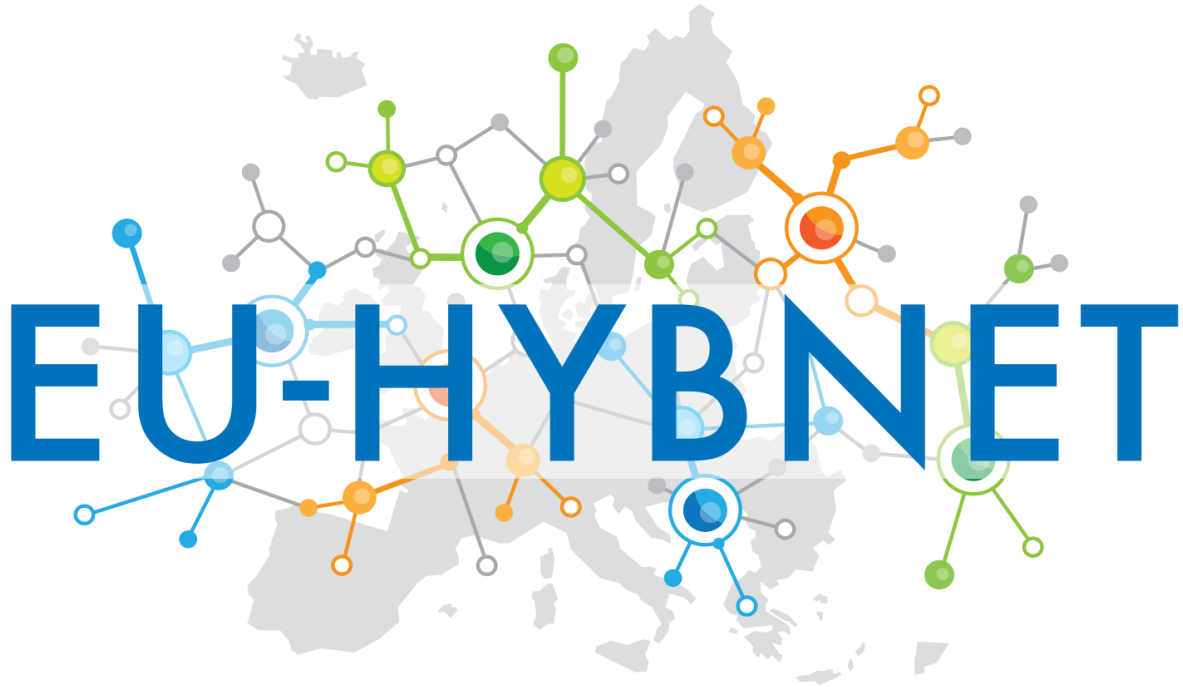

TRAINING AND EXERCISES LESSONS LEARNED REPORT

Deliverable 2.23

Lead Author: Hybrid CoE

Contributors: L3CE, Laurea
Deliverable classification: Public (PU)

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

D2.23 TRAINING AND EXERCISES LESSONS LEARNED REPORT

Deliverable number:	**2.23**	
Version:	**2.0**	
Delivery date:	**1/7/2021 and 31/8/2021**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main author:	**Maxime Lebrun**	**Hybrid CoE**
Contributors:	**Emma Lappalainen** **Rimantas Zylius** **Päivi Mattila**	**Hybrid CoE** **L3CE** **Laurea**

DOCUMENT CONTROL

Version	Date	Authors	Changes
V01	31/5/2021	Maxime Lebrun, Emma Lappalainen/ Hybrid CoE	First draft
V02	25/6/2021	Rimantas Zylius/ L3CE	Review and comments
V03	30/6/2021	Maxime Lebrun/ Hybrid CoE	Text editing
V04	30/6/2021	Päivi Mattila/ Laurea	Review
V1.0	1/7/2021	Päivi Mattila/ Laurea	Submission of the deliverable
V1.1	31/8/2021	Emma Lappalainen/ Hybrid CoE	Text editing
V1.2	31/8/2021	Päivi Mattila/ Laurea	Review
V2.0	31/8/2021	Päivi Mattila/ Laurea	Submission to the EC

DISCLAIMER

TABLE OF CONTENTS

1. Introduction 3

1.1 Overview 3

1.2 Exercises and EU-HYBNET project 4

2. Vignette on Strategic inter-agency coordination – need for damage assessment and contingency management at strategic level. 5

2.1 Dilemmas: assumptions and caveats 5

2.2 Action points 5

2.3 Impact evaluation: assessment results of the IoS 6

3. Vignette on Attacks on financial sector, vaccine chain and individual data – need for responses 7

3.1 Dilemmas: assumptions and caveats 7

3.2 Action points 7

3.3 Impact evaluation: assessment results of the IoS 7

4. Vignette on sanitary restrictions and regionalized protest and movement – need for integration 9

4.1 Dilemmas: assumptions and caveats 9

4.2 Action points 9

4.3 Impact evaluation: assessment results of the IoS 9

5. Vignette on Strategic communication and state-citizen-Media trust 11

5.1 Dilemmas: assumptions and caveats 11

5.2 Action points 11

5.2 Impact evaluation: assessment results of the IoS 11

5. CONCLUSION 13

5.2 FUTURE WORK 13

6. Bibliography 14

ANNEX I. GLOSSARY AND ACRONYMS 14

1. INTRODUCTION

1.1 OVERVIEW

This Training and Exercise Lessons Learned report concerns the results of the exercise organized as part of the project Pan-European Network to Counter Hybrid Threats (EU-HYBNET). The exercise is part of the project's Work Package (WP) number 2, *Gaps and needs of European actors against hybrid threats*. The work in this WP starts with the mapping of and analysis of most crucial gaps and needs, continues in producing of research articles on these, and ends in scenario writing and scenario-based exercise. The lessons drawn from this exercise will be used by the WP number 3, *Surveys to technology, research and innovations*, and the WP number 4, *Recommendations for innovations uptake and standardization,* in support to defining the innovation potential, needs for standardization and recommendations for uptake.

The purpose of the exercise was to contribute to enhancing the knowledge and performance of European actors against hybrid threats. The chosen game format for this project cycle was a Disruptive Technology Assessment Game (DTAG). The game was developed for four different vignettes that each targeted one of the core themes of EU-HYBNET. The EU-HYBNET project four core themes are the following: *Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; and Information and Strategic Communication*. A full account of the game proceeding itself can be found in EU-HYBNET deliverable number 2.20, *Training and exercises delivery on up-to-date topics*.

A DTAG is a seminar type wargame, used to assess potential innovations and their impact on the operating environment, in this instance a hybrid campaign. The DTAG essentially allows to employ innovations, or so-called **Ideas of Systems** (IoSs) to address problems contained in the gameplay. The IoS cards depicted under each vignette derive from Deliverable 3.1, *Identification of target areas for improvement and innovations* by TNO.

The IoS were treated on a conceptual and abstract level in order to explore their desirable outlook and potential misuse. This analysis is the result of several focus groups reflecting on the same situation. The lessons learned concern the substantial results of the reflections of those groups, not their format. They touch upon the kind of dilemmas that the participants found within the scenario and the vignettes, and also while imagining a series of action points to counter and mitigate the disruptions and crisis.

In this context, the participants exchanged on the conceptual outlook, feasibility and opportunity of the different innovations (Ideas of systems). The lessons learned must be taken as a discursive contribution to reflections around mitigating disruptions associated with hybrid threats. The elements presented in this deliverable form part of a methodology in order to contribute to the assessment of the ideas of systems. The ideas of systems, or innovations, are ideas of a varying degree of abstraction which could contribute in reducing European societies' vulnerability to hybrid threats. Together, those ideas of systems are meant as indicators of what could be done throughout policies aimed at addressing the challenges of hybrid threats across the domains of the conceptual model. While EU-HYBNET aims at highlighting new ideas of systems, an essential part of the added value of the project is to spot and link those applications and systems already in use which would provide a benefit in addressing the challenges of hybrid threats.

The lessons learned will be presented per the four vignettes. Each lesson includes 1) short description of the topic/s; 2) Identified dilemmas in this topic (assumptions and caveats); 3) Action points that the participants suggested; 4) Impact assessment of the results. This deliverable contributes in particular to the second and third lines of action of EU-HYBNET (common requirements as regards innovations that could fill gaps and needs; priorities in increasing knowledge and performance requiring standardisation).

1.2 EXERCISES AND EU-HYBNET PROJECT

The exercise is product of task (T) number 2.4, Training and exercises for needs and solutions for gaps. As stated in the Description of Action of the project, the goal of this task is to enhance knowledge and performance of European Actors against hybrid threats. In addition, T2.4 provides an arena to test innovations selected by EU-HYBNET WP3 T3.1, T3.2 and T3.3 to the identified gaps and needs. It contributes to the expected medium-term impact of the project (to take more efficient use of investments made across Europe in training facilities) by testing the innovations identified in the project cycle (specifically in task 3.1, *Definition of target areas for improvement and innovations*).

The lessons learned report will first and foremost support defining of the innovative solutions that can be fed to the EC procurement process. This is a key performance indicator under project objective 2, which is to define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats. Towards this objective, the lessons learned report may also support defining future focus areas for research articles under the four core themes.

2. VIGNETTE ON 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 of messages among agencies, responders and create the conditions for crisis management and resilience of society. The expected outcome of the use of these solutions were better situational awareness, sharing tools and specific cooperation procedures to access specific instructions on what to do.

2.1 DILEMMAS: ASSUMPTIONS AND CAVEATS

Participants highlighted a series of assumptions related to the situation and disruptions. Mobile phones infrastructure would be expected to collapse last and hold the longest because of the low amount of energy required to make it work and due to its scattered, redundant network infrastructure. On the contrary, the participants assumed rail and train networks would shut down very early on because of the important amount of energy consumed. Power grid dispatching devices being out of service or unreliable, energy dispatching was identified a core issue of the crisis while generators would only be expected to last a limited amount of time.

The participants pointed out to a series of caveats in framing their response to the disruptions. Because energy provision rationing is technically not feasible, regulating the flow of energy would entail cutting off entire zones. Differentiated power cuts into entire zones can be framed discriminatory and is an easy target for disinformation. It could be a focal point for the social demand and supply of disinformation to meet. Power cuts would further undermine the reliability of communication devices and networks. In order to counter a computational propaganda / micro-targeting campaign, the opportunity to use counter micro-targeting was discussed but was singled out as a massive reputational liability.

Other notions were following: Lack of knowledge and resources can be exploited by actors; Reactions can raise questions in terms of privacy.

2.2 ACTION POINTS

- Participants recommended to **communicate not only online but also offline** in the physical world in order to get around the foreseeable unreliability of communication networks.
- A series of priorities were identified: locating the attack sources, vectors and surfaces for better reactivity.
- In the immediate order of events, it was seen important to focus on stabilizing the power grids, use gravitational water energy for instance as a substitute in order to maintain energy supply.
- More generally, **connections and sharing of information** should be enhanced and made natural via prior sustained engagement between services and institutions dealing with power supply.
- Communications would benefit from establishing an *ad hoc* **war room**, while specially integrating locally trusted sources and relays for strategic messaging.
- Informing the public via micro-targeted approaches was deemed a reputational cost while it would only reinforce the social receptivity of disinformation as it would appear as it the state would attempt to manipulate the facts and craft its own truth.

2.3 IMPACT EVALUATION: ASSESSMENT RESULTS OF THE IOS

IoS card	Name of IoS[1]
1	**Cross-sector cyber threat info sharing platform**
	This IoS should find synergies, complementarity and continuity with the CERT-EU model in order to deepen it and integrate the channels and the circuits of disinformation supply. Horizon2020 *Concordia* project has for instance resulted in "Threat Intelligence Platforms for Europe" enabling cross sector collaboration. It is based on a mutual cyber intelligence sharing agreement among partners. Such arrangement would be a way to join up disparate sources of information, based on open-source information and partners' information.
2	**Resilient Democracy Infrastructure Platform (RDIP)**
	An RDIP would prove beneficial if it would be a bi-directional feedback loop, increasing communication outreach and preventing miscommunication to an extent. The platform would require reliable energy supply while SMS Messages would prove more direct and less costly in terms of energy. A modular system could be envisaged, with different digital configurations according to the level of crisis intensity. An EU cross border perspective is essential.
3	**Early damage assessment system**
	Algorithms with the object of a rapid damage assessment can form a system and automatize the reaction process during a severe event. This would take the form of a Critical Infrastructure Resilience Platform (CIRP) when fed with real time nowcasting or forecasting data instead of a scenario hazard. It can be turned into 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. It would be a long term investment supporting and enabling other IoSs. Metadata analysis is essential in this loop. The idea is in use within Horizon2020 projects such as I*NFRASTRESS* and *7Shield* and *EU-Circle*.

[1] The IoS cards depicted under each vignette derive from Deliverable 3.1, *Identification of target areas for improvement and innovations* by TNO.

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

Introduction: Hybrid threat actors use the opportunity of vaccine supplies arrival to recruit hackers and interfere with the supply chain logistics in order to create disruptions and shortages of medical supplies. A massive disinformation campaign takes hold with threat actors diffusing fake news stories regarding both the cybercriminals activities and the attacks on the financial system. A quantum technology enhanced cyber attack campaign targets the financial sector; hackers target the critical companies for production and distribution of vaccine and medical supplies.

3.1 DILEMMAS: ASSUMPTIONS AND CAVEATS

In a situation depicting cyber-attacks on financial institutions including or leading to data leaks of sensitive information, the participants deemed a good level of information to the population to be a key factor of disruption management and as something of which the strategic level should be competent in terms of framing other responses. The main assumptions concerned the fact that individual data leak from financial institutions could have an equally dangerous impact as logistical chains disruptions.

3.2 ACTION POINTS

- Participants deemed it necessary on a technical level to close down all possible systems in the face of quantum attacks and ban all unnecessary financial transactions
- while reviewing procedures and coming up with a digital rescue package – via a NIST structured response.
- The participants also deemed it necessary to build secure and constant communication systems with the population in order to increase transparency as to what is happening in order to counter the spread of disinformation.

3.3 IMPACT EVALUATION: ASSESSMENT RESULTS OF THE IOS

IoS card	Name of IoS
1	**Blockchain real time info management and monitoring system**
	This idea of system would be a real time operationalization of addressing the critical character of foreign direct investments monitoring. The main idea of this system would a constantly up to date visualization of transactions based on companies' and governments' information sharing. This idea raises issues in terms of market freedom and privacy and it should therefore be limited to those restrictively defined critical sectors of the economy that affect societal stability and resilience of society. The information would be verified and transactions authorized based on blockchain technology, rendering transactions transparent and giving the means of verification. Keeping the system running while tracking transactions, not getting down by threat actors, applied across infrastructures.
2	**Quantum key distribution testbed**
	Scalable solutions in different infrastructure for protection against quantum computing enhanced attacks. The *QKD* project consortium should be leveraged in order to have updates on the most relevant advances in terms of quantum secure communications. This could apply in terms of B2C and

	B2B communication as well as emergency communications in times of crisis. Quantum communication engagement would enhance the security of institutional communications.
3	**Public-private information sharing groups**
	Crowd sourcing for generating ever more complete pictures of an ongoing situation or crisis. This would need to deepen information sharing among institutions coming from the grassroots. Need to estimate a system to flow information in a double feedback loop. Possibility for thematic groups. Consideration on open source to track cyber criminals and hackers, increase the risk of prosecution for them and raise the costs of engaging cyber action.
4	**Hyper connectivity network**
	High speed information sharing to be exploited by CERT EU teams. This idea is connecting the NIS Directive article 12 establishment of CSIRT networks in order to exchange information on zera day and other vulnerabilities, including TTPs for cyber threats. This would leverage the hyper connectivity of networks.

4. VIGNETTE ON SANITARY RESTRICTIONS AND REGIONALIZED PROTEST AND MOVEMENT – NEED FOR INTEGRATION

While sanitary restrictions are underway, hybrid threat actors have identified this moment as the perfect time for action, as governments try to maintain order and threat actors attempt to cause further rifts within societies by exploiting social fault lines. Hybrid threat actors exploit this by using social media to stir discontent against the governmental regulations and furthermore, due to inefficient governmental communication even manages to convince local/regional authorities to openly oppose the government. With vaccines rollout, hybrid threat actors have exploited the critical supply chain of vaccines as well as the IT system which registers the vaccine rollout within the country. By manipulating the data of the vaccine rollout, conducting wolf-warrior diplomacy as well as spreading fake news via scientific articles that alternative medicines could help, this leads to a shortage in the alternative medicine, a fall in governmental trust and delays in vaccine rollout.

4.1 DILEMMAS: ASSUMPTIONS AND CAVEATS

Participants deemed such a situation to be especially conducive of the social receptivity to disinformation and supply of disinformation. In this sense, an important assumption concerned ways of gathering the general perception of the population, in order to assess feelings and social dynamics environment. The assumption according to which anticipating population sentiment will be difficult and unreliable in such a disinformation environment is an important measure of governmental action opportunity.

4.2 ACTION POINTS

- In order to boost situational awareness, participants recommended conducting environmental scans of media instruments to have an overview of the disinformation being spread, and make use of Facebook style fact checkers.

4.3 IMPACT EVALUATION: ASSESSMENT RESULTS OF THE IOS

IoS card	Name of IoS
1	**Emotions' detection tool and automated detection of hate speech in social media**
	Semantic analysis and machine learning are a usual part of the work with big data. By training the used algorithm to map a group of words to the most likely meaning, a detection of a particular topic can be performed. For example, several *Github projects* provide tools to detect hate speech. Such concepts are already used on Twitter to detect and censor discriminatory contents. Detection and analysis of emojis. Tools subject to spoofing, fake accounts, artificially generated content, large group of bystanders on social media. Here is a need to directly connect with and engage the social media platforms on this type of work.
2	**Smart messaging routing and notification service**
	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. 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. This idea is implemented in Horizon2020 projects *InfraStress* and *SATIE*.

3	**Resilient Democracy Infrastructure Platform**
	Medical and scientific experts in line with crisis topic. Generating open and transparent discussion. Modularity of the RDIP based in peace time for specifics of the crisis. Diffusion of important information and expert advice, crowdsourcing the gathering of information.

5. VIGNETTE ON STRATEGIC COMMUNICATION AND STATE-CITIZEN-MEDIA TRUST

In this vignette, the region Greyzone is experiencing unprecedented levels of unemployment, extremely high rates of government distrust. Conspiracy theories that the pandemic is merely a front to subdue the population have become normalized. Media organizations' buildings and journalists have become targets of violence. Media engagement with conspiracy theories continues to grow and intelligence agencies are warning of escalating unrest and violence. A video showing police beating a local citizen has become a focal point of outcry over police brutality. Escalation of AI-generated deep fake content, in visual, audio and text formats. Social media platforms witness high engagement with such content. Given the public outcry over the video of police violence from the previous inject has led to a proliferation of deep fake content on police violence. In addition, a private data analysis company known as 'Peace Data', linked to election rigging in authoritarian countries, has been flagged by intelligence agencies and investigative journalists as being involved in amplifying disinformation and inciting violence in the region. Lastly, social media companies are unable to remove conspiracy theories, disinformation, hate speech and violent content from their platform.

5.1 DILEMMAS: ASSUMPTIONS AND CAVEATS

- The main assumption by the participants was the impact of images of police violence.
- Another assumption was the absence of transparency of the circuits of creation of deepfakes and the utilization of personal data for it.
- The importance of accountability and transparency in the fight against the pandemic were core assumptions as well.

5.2 ACTION POINTS

- The participants suggested setting up a dashboard for monitoring and presenting transparency of information and procedures.
- In terms of countering deepfakes, the participants stressed the centrality of detection of fake news as it is more important pressing than timely debunking of the fake facts.
- There is also a need for inoculation of populations with fake news: increasing their immunity by informing them in advance that they might be targeted by fake news or deepfakes.

5.2 IMPACT EVALUATION: ASSESSMENT RESULTS OF THE IOS

IoS card	Name of IoS
1	**Guides to identify fakes**
	Debunking fake news using dashboard website, open source debunking platform. Integrate the usual channels of disinformation identified. Ethics and definition questions of a debunking platform are crucial. Citizen engagement and collaboration a major challenge – good faith engagement with platform a big challenge. Frameworks and working methods and definitions on deepfakes. Guide to identify fakes could be used in order to raise awareness on practices that improve abilities to detect fake images and videos online.
2	**Strategic personalized advertising**

	Due to ethical concerns, this option was not taken into further discussion.

5. CONCLUSION

The Lessons Learned report has highlighted the key assumptions and caveats of the exercise participants when they were applying the ideas of systems to the imaginary hybrid threat situations. The assumptions have demonstrated the vulnerabilities and strengths of the European actors and they should be reflected in the future exercises where participants have the opportunity to practice decision-making.

The innovation potential and usability of the ideas of systems are reflected in each vignette where they were applied. Strategic personal advertising seems to have clearly the lowest innovation potential due to its ethical constraints. The ethical aspects of information influencing must be kept in mind, and the population should be protected from all sorts of covert manipulation. Democratic societies must protect themselves also of themselves, and be vary of taking automatic systems into use, that might infringe the freedom of speech and expression.

5.2 FUTURE WORK

The importance of this deliverable (D2.23) is to contribute to the next scenario drafting and exercise delivery by pointing out the challenges and possible solutions. In addition, the D2.23 provides information for EU-HYBNET WP3 and WP4 to define the tested innovations potential, needs for standardisation and to compile recommendations of innovations uptake (incl. industrialisation) in the project.

6. BIBLIOGRAPHY

EU-HYBNET Deliverable 3.1, *Identification of target areas for improvement and innovations*, July 2021, TNO

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	Pan-European Network to Counter Hybrid Threats
EU	European Union
EC	European Commission
H2020, Horizon2020	European Commission Horizon 2020 Project Funding Program
DTAG	Disruptive Technology Assessment Game
IoS	Ideas of Systems
WP	Work Package
T	Task
OB	Project objective
Hybrid CoE	European Center of Excellence for Countering Hybrid Threats
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
Laurea	Laurea University of Applied Sciences
INFRASTRESS	"Protecting the infrastructure of Europe and the people in the European smart cities" H2020 project
7SHIELDS	"Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats" –H2020 project
EU-CIRCLE	"A pan-European Framework for Strengthening Critical Infrastructure Resilience to Climate Change" -H2020 project
CONCORDIA	"Cyber Security Competence For Research and Innovation" –H2020 project
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
SATIE	"Security for Air Transport Infrastructure or Europe" –H2020 project
TTPs	Tactics, Techniques, Procedures
NIS directive	European Commission, Security of Network and Information Systems –directive
B2C	Business to Consumer
B2B	Business to Business