinding effect because loss of benchmarks by management.
- Organisations in defence situations in times of crisis
- Expected outcomes from the organisation in defence situation
- Values are the definition of the organisation. The organisation defends / satisfies its values via its objectives, governance rules, material and immaterial means
- Dilemma solution and value satisfaction compromise
- Fields of competence of the organisation, pursuing differentiated objectives. Activities need material and immaterial means.
- Coexistence with other organisations.
- The source of danger threatens the essential means of the organisation and jeopardizes the ability of the organisation to fulfil its objectives and therefore to sustain the values that define it. The stakes are those objectives threatened by the sources of danger (accident and threat)
- Objective of the system in crisis management is to act on the system to secure the stakes (those objectives threatened by the sources of danger).
    - Strategic level gives to lower levels a series of effects to achieve – watch, anticipation, situation evaluation, decision taking, communication, prospective and planning.
    - Tactical level produces alerts, actions / operations and influence / pr.

In regards to the training schedule, the Consortium plans to schedule a two day event where in each day two vignettes will be played. In every day there will be a 20-minute lecture followed by the exercise. Lectures should be given by experts in order to fully cover the aspects identified in each vignette as prior knowledge. Preparatory activities will be also needed from the training participants before the actual training delivery.

6.1. METHODOLOGY FOR MEASURING THE TRAINING IMPACT

For the evaluation of a training, different metrics that can be used to assess the effectiveness of the training programme on trainees. Metrics can be grouped under categories, e.g., personal skills vs. team skills or technical vs. not technical. Since education effectiveness and trainee performance are not only related to the level of knowledge and skills possessed by the trainee upon the completion of the training programme but also to the amount of knowledge and skills actually gained by the trainee in the course of the training programme, this dimension is proposed to be considered as well.

Metrics monitor the accomplishment of the awareness and training programme goals and objectives by:

- quantifying the level of implementation of awareness and training,
- quantifying the effectiveness and efficiency of the awareness and training,
- analysing the adequacy of awareness and training efforts, and
- identifying possible improvements.

Moreover, it is important to consider the tools and methods for measuring and quantifying trainee performance assessment metrics. Both objective measures and subjective measures (instructor-based assessment) should be considered. It is important to mention that NIST promotes the use of Evaluation Forms and Questionnaires,

implemented in a way that eliminates the need for a lot of writing on the part of the person completing them. The key is to design the forms to be as “user-friendly” as possible.

In this context and for the purpose of the evaluation training in the EU-HYBNET, questionnaires could be used as means for the evaluation of training programmes, providing the ability to quickly elicit information about the current state of the trainee, regarding their knowledge and behaviour. Successful questionnaires should be short, relevant, close to the interests of the participants, focused and concise. Questionnaires can be used before and after a training session, at first to infer prior knowledge, competence and relevant skills, and later to extrapolate any changes, behavioural, technical or logical on the subject, measuring the understanding and know-how that the respondent has acquired from the course, and to give a conclusion whether the course has been completed successfully or not. These modules need to be conducted in a way which will support the learning method and measure the knowledge acquired during the course. Questionnaires may be administered electronically through measurement forms, which allow for the collection of a large dataset of information at the same time with relatively little effort. It is important that measurement forms are filled in while the user is still mentally engaged, otherwise results may be inaccurate, due to memory fading.

The questionnaire is a broad method which includes a set of different instrument types (e.g. scales and inventories). It can be effectively used to measure and assess behaviour, opinion and attitude towards some specific situation or topic without the involvement of an interviewer/researcher and is used to collect standardized data from large numbers of participants, which will spare resources (e.g. time and money) and permits to collect the same information in similar way, therefore allows making generalizations based on collected information.

The training is designed to test innovations in order to know which of them practitioners and other relevant actors see such that they wish to recommend for innovation uptake considerations. In this context and having the above mentioned in mind, the EU-HYBNET training evaluation should focus on both practitioners skills and innovations’ importance to the participants involved.

7. CONCLUSIONS

In this document we have described the important aspects for the implementation of the EU-HYBNET training on M12. The necessary scenario and vignettes that will be used as the backbone of the training have been described. The wargame methodology that is selected is briefly introduced as well as the DTAG tool that will be used for the implementation of the training itself.

In more detail, the current deliverable has presented one background scenario depicting a pandemic situation similar to the one of Covid-19 but with more severe effects. In order to support the training implementation, the different actors and the relevant organisations that participate in the scenario are also described in order to give a clear picture to the training participants of the general context that the vignettes will be played. Following the above, in section 5 four vignettes are introduced, each one composed by three injects and addressing each one of the four core themes of the EU-HYBNET project (i.e. [1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication). The suitable audience for each vignette is selected and the prior knowledge has been identified. The risks, the objectives and the relevant organisations associated with each vignette have also been identified. Moreover, in the same section the different innovations that could be used as Innovation Cards during the training in order to address the challenges of each inject are described with details regarding their potential usage, the possible events that could follow as well as the possible reaction of the adversarial actor. Finally, in section 6 the proposed training outline and the methodology for measuring the training impact are briefly introduced. These aspects will of course be finalized under Task 2.4 while the details for the training are designed.

Overall, the scenario and vignettes design address important challenges in the hybrid threats sphere tackling the identified practitioners needs under WP2. Based on these needs the training objectives have been set and the most suitable training format has been chosen. Moreover, the innovations, technical and non -technical ones, have been presented as playing cards in order to identify their importance to the end users in the context of a real-life situation. The innovations testing is in the central of the training in order to learn what are the innovations that may work as solutions to practitioners gaps and needs to counter hybrid threats .The deliverable serves as the first step for the implementation of the training, setting up the training principles and content.

8. FUTURE WORK

This deliverable plans the training scenarios and eventually the training activities where the most promising innovation to the identified gaps and needs will be tested. The work performed in D2.17 is of high importance in the project's proceeding and will feed information to T2.4 - Training and Exercises for Needs and Gaps. In particular, this training/knowledge exchange event is relevant to all EU-HYBNET's Network and will take place in M12, with its results reported in the relevant D2.20 – Training and exercises Delivery on up-to-date topics. It is important to highlight here that the final scenarios and vignettes can be refined in order to better serve the training needs that will occur in the future.

These changes will be introduced in D2.26 – *Training and Exercises Scenario and Training Material* in M17. More specifically, training material will be selected based on the vignettes mentioned in section 5. This will be delivered as a lecture during the training. Following the implementation of the training the Consortium could manage to identify which innovations are important for the end users. This will be fed to task 3.1 and WP4. With reference to this D2.23 "1st Training and Exercises Lessons Learned Report" is important to T3. and WP4 also because it delivers evaluation results on training itself and the innovations that are seen most promising for innovation uptake.

Lastly, the importance of D2.17 to the future project's work is that the implementation of the training activities under the scenarios developed in T2.3 will provide input to the next cycle of the identification of new Gaps and Needs under the scope of T2.1. Moreover, and since several new needs may arise in the following cycles of the project, the scenarios will be developed with the overall goal to serve these needs against hybrid threats and taking into account the four core themes as well. In addition, these specific scenarios will include elements required to test innovative solutions related to T3.2 and T3.3 serve for the training and exercises arranged in the in the following second and third cycle of EU-HYBNET respectively.

Annex I. 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.

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

[4] https://www.act.nato.int/images/stories/structure/jft/bi-sc-75-3_final.pdf

[5] https://www.innovationhub-act.org/sites/default/files/docs/DTAG%20handbook.pdf

Annex II. Glossary and acronyms

Term	Definition / description
AI	Artificial Intelligence
CBRN	Chemical, Biological, Radiological, And Nuclear
CDA	Cyber Defense Alliance
CDC	Center For Disease Control
CI	Critical Infrastructure
CSIRT	Computer Security Incident Response Teams
DCU	Digital Crime Unit
DDOS	Distributed Denial Of Service
DTAG	Disruptive Technology Assessment Game
EMCR	Emergency Message Content Router
EU	European Union
GAN	Generative Adversarial Networks
ISAC	Information Sharing And Analysis Centers
IT	Information Technology
IoS	Ideas Of Systems
KRSC	Key Resources Supply Chains
MRI	Magnetic Resonance Imaging
MS	Member States
NGO	Non-Governmental Organisations
PC	Personal Computer
PR	Personal Relation
PSYOPS	Psychological Operations
QR	Quick Response
RDIP	Resilient Democracy Infrastructure Platform
RTO	Research And Technology Organisation
SCRM	Supply Chain Risk Management
SME	Small Medium Enterprise
SMRNS	Smart Message Routing And Notification Service
SOME	Social Media

TPM	Techniques- Processes- Methodologies
TRL	Technology Readiness Level
TTP	Tactics, Techniques, And Procedures
WHO	World Health Organisation
KEMEA	Kentro Meleton Asfaleias
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
HybridCoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
NL MoD	Ministry of Defence in Netherlands
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
PPHS	Polish Platform for Homeland Security
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
URJC	University of Rey Juan Carlos
UiT	Universitetet i Tromsoe, Artic University in Norway