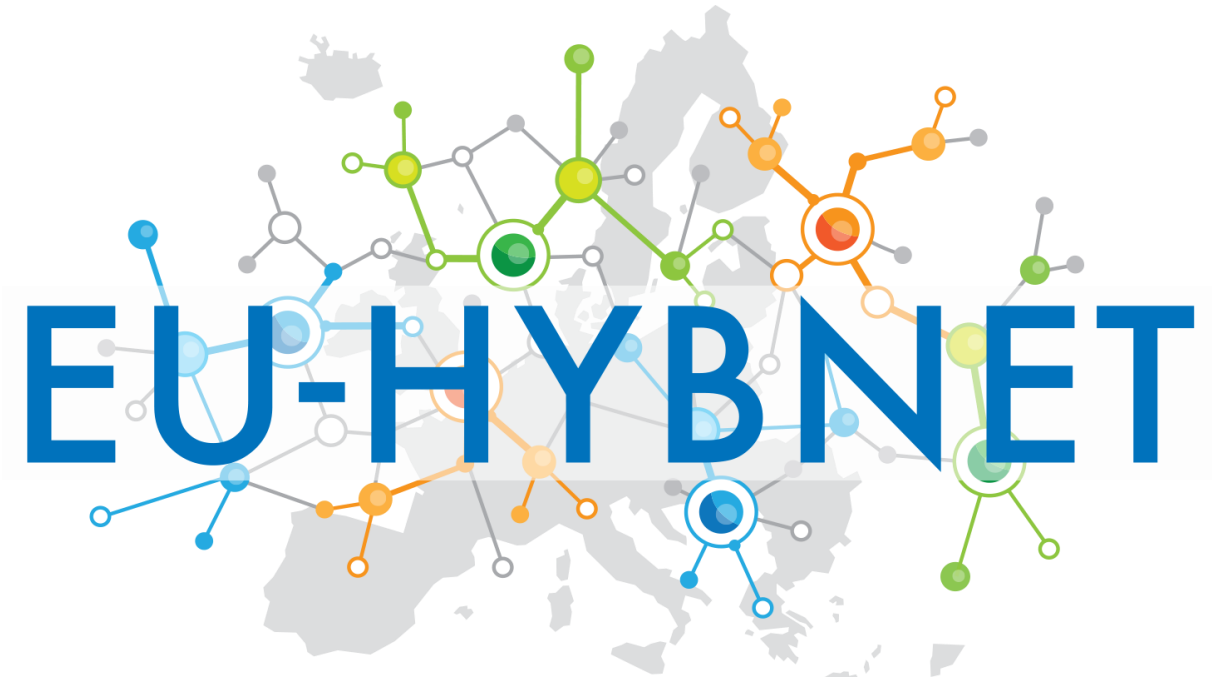

2ND POLICY BRIEFS, POSITION PAPERS, RECOMMENDATIONS REPORT

DELIVERABLE 4.13

Lead Author: Hybrid CoE

Contributors: RISE, 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

D4.13 2ND POLICY BRIEFS, POSITION PAPERS, RECOMMENDATIONS REPORT

Deliverable number:	**D4.13**	
Version:	**V1.0**	
Delivery date:	**02/6/2023**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	**Hybrid CoE**	**Maxime Lebrun & Hanne Dumur-Laanila**
Contributors:	**RISE**	**Rolf Blom**
	Laurea	**Päivi Mattila, Jari Räsänen, Isto Mattila**
	L3CE	**Rimantas Žylius**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	13/05/2023	Hanne Dumur-Laanila/ Hybrid CoE	First draft
0.2	19/05/2023	Hanne Dumur-Laanila/ Hybrid CoE	Information about next policy brief added
0.3	19/05/2023	Maxime Lebrun/ Hybrid CoE	Review
0.4	19/05/2023	Rolf Blom/ RISE	Text delivery describing the aims for next policy brief
0.5	23/3/2023	Päivi Mattila/ Laurea	Review and suggestions for text editing
0.6	24/05/2023	Jari Räsänen/Laurea	Review and suggestions for text editing
0.7	29/05/2023	Rimantas Žylius / L3CE	Review and suggestions for text editing
0.8	30/05/2023	Isto Mattila/ Laurea	Review and suggestions for text editing
0.9	30/05/2023	Hanne Dumur-Laanila and Maxime Lebrun/ Hybrid CoE	Final editing
1.0	02/06/2023	Päivi Mattila/ Laurea	Final review and submission to the EC for a 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.

CONTENTS

TABLES

FIGURES

1 INTRODUCTION

1.1 OVERVIEW

The Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET) project delivers a series of policy papers, recommendations and briefs on a variety of issues relevant to countering hybrid threats and for different levels of practitioners as appropriate. It is part of WP4, Task 4.4 consolidates the results of WPs 2, 3 and 4 in order to present some of the issue findings and area-specific considerations.

The main objective of this document is to describe policy briefs, position papers and recommendations reports delivered in EU-HYBNET Work Package (WP) 4 "Recommendations for Innovations Uptake and Standardization", Task (T) 4.4 "Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge" and their importance to the project proceeding. One policy brief will be highlighted in this document.

The project picture below describes the importance of T4.4 in the flow of project work and results delivery for wider knowledge of pan-European stakeholders.

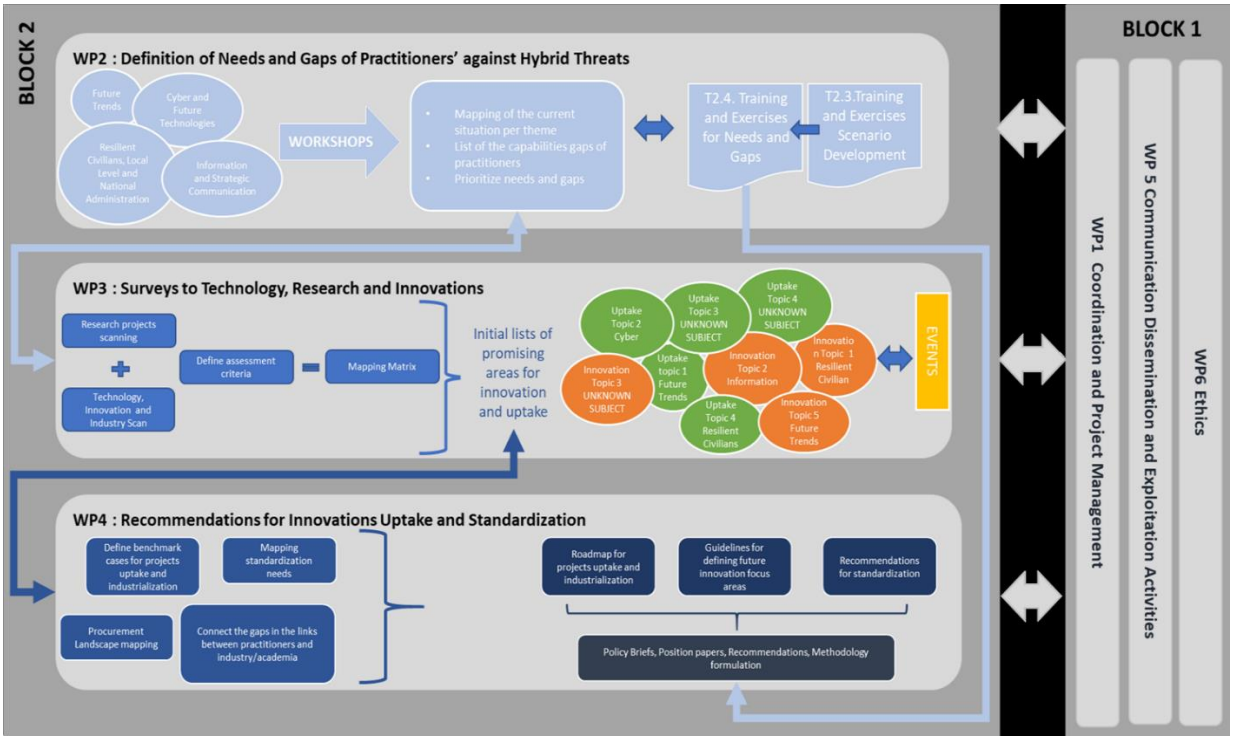

Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

This deliverable and in particular the policy briefs delivered by the EU-HYBNET project in general fulfil following project objective:

OB4: To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation for empowering the Pan-European network to effectively counter hybrid threats			
Goal		**KPI description**	**KPI target value**
4.4	To facilitate policy dialogues on future European research and innovation focus areas supporting innovation uptake	Policy related briefs written up on core research and innovation actions	-At least 7 policy briefs over 5 years for wider audiences and policy makers

1.2 STRUCTURE OF THE DELIVERABLE

This deliverable will introduce the key points of the 4th policy brief *Fame on social media, a new currency of cybercrime?*[1]

Cybercriminal activity has significantly increased in the past years, making it one of the most critical features of global security. Cybercriminal groups are more professionalised and increasingly entrepreneurial. These groups are developing their business models, diversifying products, and selling them in turn to third parties. The Russian war against Ukraine aroused incentives to use new or well-established cybercriminal groups to partake in state sponsored warfare.

The exposure for popularity and notoriety attracts especially younger audiences. The mixture of talent, reputation, achievements, and resources can leverage the individuals personal or group capabilities leading into an escalation of cyberattacks and development of more advanced technical skills.

Cybercriminal groups use public channels to claim attacks, disseminate technical advice eliciting greater publicity. The appearance and exposure of successful attacks in social media channels has turned some of the groups into social media stars attracting also younger generation.

The fourth policy brief stresses out the importance of taking actions at the European level to comprehend the fast growth of cybercriminal activity, attracting especially younger generations looking for fame on social media.

This deliverable includes the following sections:

- Section 1: Describes the content of this deliverable.
- Section 2: Highlights key findings of the 4th policy brief.
- Section 3: Provides conclusions and recommendations.
- Section 4: Shares information about up-coming policy briefs.

[1] Link to published EU-HYBNET policy briefs, including the 4th policy brief can be found at the end of this document.

2 POLICY BRIEF ON "FAME ON SOCIAL MEDIA, A NEW CURRENCY OF CYBERCRIME?"

2.1 CONTENT AND FINDINGS

The 4th EU-HYBNET policy brief *Fame on social media, a new currency of cybercrime?,* published in February 2023 addresses the trend of democratisation of cyber operations, combining it with the availability of disruptive technology and fame acquisition strategies that individuals may display as determinants of cyber operations. The policy paper analysed the reasons behind this new trend, and the opportunities and challenges that such exposure brings to law enforcement authorities and the research community.

1. NOVEL EXPOSURE OF CRIMINAL GROUPS

In the past years the professionalism of cyber activities has increased. High profile attacks, although not always technologically complex, have made Anonymous the first cybercriminal group to also be a global brand and media entity – in the sense that it also publishes content with an editorial consistency to it. The group use the internet to disrupt services provided by targets chosen by the majority if its members.

On the other hand, the Russian invasion of Ukraine has created incentives for cybercriminal groups to take part in hostilities – such as shown in the "creation" of IT Army of Ukraine. The formation of IT army created an unexpected epiphenomenon of state sponsored cyberwarfare. These new cybercriminal groups have chosen clear sides in the war, exchanged publicly information with Anonymous and declared the ownership of the attacks.

2. SOCIAL MEDIA STARS

The appearance of social media dissemination channels has turned some of these cybercriminal groups into social media stars, with a following and reach that started to shed some light on these groups' daily operations, attracting more attention, and creating the need to produce new content for these groups, which started to claim all kinds of attacks.

Cybercriminal groups are using newfound fame to finance themselves - either by request for donations, selling of merchandise, but also publicly calling for those with access to corporate and critical infrastructures to cooperate in return of monetary compensation to breach those entities.

3. NEW MARKET OPPORTUNITIES

Availability of solutions and ease of use, allied to a public awareness of success by the cybercriminal groups on social media, gives these groups a larger target audience to sell their solutions.

Observation of the drivers of cyber operations, attacks and criminality suggests a higher degree of decentralisation, individualisation, and a general distribution of capacities.

3 CONCLUSIONS

3.1 IMPLICATIONS

Rapid growth, professionalisation of cybercriminal groups and diversification of tactics, sponsored by states create new kind of challenges and implications. The reported daily amount of attacks and leaks, now amplified in social networks and mass media outlets, are creating a trove of information that will take months, if not years, to analyse. In a rapidly changing environment this information overload can be distracting and lead to the dispersion of resources.

The public attention that these attacks are getting, and the normalization of cybercrime as a valid, publicly lauded, even state sponsored activity is also attracting users from a younger generation that, up to now, didn't have the knowledge - or skills - to dive deep into a certain type of forum. This shift in terms of accessibility fosters a sense of belonging to something bigger. It creates recruitment opportunities and incentives for cybercriminal groups, it grows the potential for new victims and widens the arch of prospective targets.

Cybercriminal groups are using this newfound fame to finance themselves - either by request for donations, selling of merchandise, but also publicly calling for those with access to corporate and critical infrastructures to cooperate in return of monetary compensation to breach those entities. Moreover, the use of publicly traded Ransom as a Service (RaaS) packages, exponentially creates the potential for more disruption by criminal actors that, to this point, were not involved in cybercrime: availability of solutions and ease of use, allied to a public awareness of success by the cybercriminal groups on social media, gives these groups a larger target audience to sell their solutions.

3.2 RECOMMENDATIONS

EU-HYBNET policy brief recommendations correspond to the European Union (EU) Cybersecurity and European Union Security Union strategies. While both strategies prioritize among other focus areas, the need to foster and improve collaboration or share information between EU Member States - the EU Security Union Strategy emphasize as one of the key actions to deter and tackle on time evolving threats, including cybercrime and hybrid threats. There is no reason to believe that the social media presence of these groups will fade away, on the contrary. Cybercriminal groups have found that public notoriety can be used as a weapon towards their targets, and a good resource for recruitment.

In the light of this rising and fast evolving trend, the project recommends that:

- Reckoning with this new state of reality **requires technical expertise, timely situational awareness and communication, talents attractiveness. Using existing exchange platforms, such as the NIS[2] and other Coordination groups at European level** should be intensified.
- Based on the principle that no infrastructure is safe from an attack, a bigger effort has to be made to **create sound security measures within organizations**, taking into account that remote work, which will be more and more prevalent in the future, brings with it new challenges.

[2] The Network and Information Systems. NIS Cooperation Group is to support and facilitate strategic cooperation and the exchange of information among Member States.

- Cyber-criminal groups can exploit their social media fame-seeking and public exposure in identifying persons-of-interest in organizations, by monitoring who joins or follows their dissemination's channels. With social engineering being used in lots of high-profile attacks, internal social media policies connected with strong digital security enforcement are no longer optional, but mandatory. The interest that these public groups create in a younger generation should not be overlooked as it's both an opportunity and a threat. It is suggested to create **targeted communication campaigns and educational programs** to make use of this interest in cyber security, in order to prevent that some of this talent will join cyber-criminal groups or create their own.

4 FUTURE WORK

The next policy brief is planned to address a solution for efficient and extensive sharing of IMI[3]Information (IMII) between concerned stakeholders and IMII providers of such information. The ability and willingness to share is a key concern in the EU and Member States' efforts to improve societal resilience against national and foreign IMI activities as mitigation actions heavily rely on the ability for early detection. The solution proposed is based on the establishment of a marketplace for IMII exchange. It complements the current work performed by EEAS Strat.Com. on FIMI (partly reported in their "*1st EEAS Report on Foreign Information Manipulation and Interference Threats*"). This policy brief is expected to be ready during 2023.

Other policy briefs are expected to be written according to EU-HYBNET results on most promising innovations identified in EU-HYBNET Task 4.2. "Strategy for Innovation uptake and industrialization".

[3] Information Manipulation and Interference.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EEAS	European Union External Action
NIS	The Network and Information Systems
FIMI	Foreign Information Manipulation and Interference
OB	Objective
T	Task
RaaS	Ransom as a Service
WP	Work package
KPI	Key performance Indicator
IMI	Information Manipulation and Interference
L3CE	Lithuanian Cybercrime Center of Excellence for Training, Research & Education
RISE	Research Institutes of Sweden
Hybrid CoE	The European Centre of Excellence for Countering Hybrid Threats
LAUREA	Laurea University of Applied Sciences

ANNEX II. EU HYBNET PUBLISHED POLICY BRIEFS

EU-HYBNET Policy Brief No1. – Framing the Information Domain Vulnerabilities - June 2021. https://euhybnet.eu/policy-briefs/

EU-HYBNET Policy Brief No2. – Countering Hybrid Threats: Areas for Improvement and Developing Innovations – December 2021 https://euhybnet.eu/policy-briefs/

EU-HYBNET Policy Brief No3. – Sharing information manipulation and interference (IMI) information – February 2022 https://euhybnet.eu/policy-briefs/

EU-HYBNET Policy Brief No4. – Fame on social media, a new currency of cybercrime? – February 2023 https://euhybnet.eu/policy-briefs/