EU-HYBNET - podstawowe informacje i główne założenia projektu

Empowering a Pan-European Network to Counter Hybrid-Threats

Magda Okuniewska

Zagrożenia hybrydowe – instrumenty przeciwdziałania, inicjatywy, rekomendacje

8.12.2021, wydarzenie online

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET – główne informacje

- Projekt unijny realizowany w ramach programu Horyzont 2020
- Finansowany przez Komisję Europejską - budżet w wysokości 3.5 mln EUR
- Okres trwania: 5 lat (2020-2025)
- Konsorcjum: 23 organizacje z 16 krajów europejskich
- Koordynator techniczny projektu: Uniwersytet Nauk Stosowanych Laurea (Finlandia)
- Koordynator merytoryczny: Europejskie Centrum Doskonalenia w Dziedzinie Zwalczania Zagrożeń Hybrydowych (Hybrid CoE) z siedzibą w Helsinkach

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Partnerzy konsorcjum EU-HYBNET

1. Centralne Biuro Informatyki w Sektorze Bezpieczeństwa ZITiS (Niemcy)
2. Dyrekcja ds. Ochrony Ludności DSB (Norwegia)
3. Centrum Studiów nad Bezpieczeństwem KEMEA – MSW (Grecja)
4. Miasto Espoo (Finlandia)
5. Agencja Bezpieczeństwa Wewnętrznego (Polska)
6. Ministerstwo Obrony (Holandia)
7. "Mihai Viteazul" Narodowa Akademia Służb Wywiadu MVNIA (Rumunia)
8. Ministerstwo Transformacji Ekologicznej (Francja)
9. Estoński Urząd ds. Systemu Informacyjnego (Estonia)
10. Komenda Policji w Walencji (Hiszpania)

9. Polska Platforma Bezpieczeństwa Wewnętrznego (Polska)
10. Międzynarodowe Centrum Obrony i Bezpieczeństwa (Estonia)
11. Litewskie Centrum Doskonalenia ds. Cyberprzestępczości w zakresie Szkoleń, Badań Naukowych i Edukacji L3CE (Litwa)
12. Europejska Organizacja Bezpieczeństwa EOS (Belgia)
13. Maldita - organizacja fact checking (Hiszpania)
14. Satways Ltd. (Grecja)
15. Szpital Uniwersytecki w Mediolanie (Włochy)

16. Holenderska Organizacja Zastosowań Nauki TNO (Holandia)
17. Uniwersytet Bundeswehry w Monachium (Niemcy)
18. Universidad Rey Juan Carlos (Hiszpania)
19. Instytuty Badawcze RISE (Szwecja)
20. Uniwersytet w Tromsø (Norwegia)

22. Uniwersytet Nauk Stosowanych Laurea (Finlandia)
23. Europejskie Centrum Doskonalenia w Dziedzinie Zwalczania Zagrożeń Hybrydowych (Hybrid CoE) z siedzibą w Helsinkach

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Definicja zagrożeń hybrydowych przyjęta w ramach EU-HYBNET

Zagrożenia hybrydowe mają na celu wykorzystanie słabych punktów danego kraju i często dążą do podważenia podstawowych wartości i wolności demokratycznych.

Zagrożenia hybrydowe mogą być opisane jako szeroki wachlarz skoordynowanych i zsynchronizowanych działań, które celowo wymierzone są w słabe punkty demokracji i instytucji państwowych.

Celem jest wywarcie wpływu na różne formy podejmowania decyzji na szczeblu instytucjonalnym, lokalnym, regionalnym i państwowym, aby osiągnąć cele strategiczne przy jednoczesnym podważeniu lub/i uszkodzeniu obranego celu.

Aby skutecznie reagować na zagrożenia hybrydowe, kluczowa jest lepsza wymiana informacji, przełomowe odkrycia w dziedzinie odpowiednich badań oraz promowanie wymiany informacji wywiadowczych między sektorami, a także wewnątrz UE, jej państwami członkowskimi i partnerami.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET – cele projektu

Główne cele projektu

Rozwój europejskiej sieci mającej na celu **przygotowanie się na zagrożenia hybrydowe, ich wcześniejsze wykrywanie oraz zwalczanie**.

Rozwój sieci ekspertów możliwy jest poprzez **wzmocnienie współpracy ekspertów** z instytucji publicznych, Unii Europejskiej i NATO, służb mundurowych, przedstawicieli ośrodków naukowych, a także podmiotów reprezentujących sektor prywatny i organizacje pozarządowe.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET – 4 główne obszary tematyczne

Technologie przyszłości w cyberprzestrzeni

Kierunki rozwoju zagrożeń hybrydowych

Cywile odporni na zagrożenia, szczebel lokalny oraz administracja krajowa

Informacja i komunikacja strategiczna

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET – cykl projektu

Analiza potrzeb praktyków

Analiza rynku, innowacji i prowadzonych badań
- Co jest dostępne dziś.
- Co będzie dostępne w przyszłości.

Szkolenia i warsztaty dla praktyków

Opracowanie rekomendacji w obszarze:
standaryzacji,
regulacji prawnych
oraz dobrych praktyk

Raporty z rekomendacjami
dla policy makers

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Zadanie 4.3 – rekomendacje (zadanie nad którym obecnie pracuje PPBW)

Wybrane obszary tematyczne

Analiza potrzeb praktyków

- Fake Newsy i Dezinformacja
- Komunikacja Strategiczna
- Odporne społeczeństwo
- Cyberbezpieczeństwo
- Duże zbiory danych
- Krytyczne Towary i Surowce

Raporty zawierające następujące informacje:

- Wykaz najważniejszych dokumentów
- Opis obecnie prowadzonych działań w danym obszarze
- Rekomendacje działań

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Zadanie 4.3 – wybrane rekomendacje

Duże zbiory danych

- Dane, jak również ich przetwarzanie, postrzegane jako **dobro krytyczne** dla bezpieczeństwa państwa.
- Potrzebne są **jasne warunki przetwarzania danych**, aby zagwarantować, że osoba fizyczna nie stanie się jedynie obiektem informacji w warunkach automatycznego gromadzenia i przetwarzania danych osobowych.
- **Zdefiniowanie zasad** pozyskiwania, dostarczania i przechowywania danych; prawodawstwo dostosowane do dużych zbiorów danych i ich ochrony.

Krytyczne Towary i Surowce

- Opracowanie wspólnego podejścia krajowego w zakresie mechanizmów screeningu.
- **Wzmocnienie i poszerzenie ram regulacyjnych** w celu wspierania współpracy między partnerami publicznymi i prywatnymi, w oparciu o zasady UE.
- Należy przygotować regulacje unijne, wprowadzające **minimalne standardy ochrony infrastruktury krytycznej w trzech obszarach: ochrony fizycznej, osobowej i informatycznej** dla państwowych i prywatnych operatorów takiej infrastruktury.
- **Stworzenie ram kontroli danych i kontroli gromadzenia danych**.

Cyberbezpieczeństwo

- Integracja różnych powiązanych ze sobą technologii za pomocą spójnej strategii i dyrektyw.
- **Stworzenie Europejskiego Centrum Kompetencji Cyberbezpieczeństwa** wraz z siecią Narodowych Centrów Koordynacyjnych.
- Zwiększenia **wsparcia dla badań i rozwoju** w dziedzinie architektury i oprogramowania dla technologii kwantowych.
- Zwiększenie wydatków na **tworzenie kultury innowacji** w sektorach takich jak edukacja, przemysł czy na poziomie ogólnospołecznym.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Zadanie 4.3 – wybrane rekomendacje

Fake news i dezinformacja

- **Budowanie świadomości wśród obywateli** w zakresie sprawdzania informacji i działania platform fact-checkingowych.
- Zwrócenie szczególnej uwagi na **media lokalne** i ich pluralizm jako odgrywające ważną rolę w edukacji społeczności lokalnych.
- Organizacja **szkoleń dziennikarskich** w kontekście rozpoznawania kampanii dezinformacyjnych**,** podnoszenie wiedzy na temat dostępnych już handbooków i instrukcji.
- Wsparcie **badań naukowych** nad dezinformacją.

Odporne społeczeństwo

- **Nauka kompetencji medialnych w różnych formach** (wykładów, paneli, dyskusji, kampanii informacyjnych, itp.) powinna zostać rozszerzona na wszystkie grupy wiekowe i być dostosowana do każdej z tych grup.
- **Kampanie społeczne** związane z dezinformacją powinny być organizowane w całej UE, ale dostosowane do warunków lokalnych.
- **Współpraca przedstawicieli różnych sektorów**: mediów, nauki, biznesu, władz publicznych, społeczeństwa obywatelskiego. Współpraca powinna mieć na celu. monitorowanie dezinformacji oraz opracowywanie strategii, zaleceń i narzędzi wzmacniających odporność społeczną.

Komunikacja strategiczna

- Stworzenie, na wzór UE, niezależnego centralnego **systemu ostrzegania przed dezinformacją**. Stworzenie i uruchamianie określonych protokołów za każdym razem, gdy dezinformacja musi być rozpatrywana na poziomie krajowym lub unijnym.
- **Gromadzenie danych związanych z zagrożeniami dezinformacyjnymi** i bieżącymi kampaniami oraz przekazywanie na poziomie centralnym do rządów, odpowiednich instytucji, na poziomie regionalnym do władz lokalnych, a następnie w kolejnym kroku dystrybuowane do obywateli.
- Stworzenie ogólnodostępnych i przystępnych **narzędzi do e-learningu nt. dezinformacji dla obywateli** - może w formie interaktywnych gier albo filmów.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET jako inspiracja do dalszych działań i inicjatyw

W dniu 29 października 2021 r. odbyły się **warsztaty dla młodzieży poświęcone edukacji medialnej i krytycznemu myśleniu**. Wydarzenie zostało zorganizowane przez Młodzieżową Radę Miasta Poznania oraz Polską Platformą Bezpieczeństwa Wewnętrznego, we współpracy z europejskim projektem EU-HYBNET.

młodzieżowa rada miasta

- Więcej informacji tutaj.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

EU-HYBNET – możliwość przystąpienia jako partner stowarzyszony

Partnerzy stowarzyszeni z Polski:

Rzeczpospolita Polska
Ministerstwo
Spraw Zagranicznych

RCB
Rządowe Centrum
Bezpieczeństwa

POLICJA

DEMAGOG

PTBN
Polskie
Towarzystwo
Bezpieczeństwa
Narodowego

The Kosciuszko Institute
Ideas for Poland and Europe

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

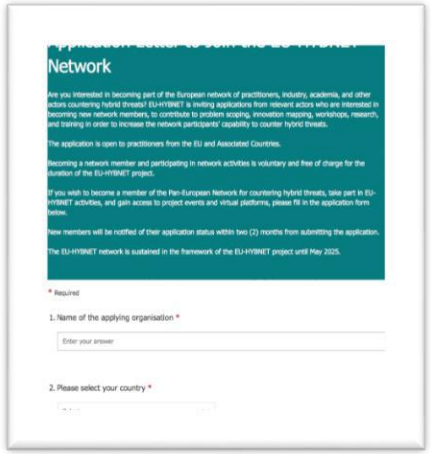
EU-HYBNET – możliwość przystąpienia jako partner stowarzyszony

- Więcej informacji o projekcie:

https://euhybnet.eu/about/

- Formularz aplikacyjny:

https://euhybnet.eu/join-the-network/



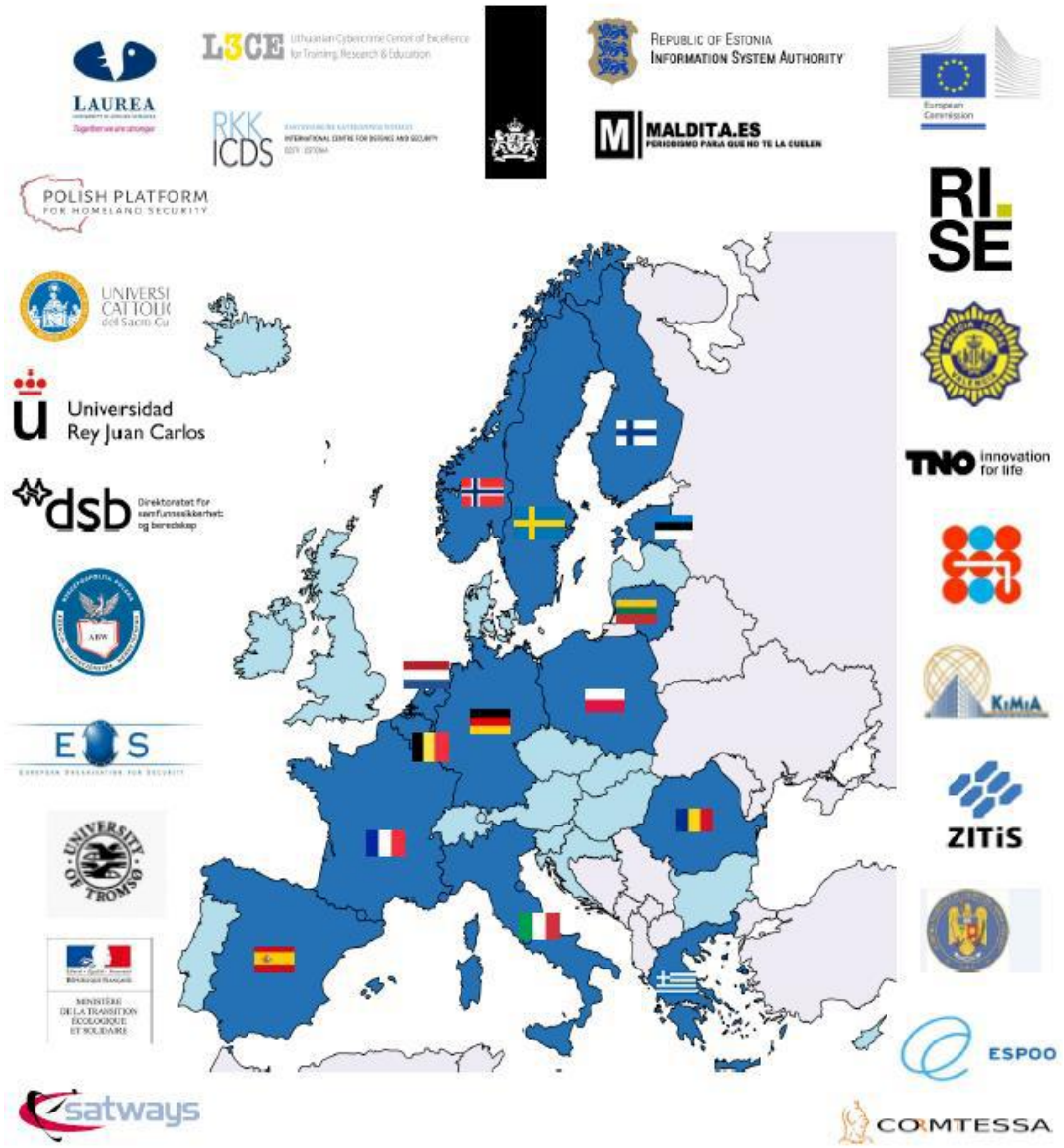
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

THANK YOU!

Magda Okuniewska

Polska Platforma Bezpieczeństwa Wewnętrznego

Magda.Okuniewska@ppbw.pl



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054