

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ЕКОНОМІЧНИХ ВІДНОСИН
НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ УКРАЇНИ
ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ В БРАТІСЛАВІ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ДУБЧИКА В ТРЕНЧИНІ
УКРАЇНСЬКА АСОЦІАЦІЯ ЕКОНОМІСТІВ-МІЖНАРОДНИКІВ
АКАДЕМІЯ ПОЛІТИКО-ПРАВОВИХ НАУК УКРАЇНИ

МАТЕРІАЛИ ДОПОВІДЕЙ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

**«МІЖНАРОДНЕ СПІВТОВАРИСТВО ТА УКРАЇНА
В СУЧАСНИХ ГЛОБАЛЬНИХ ЦИВІЛІЗАЦІЙНИХ
ПРОЦЕСАХ: АКТУАЛЬНІ ЕКОНОМІЧНІ,
ПОЛІТИКО-ПРАВОВІ, БЕЗПЕКОВІ
ТА СОЦІАЛЬНО-ГУМАНІТАРНІ АСПЕКТИ»**

18 – 19 квітня 2023 року

Ужгород – 2023

ГІБРИДНІ ЗАГРОЗИ ТА ЇХ ВПЛИВ НА СУСПІЛЬСТВО

prof. Ing. Korauš Antonín PhD

*Akadémia policajného zboru v Bratislave,
Slovakia*

Анотація. Гібридні загрози стосуються виду безпекового виклику, який поєднує різні елементи, тактики і техніки з конвенційної і неконвенційної війни, а також з різних галузей, таких як кібернетичні, інформаційні та психологічні операції. Ці загрози характеризуються своєю комплексною і багатогранною природою, часто заму́тнюючи розмежування між військовими та невійськовими діями.

Ключові слова: гібридні загрози, публічна адміністрація, дезінформація, фальшиві новини, демократія

Вступ

Ми визначаємо їх як сукупність тиску та підривної дій, конвенційних і неконвенційних, військових і невійськових методів, які державні та недержавні суб'єкти можуть координованим способом використовувати для досягнення конкретних цілей без формального оголошення війни і під порогом звичайної реакції.

Одним з основних цілей гібридного впливу є ослаблення функціонування основних атрибутів демократичних і відкритих суспільств. Часто їх метою є поглиблення соціальної і політичної поляризації на національному та міжнародному рівні, політична дестабілізація, підживлення соціальної напруги, підриив довіри до державних та громадських інституцій та загалом ослаблення демократичного прийняття рішень.

На сьогоднішній день існує десятки інструментів гібридних активностей (наприклад, зловживання вразливостей у публічній адміністрації, дезінформація, кібершпиунство та промисловий шпигунаж, зловживання правових норм, процесів, інституцій та аргументів) і різних підлеглих та підриивних дій, а також кон-

венційних і неконвенційних методів, наприклад, дипломатичних, військових, економічних і технологічних.

Найвиразнішим проявом гібридної діяльності в Словацькій Республіці є навмисне створення та поширення дезінформації, а також все більш інтенсивні й складні кібератаки. Зростання значення гібридних загроз для нашої безпеки та потреба систематично посилювати нашу стійкість до них відображається в Безпековій стратегії Словацької Республіки. У документі, який разом з Оборонною стратегією Словацької Республіки створює стратегічний каркас для формування політики держави щодо безпеки та оборони. Важливим етапом у зміцненні стійкості було схвалення Плану дій з координації боротьби з гібридними загрозами урядом Словацької Республіки у березні 2022 року. Цей міжрезортний документ містить ряд заходів щодо посилення потужностей держави для боротьби з гібридними загрозами, впровадження координаційних механізмів, зміцнення потужностей та координації стратегічної комунікації, освіти та підвищення свідомості щодо гібридних загроз, обмеження зовнішнього впливу на академічні установи, засоби масової інформації, виборчі процеси та економічну сферу.

Гібридні загрози та їхній соціальний вплив

Вплив гібридних загроз на суспільство може бути значним і широким. Ці загрози стосуються не лише традиційних військових і безпекових секторів, але також критичної інфраструктури, політичних систем, економіки та соціальної єдності. Вони використовують вразливості в різних сферах, намагаються підірвати довіру, порушувати функціонування та маніпулювати громадською думкою.

Одним з ключових аспектів гібридних загроз є використання маніпуляції інформацією та кампаній дезінформації. Шляхом поширення фальшивих новин, пропаганди та онлайн-маніпуляцій зловмисники можуть формувати громадське сприйняття, сіяти розкол і підірвати довірливість інституцій. Це може призвести до підірвання довіри до урядів, ЗМІ та демократичних процесів, що в

кінцевому рахунку впливає на стабільність та стійкість суспільств.

Іншим важливим впливом гібридних загроз є їхня здатність використовувати технологічні досягнення. Швидкий розвиток технологій надає гібридним акторам нові можливості для здійснення кібератак, руйнування критичної інфраструктури та шпигунажу. Взаємозв'язок сучасного суспільства збільшує вразливість перед такими атаками, оскільки системи та мережі стають все більш залежними та надійними від цифрової інфраструктури.

Крім того, гібридні загрози можуть мати економічні наслідки. Порушення критичної інфраструктури, крадіжка інтелектуальної власності та економічний шпигунаж можуть завдати шкоди підприємствам та національним економікам. Витрати на захист від гібридних загроз та на подальше відновлення можуть бути значними і впливати на економічний ріст та стабільність.

Вирішення гібридних загроз вимагає комплексного та багатовимірного підходу. Це включає посилення заходів кібербезпеки, покращення здатностей в галузі отримання інформації, боротьбу з кампаніями дезінформації та підтримку стійкості у суспільствах. Співпраця та координація між урядами, приватним сектором та громадськими організаціями є необхідними для ефективного зменшення впливу гібридних загроз.

Висновок: гібридні загрози становлять значні виклики для суспільств по всьому світу. Їх вплив розширюється поза традиційну сферу безпеки і впливає на політичні, економічні та соціальні сфери. Розуміння цих загроз та розробка активних заходів для їх усунення є необхідними для захисту національної безпеки, демократичних процесів та благополуччя суспільства в постійно змінному безпековому середовищі.

Які є підходи до боротьби з гібридними загрозами у публічному управлінні?

Боротьба з гібридними загрозами у публічному управлінні вимагає комплексного та координованого підходу. Ось кілька важливих підходів, які можна розглянути:

1.Інформованість та аналіз: Важливо, щоб органи публічного управління мали достатню інформацію про гібридні загрози та їх характеристики. Важливо відстежувати поточні події, тренди та тактики, якими користуються гібридні актори. Також важливо мати здатність аналізувати цю інформацію та передбачати потенційні загрози.

2. Співпраця та координація: Ефективна боротьба з гібридними загрозами потребує співпраці між різними органами публічного управління, правоохоронними органами, сектором кібербезпеки та іншими відповідними суб'єктами. Важливо створити механізми обміну інформацією, обміну *beweisenden Verfahren* та координації заходів.

3. Підвищення кібербезпеки: Гібридні загрози часто включають кібератаки. Важливо покращити кіберстійкість публічного управління шляхом впровадження міцних заходів безпеки, навчання працівників та регулярного моніторингу та тестування вразливостей систем.

4. Моніторинг та виявлення дезінформації: Гібридні загрози часто включають дезінформаційні кампанії. Важливо мати механізми моніторингу та виявлення дезінформації, ідентифікації її джерел і швидко реагувати на поширення неправдивої інформації. Добрими практиками є співпраця з медіа, громадським суспільством та технологічним сектором.

5. Освіта та свідомість: Освіта та інформованість є важливими для запобігання та захисту від гібридних загроз. Важливо забезпечувати фахову підготовку працівників публічного управління у сфері кібербезпеки, виявлення дезінформації та реагування на гібридні загрози. Також важливо підвищувати свідомість громадськості про гібридні загрози та поліпшувати здатність громадян розпізнавати та розкривати дезінформацію.

6.Інновації та технологічні рішення: Гібридні загрози часто використовують технологічні засоби та нові технології. Важливо інвестувати в інновації в галузі кібербезпеки, аналізу даних та моніторингу, щоб покращити здатність виявляти та вирішувати гібридні загрози. Ці підходи разом з ретельною стратегією та координова-

ними заходами можуть посилити стійкість публічного управління до гібридних загроз і допомогти захистити демократичні процеси, критичну інфраструктуру та стабільність суспільства.

Заклучення

Гібридні загрози становлять серйозний виклик для сучасних суспільств і мають значний вплив на різні сфери життя. Їх складна природа і здатність поєднувати різні елементи і техніки з різних галузей, таких як війна, кібербезпека і дезінформація, роблять їх небезпечними і складними для виявлення і вирішення.

Вплив гібридних загроз на суспільство є дуже широким. Вони можуть порушити політичні системи, підривати довіру до інституцій, дестабілізувати економіку та загрожувати критичній інфраструктурі. Маніпуляція інформацією та дезінформаційні кампанії можуть мати серйозний вплив на громадську думку та соціальну єдність. Технологічні досягнення надають гібридним акторам нові інструменти для здійснення кібератак і шпигунства, що підвищує вразливість сучасних суспільств.

Боротьба з гібридними загрозами потребує комплексного і координованого підходу. Необхідно, щоб органи державного управління, сили безпеки, сектор кібербезпеки та громадське суспільство об'єдналися та співпрацювали. Покращення інформованості, аналіз загроз, зміцнення кібербезпеки, моніторинг і виявлення дезінформації, освіта та свідомість громадськості - це ключові кроки у боротьбі з гібридними загрозами.

Необхідно, щоб суспільство активно залучалося до вирішення та запобігання гібридним загрозам. Превентивні заходи та спільні зусилля всіх зацікавлених сторін є найефективнішим шляхом захисту суспільства від цих складних загроз.

Необхідно, щоб спільноти активно залучалися до вирішення та запобігання гібридним загрозам. Превентивні заходи та співпраця між різними суб'єктами є ключем до зміцнення стійкості суспільства від гібридних загроз та збереження стабільності, демократичних процесів та загального благополуччя.

У контексті швидкозмінного безпекового середовища необхідно постійно моніторити та пристосовувати заходи для боротьби з гібридними загрозами. Тільки таким активним підходом ми можемо утримувати крок з новими стратегіями та тактиками гібридних загроз. Важливо створювати та зміцнювати співпрацю між різними акторами, включаючи уряди, силові структури, академічні установи, приватний сектор та громадське суспільство.

Освіта та свідомість про гібридні загрози також є ключовими. Ми повинні інвестувати в інформованість та освіту не лише про існуючі загрози, але й про нові тенденції та техніки, якими користуються гібридні загрози. Також важливо підтримувати критичне мислення та здатність розпізнавати маніпулятивну інформацію та дезінформацію.

Крім того, ми повинні зміцнювати наші кібернетичні оборонні можливості та вдосконалювати навички ідентифікації, моніторингу та ліквідації кібернетичних загроз. Тісна співпраця між безпековими агентствами та технологічною промисловістю є необхідною для швидкого обміну інформацією та інновацій у боротьбі з гібридними загрозами.

Нарешті, важливим аспектом боротьби з гібридними загрозами є збереження відкритого та вільного інформаційного середовища. Підтримка свободи преси, критичних медіа та прозорості урядових заходів сприяє зміцненню стійкості суспільства до дезінформації та маніпуляцій.

Виклики, які становлять гібридні загрози, не можна недооцінювати. Однак за допомогою ефективного та координованого підходу ми можемо збільшити стійкість суспільства та мінімізувати їх негативний вплив. Це є нашою спільною відповідальністю працювати разом над будівництвом більш безпечного та стійкого суспільства, яке готове протистояти цим новим та складним загрозам.

У висновку очевидно, що гібридні загрози мають значний та широкомасштабний вплив на суспільство. Їх складна природа та здатність замути межі між військовими та невійськовими діями роблять їх дуже небезпечними та складними для контролю.

Вплив гібридних загроз проявляється на різних рівнях суспільства. Політичні системи, критична інфраструктура, економіка та соціальна сплітненість зазнають ризику. Маніпуляція інформацією та дезінформація мають негативний вплив на громадське сприйняття, довіру до інституцій та стабільність демократичних процесів.

Швидкий технологічний прогрес та залежність суспільства від цифрової інфраструктури збільшують вразливість до кібератак та порушення критичної інфраструктури. Економіка також страждає через втрату інтелектуальної власності та економічного шпигунства.

Боротьба з гібридними загрозами вимагає комплексних та координованих заходів. Посилення кібербезпеки, моніторинг дезінформації, співпраця між різними суб'єктами та підвищення свідомості є важливими факторами в цьому процесі.

Необхідно, щоб суспільство та уряди прийняли заходи для захисту від гібридних загроз та зміцнення стійкості. Тільки через співпрацю, інформованість та профілактичні заходи ми можемо досягти стабільності, захисту демократії та благополуччя нашого суспільства в сучасному динамічному та постійно змінюючомуся безпековому середовищі.

Вплив гібридних загроз проявляється в багатьох аспектах суспільства. Політичні системи знаходяться під загрозою, критична інфраструктура піддається ризику, економіка може бути ослаблена, а соціальна єдність може бути порушена. Маніпуляція інформацією та дезінформація мають дестабілізуючий вплив на громадську думку та довіру до інституцій.

Разом із швидким розвитком технологій та взаємопов'язаністю суспільства гібридні загрози стають все більш складними. Кібератаки, порушення критичної інфраструктури та економічний шпигунаж мають серйозні наслідки для безпеки та процвітання.

Для боротьби з гібридними загрозами потрібний комплексний набір заходів. Це включає поліпшення кібербезпеки, зміцнення потужностей виявлення та реагування на загрози, покращену співпрацю між урядами та секторами суспільства, а також

підвищення свідомості про гібридні загрози на всіх рівнях суспільства.

Однорідний та злагоджений підхід є ключовим фактором для ефективного захисту від гібридних загроз. Суспільство повинно працювати разом, використовувати свої здібності та ресурси та активно брати участь у боротьбі з цими загрозами.

У кінцевому підсумку важливо розуміти, що гібридні загрози не є ізольованим явищем, а є складовою динамічного безпекового середовища, в якому ми живемо. Тому важливо постійно розвивати наші здібності, зміцнювати стійкість суспільства та працювати над захистом нашої демократії, стабільності та процвітання.

Подяка

Цей внесок був створений в рамках національного проекту «Підвищення стійкості Словаччини до гібридних загроз шляхом зміцнення потенціалу публічного управління», код проекту ITMS2014+: 314011CDW7. Цей проект фінансується з Європейського соціального фонду.

Список використаної літератури

1. Berzins, J. (2018). Countering hybrid threats: the European Union's response. *Contemporary Security Policy*, 39(3), 417-440.
2. Blighe, K., Lun, A. (2021). PCAtools: everything Principal Component Analysis. Dostupné na internete. <https://bioconductor.org/packages/release/bioc/vignettes/PCAtools/inst/doc/PCAtools.html>
3. Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 1- 19.
4. Čavojský, M., & Szalay, L. (2019). Hybrid Threats and Slovakia's Security Environment. In 31st International Scientific Conference on Economic and Social Development - «Legal Challenges of Modern World» (pp. 491-500). Varazdin Development and Entrepreneurship Agency.

5. Çifci, H. (2022). Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework. <https://www.researchsquare.com/article/rs-2159915/latest.pdf>
6. Ciupercă, E. M., Donnelly, N., Gartland, A., & Stanciu, A. (2022). The Digital Divide in Education-Macrocultural Comparative Analysis between Ireland and Romania. *IFAC-PapersOnLine*, 55(39), 99-104.
7. Dragulescu, A. and Cole Arendt (2020). *xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files*. R package version 0.6.5. <https://CRAN.R-project.org/package=xlsx>
8. Európska rada a Rada EÚ (2023) Kybernetická bezpečnosť: ako EÚ bojuje proti kybernetickým hrozbám dostupné online: <https://www.consilium.europa.eu/sk/policies/cybersecurity/>
9. Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, 32(1), 63-71.
10. Korauš, A., Kurilovská, L., Šišulák, S. (2022). Zvyšovanie kompetencií a informovanosti pracovníkov verejnej správy v kontexte súčasných hybridných hrozieb. Praha: Relik (379-388).
11. Tuvsud: Audit kybernetickej bezpečnosti Dostupné na <https://www.tuvsud.com/sk-sk/cinnosti/kyberneticka-bezpecnost/audit-kybernetickej-bezpecnosti>
12. Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical indicators of cybersecurity development in the context of digital transformation of economy and society. *Science and Innovation*, 17(3), 3-13
13. Wlachovský, M., Vyhodnocovanie informačného prostredia a strategická komunikácia ako nástroj v boji proti hybridným hrozbám, MepoForum.sk, 2018. URL: <http://mepoforum.sk/staty-regiony/europa/staty-eu-plus/vysehradska-%204/slovensko/vyhodnocovanie%20informacneho-prostredia-a-strategicka-komunikacia-ako-nastroj-v-boji-proti-hybridnym-hrozbam-miroslav-wlachovsky>

М 58 Міжнародне співтовариство та Україна в сучасних глобальних цивілізаційних процесах: актуальні економічні, політико-правові, безпекові та соціально-гуманітарні аспекти: матеріали доповідей Міжнародної науково-практичної конференції (м. Ужгород, 18-19 квітня 2023 року) / за заг. ред.: М.М. Палінчак, М.М. Король, В.В. Химинець. Ужгород: Вид-во УжНУ «Говерла», 2023. 504 с.

ISBN 978-617-7825-98-1

У збірнику викладено матеріали доповідей учасників Міжнародної науково-практичної конференції «Міжнародне співтовариство та Україна в сучасних глобальних цивілізаційних процесах: актуальні економічні, політико-правові, безпекові та соціально-гуманітарні аспекти» (м. Ужгород, 18-19 квітня 2023 року), у яких розглядаються розробки конкретних науково-прикладних рекомендацій щодо розв'язання системних проблем, окреслення стратегічних пріоритетів подальшої трансформації суспільства і економіки України в умовах сучасних викликів.

УДК 327(063):323.2(477)

Наукове видання

**МІЖНАРОДНЕ СПІВТОВАРИСТВО ТА УКРАЇНА В
СУЧАСНИХ ГЛОБАЛЬНИХ ЦИВІЛІЗАЦІЙНИХ ПРОЦЕСАХ:
АКТУАЛЬНІ ЕКОНОМІЧНІ, ПОЛІТИКО-ПРАВОВІ,
БЕЗПЕКОВІ ТА СОЦІАЛЬНО-ГУМАНІТАРНІ АСПЕКТИ**

**Матеріали доповідей міжнародної
науково-практичної конференції
(м. Ужгород, 18-19 квітня 2023 року)**

*За заг. ред.: М. М. Палінчак, М. М. Король, В. В. Химинець
Технічний редактор: В. О. Співак*

Гарнітура CharterITC. Формат 60х84/16. Ум.друк.арк. 28,8. Обл.вид.арк. 21,82.
Зам. № 53. Наклад 50 прим.

Редакційно-видавничий відділ ДВНЗ «УжНУ»: 88000, м.Ужгород,
вул. Заньковецької, 89. E-mail: dep-editors@uzhnu.edu.ua

Видавництво Ужгородського національного університету «Говерла».
88000, м. Ужгород, вул. Капітульна, 18.

Свідоцтво Серія 3т № 32 від 31 травня 2006 року