# Hybrid Threats Glossary

# Глосарій з гібридних загроз

"Academic Response to Hybrid Threats"
Erasmus+ Capacity Building Project WARN
610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP

**Disclaimer**

This project has been funded with support from the European Commission.

This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained therein.

**Project information**

Academic Response to Hybrid Threats (WARN) aims to renew the different curricula by introducing unique content that builds awareness of hybrid threats and innovative gamified teaching methods that proactively provide skills and competencies to tackle complex threats. It is a five-year project funded under the EU's Erasmus+ programme. More information can be found here: warn-erasmus.eu

**Project Partners**

University of Jyvaskyla (Finland)
Universidade de Coimbra (Portugal)
ECAM-EPMI Graduate School of Engineering (France)
Tartu Ulikool (Estonia)
Kharkiv National University of Radio Electronics (Ukraine)
Ukrainian Catholic University (Ukraine)
State University of Infrastructure and Technologies (Ukraine)
National University of Ostroh Academy (Ukraine)
Kharkiv Regional Institute of Public Administration of V. N. Karazin Kharkiv National University (Ukraine)
State Higher Education Institution "Donbas State Pedagogical University (Ukraine)
National Academy of Managerial Staff of Culture and Arts (Ukraine)
Ministry of Education and Science of Ukraine (Ukraine)

# ЗМІСТ / CONTENTS

## Упорядники / Compilers

| | | |
|---|---|---|
| **Балашов Едуард**<br>Balashov Eduard | **НУОА**, Національний університет "Острозька академія"<br>NUOA, National University of Ostroh Academy | 1.0, 2.0 |
| **Білоконь Михайло**<br>Bilokon Mykhailo | **ХНУ**, Харківський національний університет імені В.Н.Каразіна<br>KhKNU, V. N. Karazin Kharkiv National University | 1.0, 2.0 |
| **Василиця Оксана**<br>Vasylytsia Oksana | **УКУ**, Український католицький університет<br>UCU, Ukrainian Catholic University | 1.0 |
| **Величко Лариса**<br>Velychko Larysa | **ХНУ**, Харківський національний університет імені В.Н.Каразіна<br>**KhKNU**, V. N. Karazin Kharkiv National University | 1.0 |
| **Головянко Марія**<br>Golovianko Mariia | **ХНУРЕ**, Харківський національний університет радіоелектроніки<br>**NURE**, Kharkiv National University of Radio Electronics | 1.0, 2.0 |
| **Грицук Оксана**<br>Hrytsuk Oksana | **ГІІМ ДВНЗ ДДПУ**, Горлівський інститут іноземних мов державного вищого навчального закладу "Донбаський державний педагогічний університет"<br>HIFL SHEI DSPU, Horlivka Institute for Foreign Languages of the State Higher Education Institution “Donbas State Pedagogical University” | 2.0 |
| **Гришко Світлана**<br>Gryshko Svitlana | **ХНУРЕ**, Харківський національний університет радіоелектроніки<br>NURE, Kharkiv National University of Radio Electronics | 1.0, 2.0 |
| **Докашенко Галина**<br>Dokashenko Galyna | **ГІІМ ДВНЗ ДДПУ**, Горлівський інститут іноземних мов державного вищого навчального закладу "Донбаський державний педагогічний університет"<br>HIFL SHEI DSPU, Horlivka Institute for Foreign Languages of the State Higher Education Institution “Donbas State Pedagogical University” | 1.0, 2.0 |
| **Завгородній Валерій**<br>Zavhorodnii Valerii | **ДУІТ**, Державний університет інфраструктури та технологій<br>SUIT, State University of Infrastructure and Technology | 1.0 |
| **Засадко Валентина**<br>Zasadko Valentyna | **УКУ**, Український католицький університет<br>UCU, Ukrainian Catholic University | 1.0 |
| **Карпенко Оксана**<br>Karpenko Oksana | **ДУІТ**, Державний університет інфраструктури та технологій<br>SUIT, State University of Infrastructure and Technology | 1.0, 2.0 |

| | | |
|---|---|---|
| **Конопка Наталія**<br>Konopka Natalia | **НУОА**, Національний університет "Острозька академія"<br>NUOA, National University of Ostroh Academy | 2.0 |
| **Концур Вікторія**<br>Kontsur Viktoriia | **ГІІМ ДВНЗ ДДПУ**, Горлівський інститут іноземних мов державного вищого навчального закладу "Донбаський державний педагогічний університет"<br>HIFL SHEI DSPU, Horlivka Institute for Foreign Languages of the State Higher Education Institution “Donbas State Pedagogical University” | 1.0 |
| **Копієвська Ольга**<br>Kopiievska Olha | **НАКККіМ**, Національна академія керівних кадрів культури і мистецтва<br>**NAMSCA**, National Academy of Culture and Arts Management | 1.0, 2.0 |
| **Ланюк Євген**<br>Laniuk Yevhen | **УКУ**, Український католицький університет<br>UCU, Ukrainian Catholic University | 1.0 |
| **Наумов Іван**<br>Naymov Ivan | **ГІІМ ДВНЗ ДДПУ**, Горлівський інститут іноземних мов державного вищого навчального закладу "Донбаський державний педагогічний університет"<br>HIFL SHEI DSPU, Horlivka Institute for Foreign Languages of the State Higher Education Institution “Donbas State Pedagogical University” | 1.0 |
| **Рева Тетяна**<br>Reva Tetiana | **НАКККіМ**, Національна академія керівних кадрів культури і мистецтва<br>**NAMSCA**, National Academy of Culture and Arts Management | 1.0, 2.0 |
| **Титаренко Марія**<br>Tytarenko Mariia | **УКУ**, Український католицький університет<br>UCU, Ukrainian Catholic University | 1.0 |
| **Худолій Анатолій**<br>Khudoliy Anatoliy | **НУОА**, Національний університет "Острозька академія"<br>NUOA, National University of Ostroh Academy | 2.0 |
| **Чех Мирослава**<br>Chekh Myroslava | **УКУ**, Український католицький університет<br>UCU, Ukrainian Catholic University | 1.0, 2.0 |

# 1 Вступ до глосарію-1.0 (2021)

> *Тема рясніє великою кількістю неточних термінів, змішуючи класичні уявлення (вплив, пропаганда, дезінформація) з неологізмами (фейкові новини, пост-правда, фактчекінг), множення яких сигналізує про нездатність існуючої лексики описати соціальний світ що повністю трансформується (Vilmer et al., 2018, p.18).*

Ідея цього глосарію з'явилась у команди WARN-проєкту "Академічна протидія гібридним загрозам" (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP) під час виконання найперших завдань проєкту. Загальна мета проєкту – заповнити розрив у навичках безпеки в різних сферах професійної діяльності для підвищення цивільної стійкості до гібридних загроз в Україні. Для цього кожен із сімох український вишів-учасників проєкту має оновити освітні програми в різних галузях, додавши до них відповідні компетентності.

Проблема, з якою ми одразу зіткнулись – це відсутність "професійної мови", тобто єдиного термінологічного апарату, яким ми маємо спілкуватись, обговорювати, досліджувати, розробляти, ставити питання й шукати відповіді… Гібридні загрози почали впливати на роботу нашої команди, одразу продемонструвавши свою невловимість – їх складно сформулювати й описати, не потрапивши у пастку помилкових визначень. Саме тому нашим першим кроком й стала розробка термінологічного апарату, який ми зможемо покласти в основу контенту оновлених освітніх програм.

Інша проблема, яку ми вирішували, створюючи цей глосарій, – на які джерела спиратись? Ми в Україні багато говоримо про гібридні загрози, бо це питання є болісним для нас. Але, не заперечуючи якості та важливості вітчизняних досліджень в цій галузі, все ж таки маємо визнати їх фрагментарний характер та відсутність системних рішень, упроваджених у захисні суспільні механізми.

Головні принципи, якими ми керувались, створюючи глосарій, – це авторитетність джерел, які мають бути беззаперечними та визнаними світовоюспільнотою фахівців з гібридних загроз, та системність підходу. І тут ми вже не вагалися довго, бо програма Erasmus+ надає унікальні можливості отримання такої інформації від наших європейських партнерів.

Підхід ЄС вирізняється своєю системністю та практичністю: офіційні установи й організації вже визначили основні гібридні загрози та базові контрзаходи (проактивність, професійні тренінги з питань безпеки та навчальні програми зі спеціальними компонентами та методами безпеки для підвищення стійкості як установ, так і окремих людей тощо). Так, у ЄС розроблена Спільна система боротьби з гібридними загрозами (A Joint Framework On Countering Hybrid Threats), запущена в 2016 році. А в 2014-му почав роботу перший Центр передового досвіду з протидії гібридним загрозам Hybrid CoE у Гельсінкі, філії якого згодом були відкриті у багатьох столицях ЄС. Підхід ЄС для досягнення стійкості заснований на забезпеченні своєчасної та достовірної інформації для громадян та осіб, які приймають рішення; на розвитку культури; на підвищенні рівня освіти; заохоченні до обміну інформацією між установами та організаціями; зміцненні спеціалізованих органів та установ держави; на прийнятті законодавчих заходів, адаптованих до нових викликів; та на широкому охопленні населення. Саме на цей систематичний європейський підхід, який дозволяє підвищити загальний рівень безпеки суспільства, ми спираємось, створюючи глосарій.

Джерела, які ми використовуємо – це, в першу чергу, напрацювання Hybrid CoE (європейської експертної установи з питань дослідження гібридних загроз), що знаходяться у відкритому доступі, а також джерела інформації, рекомендовані Hybrid CoE. Крім того, із великою вдячністю користуємось матеріалами, які надано нашими європейськими партнерами:

- Університет Ювяскюля, Фінляндія (координатор проєкту)
- Університет Коїмбри, Португалія,
- Вища інженерна школа ECAM-EPMI, Франція,
- Університет Тарту, Естонія,

а також асоційованим партнером проекту – Лабораторією гібридних стратегій TNO (Нідерланди).

Щоб створити цей глосарій, ми цитували безпосередньо текст як європейських, так і американських авторів. Тому він не зовсім схожий на класичний глосарій, і тому тут немає мовної одноманітності. Але ми вважаємо, що прямі цитати допомагають нам уникнути помилок у визначеннях. Натомість кожен термін нашого глосарію є "точкою доступу" до більш докладного роз'яснення, дослідження, ілюстрацій, наданих професіоналами, а сам глосарій знайомить із дивовижним "визерунком" гібридних загроз.

## Introduction to the Glossary-1.0 (2021)

> *The subject is riddled with an abundance of imprecise terms, mixing classical notions (influence, propaganda, disinformation) with neologisms (fake news, post-truth, fact-checking), whose multiplication "signals the inability for the existing vocabulary to describe a social world that is completely transforming"*(Vilmer et al., 2018, p. 18).

This glossary was envisaged by the team of the WARN-project *Academic Response to Hybrid Threats* (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP) at the very beginning of the project implementation. The overall goal of the project is to increase civic resilience to hybrid threats in Ukraine by filling the gap in security skills in various societal groups and professional domains. . Having this goal in mind, teams of seven Ukrainian universities participating in the project are updating the curricula of various study programmes, adding relevant competencies. The first problem that we faced pursuing our goal was the lack of 'professional language'—that is, a common terminological apparatus to discuss, analyse, research, develop, ask questions, and give answers… In fact, hybrid threats appeared to be elusive and ambiguous even conceptually – they are hard to define and describe without falling into the trap of inconsistent definitions. That is why our first step is to develop a glossary which will lay the foundation for the future curricula content.

Another problem when creating this glossary was to find reliable sources. In Ukraine, we talk much about hybrid threats because they cause huge harm to our environment. However, not denying the quality and importance of the national research in this field, we still have to admit that it is rather incomplete and lacks systemic solutions that could be introduced into civic defence mechanisms.

Thus, the credibility of the information, i.e., international recognition of both the information and sources of the information, and the systematic approach were defined as the main design principles. This is where we benefit from the Erasmus+ programme, providing unique opportunities to get access to reliable information via our European partners.

The approach applied by the European Union is systematic and practical: official institutions and organisations have already identified the main hybrid threats and basic countermeasures (the latter include proactivity, professional security training and study programmes curricula with special components and security methods to improve the resilience of both institutions and individuals). In 2016, the European Union launched

the Joint Framework on Countering Hybrid Threats, and in 2014, the first European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was formally established with headquarters in Helsinki, Finland, and offices in many EU capitals. The EU's approach to sustainability is based on providing timely and accurate information to citizens and decision-makers, developing a security culture, improving education, encouraging the exchange of information between institutions and organisations, strengthening specialised bodies and state institutions, and adopting legislative measures to confront new challenges and protect the population to the greatest extent possible. This systematic European approach to increasing overall societal security was chosen as a fundamental one for the project and, consequently, for the glossary creation.

Our information sources are various open-access publications produced by Hybrid CoE, which is a European expert institution for studying hybrid threats. Besides these, we have used the materials provided by our European Union partners from:

– University of Jyväskylä, Finland (project coordinator),
– University of Coimbra, Portugal,
– ECAM EPMI Graduate School of Engineering, France,
– University of Tartu, Estonia, and
– TNO’s Hybrid Strategies Lab, Netherlands, our associate partner in the project.

To compose the glossary we cite works of both European and American authors directly. Therefore, the glossary differs from the classic ones and has no traditional linguistic uniformity. However, this way we also avoid mistakes in definitions. Therefore, each concept in our glossary serves as a link to more detailed explanations, studies, and illustrations by experts, specifying the prodigious patterns of hybrid threats.

# 2 Передмова до глосарію-2.0 (2024)

*Анатолій Худолій (НУОА, Національний університет "Острозька академія")*

*Наталія Конопка (НУОА, Національний університет "Острозька академія")*

Наше століття зазнало політичних, економічних, соціальних змін. Європейська співдружність країн, які сформували Європейський Союз, зустрілися з низкою викликів, від терористичних загроз до неспровокованої повномасштабної війни росії проти України у лютому 2022 року. Війна у Сирії, нестабільна ситуація на Близькому Сході, політичні переслідування, низький рівень життя – всі ці чинники стали тригером для посилення міграційних процесів, змушуючи тисячі мігрантів шукати кращого життя у ЄС. Разом із економічними, політичними та соціальними проблемами посилились військові конфлікти, гібридні загрози. Останні впливають на всі сфери суспільно-політичного життя європейських країн, підривають економіку, порушують стабільність, сіють сумніви серед населення у сьогоднішньому дні. Словник-довідник адресовано, насамперед тим, хто вивчає тему гібридних загроз. Водночас, ним, з успіхом, можуть скористатися учні, студенти, перекладачі і всі, хто вивчає англійську мову і хоче її вдосконалити. Слід зауважити, що глосарій є лише практичним інструментом, призначеним для використання у конкретних ситуаціях, не підручником.

Глосарій 2.0 об’єднує науковців різних сфер, оскільки пропонує вибірку термінів, об’єднаних спільною тематикою – гібридними загрозами. Він знайде свого читача з огляду на логічно скомпонований зміст і композиційну будову. У книзі автори подали терміни та їхні визначення, враховуючи контекст. У дусі наукової принциповості запропоновано не лише терміни, але й їхні дефініції англійською та українською мовами. Відмінністю глосарію є те, що автори здійснили вибірку термінів, що мають як вузькоспеціалізовану спрямованість, так і міждисциплінарний характер, що задовольнить смаки фахівців різних сфер.

Зростаюча роль інформаційної сфери на сучасному етапі характеризує розвиток суспільства. Інформація стала невід’ємною частиною життя сучасного інформаційного суспільства, тому, з урахуванням вищезгаданого чинника, сформувалась важлива залежність національної безпеки держави від забезпечення інформаційної безпеки, яка потребує зміцнення, зважаючи на факт швидкого розвитку інформаційних технологій, як наслідку інформаційної революції та процесу глобалізації. Жодна країна не може захистити себе,

використовуючи лише воєнно-технічні засоби, тому державна безпека стає комплексним явищем, що охоплює соціально-політичні, економічні, інформаційні та інші заходи. Зі зростанням швидкості поширення інформації, її ускладненням, виникає потреба у номінаціях на позначення тих або інших явищ суспільно-політичного життя, особливо з урахуванням чинника зовнішніх загроз, серед яких – гібридна війна. При цьому, війна у міжнародних відносинах перетворюється на зброю, яка оминає кордони і проникає у всі сфери суспільного життя, нерідко загрожуючи існуванню самої держави. Інформаційне протиборство вимагає термінологічного інструментарію, який би допоміг, як фахівцям, так і початківцям, орієнтуватися у реаліях сьогодення. Таким завданням і відповідає це глосарій.

Слід зауважити, що Глосарій (версія 2.0) з'явилась внаслідок того, що базова версія (Глосарій 1.0) пройшла пілотне застосування і в процесі тонкого налаштування була доопрацьована. Глосарій з гібридних загроз (версія 2.0) є результатом кількарічної наукової роботи представників різних наукових галузей команди WARN – проєкту Академічна протидія гібридним загрозам; (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP. Проект об'єднав вітчизняні та зарубіжні вищі заклади освіти з метою заповнення прогалин у вивченні гібридних загроз у різних сферах життя суспільства для підвищення стійкості суспільства в Україні до подібного роду викликів.

З огляду на необхідність створення спільних проектних результатів, які би вміщував новітні матеріли та відповідав би вищезазначеним навчальним цілям, а також для впорядкування великого масиву матеріалів, наданих нашими європейськими партнерами (Університет Ювяскюля, Вища інженерна школа ECAM-EPMI, Коїмбри, Університет Тарту), укладачами даного глосарію було створено картотеку, що охоплює англійські та українські терміни, виокремлені із сучасних видань. Внаслідок опрацювання такого корпусу мовних одиниць, було виокремлено ключові терміни, їхні варіанти, синоніми, запропоновано варіанти перекладу, підібрано перелік українських аналогів у максимально повному вигляді та створено цей Глосарій 2.0.

Оскільки одна з першорядних цілей цієї нашої праці полягала в ознайомленні користувачів з темою гібридної війни і гібридних загроз, то було вирішено побудувати глосарій за одним із поширених способів систематизації термінологічного матеріалу – за алфавітним принципом.

Основними перевагами видання є системність, прагматичність, міждисциплінарність та логічність підходу до представлення термінів, які

охоплюють такі напрями як: національна безпека, міжнародні відносини, політологія, публічне управління та адміністрування, менеджмент організацій, фінансово-економічна безпека, кібербезпека, інженерія програмного забезпечення, системи штучного інтелекту, середня та вища освіти, соціокультурна діяльність, медіа комунікації та ін.

Важливою перевагою глосарію є апеляція до достовірних та авторитетних джерел, що дозволило врахувати новітні тенденції та передовий досвід у вивченні гібридних загроз в умовах радикальних змін міжнародного безпекового середовища. Кожен термін супроводжується англомовним відповідником із зазначеннях використаного джерела, відтак це дозволяє не лише познайомитися із змістом поняття, але й збільшити обізнаність про сучасні наукові та практичні напрацювання у вивчені проблеми. Глосарій дає можливість познайомитися та зрозуміти ключові терміни у вивченні витоків, сутності, особливостей та динаміки гібридних загроз та шляхів їх протидії, а також проливає нове світло на природу глобальних безпекових викликів.

Термінологічні одиниці, структурно, представлені словами, словосполученнями та реченнями, які віддзеркалюють сукупність базових понять, що корелюють із темою гібридних загроз і, які, в свою чергу, репрезентують той або інший аспект гібридної війни, економічний, політичний чи військовий домен. Глосарій 2.0 – про нову сферу сучасного життя цивілізації – гібридні загрози. Терміни віддзеркалюють їхній влив на всі сфери життя сучасного суспільства – від політики до культури. На підставі сучасних зарубіжних досліджень подано та уточнено низку ключових понять, що стосуються гібридної війни та гібридних загроз. Виокремлено основні термінологічні ознаки гібридної війни в контексті російсько-українського протистояння. Гібридна війна стала викликом для України, європейської та всієї міжнародної спільноти і становить загрозу існуючому світовому порядку. Такий стан речей потребує осмислення та аналізу, як з політичної, економічної, військової та лінгвістичної точок зору. Цій меті і підпорядкований глосарій 2, який охоплює цілу низку сфер, дотичних до гібридних загроз.

Термінологічні одиниці, представлені у Глосарії 2.0, характеризують економічну, інформаційну, військово-політичну та інші складові сучасних викликів, які постали перед ЄС, і гібридних загроз, зокрема. Значною мірою, низка термінів корелює з російсько-українською війно та гібридними загрозами, які створює російська федерація. Увагу акцентовано на інформаційній складовій, як одній із базових сфер гібридної війни. В український науковий обіг вперше введено термінологічні

одиниці на позначення особливостей гібридних загроз, інформаційної війни тощо. Терміни представлені низкою понять, подекуди, синонімічних за змістом, проте, які релевантні до теми глосарію, а саме – гібридним загрозам.

Матеріал має безумовну цінність – в ній з науковою точністю, глибиною і конкретністю описана і структурована нова сфера – сучасних викликів і гібридних загроз, які стали компонентом сучасного життя, незалежно від країни, оскільки не існує кордонів для поширення інформації, фейків, підміни понять тощо. Слід віддати належне авторам глосарію, які виявили та описали феномен гібридних загроз сучасності і презентували його у вигляді термінологічних одиниць. Представлені у Глосарії 2.0 терміни мають практичне значення. Йдеться про такі питання, як вплив медіа на психологічний стан громадян, їхні знання, компетенцію, переконання, рівень агресії, формування актуальних тем у суспільстві, поведінку виборців, інформаційний захист тощо.

Глосарій 2.0 стане важливим інструментом не лише для студентів, науковців, працівників органів державної влади, міського самоврядування, правоохоронних структур та всіх тих, хто цікавиться, вивчає та використовує подібну термінологію у освіті та роботі, але й для кожного громадянина – для підвищення освіченості та готовності до захисту та протидії гібридним загрозам.

Зважаючи на героїчну боротьбу Українського народу за Незалежність Української Держави, вживання маленької літери при написанні назв «російська федерація», «росія», «москва» тощо не вважається помилкою у правописі (рішення Національної комісія зі стандартів державної мови від 15.09.2023, протокол № 83).

## Foreword to the Glossary-2.0 (2024)

*Anatoliy Khudoliy (National University of Ostroh Academy, NUOA)*

*Natalia Konopka (National University of Ostroh Academy, NUOA)*

Our century has seen political, economic, and social changes. The European community of countries that formed the European Union faced a number of challenges, from terrorist threats to Russia's unprovoked full-scale war against Ukraine in February 2022. The war in Syria, the unstable situation in the Middle East, political persecution, and low living standards have all triggered an increase in migration, forcing thousands of

migrants to seek a better life in the EU. Along with economic, political and social problems, military conflicts and hybrid threats have intensified. The latter affect all spheres of socio-political life in European countries, undermine the economy, disrupt stability, and sow doubts among the population about the present. The EU responds to current challenges by informing citizens about the threat of hybrid warfare. As a result, European countries are implementing relevant projects - one of which is *Academic Response to Hybrid Threats – WARN* (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). The WARN project resulted in a glossary. The problem we faced was the lack of a "professional language," that is, a common terminology that researchers could use. And the first significant step of our team was to develop a terminology that forms the basis of the content of the updated educational programmes. The overall goal of the project is to fill the terminological gap in various areas of professional activity in order to increase civilian resilience to hybrid threats in Ukraine.

The Glossary 2.0 is intended primarily for those who study the topic We intend to update the glossaryof hybrid threats. At the same time, it can also be used by students, translators, and anyone who learns English and wants to improve it. It should be noted that the glossary is only a practical tool intended for use in specific situations, not a textbook.

The Glossary 2.0 brings together scholars from different fields, as it offers a selection of terms united by a common theme - hybrid threats. It will find its reader due to its logically organized content and compositional structure. In the book, the authors present terms and their definitions, taking into account the context. In the spirit of scientific integrity, not only the terms but also their definitions are offered in English and Ukrainian. The difference of the book is that the authors have selected terms that are both highly specialized and interdisciplinary in nature, which will satisfy the tastes of specialists in various fields.

The growing role of the information sphere at the present stage characterizes the development of society. Information has become an integral part of the life of the modern information society, so, taking into account the above factor, an important dependence of the national security of the state on ensuring information security has been formed, which needs to be strengthened, given the rapid development of information technology as a result of the information revolution and globalization. No country can defend itself using military and technical means alone, so state security is becoming a complex phenomenon that encompasses socio-political, economic and

information measures. As the speed of information dissemination increases and becomes more complex, there is a need for nominations to denote certain phenomena of socio-political life, especially in view of the factor of external threats, including hybrid warfare. At the same time, war in international relations is turning into a weapon that bypasses borders and penetrates all spheres of public life, often threatening the existence of the state itself. Information warfare requires a terminological toolkit that would help both experts and beginners navigate the realities of today. This glossary meets these objectives.

It should be noted that the Glossary (version 2.0) appeared as a result of the fact that the basic version (Glossary 1.0) was piloted and fine-tuned. The Hybrid Threats Glossary (version 2.0) is the result of several scientific works of the various scientific fields representatives of the WARN team - the project "Academic Response to Hybrid Threats" (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). The project unified the domestic and foreign higher education institutions with the aim of compensating for the gaps in the study of hybrid threats in various spheres of societal life to increase the resilience of society in Ukraine to similar challenges.

Given the need to create joint project outputs that would contain the latest materials and meet the above-mentioned learning objectives, as well as to organize the large array of materials provided by our European partners (University of Jyväskylä, ECAM-EPMI Graduate School of Engineering, University of Coimbra, University of Tartu), the compilers of this glossary have created a card index covering English and Ukrainian terms extracted from modern publications. As a result of processing this corpus of language units, key terms, their variants, and synonyms were identified, translation options were suggested, a list of Ukrainian equivalents was compiled in the most complete form, and this Glossary 2.0 was created.

Since one of the primary goals of this project was to familiarize users with the topic of hybrid warfare and hybrid threats, it was decided to build Glossary 2.0 according to one of the most common ways of systematizing terminology - alphabetically.

The main advantage of Glossary 2.0 is the systematic, pragmatic, interdisciplinary and logical approach to the presentation of terms that cover such areas as national security, international relations, political science, public management and administration, management of organizations, financial and economic security, cyber security, software engineering, systems of artificial intelligence, secondary and higher education, socio-cultural activities, media communications, etc.

An important advantage of Glossary 2.0 is the appeal to reliable and authoritative sources, which made it possible to take into account the latest trends and best practices in the study of hybrid threats in the conditions of radical changes in the international security environment. Each term is accompanied by an English-language equivalent indicating the source used, thus allowing not only to get acquainted with the meaning of the concept, but also to increase awareness of modern scientific and practical developments in the studied problems. The Glossary 2.0 provides an opportunity to learn and understand key terms in the study of the origins, essence, features and dynamics of hybrid threats and ways of countering them, and also sheds new light on the nature of global security challenges.

Terminological units are structurally represented by words, phrases and sentences that reflect a set of basic concepts that correlate with the topic of hybrid threats and, in turn, represent one or another aspect of hybrid warfare, whether it is economic, political or military domain. The Glossary 2.0 is about a new sphere of modern civilization - hybrid threats. The terms reflect their impact on all spheres of modern society, from politics to culture. Based on modern foreign research, a number of key concepts related to hybrid warfare and hybrid threats are presented and clarified. The main terminological features of hybrid warfare in the context of the Russian-Ukrainian confrontation are highlighted. Hybrid warfare has become a challenge for Ukraine, the European and the entire international community and poses a threat to the existing world order. This state of affairs requires comprehension and analysis from the political, economic, military, and linguistic points of view. This is the purpose of the Glossary, which covers a number of areas related to hybrid threats.

The terminological units presented in the Glossary 2.0 characterize the economic, informational, military and political components of the current challenges facing the EU and hybrid threats in particular. To a large extent, a number of terms correlate with the Russian-Ukrainian war and hybrid threats posed by the Russian Federation. Attention is focused on the information component as one of the basic areas of hybrid warfare. For the first time, terminological units have been introduced into Ukrainian scientific circulation to denote the peculiarities of hybrid threats, information warfare, etc. The terms are represented by a number of concepts, sometimes synonymous in meaning, but relevant to the topic of the glossary, namely, hybrid threats.

The Glossary 2.0 has an unconditional value - it describes and structures a new area with scientific precision, depth and specificity - modern challenges and hybrid threats that have become a component of modern life, regardless of the country, as there are no

borders for the dissemination of information, fakes, substitution of concepts, etc. The authors of Glossary 2.0 should be commended for identifying and describing the phenomenon of hybrid threats of our time and presenting it in the form of terminological units. The terms presented in the glossary are of practical importance. They address issues such as the impact of the media on the psychological state of citizens, their knowledge, competence, beliefs, level of aggression, the formation of topical issues in society, voter behaviour, information protection, etc.

The Glossary 2.0 will become an important tool not only for students, scholars, government officials, municipalities, law enforcement agencies, and all those who are interested in, study, and use such terminology in their education and work, but also for every citizen to increase their awareness and readiness to protect and counter hybrid threats.

## 3. Подяка європейським експертам

Шановні експерти, колеги!

Щиро дякуємо за ваші знання, коментарі, пропозиції та виправлення, висловлені до версії глосарію 1.0. Ми цінуємо те, що ви поділилися своїм досвідом щодо термінології гібридних загроз, структури та складання Глосарію.

Представники нашої UA-команди, які працювали над вдосконаленням Глосарію та створенням версії 2.0., уважно вивчили усі ваші коментарі, якими потім поділилися серед інших українських колег та дослідників з консорціуму університетів у середовищі WARN. Ваші пропозиції допомогли нашим командам зосередитися на термінах, які більше стосуються гібридних загроз у відповідних сферах нашого проекту. В результаті ми вирішили не включати частину запропонованих термінів до Глосарію 2.0, оскільки вони були спрямовані здебільшого на дослідницькі цілі, однак ми вважаємо, що термінологія, представлена в Глосарії 2.0, повинна використовуватися здебільшого в навчальному процесі.

Ми щиро вдячні експертам з **Університету Ювяскюля (Фінляндія)**, оскільки надані ними матеріали не лише заклали основу Глосарію 1.0, а й сформували мейнстрім його оновлення до версії 2.0. Команда високо цінує редакцію та виправлення, внесені в першу версію нашими колегами з **Коїмбрського університету (Португалія)**. Оскільки наші французькі колеги (**Вищі інженерна школа ECAM-EPMI**) підкреслили важливість термінології, тісно пов'язаної з гібридними загрозами в кібербезпеці, деякі з них були включені до вдосконаленої версії та стали цінним доповненням до термінології Глосарію 2.0. Ми щиро вдячні за цінні рекомендації та коментарі наших естонських колег (**Університет Тарту**) щодо певної конкретної термінології, яка була частково впроваджена в Глосарій 2.0 відповідно до цілей нашого проекту, зосередженого головним чином на навчанні.

Для складання Глосарію 2.0 українська команда опрацювала велику кількість матеріалів, статей та документів, рекомендованих європейськими партнерами проекту. Вони стали джерелом усіх визначень і термінології. Однак кожен термін у Глосарії 2.0 є «точкою доступу» до більш детальних пояснень, досліджень та ілюстрацій, наданих професіоналами. Читач має можливість самостійно ознайомитися з ними за списком літератури, що міститься в глосарії. Загалом, ми хотіли б визнати, що ми намагалися вдосконалити версію Глосарію 2.0 і дотримуючись рекомендацій і коментарів усіх наших колег з ЄС до першої версії, якою поділилися колеги-викладачі та дослідники в нашому середовищі WARN в

Україні. Ваш досвід був цінною частиною досягнень цього результату проекту, і ми щиро сподіваємося, що Глосарій 2.0 представить широкий спектр корисних термінів щодо гібридних загроз для українських студентів, викладачів і дослідників.

З повагою

Команда розробки UA Glossary 2.0.

## Acknowledgment of our European Experts' Contributions

Dear Experts, Colleagues,

Thank you so much for your expertise, comments, suggestions and corrections expressed to our Glossary 1.0 version. We sincerely thank you for sharing your experience related to the terminology of hybrid threats and structure and compilation of the Glossary.

The project team of UA representatives has worked on improving the Glossary and creating version 2.0. carefully studied all your comments, which were then shared among other Ukrainian colleagues and researchers from the consortium universities in WARN-environment. Your suggestions have helped our teams to closely focus on the terms more related to hybrid threats in the relevant spheres of our project. We decided not to include part of the suggested terms in Glossary 2.0 as they were directed mostly at research purposes. However, we consider that the terminology presented in Glossary 2.0 shall be mostly used in the teaching process.

We are truly thankful to the experts from the **University of Jyväskylä** as the materials provided by them not only laid the foundation for Glossary 1.0 but also formed the mainstream of its update to version 2.0. The team greatly appreciates the editorship and corrections made in the first version by our colleagues from **Coimbra University**. As our French colleagues (**ECAM-EPMI** Graduate School of Engineering) emphasised the importance of terminology closely related to hybrid threats in cybersecurity, a number of them have been included in the improved version and have become a valuable addition to the Glossary 2.0 terminology. We truly appreciate the valuable recommendation and comments from our Estonian colleagues (**University of Tartu**) regarding some specific terminology, which have been partly implemented in Glossary 2.0 according to the aims of our project, primarily focused on teaching.

To compile the Glossary 2.0, the Ukrainian team processed a large number of materials, articles, and documents recommended by the project's European partners. They became the source of all definitions and terminology. However, each term in Glossary 2.0 is an "access point" to a more detailed explanation, research, and illustrations provided by professionals. The reader has the opportunity to access them independently through the list of references contained in the glossary. Overall, we would like to acknowledge that we tried to improve the Glossary 2.0 version and follow the recommendations and comments of all our EU colleagues to the first version that has been shared among the teaching and research colleagues in our WARN-environment in Ukraine. Your expertise has been a very valuable part of accomplishing this project result, and we sincerely hope that Glossary 2.0 will present a wide range of useful terms on hybrid threats to Ukrainian students, teachers and researchers.

Sincerely,

UA Glossary 2.0 Development Team

# 4 ГЛОСАРІЙ-2.0 / GLOSSARY-2.0

## A

| № | UA | EN | Джерело |
|---|---|---|---|
| 1. | **Автократія**<br>правляча система, в якій лідер (диктатор або король) має необмежену владу. | **Autocracy**<br>a ruling system in which the leader (dictator or king) has unlimited power. | Sazonov et al. (2016) - p.20 |
| 2. | **Агент Ікс**<br>шкідливе програмне забезпечення, яке дозволяє віддалено виконувати команди, передавати файли та реєструвати ключі;<br>функція, яка реєструє кожне натискання клавіші на скомпрометованому комп'ютері, що забезпечує легкий доступ до паролів. X-Agent налаштований роботу як на комп'ютері, так і на мобільних платформах. | **X-Agent**<br>a malware that allows for remote commands, file transmissions, and keylogging,<br>a feature that records every keystroke made on a compromised computer which allows for easy access to passwords. X-Agent is also configured to be capable of running on both computer and mobile platforms. | Treverton et al. (2018) - p.41-42 |
| 3. | **Агент культури**<br>1) людина, яка сприяє змінам, висвітлюючи та досліджуючи безліч способів впливу культурних практик на наші суспільства.<br>2) концепція культури як агентства, що являє собою низку креативних видів діяльності, які сприяють розвитку суспільства, зокрема педагогіку, дослідження, активізм та мистецтво. | **Cultural agent**<br>1) is an individual who promotes change by highlighting and exploring the many ways in which cultural practices affect our societies.<br>2) the conception of the culture as an agency, which refers to a range of creative activities that contribute to society, including pedagogy, research, activism, and the arts. | Sommer, D. (2021)<br>Barbero et al. (2006) |
| 4. | **Агресія збройна** | **Armed aggression**<br>The use of armed force by a state or a group of states against any country. | Horbulin (2017) – p.156 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Застосування іншою державою або групою держав збройної сили проти будь-якої країни. | | |
| 5. | **Адаптація держави до мережевого управління**<br><br>процес вбудовування держави у технічні й операційні мережі, що супроводжується залученням до формування стандартів і практик у середовищі за участю багатьох зацікавлених сторін. Реалізація даного процесу неможлива шляхом встановлення прямого ієрархічного контролю над ним. Це робить його вразливим до гібридних загроз. | **Adaptation of the state to network management**<br><br>This is the process of embedding the state into technical and operational networks, accompanied by the involvement in the formation of standards and practices in an environment with the participation of multiple stakeholders. The implementation of this process cannot be achieved through the establishment of direct hierarchical control over it. This makes it vulnerable to hybrid threats. | Milton et al. (2013) - p.100 |
| 6. | **А́ктори гібридних загроз**<br><br>Зловмисники, які створюють гібридні загрози та беруть участь у гібридних впливах.<br>Їх об'єднує те, що вони мають демонструвати здатність до синхронізації різних інструментів із конкретними вразливостями жертви для створення лінійних та нелінійних ефектів.<br>Актори можуть бути як *державним акторами гібридних загроз*, так і *недержавнимми акторами гібридних загроз*<br>Актори є одним з 4-х ключових елементів у *Концептуальної моделі гібридних загроз* | **Actors of hybrid threats**<br><br>Criminals who create hybrid threats and engage in hybrid influence. What they have in common is the ability to synchronize various tools with specific vulnerabilities of the target to create linear and nonlinear effects. The actor can be both *states actors of hybrid threats* and *non-state actors of hybrid threats.*<br>Actors are one of the 4 key elements in the *Conceptual model of hybrid threats* | MCDC (2017) – p.8 |
| 7. | **Акультурація**<br><br>процес, який втілює людина/агент (це не процес, який трапляється з людиною) після зустрічі та приєднання до культурної | **Acculturation**<br><br>a process executed by an agentic individual (it is not a process that happens to an individual) after meeting and entering a cultural | Chirkov, V. (2009) – p.94<br><br>Maehler et al. (2019) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | спільноти, яка відрізняється від культурної спільноти, де вона була соціалізована. | community that is different from the cultural community where he or she was originally socialized. | |
| 8. | **Акустична війна**<br><br>сукупність дій, під час яких використовується акустична енергія у підводному середовищі задля провокування, спонукання, обмеження або попередження застосування ворогом акустичного спектру, а також впровадження будь-яких заходів задля запобігання його використання проти дружніх сил. | **Acoustic warfare**<br><br>in an underwater environment, the use of acoustic energy to provoke, exploit, restrict or prevent hostile use of the acoustic spectrum and the implementation of any measures taken to restrict its use to friendly forces. | NSA (2013) – p. 2-A-1 |
| 9. | **Аналіз загрози гібридної війни**<br><br>аналіз / процес, призначений для врахування всіх інструментів гібридної війни МПЕСІ. В той час, як військові зосереджуються на мілітарному (військовому) М-компоненті, експертів з цивільних питань та приватний сектор залучають для надання допомоги в аналізі нетрадиційних загроз, а саме невійськових інструментів гібридної війни (політичних, економічних, громадянських, інформаційних). Ключем до успіху цього процесу є розуміння того, як конкретні учасники гібридної війни адаптують атаки під конкретні вразливості намічених цілей у всьому спектрі ПМЕСІІ-доменів. | **Hybrid warfare threat analysis**<br><br>an analysis/process designed to account for all MPECI instruments of a hybrid warfare threat. While the military focuses on the M (military), civilian subject matter experts and the private sector are brought in to assist non-traditional (not military) threat analysis of political, economic, civil, informational hybrid warfare tools. The key to the success of this process is understanding how specific hybrid warfare actors tailor attacks to specific vulnerabilities of intended targets across the PMESII spectrum. | MCDC (2017) – p.31 |
| 10. | **Аналіз центру ваги**<br><br>методологія військового планування, що походить з книги Карла фон Клаузевіца "Про війну", | **Centre of gravity analysis**<br><br>a military-planning methodology derived from Carl von Clausewitz's book On War to identify the 'source' or 'hub' of power in a system. | MCDC(a) (2019) – p.89 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | для виявлення "джерела" чи "центру" влади в системі. | | |
| 11. | **Аналіз цільової аудиторії**<br><br>це процес пошуку та дослідження відповідної цільової аудиторії. Використовується, зокрема, для проведення інформаційно-психологічних операцій. | **Target Audience Analysis (TAA)**<br><br>is the process of finding and researching a suitable target audience. It is used, in particular, for conducting informational and psychological operations. | Kalenský et al. (2024) |
| 12. | **Аннексія Криму**<br><br>на початку 2014 року, після протестів на Майдані та втечі Януковича із влади та з України 21 лютого, москва перейшла від риторики до кампанії гібридної війни. У ніч на 27 лютого 2014 року російський спецназ зайняв місцевий орган влади в АР Крим. Водночас російські війська, раніше розміщені в Криму та місті Севастополі згідно з Договором про Чорноморський флот 1997 року, почали облогу та напади на українські війська, урядові будівлі та інфраструктуру, прямо порушуючи Будапештський меморандум 1994 року, який гарантував територіальну цілісність України. 16 березня російська влада та проросійські сепаратисти провели незаконний "референдум" щодо приєднання Криму та Севастополя до росії із малоймовірним результатом - 96,7% підтримки анексії. Пізніше сам путін визнав, що під час "референдуму" в Криму було близько 20 тисяч російських військовослужбовців, що сприймалося як вплив на | **Annexation of Crimea**<br><br>by early 2014, following the Maidan protests and Yanukovich's departure from government and Ukraine on 21 February, Moscow changed from rhetoric to a hybrid warfare campaign. On the night of 27 Feb 2014, Russian special forces took over the local legislature of Ukraine's Autonomous Republic of Crimea. At the same time, Russian troops, previously stationed in Crimea and the city of Sevastopol under the Black Sea Fleet Treaty of 1997, started besieging and attacking Ukrainian troops, government buildings, and infrastructure in direct violation of the 1994 Budapest Memorandum which guaranteed the territorial integrity of Ukraine. On 16 March, Russian authorities and pro-Russian separatists conducted an illegal "referendum" for Crimea and Sevastopol to join Russia with the reported but unlikely outcome of 96.7 percent supporting annexation. Putin himself later acknowledged that around twenty thousand Russian troops were present in Crimea during the "referendum," which has been perceived as | Grigas (2016) – p.127 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | результат. Через два дні після "референдуму", російська федерація підписала договір про приєднання Криму та міста Севастополя і, таким чином, запровадила те, що світ вважає незаконною анексією українських територій. | influencing the outcome. Two days after the “referendum,” the Russian Federation signed the treaty of accession for Crimea and the city of Sevastopol, and thus enacted what the world considers an unlawful annexation of Ukrainian territories. | |
| 13. | **Аномія**<br><br>соціальна ситуація, коли старі інститути перестають функціонувати стабільно й люди вже не можуть розраховувати на отримання очікуваних винагород за відповідними очікуваними стандартами (концепція Дюргейма).<br><br>відсутність (знецінення) норм, що проявляється у формі деінституціоналізації правових (законних) засобів суспільства (концепція Мертона).<br><br>Таким чином, цілі, до яких навчили прагнути людей (наприклад, досягти процвітання завдяки добре оплачуваній роботі), не відповідають інституціоналізованим наявним засобам та нормам, які влада може запропонувати людям. | **Anomie**<br><br>the social situation when old institutions are no longer functioning in a stable way and people no longer can count on receiving the expected rewards for conforming to expected standards (conception of Durkheim).<br><br>normlessness, manifested in such a form as a deinstitutionalization of the legitimate means of society (conception of Merton)<br><br>So the goals toward which people have been taught to aspire (e.g., to achieve prosperity by holding a well-paid job) do not correspond to the institutionalized means that are actually available and the norms by which people are supposed to compete. | Spencer & Lalgee (2008) – p.1970 - 1982<br><br>Deflem (2018) – P.147 |
| 14. | **Антизахідництво**<br><br>Це один з концептів *Нової моделі внутрішнього контролю над росією.*<br>Передбачає просування ідеї про історичні складні відносини із західними країнами та відчуття росії аутсайдером у | **Anti-Westernism**<br><br>One of the concepts of a *New model for controlling Russia internally*<br>It involves promoting the idea of historical complex relationship with the Western countries and feeling of Russia as an underdog in European / Global politics. It is created by | Cullen et al. (2021) – p.19 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | європейській/світовій політиці. Створюється російською пропагандою для формування *російськості* | Russian propaganda to form *russianness* | |
| 15. | **Асиметрія гібридних загроз**<br><br>Основна властивість гібридних загроз, що створюється парадоксальністю відносин, у яких слабший супротивник здатний завдавати шкоди та навіть нав'язувати свою „волю" сильнішій стороні, тоді як сильніший не завжди може захищати свої інтереси та підкоряти слабшого.<br><br>Асиметричні загрози не потребують еквівалентних можливостей чи цілей, і тому дуже приваблюють:<br><br>- як недержавних суб'єктів, які прагнуть досягти політичної або кримінальної мету,<br><br>- так і державних діячів, які прагнуть досягти цілей переконливими засобами заперечення. | **Asymmetry of hybrid threat**<br><br>A basic property (strength) of hybrid threats, which is created by the paradoxical nature of relations in which the weaker opponent is able to cause detriment and even impose its „will" over the more powerful side, while powerful cannot always be at their interests and to subjugate the weak.<br><br>The asymmetrical threat does not require equivalence of capability or aim and so holds great appeal to both the non-state actor, seeking to advance a political or criminal end, and the state actor, seeking to achieve ends through plausibly deniable means. | MCDC(b) (2019) – p.1<br><br>Hristov (2017) – p.468 |
| 16. | **Астротурфінг**<br><br>(посилання на бренд штучного газону "AstroTurf").<br><br>явище, коли команди кібервійськ керують підробленими обліковими записами, щоб замаскувати себе та свої інтереси і зробити так, щоб навколо спонсора (особи чи організації) створювалась ніби-то природня активність . | **Astroturfing**<br><br>(a reference to a brand of artificial turf "AstroTurf").<br><br>a phenomenon where cyber troop teams run fake accounts to mask their identity and interests and make the identity of a sponsor or organization appear as grassroots activism.<br><br>This technique creates an artificial sense of popularity. | Bradshaw & Howard (2017) – p.11<br><br>Vilmer et al. (2018) - p.87 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Техніка полягає в тому, щоб створити видимість популярності.<br><br>Див. також: *Боти* | see also: *Bots* | |
| 17. | **Атрибуція**<br><br>визначення справжнього джерела гібридної загрози, приписування доказів конкретному нападнику. | **Attribution**<br><br>identifying the true source of the hybrid threat, and prescription of evidence to a specific attacker. | Методика навчання в умовах гібридних загроз (2023) |

## Б

| № | UA | EN | Джерело |
|---|---|---|---|
| 18. | **Багатовекторність зовнішньої політики України**<br><br>концепція зовнішньої політики, сформована наприкінці 90-х років XX ст., яка мала на меті встановити певний баланс інтересів та зовнішньополітичної діяльності України у трьох основних напрямках – російському, європейському та східному (Чорноморський регіон та країни Азії). За лаштунками української політики багатовекторності стояла необхідність жорсткого вибору на користь одного з двох варіантів - проросійського або проєвропейського. Відносна рівновага векторів мала тимчасовий характер, політика багатовекторності виявилася неефективною і зрештою, під час Революції гідності наприкінці 2013 - початку 2014 рр, .була остаточно зруйнована. | **Multi-vector foreign policy of Ukraine.**<br><br>the concept of foreign policy which emerged in the late 1990s.It aimed at establishing a balance of interests and foreign political activities of Ukraine in three core directions – Russian, European and Eastern (the Black Sea region and Asia). This Ukrainian multi-vector foreign policy was determined by the need of making a clear choice between two options – pro-Russian or pro-European. The relative balance of the vectors was temporary, and the ineffective multi-vector policy was finally ruined in consequence of the Revolution of Dignity at the end of 2013 – beginning of 2014. | Horbulin (2017) – p.158 |
| 19. | **Базова лінія**<br><br>контрольна точка, яка дозволяє ідентифікувати показники та події, а також вимірювати відхилення від цієї контрольної точки. Встановлення базової лінії є ключовою частиною процесу самооцінки гібридної війни. | **Baseline**<br><br>a reference point to allow for the identification of indicators and events as well as the measurement of variation away from that reference point. Establishing a baseline is a key part of the hybrid warfare self-assessment process. | MCDC (2017) – p.31 |
| 20. | **Беллінгкет**<br><br>незалежний колектив дослідників, громадських журналістів, заснований у 2014 році. | **Bellingcat**<br><br>an independent investigative collective of researchers, investigators and citizen journalists, | Bellingcat (n.d.) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Використовують методи вивчення відкритих джерел для дослідження різноманітних тем, що становлять суспільний інтерес. | founded in 2014. They use open source research methods to investigate a variety of subjects of public interest. | |
| 21. | **Бізнес-модель на основі залежності та збору даних**<br><br>Принцип функціонування платформ соціальних медіа, які спроектовані в такий спосіб, щоб якомога довше утримувати користувачів на сайті, збирати дані про все, що вони роблять, і продавати їх рекламодавцям. Розуміння саме рекламодавців як своїх клієнтів, а не користувачів, призвело до оманливих практик, які використовують тактику пропаганди за рахунок громадськості. | **Business Model Based on Addiction and Data Capture**<br><br>The principle of functioning of the social media platforms that are engineered to keep users on the site as long as possible, collect data on everything they do, and sell it to advertisers. Treating advertisers as their clients, rather than users, has led to deceptive practices that exploit tactics of propaganda at the expense of the public. | Gorbis et al. (2019) – p.4 |
| 22. | **Біо-хакінг**<br><br>Секвенування та синтезування ДНК, а також зловживання цим.<br><br>Приклади "гібридного" застосування: Створення нової біологічної зброї на основі технології синтетичної біології, наприклад, вірусів. | **Bio-hacking**<br><br>DNA sequencing and synthesis and the misuse of this.<br><br>Examples of hybrid applications: Creation of new biological weapons based on synthetic biology technology, such as viruses. | Bekkers et al. (2019) – p.27 |
| 23. | **Близьке зарубіжжя (пострадянський простір)**<br><br>(один із наративів, що окреслює сфери інтересів кремля)<br><br>це ті колишні радянські республіки, які зараз є незалежними державами.<br><br>росія вважає, що ці слабкіші (особливо в економічному сенсі) країни повинні "природним | **"Near abroad" (post-Soviet space)**<br><br>(one of the narratives that outline the Kremlin's spheres of interest)<br><br>those ex-Soviet republics that are now independent states.<br><br>Russia assumes that these weaker (especially in an economic sense) countries should ‘naturally’ gravitate | Rotaru (2018) – p.1<br><br>Simons (2015) – p.4 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | чином" тяжіти і тягнутись до сильнішої російської держави, посилаючись на спільний з росією історичний досвід, культуру, мову тощо. | and be drawn to the stronger Russian state referring to shared historical experience, culture, language and so forth of these countries with Russia | |
| 24. | **Блог**<br><br>скорочена версія веб-журналу, яка вказує на його походження як набір щоденникових записів або пов'язаного вмісту, розміщеного в Інтернеті з різних причин, здебільшого особистого характеру. Шанс для читачів залишати коментарі в інтерактивному форматі - нова функція блогу порівняно із звичайною журналістикою. Вплив блогів викликає великі суперечки, оскільки в небагатьох є власна велика аудиторія, але вони представляють значне відкриття доступу громадськості та виклик інституційному контролю публічної інформації. | **Blog**<br><br>The word is a shortened version of weblog, which indicates its origin as a set of diary entries or related content posted on the Internet for a variety of reasons, mostly of a personal nature. The chance for readers to leave comments in an interactive format is a novel feature of the blog compared to normal journalism. The influence of blogs is much disputed, since few have any large audience of their own, but they represent a significant opening of public access and a challenge to institutional control of public information. | McQuail's, D. (2010) – p. 549 |
| 25. | **Борг Януковича**<br><br>Інструмент фінансового тиску на Україну з метою доведення її до стану дефолту в умовах гібридної війни з боку рф. Заборгованість України перед росією, сформована шляхом викупу російським Фондом національного добробуту ( ФНД) у грудні 2013 року дворічних євробондів із купоном 5% (цінні папери українського уряду, що були розміщені на Ірландській фондовій біржі) на загальну суму $ 3 млрд та з терміном погашення 20 грудня | **Yanukovych Debt**<br><br>The instrument of the RF financial pressure on Ukraine to lead it to default in the condition of hybrid war. The debt of Ukraine to Russia resulting from the buyout of two-year 5 % coupon Eurobonds (Ukrainian government securities listed securities listed on Irish stock exchange) for the total amount of $3 bln and maturity on 20 December 2015 by the Russian National Wealth Fund (NWF) in December 2013. It had political grounds only (refusal | Horbulin (2017) – p.159 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | 2015 року. Була сформована суто на політичних умовах (відмова від євроінтеграційного курсу України). | from the European integration of Ukraine). | |
| 26. | **Боти**<br><br>автоматизовані або напівавтоматизовані суб'єкти, як-от фрагменти коду, призначені для взаємодії користувачами-людьми та їхньої імітації (для обміну певними типами інформації в соціальних мережах або для відповіді на поширені запитання на платформах обслуговування клієнтів тощо).<br><br>Є одним із інструментів *Технічного Використання*. В області інформаційного впливу вони можуть використовуватися для посилення відібраних повідомлень в Інтернеті, спам-форумів та коментарів, наприклад, для публікації повідомлень в соціальних мережах або для здійснення кібератак.<br><br>див. також: *Астротурфінг*. | **Bots**<br><br>automated or semi-automated actors like bits of code designed to interact with and mimic human users (for sharing certain types of information on social media or for answering frequently asked questions on a customer service platform etc).<br><br>Are one of the *Technical Exploitation* tools. In the field of information influence, they can be used to reinforce selected messages online, spam forums and comment fields, like or share posts on social media, or to carry out cyber-attacks.<br><br>see also: *Astroturfing*. | Bradshaw & Howard (2017) – p.11, 83<br><br>MSB (2018) – p.19, 23 |
| 27. | **"Бульбашки фільтрів"**<br><br>алгоритми персоналізації, який використовується пошуковими системами та соціальними мережами.<br><br>Через це результати пошуку в Google не однакові для всіх користувачів; вони залежать від уподобань користувача, які випливають з його історії пошуку та геолокації. | **“Filter Bubbles”**<br><br>personalization algorithms used search engines and social networks.<br><br>Because of this, the search results in Google are not the same for all users; they depend on the preferences of the user as deduced from his or her search history and geolocation.<br><br>see also: *Micro-Targeting, Internet-Cocooning* | Vilmer et al. (2018) - p.31<br><br>Pariser (2011) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | див. також: *Мікро-таргетування, Інтернет-Кокон* | | |

## В

| № | UA | EN | Джерело |
|---|---|---|---|
| 28. | **Валентність повідомлення**<br>сила привабливості (доброти) або огидності (поганості) повідомлення, події чи речі. | **Valence Of A Message**<br>the power of attractiveness (goodness) or averseness (badness) of a message, event or thing. | Bradshaw & Howard (2017) – p. 9 |
| 29. | **Велика Вітчизняна війна (1941 - 1945)**<br>один із кремлівських наративів, російська інтерпретація історії.<br>Сакралізована перемога СРСР над нацизмом є центральним елементом політики пам'яті сучасної росії. Це становить важливу тему в ідеологічному наступі кремля, який покликаний легітимізувати великодержавні амбіції росії. Месіанський міф про порятунок світу від абсолютного зла має прикривати темні глави радянської історії та легітимізувати всі наступні радянські чи російські війни та військові інтервенції, починаючи з Угорщини, переходячі до Чехословаччини та Афганістана і закінчуючи Україною та Сирією. | **Great Patriotic War of 1941–1945**<br>one of the Kremlin narratives, the Russian interpretation of history<br>The sacralised Soviet victory over Nazism is a central element of the politics of memory, as utilised by the Russian state today. It constitutes an important theme in the Kremlin's ideological offensive that is intended to legitimise Russia's great-power ambitions. The messianic myth of saving the world from absolute evil is supposed to cover up the darker chapters of Soviet history and to legitimise all subsequent Soviet or Russian wars and military interventions, starting with Hungary, through Czechoslovakia and Afghanistan and ending with Ukraine and Syria. | Rotaru (2018) – p.9<br>Domańska (2019) – p.1 |
| 30. | **Великі дані**<br>культурно-технологічне явище, яке описує максимізацію обчислювальної потужності та алгоритмічної точності для збору, аналізу, зв'язку та порівняння великих масивів даних, а також процес використання великих масивів даних для виявлення закономірностей з метою створення економічних, | **Big Data**<br>a cultural and technological phenomenon that describes the maximisation of computation power and algorithmic accuracy to gather, analyse, link, and compare large data sets as well as the process of drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims. | Neudert & Marchal (2019) – p.5 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | соціальних, технічних , а також юридичних претензій. | | |
| 31. | **Великодержавність**<br><br>Це один з концептів *Нової моделі внутрішнього контролю над росією.*<br>Передбачає просування ідеї про глибоке відчуття росії як "Великої Держави" та потребу захистити цю ідентичність. Створюється російською пропагандою для формування *російськості* | **Greatpowerness**<br><br>One of the concepts of *a New model for controlling Russia internally.* It involves promoting the idea of deep sense of Russia as a Great Power and a need to protect that identity. It is created by Russian propaganda to form *russianness* | Cullen et al. (2021) – p.19 |
| 32. | **Вертикальна ескалація**<br><br>посилене використання одного конкретного засобу МПЕСІ | **Vertical escalation**<br><br>the intensified use of one specific means (*MPECI*) | MCDC(a) (2019) – p.90 |
| 33. | **Виклики сірої зони**<br><br>див. *Допорогові Виклики* | **Gray Zone Challenges**<br><br>see *Sub-Threshold Challenges* | |
| 34. | **Викривання дезінформації**<br><br>це захід реагування, який застосовують тоді, коли дезінформація вже відбулася. Під викриванням розуміємо процес демонстрації того, що переконання або теорія, не відповідає дійсності; неправдивості історії, ідеї, твердження тощо. Викривання можна розглядати як триступеневий процес: перший крок - аналіз дезінформації; другий - прийняття рішення про те, чи варто витрачати час і ресурси на розвінчання неправдивого твердження; якщо прийнято рішення діяти проти дезінформації, то третій крок - планування і викривання. | **Debunking of disinformation**<br><br>is a response measure adopted when disinformation has already taken place. Debunking is defined as the process of showing that something, such as a belief or theory, is not true, or to show the falseness of a story, idea, statement, etc. Debunking can be seen as a three-step process: the first step is to analyse the disinformation; the second is to decide whether it is worth investing time and resources to debunk the false claim; if the decision is taken to act against disinformation, the third step is to plan and execute the debunking. | Kalenský et al. (2024) |

| № | UA | EN | Джерело |
|---|---|---|---|
| 35. | **Витік**<br><br>є одним із методів "*Символічних Дій*"<br><br>оприлюднення інформації, отриманої неправомірними способами. Має символічне значення, оскільки, як правило, розкриває злочини та укриття фактів, не призначені для очей громадськості.<br><br>Якщо витік використовується для інформаційного впливу, інформація вирівається з контексту і використовується для делегітимізації суб'єктів, а також спотворення інформаційного середовища. Витік інформації іноді відбувається внаслідок злому IT-систем або крадіжки.<br><br>Наслідки цих витоків варіюються від пошкодження оперативної безпеки (збору розвідданих) до підриву довіри до політичної системи країни та її керівництва.<br><br>Див. також "*Витік Макрона*" | **Leaking**<br><br>is one of the "*Symbolic Actions*"<br><br>releasing information that has been obtained by illegitimate means. It carries symbolic weight as it traditionally reveals injustices and cover-ups not meant for the public eye.<br><br>When used as an information influence activity, leaked information is taken out of context and is used to delegitimize actors and distort the information environment. Leaked information is sometimes obtained through hacking of IT-systems or theft.<br><br>The consequences of these leaks range from damaging operational (intelligence-gathering) security to undermining trust in a nation's political system and its leadership.<br><br>See also *"Macron Leaks".* | MSB (2018) – p.19, 27<br><br>Treverton et al. (2018) - p.58 |
| 36. | **"Витік Макрона"**<br><br>інцидент, який стався в 2017 році - буквально за два дні до другого та останнього туру президентських виборів, коли внаслідок хакерської атаки 9 гігабайт даних було перехоплено з передвиборчого штабу команди Еммануеля Макрона.<br><br>Ці цілеспрямовані дії проти кандидата в президенти Еммануеля Макрона та організована проти нього кампанія | **"Macron Leaks"**<br><br>incident of the release in 2017—just two days before the second and final round of the presidential elections—of 9 gigabytes of data that were hacked from Emmanuel Macron's campaign team.<br><br>These targeted actions against presidential candidate Emmanuel Macron and the orchestrated campaign against him (that started several months earlier, through numerous information manipulation | Vilmer et al. (2018) - p.106 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | (яка розпочалася кількома місяцями раніше, завдяки численним операціям із маніпуляцій інформацією) розглядалися як спроба втручання у вибори президента Франції 2017 року. | operations) seen as the attempted interference in the 2017 French presidential election. | |
| 37. | **Відкриття (як спосіб виявлення гібридних загроз)**<br><br>процес збирання й правильного інтерпретування інформації, пов'язаної з потенційно ворожою дією супротивника, про яку раніше не було відомо.<br><br>Містить підходи до виявлення неоднозначних або прихованих гібридних загроз шляхом знаходження та фільтрування непередбачених аномалій.<br><br>Це спроба вирішити проблему "*Невідомих Невідомих*" (на відміну від *Моніторингу*). | **Discovery (as a way to detect hybrid threats)**<br><br>a process of capturing and then correctly interpreting information related to a potentially hostile adversarial action that has not been previously conceived.<br><br>Includes approaches to discovering ambiguous or hidden hybrid threats by finding and filtering unanticipated anomalies.<br><br>This is an attempt to manage the problem of "*Unknown Unknowns*" (by contrast of *Monitoring*). | MCDC(a) (2019) – p.26, 33 |
| 38. | **Відмивання (інформаційне)**<br><br>Відмивання означає поступове спотворення та деконтекстуалізацію інформації в такий спосіб, що стає неможливим визначити, чи є її джерело істинним чи хибним.<br><br>Ця стратегія може використовувати *Оманливі Ідентичності, Дезінформацію, Технічні Маніпуляції* та *Символічні Дії* у поєднанні із *Соціальним / Когнітивним Зломом*, щоб зіткати павутину неправдивої інформації. | **Laundering (informative)**<br><br>Laundering refers to gradually distorting and de-contextualizing information, so that it becomes impossible to tell if its source is true or false.<br><br>This strategy may use *Deceptive Identities, Disinformation, Technical manipulation*, and *Symbolic Acts* in combination with *Social/Cognitive Hacking* to create a web of false information (see *Influence Campaigns*). | MSB (2018) – p.29 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 39. | **Відмивання грошей**<br><br>процес, за допомогою якого надходить велика кількість незаконно отриманих грошей (від торгівлі наркотиками, терористичної діяльності чи інших злочинів), і створюється враження, що вони походять із законного джерела. Це конвертація "чорних" грошей у "білі" гроші. | **Money laundering**<br><br>the process by which large amount of illegally obtained money (from drug trafficking, terrorist activity or other serious crimes) is given the appearance of having originated from the legitimate source. It is the conversion of black money into white money. | Kumar (2012) – p.113 |
| 40. | **Відновлюваність**<br><br>здатність повертатись до нормального функціонування після того, як система зазнала певного збою, впливу чи порушення. Одна зі складових *Стійкості.* | **Recovery**<br><br>the ability to return to normal functioning after experiencing a failure, impact, or disturbance. One of the components of *Resilience.* | Gryshko et al. (2024) |
| 41. | **Відомі невідомі**<br><br>Параметри, які характеризують режими гібридної атаки; ми знаємо природу цих параметрів, але нам невідомі їх значення.<br><br>Тобто це параметри, "про які ми знаємо, що можемо їх не знати" (на відміну від "*Невідомі Невідомі*") | **Known unknowns**<br><br>Parameters that characterize hybrid attack modes; we know the nature of these parameters, but we do not know their values.<br><br>That is, these are parameters "that we know we may be unaware of" (by contrast "*Unknown Unknowns*") | MCDC(a) (2019) – p.26 |
| 42. | **Війна за громадську думку**<br><br>Один з 3-х елементів китайської стратегії "*Три війни*" Операції з метою впливу на внутрішню і міжнародну підтримку шляхом використання вибіркової інформації, що подається через різні засоби мас-медіа, міжнародні організації, академічні форуми тощо. Це застосування теорії про те, як контролювати маси. Специфічні методи формування громадської думки Китаю: прямий | **Public Opinion Warfare**<br><br>One of the 3 elements of the Chinese strategy "*Three Warfares*" Operations to influence both domestic and international support by the use of selective information delivered through different media, international organisations, academic forums etc. Here the theories relating to how to control masses applies. Specific tools that are used to frame public opinion in China include: direct | Cullen et al. (2021) – p.21 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | контроль зверху вниз; упередженність щодо позитивних історій та цензура негативних історій; інтенсивне використання гасел для передачі повідомлень. | top-down control, a bias towards positive stories and censorship of negative stories, heavy use of slogans to convene the message. | |
| 43. | **"Війна нового покоління"**<br>російська військова доктрина<br>див. *Доктрина Герасимова* | **'New generation warfare'**<br>the Russian military doctrine<br>*See: Gerasimov doctrine* | |
| 44. | **Військовий домен гібридних загроз**<br>Збройні сили та допоміжна інфраструктура придбані, навчені, розвинуті та підтримані для досягнення та захисту цілей національної чи організаційної безпеки. Це також стосується аспектів внутрішньої безпеки країни.<br>Один з 6-ти *ПМЕСІІ*-доменів. Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | **Military domain of hybrid threats**<br>The armed forces, and supporting infrastructure, acquired, trained, developed and sustained to accomplish and protect national or organisational security objectives. This also covers the internal security aspects of a country. One of the 6 *PMESII*-domains. One of the 13 domains in the *Conceptual model of hybrid threats* | NATO (2013) – p.1-8 |
| 45. | **Військові інструменти гібридних загроз**<br>Військовий інструмент означає застосування військової сили, включно із погрозою або використанням летальної та нелетальної сили, щоб примусити, стримувати, протидіяти або перемогти супротивника, включаючи підрив і знищення його критично важливого військового та невійськового потенціалу. Це також може стосуватися конструктивного використання військових сил для забезпечення та/або підтримки стабілізації і відновлення або як інструмент | **Military instruments of hybrid threats**<br>The military instrument refers to the application of military power, including the threat or use of lethal and non-lethal force, to coerce, deter, contain or defeat an adversary, including the disruption and destruction of its critical military and non-military capabilities. It can also refer to the constructive use of military forces to secure and/or support stabilization and reconstruction or as a tool in helping solve complex humanitarian disasters and emergencies. One of the 5 *MPECI*-instruments. A | NATO (2013) – p.1-9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | допомоги у вирішенні складних гуманітарних катастроф і надзвичайних ситуацій. Один з 5-ти *МПЕСІ*-інструментів. Група інструментів у *Концептуальній моделі гібридних загроз* | set of tools in the *Conceptual model of hybrid threats* | |
| 46. | **Військово-цивільна адміністрація**<br><br>Тимчасовий державний орган в одному чи декількох населених пунктах, адміністративному районі чи області, що діє у складі Антиценрористичного центру при при Службі безпеки України і призначений для забезпечення дії Конституції та законів України, забезпечення безпеки і нормалізації життєдіяльності населення, правопорядку, участі у протидії диверсійним проявам і терористичним атакам, недопущення гуманітарної катастрофи в районі проведення антитерористичної операції. | **Civil military administration.**<br><br>The temporary public authority in one or more settlements, an administrative district or region, acting within the framework of the Anti-Terrorist CenteroperatingCenter operating under the Security Service of Ukraine. It's aim is toensuretonsure the enforcement of the Constitution and laws of Ukraine, security and recovery of public activities, law enforcement, participation in combating sabotage and terrorist attacks, prevention of humanitarian catastrophe in the area of carrying out anti-terrorist operation. | Horbulin (2017) – p.156 |
| 47. | **Внутрішньо переміщені особи (ВПО)**<br><br>люди або групи людей, які були змушені залишити свої будинки або місця звичайного проживання, зокрема, внаслідок, або задля уникнення наслідків збройного конфлікту, масових проявів насильства, порушення прав людини, природних або техногенних катастроф, і які не перетинали державний кордон. | **Internally displaced persons (IDPs).**<br><br>people or groups of people who were forced to leave their houses or place of residence, in particular, due to or in order to eliminate the effects of a military conflict, mass violence, human rights abuse, natural or man-made disasters, and who did not cross the state border. | Horbulin (2017) – p.158 |
| 48. | **Внутрішньодержавні війни** | **Intrastate wars** | Hosaka, S. (2021) – p.94 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | війни, що не ведуться між членами міжнародної системи, а відбуваються переважно на визнаній території держави. Вони поділяються на «громадянські війни», «внутрішні регіональні війни» та «міжетнічні війни» залежно від типу учасників бойових дій. | wars that are not fought between members of the international system, and take place predominantly within the recognized territory of a state. They are subdivided into “civil wars,” “regional internal wars,” and “intercommunal wars,” depending on the type of the combatants. | |
| 49. | **Вразливості**<br><br>персонал, діяльність, ресурси або процеси потенційної цілі ("жертви", мішені), які можуть бути використані або спеціально поставлені під загрозу потенційним супротивником. | **Vulnerabilities**<br><br>personnel, activities, resources or processes within a potential target that are susceptible of being exploited or created (deliberately exposed to risk) by a potential adversary. | MCDC(a) (2019) – p.90 |

## Г

| № | UA | EN | Джерело |
|---|---|---|---|
| 50. | **Галоп Гіша**<br><br>є одним із методів *Риторики Викривлення.*<br><br>Засипання опонента потоком аргументів, фактів та джерел, багато з яких хибні або не пов'язані з проблемою. | **Gish-Gallop**<br><br>is one of the *Malign Rhetoric* methods.<br><br>Overwhelming an opponent with a flood of arguments, facts and sources, many of which are spurious or unrelated to the issue. | MSB (2018) – p.19, 26 |
| 51. | **«Гаряча» дипломатія**<br><br>надзвичайно гостра дипломатична боротьба, що супроводжується спалахами збройних заворушень і повстань. Її формула – «ані миру, ані війни». | **"Hot" diplomacy**<br><br>the extremely intense diplomatic struggle punctuated by outbreaks of armed unrests and uprisings. Its formula is “neither peace, nor war”. | Fridman (2017) - p. 65 |
| 52. | **Гібридна адхократія**<br><br>неформальний та деінституціоналізований стиль управління, при якому офіційні обов'язки та назви посад мають набагато менше значення, ніж те, як можна задобрити керівника; ваша роль і завдання сьогодні можуть не бути такими самими завтра, навіть якщо ваша офіційна позиція залишається незмінною. | **Hybrid adhocracy**<br><br>informal and de-institutionalised style of governance in which formal responsibilities and job titles matter much less than how one can please the leader; your role and tasking today may well not be the same tomorrow, even if your formal position remains unchanged. | Galeotti (2020) – p.4 |
| 53. | **Гібридна війна**<br><br>1) синхронізоване використання багатьох інструментів сили, підібраних з урахуванням конкретних вразливостей у всьому спектрі соціальних функцій для досягнення синергетичних ефектів. | **Hybrid warfare, Hybrid war**<br><br>1) the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.<br><br>The Analytical Framework for understanding hybrid warfare is | MCDC(a) (2019) – p.12<br><br>MCDC (2017) – p.7-8, 31<br><br>MCDC(b) (2019) – p.1 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Аналітична модель для розуміння гібридної війни складається з трьох взаємозалежних частин:<br>- критичні функції та вразливості захисника;<br>- синхронізоване використання зловмисником декількох засобів та використання горизонтальної ескалації; і<br>- лінійні та нелінійні ефекти від гібридних атак.<br>2) невійськові аспекти того, що раніше передбачалось досягти в результаті військової кампанії.<br>3) вид змішаних воєнно-політичних, розвідувально-економічних операцій, які росія розпочала в Україні.<br>4) стратегічне використання (невизначеної) сили для завоювання території або досягнення іншої стратегічної мети.<br>навмисна силова гра, спрямована на передавання повідомлення з використанням неоднозначності дій, достатньої, щоб уникнути помсти чи ескалації.<br>вона є найбільш *туманною* формою війни з огляду на навмисні заплутування, що відбуваються задля приховування особистості держави-злочинця.<br>5) використання багатьох інструментів сили та впливу з акцентом на невійськові інструменти, для реалізації своїх національних інтересів поза власними кордонами. | composed of three interlocking parts:<br>- defender's critical functions and vulnerabilities;<br>- attacker's synchronized use of multiple means and exploitation of horizontal escalation; and<br>- linear and non-linear effects of an hybrid warfare attack.<br>2) the non-military aspects of what had previously been presumed to be achieved through a military campaign.<br>3) the kind of blended military-political-intelligence-economic operations Russia has launched in Ukraine<br>4) the strategic application of the use of (ambiguous) force to gain territory or attain another strategic goal<br>deliberate powerplay aimed at communicating a message whilst utilizing enough ambiguity of action to avoid retaliation or escalation.<br>it is representing the *foggiest* form of war given the deliberate obfuscations that occur in hiding the identity of the perpetrator state.<br>5) using multiple instruments of power and influence, with an emphasis on nonmilitary tools, to pursue its national interests outside its borders.<br>6) a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, | Galeotti (2015)<br>Mumford (2020) – p.3, 4<br>Treverton et al. (2018) - p.18<br>Chivvis (2017)<br>Pawlak (2017) – p. 2<br>Galeotti (2020) – p.4 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | 6) ситуація, коли країна вдається до відкритого використання збройних сил проти іншої країни або недержавного суб'єкта, до того ж поєднуючи інші засоби (такі як економічні, політичні та дипломатичні). На відміну від *Гібридних загроз, Гібридного конфлікту*)<br><br>7) Російське трактування (**Гібрідная война**): "західний підхід до дестабілізації режимів шляхом диверсії, яка може призвести до насильницького втручання." | and diplomatic). By contrast of *Hybrid threat, Hybrid conflict*<br><br>7) Russian interpretation (**Gibridnaya voina**): "the western approach to destabilising regimes through subversion that may lead to violent intervention". | |
| 54. | **Гібридна загроза на муніципальному рівні**<br><br>шкідливий вплив, спрямований на критичні операції територіальної громади. Критичні операції стосуються інфраструктури, процесів та організацій, необхідних для основних операцій міста, а також, можливо, деяких осіб. | **Hybrid Threat from the perspective of a municipality**<br><br>is harmful influencing targeted at critical operations of the municipal community. Critical operations refer to the infrastructure, processes and organisations necessary for the city's basic operations as well as, possibly, some individuals. | Harjanne et al. (2018) – p.6 |
| 55. | **Гібридний Бюлетень**<br><br>переодічний звіт Центру аналізу гібридних загроз ЄС (EU Hybrid Fusion Cell), що є частиною Розвідувального та ситуаційного центру ЄС (EU INTCEN), , який містить аналіз поточних загроз і гібридних питань, розповсюджується між інституціями та органами ЄС, а також національними контактними пунктами з 2017 року. | **Hybrid Bulletin**<br><br>a periodical report of EU Hybrid Fusion Cell (within the EU Intelligence and Situation Centre), analysing current threats and hybrid issues, shared directly within the EU institutions and bodies and national points of contact since 2017. | European Commission (2017) |
| 56. | **Гібридний вплив**<br><br>цілеспрямований тиск, який чинить певна сторона, | **Hybrid influencing**<br><br>conscious influence exerted by a party, utilizing multiple influence | Harjanne et al. (2018) - p.5 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | використовуючи різні методи впливу для досягнення своєї мети. Мета гібридного впливу - послабити та / або завдати шкоди визначеній цілі. Гібридному впливові притаманне заплутування зв'язків між дійовою особою, методами та цілями.<br><br>Тоді як *Гібридна Загроза* є втіленням методів впливу. | methods in order to reach their goal. The purpose of hybrid influencing is to weaken and/or harm the target. Hybrid influencing is characterized by obfuscation of the connection between the actor, the methods and the goals.<br><br>While a *Hybrid Threat* is an embodiment of influence methods that has been deemed to be a threat. | |
| 57. | **Гібридний конфлікт**<br><br>ситуація, коли сторони конфлікту утримуються від відкритого використання збройних сил один проти одного, натомість покладаючись на комбінацію військових залякувань (відсутність нападу), експлуатації економічних та політичних вразливостей та дипломатичних чи технологічних засобів для досягнення своїх цілей<br><br>(на відміну від *Гібридної загрози, Гібридної війни*) | **Hybrid conflict**<br><br>a situation in which parties to the conflict refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives.<br><br>(by contrast of *Hybrid threat, Hybrid war*) | Pawlak (2017) – p. 2 |
| 58. | **Гібридні загрози**<br><br>1) скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів, за використанням широкого кола засобів.<br><br>2) "Термін гібридна загроза належить до дії […], метою якої є підрив або нанесення шкоди цілі, впливаючи на прийняття рішень [...] Дії можуть мати місце, наприклад, у політичній, | **Hybrid Threats**<br><br>1) coordinated and synchronised action, that deliberately targets democratic states' and institutions systemic vulnerabilities, through a wide range of means.<br><br>2) "The term hybrid threat refers to an action […] whose goal is to undermine or harm the target by influencing its decision-making [...] Activities can take place, for example, in the political, economic, military, civil or information domains." | Hybrid CoE(a) (n.d.)<br><br>NATO (2010) – p.2<br><br>Treverton et al. (2018) - p. 10<br><br>Pawlak (2017) – p. 2 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | економічній, військовій, цивільній або інформаційній сферах."<br><br>3) "…загрози, створені супротивниками, з можливістю одночасно адаптивно застосовувати звичайні та нетрадиційні засоби для досягнення своїх цілей."<br><br>4) "Мета - досягти результатів без реальної війни. Об'єктом є суспільства-супротивники, а не бійці. Таким чином, різниця між учасниками бойових дій та цивільними громадянами, розмиваючись десятиліттями, майже повністю руйнується. І тактика полягає в одночасному застосуванні низки можливих інструментів, від загрози війни до пропаганди та всього, що є між ними".<br><br>5) явище, що виникає в результаті конвергенції та поєднання різних елементів, які разом утворюють більш складну та багатовимірну загрозу (на відміну від *Гібридного Конфлікту, Гібридної війни*)<br><br>6) Соціально небезпечні події, явища або процеси, породжені змінами у глобальному безпековому довкіллі в результаті синергії, утвореної від використання агресором і) звичайних збройних сил та можливостей та іі) нетрадиційних форм ведення війни (тероризм, злочинна діяльність, "громадянська війна", диверсія тощо), а також ііі) невійськові способи впливу, які | 3) "…posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."<br><br>4) "The goal is to achieve outcomes without actual war. The target is opposing societies, not combatants. Thus, the distinction between combatants and citizens, blurring for decades, breaks down almost entirely. And the tactic is the simultaneous employment of the range of possible instruments, from threats of war to propaganda and everything in between."<br><br>5) is a phenomenon resulting from the convergence and interconnection of different elements, which together form a more complex and multidimensional threat (by contrast of *Hybrid conflict, Hybrid war*).<br><br>6) The socially dangerous events, phenomenon or processes originated from the changes of global security environment as a result of the synergy from the use by aggressor of i) conventional armed forces and capabilities and ii) unconventional forms of warfare (terrorism, criminal activities, «civil war», subversion etc.) as well as iii) non-military modes of impact which has been transformed into a weapon on various fields of operation (diplomatic, informational, economic, financial, trade, social ones etc.). | Horbulin (2017) – p.157 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | трансформувались у зброю в різних сферах операцій (дипломатичних, інформаційних, економічних, фінансових, торгових, соціальних тощо).<br><br>мають на меті примусити об'єкт агресії до вимог, що суперечать його національним інтересам, незалежно від оголошення війни.<br><br>Одним із можливих способів здійснення гібридних загроз є організація та підтримка сепаратистських рухів, які можуть порушити суверенітет та територіальну цілісність об'єкта агресії. | aim at forcing the object of aggression to the requirements that are contrary to its national interests regardless of a declaration of war.<br><br>One of possible way for conducting Hybrid threats is the organization and support of separatist movements which could breach the sovereignty and territorial integrity of the object of aggression. | |
| 59. | **Гібридність на політичному рівні**<br><br>можливість для держави або могутнього недержавного утворення, що бажає кинути виклик міжнародному порядку силою. | **Hybridity at the political level**<br><br>an option for a state or a powerful non-state entity willing to challenge the international order by force. | Facon et al. (2018) – p.9 |
| 60. | **Горизонтальна ескалація**<br><br>одночасне застосування різних інструментів МПЕСІ-спектру (військових, політичних, економічних, цивільних, інформаційних тощо). | **Horizontal escalation**<br><br>the applied combination of multiple military, political, economic, civil, informational (*MPECI*) means. | MCDC(a) (2019) – p.89 |
| 61. | **Громадська безпека**<br><br>функція урядів держав, що забезпечує захист громадян країни, осіб на її території, організацій та інституцій від загроз їх добробуту та процвітанню громад. | **Public safety**<br><br>the function of governments which ensures the protection of citizens, persons in their territory, organizations, and institutions against threats to their well-being – and to the prosperity of their communities. | DRDC CSS (2013) – p.9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 62. | **Громадські демонстрації**<br><br>є одним із методів "*Символічних дій*".<br><br>Законні демонстрації - це символічні дії, що використовуються для просування певного політичного питання або позиції. Проте ворожі гравці можуть використовувати демонстрації для створення помилкового враження сильної підтримки або неприязні до проблеми (див. також *Астротурфінг*). | **Public Demonstrations**<br><br>is one of the "*Symbolic Actions*" methods.<br><br>Legitimate demonstrations are symbolic actions used to promote a certain political issue or position. Hostile actors can, however, exploit demonstrations to falsely give the impression of strong support or dislike of an issue (see also: *Astroturfing*). | MSB (2018) – p.19, 27 |
| 63. | **Громадянська війна**<br><br>збройний конфлікт, що відповідає таким умовам: а) військові дії всередині метрополії члена державної системи; б) активна участь національного уряду; в) ефективний опір обох сторін; г) загалом щонайменше 1000 смертей у боях протягом кожного року війни. Громадянські війни можуть бути ініційовані контролюючим центральним урядом або через місцеві уряди. У громадянських війнах одна сторона - національний уряд, а інша - недержавні організації. | **Civil war**<br><br>armed conflict meeting the following conditions: a) military action internal to the metropole of the state system member; b) the active participation of the national government; c) effective resistance by both sides; and d) a total of at least 1,000 battle deaths during each year of the war. Civil wars can be initiated for control of the central government or over local issues. Civil wars involve the national government as one side and a non-state entity as the other. | Hosaka (2021) - pp. 92-94. |
| 64. | **Громадянське суспільство**<br><br>форми соціальних організацій, які пропонують альтернативи тоталітаризму або надмірному державному контролю. Ключовим аспектом є існування проміжної "зони" між приватним життям та | **Civil society**<br><br>forms of social organization that offer alternatives to totalitarianism or excessive government control. The key aspect is the existence of an intermediate 'zone' between private life and the state, where | McQuail's, D. (2010) – p. 550 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | державою, де незалежні добровільні колективні об’єднання та організації можуть вільно діяти. Передумовою цього є свобода об'єднань та вираження поглядів, а також - необхідні засоби, серед яких особливо важливими є засоби масової інформації. | independent voluntary collective associations and organizations can operate freely. A precondition for this is freedom of association and expression, including the necessary means, amongst which the media are very important. | |
| 65. | **Громадянські інструменти гібридних загроз**<br><br>Громадянські інструменти стосуються використання повноважень, які містяться в таких сферах, як судова система, поліція, освіта, громадська інформація та цивільна адміністрація та допоміжна інфраструктура, що може забезпечити доступ до медичного обслуговування, їжі, електроенергії та води. Вони також містять адміністративний потенціал міжнародних, урядових і неурядових організацій. Громадянські інструменти контролюються та виконуються суверенними державами, міжнародними та неурядовими організаціями.<br>Один з 5-ти *МПЕСІ*-інструментів. Група інструментів у *Концептуальній моделі гібридних загроз* | **Civil instruments of hybrid threats**<br><br>The civil instrument refers to the use of powers contained within areas such as the judiciary, constabulary, education, public information and civilian administration and support infrastructure, which can lead to access to medical care, food, power and water.<br>It also includes the administrative capacities of international, governmental and non-governmental organizations. The civil instrument is controlled and exercised by sovereign nations, IOs and NGOs.<br>One of the 5 *MPECI*-instruments. A set of tools in the *Conceptual model of hybrid threats* | NATO (2013) – p.1-9 |
| 66. | **Груповий саботаж**<br><br>це не колективний саботаж усієї групи, а цілеспрямований саботаж окремих учасників у групі. | **Group sabotage**<br><br>not collective sabotage of the entire group, but targeted sabotage of individual contributors within the group. | Jaegher (2022) |

# Д

| № | UA | EN | Джерело |
|---|---|---|---|
| 67. | **Даркнет**<br><br>мережева сфера, яка не дотримується правил, що регулюють Інтернет, особливо сприяє обміну незаконно набутою інформацією. | **Darknet**<br><br>a network sphere that does not abide by the rules governing the internet, is particularly conducive to the exchange of illegally acquired information. | Vilmer et al. (2018) - p.48 |
| 68. | **Дезінформація**<br><br>навмисне розповсюдження інформації, яка є повністю або частково неправдивою (на відміну від *Помилкової Інформації*)<br><br>свідомо неправдива або оманлива інформація, створена, представлена та розповсюджена з метою отримання економічної вигоди або навмисного обману громадськості<br><br>неправдива, неточна або оманлива інформація, розроблена, представлена та популяризована з метою навмисного заподіяння шкоди суспільству або для отримання прибутку.<br><br>Один із методів інформаційного впливу (див. *Кампанії Впливу*).<br><br>Означає поширення неточної або маніпулятивної інформації з явним наміром обдурити та ввести в оману свою аудиторію. Цифрові платформи принципово змінили спосіб функціонування дезінформації. Некоректний контент може складатися з різних елементів, якими маніпулюють, як-от текст, зображення, відео та | **Disinformation**<br><br>the intentional dissemination of information that is wholly or partly false (as opposed to *Misinformation*)<br><br>verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public<br><br>false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.<br><br>one of the information influence techniques (see *Influence Campaigns*).<br><br>Refers to inaccurate or manipulated information spread with an explicit intention to deceive and mislead its audience. Digital platforms have fundamentally changed the way disinformation operates. Flawed content may consist of various manipulated elements such as text, image, video and audio. Disinformation can be used to support false narratives, sow confusion, and discredit legitimate information, individuals and organizations. | Vilmer et al. (2018) - p.19<br><br>European Commission (2020)<br><br>European Commission (2018)<br><br>MSB (2018) – p.19, 25 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | аудіо. Дезінформація може бути використана для підтримки неправдивих уявлень, внесення сум'яття та дискредитації законної інформації, осіб та організацій.<br><br>Сюди входять: *Фабрикація, Маніпулювання, Невірне Призначення, Сатира та Пародія тощо.* | it includes: *Fabrication, Manipulation, Misappropriation, Satire and Parody* etc. | |
| 69. | **Делегування конфлікту**<br><br>Стратегія, згідно з якою іноземний уряд передає матеріальні ресурси або військову експертизу недержавній збройній групі для націлювання на конкретного супротивника.<br><br>Ключовими елементами делегування конфліктів є взаємодія між державним спонсором (або спонсорами) та актором, а саме передача можливостей від замовника до виконавця (агента); і внаслідок цього контроль першого над другим, тобто здійснення впливу на цілі, стратегії та тактику актора. Механізми делегування різноманітні. Можна стверджувати, що можливості та вплив можуть також бути розвернутими в іншому напрямку, від НДА [недержавного актора] до його державного патрона. Також можливо, що державні та недержавні актори просто є союзниками або паралельно працюють над подібними цілями без будь-яких ієрархічних відносин. | **Conflict delegation**<br><br>A strategy in which a foreign government commits material resources or military expertise to a non-state armed group to target a perceived adversary.<br><br>The key elements in conflict delegation are the interaction between the state sponsor (or sponsors) and the actor, namely the transfer of capabilities from the principal to the agent; and the resulting control by the former over the latter, that is, exerting influence over the actor's aims, strategies and tactics. The mechanisms of delegation vary. Arguably, the capabilities and influence may also flow in the other direction, from the NSA [non-state actor] towards its state patron. It is also possible for state and non-state actors to simply be allies, or to work in parallel towards similar goals without any hierarchical relationship. | Karlén et al. (2021)<br><br>Jokinen et al. (2022) |

| № | UA | EN | Джерело |
|---|---|---|---|
| 70. | **"День Перемоги"**<br>один із кремлівських наративів, російська інтерпретація історії<br>День Перемоги відзначається в росії щороку 9 травня.<br>Для росіян це джерело гордості та патріотизму, і його відзначають як звільнення територій від фашизму, для титульних народів Балтії це "обмін" одного репресивного режиму на інший.<br>Окрім демонстрації сили та створення міфів про непереможність чи неминучість, День Перемоги покликаний пробудити колективні спогади в "*Близькому Зарубіжжі*" про спільні жертви та спільну перемогу під час "Великої Вітчизняної війни" (1941 - 1945), щоб зберегти ностальгію старшого покоління за минулим. | **"Victory Day"**<br>one of the Kremlin narratives, the Russian interpretation of history<br>Victory Day is celebrated in Russia annually on May 9<br>To Russians it is a source of pride and patriotism and celebrated as having liberated territories from fascism, to the titular peoples of the Baltic States it marks the 'trading' of one repressive regime for another.<br>Beyond projecting power and creating myths of invincibility or inevitability, Victory Day is meant to awaken collective memories in the *Near Abroad* about the common sacrifices and common victory during "Great Patriotic War" (1941 - 1945), to maintain the nostalgia of the older generation for past times. | Rotaru (2018) – p.9<br>Simons (2015) – p.6 |
| 71. | **Державна інформаційна політика**<br>Сукупність основних напрямів і способів діяльності держави щодо одержання, використання, поширення та зберігання інформації. | **Government information policy**<br>There is the total of core areas and activities of a state to collect, use, disseminate and store information. | Horbulin (2017) – p.157 |
| 72. | **Державне управління**<br>Процес перетворення державної політики на результати. *Дихотомія* "політика-адміністрація" підкреслюється як фундаментальна риса європейських суспільств. Тобто, державне управління існує для виконання закону та правил. | **Public administration**<br>the process of translating public policies into results. The politics-administration dichotomy is emphasized as a fundamental feature of European societies. In other words, public administration exists to implement the law and rules. | Cullen et al. (2021) – p.30 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | One of the 13 domains in the *Conceptual model of hybrid threats* | |
| 73. | **Державні актори гібридних загроз**<br><br>Державні організації, установи та їх представники в країнах з більш-менш авторитарними або тоталітарними поглядами на владу. Їх мета полягає в тому, щоб націлитися на системну вразливість демократій, використовуючи всі інструменти, які є в розпорядженні авторитарної держави.<br><br>Використання гібридних загроз як механізму підтримки для просування стратегічних інтересів є характерним для:<br><br>• ревізіоністських країн - Китаю та Росії,<br><br>• країн-ізгоїв: Ірану та Північній Кореї.<br><br>Є одним з елементів *Концептуальній моделі гібридних загроз*, відносятся до групи *Актори / гравці гібридних загроз* | **State actors of hybrid threats**<br><br>State organizations, institutions and their representatives in other countries with more or less authoritarian or totalitarian views of power. The aim is to target the systemic vulnerabilities of democracies while using all the tools that an authoritarian state has at its disposal.<br><br>The use of hybrid threat activity as a support mechanism to advance strategic interests is characteristic of:<br><br>• the revisionist states - China and Russia,<br>• the rogue states - Iran and North Korea.<br><br>One of the elements of the *Conceptual model of hybrid threats*. It refers to a group of *Actors of hybrid threats* | Cullen et al. (2021) – p.15 |
| 74. | **Десек'юритизація в політичній сфері**<br><br>перенесення питань із надзвичайного режиму до нормального переговорного процесу в політичній сфері. | **Desecuritization**<br><br>the shifting of issues out of emergency mode and into the normal bargaining processes of the political sphere | Buzan et al. (1998) - p.4 |
| 75. | **Дефіцитна інформація**<br><br>достовірна інформація, що поширюється з метою заподіяння шкоди, часто шляхом переміщення | **Mal-information**<br><br>genuine information is shared to cause harm, often by moving | Wardle & Derakhshan (2017) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | інформації, призначеної для того, щоб залишатися приватною, у публічну сферу. | information designed to stay private into the public sphere. | |
| 76. | **Джамінг / Глушіння**<br><br>Це методи *РЕБ*, які перешкоджають користувачам отримувати призначені сигнали, і можуть бути реалізовані двома основними методами: глушіння висхідної лінії зв'язку та глушіння низхідної лінії зв'язку.<br>Глушіння висхідній лінії зв'язку спрямовані на супутник і погіршують послуги для всіх користувачів у зоні прийому супутника.<br>Глушіння низхідній лінії зв'язку мають локалізований ефект, оскільки вони спрямовані на наземних користувачів, наприклад підрозділ сухопутних військ, який використовує супутникову навігацію для визначення свого місцезнаходження. | **Jamming**<br><br>It`s *EW*-techniques which prevent users from receiving intended signals and can be accomplished by two primary methods: uplink jamming and down-link jamming. Uplink jamming is directed toward the satellite and impairs services for all users in the satellite reception area.<br>Downlink jamming has a localized effect because it is directed at ground users, such as a ground forces unit using satellite navigation to determine their location. | DIA (2022) – p. 44 |
| 77. | **Дипломатичне прикриття**<br><br>Одна з форм та дій неоголошеної гібридної війни, мета яких - використання дипломатії для приховування та нівелювання участі агресора в діях проти суверенної держави | **Diplomatic cover**<br><br>One of the forms and actions of non-declared hybrid warfare aims at the use of diplomacy to conceal and minimize the aggressor's role in the activities undermining state's sovereignty. | Horbulin (2017) – p.157 |
| 78. | **Директива про тимчасовий захист**<br><br>набір мінімальних стандартів для надання тимчасового захисту у випадку масового напливу переміщених осіб та заходів щодо сприяння збалансованості зусиль між державами-членами щодо | **The temporary protection directive**<br><br>a set of the minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures to promote a balance of efforts between Member States in receiving such | Jauhiainen et al. (2022) – p.5 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | прийому таких осіб та відповідальності за їхній захист. Ця директива гарантує українцям, які тікають від війни, що триває в Україні, право на тимчасовий захист і доступ до житла, працевлаштування, медичну допомогу, освіту для дітей та соціальне забезпечення в державах-членах Європейського Союзу (ЄС). | persons and bearing the responsibility for their protection. It directive guarantees the right to temporary protection and access to accommodation, employment, health (medical) care, education for children and social welfare in European Union (EU) member states for Ukrainians fleeing the on-going war in Ukraine. | |
| 79. | **Діагностика DIDI**<br><br>діагностичний тест на інформаційну активність (обман, намір, зрив, втручання).<br><br>Така діагностика дає можливість як своїм користувачам, так і громадській думці відрізнити маніпуляції інформацією від більш відвертих операцій впливу.<br><br>Щоб кваліфікуватися як дезінформація, інформаційна діяльність має 1) містити оманливі елементи; 2) мати намір заподіяти шкоду; 3) бути руйнівною; та 4) призводити до втручання | **DIDI diagnostic**<br><br>a diagnostic test on informational activities (Deception, Intention, Disruption, Interference).<br><br>Such a diagnostic offer the possibility for both its users as well as public opinion to differentiate information manipulation from more sincere operations of influence.<br><br>To qualify as disinformation, an informational activity must 1) contain deceptive elements; 2) have the intention to harm; 3) be disruptive; and 4) lead to interference | Vilmer et al. (2018) - p.121<br><br>MSB (2018) - – p.9, 10,16 |
| 80. | **Діпфейк**<br><br>такі фейкові новини, які дуже переконливо створюють ефект реальності.<br><br>Є одним із інструментів *Технічного Використання*.<br><br>Техніка синтезу зображень на основі штучного інтелекту, яка передбачає створення підробленого, але надзвичайно реалістичного відеовмісту, що | **Deep Fake**<br><br>such fake news that can very convincingly reproduce the effects of reality.<br><br>Is one of the *Technical exploitation* tools.<br><br>An artificial intelligence-based image synthesis technique that involves creating fake but highly realistic video content misrepresenting the | Vilmer et al. (2018) - p.149<br><br>MSB (2018) – p.19, 23<br><br>Neudert & Marchal (2019) – p.5 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | спотворює слова чи дії політиків та знаменитостей.<br><br>Використовує алгоритми навчання для імітації рухів голосу та рота для маніпулювання аудіо та відео матеріалом.<br><br>Наприклад, це може бути використано для створення підроблених кліпів реального політика, який виголошує фальшиву промову. Більш просунуті методи можуть накласти, наприклад, обличчя на вже наявні відеозаписи. | words or actions of politicians and celebrities.<br><br>The use of learning algorithms to imitate voice and mouth movements for manipulating audio and video. This can for example be used to produce fake clips of a real politician delivering a faked speech. More advanced techniques can superimpose e.g. faces onto pre-existing video footage. | |
| 81. | **Доброчесність**<br><br>один із інструментів "гібридної оборони"<br><br>це "поведінка та дії, що відповідають набору моральних чи етичних принципів та стандартів, прийнятих як окремими особами, так і установами, що створюють бар'єр для корупції". | **Integrity**<br><br>one of the 'hybrid defence' instrument<br><br>is 'behaviours and actions consistent with a set of moral or ethical principles and standards, embraced by individuals as well as institutions that create a barrier to corruption'. | MCDC(b) (2019) – p.3<br><br>Transparency International (b) |
| 82. | **Доктрина Герасимова** (російська "*Війна Нового Покоління*")<br><br>російська військова доктрина, її автором є генерал В. Герасимов, начальник генерального штабу зс рф<br><br>"У двадцять першому столітті ми спостерігаємо тенденцію до стирання меж між станом війни та миру. [...] Роль невійськових засобів для досягнення політичних і стратегічних цілей зросла, здебільшого, вони перевищили силу зброї в її ефективності. Фокус застосовуваних методів конфлікту | **Gerasimov doctrine** (The Russian "*New Generation Warfare*")<br><br>the Russian military doctrine, its autor is Gen. Valery Gerasimov, the chief of the General Staff of the Russian Federation Armed Forces.<br><br>"In the twenty-first century we have seen a tendency toward blurring the lines between the states of war and peace. […] The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. The focus of applied | Vilmer et al. (2018) - p.55<br><br>Gerasimov (2016) – p.24 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | змінився у напрямку широкого використання політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів - застосовуваних у координації з протестним потенціалом населення. Усе це доповнюється військовими засобами прихованого характеру, зокрема проведенням акцій інформаційного конфлікту та діями сил спеціальних операцій" | methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces" | |
| 83. | **Доктрина "обмеженого суверенітету"** (доктрина Брежнєва)<br><br>цей термін належить радянській політиці, сформульованій в 1968 році для виправдання колективного військового втручання членів Варшавського договору в Чехословаччину. Доктрина Брежнєва проголошувала, що будь-яка загроза соціалістичному правлінню в будь-якій державі радянського блоку у Східній Європі є загрозою для соціалістичної спільноти в цілому.<br><br>Доктрина була розроблена для виправдання військових інтервенцій у соціалістичні держави як засіб самозахисту від ворожих ідеологій капіталізму та ліберальної демократії. | **Doctrine of "limited sovereignty"** (The Brezhnev doctrine)<br><br>this term refers to the Soviet policy formulated in 1968 in order to justify the collective military intervention of the Warsaw Pact members in Czechoslovakia. The Brezhnev doctrine proclaimed that any threat to socialist rule in any state of the Soviet bloc in Eastern Europe was a threat to the socialist community as a whole<br><br>The doctrine had been devised to justify military interventions in fellow socialist states as a means of self-defence against the hostile ideologies of capitalism and liberal democracy. | Domańska (2019) – p.7 |
| 84. | **Домени гібридних загроз**<br><br>Сфери життя суспільства, які стають мішенню акторів / гравців | **Domains of Hybrid Threats**<br><br>Spheres of societal life targeted by actors of hybrid threats. These | Cullen et al. (2021) – p.13 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | гібридних загроз. Такі домени характеризуються наявністю суспільних інтересів та критичних функцій, національною безпекою та здатністю держави приймати рішення. Саме в цих доменах має бути забезпечена стійкість проти гібридних загроз.<br><br>Домени є одним з чотирьох ключових елементів Концептуальної моделі гібридних загроз, яка містить 13 доменів. Інша модель – ПМЕСІІ, містить спектр з 6 доменів гібридних загроз. | domains are characterized by the presence of societal interests and critical functions, national security, and the state's decision-making capacity. Resilience against hybrid threats must be ensured in these domains.<br><br>Domains are one of the four key elements of the Conceptual Model of Hybrid Threats, which comprises 13 domains. Another model, PMESII, includes a spectrum of 6 domains of hybrid threats. | |
| 85. | **Допорогові виклики** (або ***виклики сірої зони***)<br><br>Загрози, виявлення та реагування на які ускладнюється допороговими значеннями їх параметрів.<br><br>Вони є "спробами досягнення цілей своєї безпеки, не вдаючись до прямого та значного застосування сили". | **Sub-Threshold Challenges** (or **gray zone challenges**)<br><br>Threats, detection and response to which are complicated by subthreshold values of their parameters.<br><br>They are “attempts to achieve one’s security objectives without resort to direct and sizable use of force.” | CSIS (2018)<br><br>Takahashi (2018) – p.787 - 810 |
| 86. | **Дослідження (міжнародної) безпеки**<br><br>вивчення загрози застосування та контролю військової сили, яке передбачає, що конфлікти між державами завжди можливі й те що використання військової сили має далекосяжні наслідки для держав і суспільств. Вивчення умов, які роблять застосування сили більш імовірним, способи, якими застосування сили впливає на окремих людей, держави і | **Security studies**<br><br>assumes that conflict between states is always a possibility and that the use of military force has far-reaching effects on states and societies. Accordingly, security studies may be defined as the study of the threat, use, and control of military force. It explores the conditions that ‘make the use of force more likely, the ways that the use of force affects individuals, states, and societies, and the specific policies that states adopt | Walt (1991) – p.212 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | суспільства, а також конкретна політика, яку держави приймають для підготовки, запобігання або участі у війні. | in order to prepare for, prevent, or engage in war | |

## E

| № | UA | EN | Джерело |
|---|---|---|---|
| 87. | **Економічний важель**<br><br>Це форма економічного впливу у вигляді допомоги з боку іноземних держав, санкцій та використання позичених ресурсів як розмінних монет для тиску на іноземний уряд. Ця форма важелів впливу навряд чи є новою, але вона залишається одним із найважливіших та найефективніших інструментів впливу на прийняття рішень в іншій країні. Економічний вплив не обмежується лише торгівлею, а також включає інші галузі, як-от енергетика та туризм. | **Economic Leverage**<br><br>This is a type of economic influence in the form of foreign aid assistance, sanctions, and the use of loaned resources as bargaining chips to put pressure on a foreign government. This form of leverage is hardly new by any means, but it remains one of the most important and effective tools to influence decision-making in another country. Economic influence is also not solely limited to trade, but also includes other industries such as energy and tourism. | Treverton et al. (2018) - p. 64 |
| 88. | **Економічний домен гібридних загроз**<br><br>Складається із поєднання виробництва, розподілу та споживання всіх товарів і послуг у країні чи організації. Він містить не лише економічний розвиток країни, а й розподіл багатства Один з 6-ти *ПМЕСІІ*-доменів. Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | **Economic domain of hybrid threats**<br><br>Composed of the sum total of production, distribution and consumption of all goods and services for a country or organisation. It includes not only economic development of a country, but also the distribution of wealth. One of the 6 *PMESII*-domains. One of the 13 domains in the *Conceptual model of hybrid threats* | NATO (2013) – p.1-8 |
| 89. | **Економічні інструменти гібридних загроз**<br><br>Економічні інструменти загалом стосуються ініціатив, стимулів і санкцій, призначених для впливу на потік товарів і послуг, а також фінансової підтримки державних і недержавних суб'єктів, залучених у кризу. | **Economic instruments of hybrid threats**<br><br>The economic instrument generally refers to initiatives, incentives and sanctions designed to affect the flow of goods and services, as well as financial support to state and non-state actors involved in a crisis. One of the 5 *MPECI*-instruments. A | NATO (2013) – p.1-9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Один з 5-ти *МПЕСІ*-інструментів. Група інструментів у *Концептуальній моделі гібридних загроз* | set of tools in the *Conceptual model of hybrid threats* | |
| 90. | **Електронний уряд**<br>електронне управління або застосування інформаційних та комунікаційних технологій для надання державних послуг. | **E-governance**<br>electronic governance, or the application of information and communication technologies for delivering government services. | Neudert & Marchal (2019) – p.5 |
| 91. | **Енергетична безпека**<br>спроможність країни технічно надійним та безпечним, економічно ефективним, здійсненним та екологічно прийнятним способом задовольняти потреби суспільства в паливно-енергетичних ресурсах для гарантування: належного рівня життєдіяльності населення; сталого функціонування національної економіки в режимах звичайного та особливого стану; можливості керівництва держави у формуванні і здійсненні політики захисту національних інтересів. | **Energy security**<br>The capability of the country to meet its energy demand in technically reliable and safe, cost effective, feasible and environmentally friendly way to ensure: adequate levels of the population livelihood; sustainable functioning of the national economy in normal and crisis conditions; capabilities of the government to establish and execute the policy protecting national interests. | Horbulin (2017) – p.157 |
| 92. | **Ефект приєднання до більшості**<br>явище, яке використовується для *Когнітивного Злому*.<br>Люди, які відчувають себе частиною більшості, частіше висловлюють свої думки. Наприклад, боти можуть бути використані для збільшення початкової кількості лайків, коментарів та репостів в соціальних мережах, щоб полегшити подальше залучення "реальних" користувачів. Це | **Bandwagon Effect**<br>a phenomenon that is used in *Cognitive Hacking*.<br>People who feel like part of the majority are more likely to air their opinions. For example, bots can be used to boost the initial number of likes, comments and shares of a social media entry to facilitate further engagement from “real” users. This gives the impression of | MSB (2018) – p.19-20, 45 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | створює враження соціального визнання, яке апелює до необхідності соціальної відповідності.<br>(на відміну від ефекту *Спіралі Мовчання*). | social acceptance, which appeals to the need for social conformity.<br>(by contrast of *Spiral of Silence* effect) | |
| 93. | **Ефекти (у контексті гібридної війни)**<br>зміна стану об'єкту (цільової системи) в результаті дій проти конкретних вразливостей цієї цільової системи | **Effects (In hybrid warfare)**<br>a change of state of an entity (a target system) as the result of actions against specific vulnerabilities of that target system. | MCDC(a) (2019) – p.89 |

## Є

| № | UA | EN | Джерело |
|---|---|---|---|
| 94. | **Євразія**<br><br>(суміш Європи та Аравії) концепція, яку використовують для опису ультраправої ісламофобської *Теорії Змови*, в якій беруть участь глобалістичні організації, імовірно очолювані французько- та арабськомовними державами, для ісламізації та аравізації Європи, тим самим послаблюючи її існуючу культуру та підриваючи попереднє рівняння на США та Ізраїль.<br><br>Є прикладом анти-наративів, які атакують "наші інституції";<br><br>інструмент гібридного впливу. | **Eurabia**<br><br>(a portmanteau of Europe and Arabia) the concept, used to describe a far-right Islamophobic conspiracy theory, involving globalist entities allegedly led by French and Arab powers, to Islamise and Arabise Europe, thereby weakening its existing culture and undermining a previous alignment with the U.S. and Israel.<br><br>the example of the anti narratives that attack "our institutions";<br><br>a hybrid influence tool. | Vilmer et al. (2018) - p.78<br><br>Brown (2019) |
| 95. | **Євромайдан**<br><br>рух України 2014-го року, який прагнув наблизити країну до Заходу. | **Euro-maidan**<br><br>the 2014 Ukraine's movement, which sought to bring the country closer to the West. | Grigas (2016) – p.28, 109 |
| 96. | **Європейський центр з протидії гібридним загрозам (Hybrid CoE)**<br><br>міжнародний центр для практиків та експертів, що розвиває можливості держав-учасниць та інституцій і посилює співпрацю між ЄС та НАТО у протидії гібридним загрозам; розташований у Гельсінкі, Фінляндія | **European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)**<br><br>an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland | Hybrid CoE(b) (n.d.) |
| 97. | **Євроскептицизм**<br><br>напрям політичної думки в країнах Європи, що ставить під сумнів доцільність процесу політичної, правової та економічної інтеграції | **Euroscepticism**<br><br>the way of political thinking in European countries, which questions the advantages of political, legal and economic integration within the EU | Horbulin (2017) – p.157 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | європейських держав у межах ЄС і власне самого існування Європейського Союзу як наднаціонального інституціоналізованого утворення. | member-countries to the extent of principle opposition to the existence of the European Union as a supranational institutionalized unity. | |

## З

| № | UA | EN | Джерело |
|---|---|---|---|
| 98. | **Загальна безпека**<br><br>спосіб розширити межі світу, в якому домінує гонка озброєнь, до альтернативного світу, в якому держави та народи визнають пріоритетними спільні інтереси у виживанні та мирному розвитку. | **Common Security**<br><br>a way of moving beyond a world dominated by the arms race and towards an alternative world which would be marked by states, and peoples, recognizing their common interests in survival and peaceful development. | Butfoy (1997) |
| 99. | **"Заїжджена платівка"**<br><br>один з методів введення ідеологічного змісту.<br><br>Означає послідовне повторення власних думок та оцінок, не дозволяючи при цьому іншим учасникам дискусії вивести нас із рівноваги, але все одно звертаючись до них, наприклад, "американці хочуть пограбувати Україну", неодноразово повторюване на різних рівнях дискусій.<br><br>див. також *"Побудова платформ"* | **'Broken Record'**<br><br>is one of the methods of introducing ideological content.<br><br>means the consistent reiterating of one's opinions and evaluations, while not allowing other discussion participants to throw us off balance, but still referring to them, e.g. "the Americans want to rob Ukraine" repeated many times in different levels of discussions.<br><br>see also *'Building Platforms'* | Szwed (2016) – p. 81 |
| 100. | **Заманювання**<br><br>це вид шахрайства, зміст якого полягає в тому, щоб спонукати жертву до виконання певного завдання, надаючи їй вільний доступ до чогось, що вона бажає отримати. Наприклад: флешка, заражена кейлоггером з написом «Мої приватні фото», залишена на порозі будинку жертви. Політики безпеки, такі як «повітряний проміжок» і блокування несанкціонованого програмного та | **Baiting**<br><br>involves luring the victim into performing a specific task by providing easy access to something the victim wants. Example: a USB flash drive infected with a keylogger and labelled "My private pics" left on the victim's doorstep. Security policies such as an air gap and the blocking of non-authorised software and hardware will thwart most attempts, though staff should also be | ENISA (n.d.) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | апаратного забезпечення, допоможуть запобігти більшості спроб, хоча співробітникам також слід нагадати про те, що не варто довіряти невідомим джерелам. | reminded not to trust unknown sources. | |
| 101. | **Заморожений конфлікт**<br><br>конфліктні ситуації, коли немає активних широкомасштабних бойових дій (хоча може бути менш масштабне насильство), існує довготривале взаємне погодження щодо припинення вогню, але спроби досягти політичного врегулювання чи миру є безуспішними. | **Frozen conflict**<br><br>situations of conflict where there are no active large-scale hostilities (although there may be smaller-scale violence), there is a durable mutually agreed ceasefire, but efforts to achieve a political settlement or peace are unsuccessful. | MacFarlane, (2009) – p.23 |
| 102. | **Затяжний конфлікт**<br><br>глибоко вкорінений або нерозв'язний конфлікт. Затяжний конфлікт має такі особливості:<br><br>• має багато різних джерел конфлікту, розташованих на кількох рівнях, таких як індивідуальний, груповий, громадський, і їхня взаємодія живить або підтримує ворожнечу.<br><br>• часто відбувається у місцях, де існують інші проблеми суспільства (безробіття, житлова проблема, продовольча проблема тощо), і спричиняє «конфліктні пастки», що призводить до довготривалих моделей страждань і травм.<br><br>• джерела ворожнечі в цих ситуаціях (проблеми, лідери, політика тощо) часто змінюються і в будь-який момент часу можуть | **Protracted conflict**<br><br>deep rooted or intractable conflict. Protracted conflict has such features:<br><br>• It has many different sources of conflict located at multiple levels such as individual, group, communal and their interaction with each other often feed or sustain hostilities.<br><br>• It os often situated in places where other community problems (unemployment, housing, nutrition problems etc.) exist and cause ‘conflict traps’ by resulting in long-term patterns of misery and trauma.<br><br>• The sources of hostilities in these settings (issues, leaders, policies etc.) often change constantly and at any given time might be more or less determining of the conflict.<br><br>• Each case is different and has its own set of factors. Generalisations | Cantekin (2016) – p. 417 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | стати визначальними причинами конфлікту.<br>• кожен випадок відрізняється і має свій набір факторів. Узагальнення від одного випадку до іншого часто є проблематичним.<br>• має тенденцію бути стійким до традиційних або звичних методів миротворчості та часто продовжує існувати. | from one case to another are frequently problematic.<br>• It tends to be resistant to traditional or familiar methods of peace-making and it often continues to exist. | |
| 103. | **Захист критичної інфраструктури**<br>комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури | **Critical infrastructure protection.**<br>the set of measures implemented in regulatory, institutional and technology tools directed toward assurance of critical infrastructure safety, security and resilience | Horbulin (2017) – p.156 |
| 104. | **Зворотня психологія**<br>Один з методів *маніпуляції.*<br>Спонукання опонента зробити щось, що він сприйме як шкідливе для маніпулятора, в той час як фактично він приймає рішення, заздалегідь підготовлене маніпулятором.<br>Використовується для *рефлексивного контролю* | **Reverse psychology**<br>This is one of the methods of *manipulation.*<br>Prompting the opponent to do something that he will perceive as being harmful to the manipulator, while actually taking a decision that has been prepared before-hand by the manipulator.<br>It is used for *reflexive control* | Cullen et al. (2021) – p.19 |
| 105. | **«Зелені чоловічки» / "увічливі люди"**<br>професіональні солдати в уніформі без розпізнавальних знаків. | **"Little Green Men" / “polite people”**<br>professional soldiers in uniforms without markings | Freedman (2014)<br>Treverton et al. (2018) - p. 17 |
| 106. | **Злісна проблема** | **Wicked problem** | Ritchey (2013) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | (1) Проблеми, які є погано визначеними, неоднозначними та пов’язаними з серйозними моральними, політичними та професійними питаннями. Оскільки вони сильно залежать від зацікавлених сторін, часто немає консенсусу щодо того, в чому полягає проблема, не кажучи вже про те, як з нею впоратися. Перш за все, злісні проблеми не є статичними: це суміш складних, взаємопов'язаних питань, що розвиваються в динамічному соціальному контексті. Часто нові форми злісних проблем виникають у результаті спроби зрозуміти і розв'язати іншу.<br><br>(2) Новий вид дилем в попереджувальній розвідці. | (1) Wicked problems are ill-defined, ambiguous and associated with strong moral, political and professional issues. Since they are strongly stakeholder dependent, there is often little consensus about what the problem is, let alone how to deal with it. Above all, wicked problems won’t keep still: they are sets of complex, interacting issues evolving in a dynamic social context. Often, new forms of wicked problems emerge as a result of trying to understand and treat one of them.<br><br>(2) A new set of dilemmas in warning intelligence. | Cullen (2018) – p.2 |

I

| № | UA | EN | Джерело |
|---|---|---|---|
| 107. | **Ідеальний шторм**<br><br>Незвичайна комбінація подій або речей, які призводять до надзвичайно поганих або потужних результатів. | **Perfect storm**<br><br>A perfect storm is an unusual combination of events or things that produce an aunusually bad or powerful results. | Collins English Dictionary (n.d.)<br><br>Calus (2023) – p.6 |
| 108. | **Імітатори та самозванці**<br><br>метод, який використовується в інформаційних впливах типу *Оманливих Ідентичностей*.<br><br>Імітатори видають себе за когось іншого, тобто приймають чужу особисту чи професійну особистість. Самозванці не видають себе за когось іншого, а роблять вигляд, що володіють досвідом чи повноваженнями, яких у них немає, наприклад той, хто помилково заявляє, що є лікарем. | **Impersonators & Imposters**<br><br>a method used in *Deceptive Identities* type informational influences.<br><br>Impersonators pretend that they are someone else, i.e. adopt someone else's personal or professional identity. Impostors do not pretend that they are someone else but pretend to possess expertise or credentials that they do not have, e.g. someone who falsely claims to be a medical doctor. | MSB (2018) – p.19-20 |
| 109. | **Імпортозаміщення в оборонно-промисловому комплексі**<br><br>заміщення імпорту комплектуючих для створення вітчизняної воєнної продукції, шляхом налагодження їх вітчизняного виробництва або імпорту з інших країн. | **Import substitution in defense industry**<br><br>the phasing out the import of parts for manufacturing domestic military products by setting up home production or import from other countries. | Horbulin (2017) – p.157 |
| 110. | **Індивідуальне таргетування**<br><br>стратегія кібервійськ, що передбачає вибір особи чи групи для впливу на соціальні мережі (як у формі співпраці, так і у формі домагань) | **Individual targeting**<br><br>a cyber troop strategy that involves selecting an individual or group to influence on social media (both in the form of collaboration and in the form of harassment) | Bradshaw & Howard (2017) – p.9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 111. | **Індикатори**<br><br>вимірювані змінні величини, необхідні для чіткої та достатньої ідентифікації, опису, представлення та моніторингу явища гібридних загроз відповідно до визначеного базового рівня. | **Indicators**<br><br>measurable variables necessary to clearly and sufficiently identify/ describe/represent/monitor a hybrid threats phenomenon in relation to a specific baseline. | MCDC (2017) – p.31 |
| 112. | **Інституційний механізм**<br><br>Це система процесів, технічних засобів, людей та навичок, необхідних національним урядам та транснаціональним установам для реалізації стратегій протидії гібридній війні. | **Institutional machinery**<br><br>it is a system of the processes, mechanisms, people and skills required in national governments and multinational institutions to implement strategies to counter hybrid warfare. | MCDC(a) (2019) – p.90 |
| 113. | **Інструменталізована міграція**<br><br>ситуація, коли третя країна провокує нелегальні міграційні потоки, активно заохочуючи або сприяючи переміщенню громадян третіх країн до зовнішніх кордонів. Він характеризується трьома основними ознаками: (1) передбачає нерегулярне переміщення осіб на територію однієї держави у (2) спосіб, який навмисно підбурюється або використовується іншою, держава як (3) засіб примусу до досягнення політичних, стратегічних або інших переваг. | **Instrumentalised migration**<br><br>a situation where a third country instigates irregular migratory flows into the Union by actively encouraging or facilitating the movement of third country nationals to the external borders. It is characterized by three essential features: it involves the irregular movement of persons into the territory of one State in a manner that is deliberately instigated or exploited by another State as a means to coerce the former in pursuit of political, strategic or other benefits. | Sari A. (2023) |
| 114. | **Інструменти** сили<br><br>це інструменти гібридних загроз, які є одним з чотирьох ключових елементів *Концептуальної моделі гібридних загроз*. Спектр таких інструментів визначається *МПЕСІ-* | **Instruments of power**<br><br>These are the tools of hybrid threats, which are one of the 4 key elements of the *Conceptual Model of Hybrid Threats*. The spectrum of such tools is determined by the | MCDC(a) (2019) – p.90 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | середовищем. Коли ці складові "озброєні", інструменти сили можуть стати знаряддям атаки. | *MPECI* environment. When these components are "weaponized" the instruments of power can become tools of attack. | |
| 115. | **Інтелектуальна лінь**<br>неспроможність систематично проявляти критичне мислення та наївний вибір розповсюдження інформації без пошуку доказів, що підтверджують цю інформацію. | **Intellectual Laziness**<br>the failure to systematically exercise critical thinking and choosing to relay information naively without looking for evidence to support that information. | Vilmer et al. (2018) - p.31 |
| 116. | **Інтернет речей (IoT):**<br>Мережа фізичних пристроїв, транспортних засобів, побутової техніки та інших елементів, вбудованих в електроніку, програмне забезпечення, датчики, виконавчі механізми та засоби зв'язку, що дозволяє цим речам підключатися, збирати та обмінюватися даними.<br>Приклади "гібридних" застосувань: злом майбутніх автономних автомобілів та систем дорожнього руху в такий спосіб, щоб узяти під контроль ці автомобілі та системи. Після того, як управління перейде під контроль, хакер може розбити автомобілі або спровокувати зіткнення, щоб створити хаос та жертви. | **The Internet of Things (IoT):**<br>The network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, which enables these things to connect, collect and exchange data.<br>Examples of hybrid applications: E.g. hacking future autonomous cars and traffic systems in such a way that the control of these cars and systems can be taken over. Once control is taken over the hacker can cause the cars to crash or to cause collisions in order to create chaos and casualties. | Bekkers et al. (2019) – p.26 |
| 117. | **Інтернет-кокон**<br>ефект ізоляції користувачів Інтернету в закритих когнітивних просторах, де вони знаходяться під впливом лише того змісту, який підтверджує їхні переконання. | **Internet-cocooning**<br>the effect of internet users insulation “in closed cognitive spaces where they were only exposed to content that supported their beliefs. The engine would become a tool of | Vilmer et al. (2018) - p.31 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Пошуковик стає інструментом підтвердження, а не інформування.<br><br>це комфортні когнітивні простори, що підтверджують забобони, а не протистоять забобонам інших.<br><br>див. також: *Мікро-таргетування*, *Бульбашки Фільтрів* | confirmation rather than information.<br><br>comfortable cognitive spaces that confirm prejudices rather than confront them with the prejudices of others<br><br>see also: *Micro-Targeting, Filter Bubbles* | |
| 118. | **Інформаційна безпека**<br><br>стан захищенності життєво важливих інтересів людей, суспільства та держави, за якого досягається запобігання шкоді через: неповноту, невчасність та недостовірність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації. | **Information security**<br><br>the condition of securing vital interests of people, society and state, which prevents damage arising out of incompleteness, unseemliness and unreliability of information in use; adverse information influence; adverse effects of using information technologies; unauthorised distribution, use and breach of integrity, confidentiality and accessibility of information. | Horbulin (2017) – p.157 |
| 119. | **Інформаційна війна**<br><br>є частиною військових операцій, метою яких є досягнення військових цілей за допомогою різних нетрадиційних засобів, включаючи нові засоби комунікації та розповсюдження інформації.<br><br>протиборство в інформаційному просторі, яке ініціюється агресором з метою здійснення комплексного впливу на соціальне, економічне, військове та політичне життя супротивника задля досягнення своїх стратегічних цілей щодо атакованої держави. | **Information war**<br><br>is a part of warfare operations whose aim is to achieve military objectives by using different unconventional means, including new instruments of communication and information dissemination.<br><br>the combat in information environment, initiated by the aggressor to comprehensively affect social, economic, military and political life of the opponent to | Szwed (2016) – p. 19<br><br>Horbulin (2017) – p.158 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | | achieve its strategic goals regarding the attacked country. | |
| 120. | **Інформаційна маніпуляція**<br>1) навмисне та масове розповсюдження неправдивих або упереджених новин у ворожих політичних цілях<br>2) неточне або оманливе твердження про факт, яке може змінити чесність майбутнього голосування і яке поширюється навмисно, штучно або автоматично та масово серед громадськості в Інтернеті через служби зв'язку. | **Information Manipulation**<br>1) the intentional and massive dissemination of false or biased news for hostile political purposes<br>2) inexact or misleading allegation of a fact that could alter the sincerity of an upcoming vote and that is spread deliberately, artificially or automatically and massively to the online public through a communication service. | Vilmer et al. (2018) - p.11<br>Guillaume (2019) – p.4 |
| 121. | **Інформаційна присутність**<br>реалізація національних інтересів в інформаційній сфері через поширення офіційної інформації, інтерпретацій та наративів, уможливлена спроможністю (у тому числі – технічною) доносити їх до широкої громадськості та конкретних цільових аудиторій. | **Information presence**<br>the implementation of national interests in the information field via disseminating official information, interpretations and narratives, enabled by the capacity (including technical) to communicate them to the general public and specific target audiences. | Horbulin (2017) – p.157 |
| 122. | **Інформаційний домен гібридних загроз**<br>Уся інфраструктура, організація, персонал і компоненти, які збирають, обробляють, зберігають, передають, відображають, поширюють і діють на основі інформації.<br>Охоплює *інформаційний простір*. Один з 6-ти *ПМЕСІІ*-доменів. Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | **Information domain of hybrid threats**<br>The entire infrastructure, organisation, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. Encompasses the *Information environment*.<br>One of the 6 *PMESII*-domains. One of the 13 domains in the *Conceptual model of hybrid threats* | NATO (2013) – p.1-8 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 123. | **Інформаційний простір**<br><br>(1) у безпековому контексті: середовище на території держави, у якому на основі наявної інформаційної інфраструктури здійснюється формування, збір, зберігання та поширення інформації (як національного, так і закордонного походження), а також інформаційна взаємодія організацій та громадян і задоволення їхніх інформаційних потреб відповідно до чинного національного законодавства.<br><br>(2) У технічному контексті: сукупність осіб, організацій і систем, які збирають, обробляють, поширюють або діють на основі інформації. Концептуально інформаційне середовище можна розділити на три виміри:<br><br>• Фізичний вимір – охоплює земну кулю і усі можливі матеріальні об'єкти.<br><br>• Когнітивний вимір – містить наше індивідуальне та колективне знання, сприйняття, розуміння та мудрість.<br><br>• Віртуальний вимір – визначає, де і як інформація збирається, обробляється, зберігається, поширюється та захищається в цифровому вигляді. | **Information environment**<br><br>(1) in the security context: the landscape, where the available information infrastructure of the country is used to generate, collect, store and disseminate information (from home and abroad), and information interaction of organizations and citizens and meeting their information needs according to the national law in force.<br><br>(2) in a technical context: 2) the aggregate of individuals, organisations, and systems that collect, process, disseminate or act on information.<br><br>The information environment can be conceptually divided into three dimensions:<br><br>• The physical dimension encompasses the globe, and furthermore, every conceivable tangible object.<br><br>• The cognitive dimension entails our individual and collective knowledge, perception, understanding and wisdom.<br><br>• The virtual dimension entails where and how information is collected, processed, stored, disseminated, and protected digitally. | Horbulin (2017) – p.157<br><br>Van Haaster (2019) – p.136<br><br>Pijpers & Ducheine (2020) – p.4 |
| 124. | **Інформаційний суверенітет**<br><br>різновид національно-державного суверенітету; невідчужувана юридична якість незалежної держави, яка символізує її | **Information sovereignty**<br><br>the kind of national state sovereignty; unalienable legal property of an independent state, which symbolizes its political and | Horbulin (2017) – p.157 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | політико-правову самостійність, вищу відповідальність та цінність як первинного суб'єкта міжнародного права. Інформаційний суверенітет означає, що всі правила поведінки в інформаційному просторі певної держави встановлює тільки вона сама, і ніхто інший. Несуверенна держава є у цьому сенсі несамостійною, перебуває під зовнішнім управлінням, тобто є колонією, напівколонією, складовою іншої країни тощо. | legal independence, higher responsibility and value as a primary subject of international law. Information sovereignty means that all the rules of behavior in the information environment of a country are established by this country only, without interference. A non-sovereign country is dependent in this respect, being under external control, i.e. being a colony, a semi-colony, a part of another country, etc. | |
| 125. | **Інформаційні операції**<br>використання інформації як зброї для досягнення стратегічних цілей - слугують важливими інструментами завдяки своїй корисності в спробах сформувати політичний дискурс та популярний наратив у багатьох країнах. | **Information operations**<br>the weaponizing of information for strategic objectives – serve as important tools due to their utility in trying to shape the political discourse and popular narrative in many countries. | Treverton et al. (2018) - p. 53 |
| 126. | **Інформаційно-психологічна операція**<br>сукупність узгоджених та взаємопов'язаних за метою, завданнями, об'єктами і часом інформаційних та психологічних акцій, атак і заходів, що проводяться одночасно або послідовно за єдиним задумам та планом для вирішення завдань інформаційно-психологічного впливу на емоції, мотиви , установки та поведінку цільової аудиторії. | **Information psychological operation**<br>the total of agreed and interrelated information and psychological actions, attacks and events in terms of their goal, objectives, parties and time, which are held simultaneously or consecutively following a single idea and plan to reach the objectives of information psychological effect on emotions, motives, beliefs and behavior of the target audience. | Horbulin (2017) – p.157 |
| 127. | **Інфосек** | **Infosec** | ISO/IEC 27000:2009 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | інформаційна безпека (від скороченої англійської назви) як міждисциплінарна галузь знань та професійної діяльності, що включає практику захисту інформації шляхом зменшення інформаційних ризиків. Можуть бути задіяні такі властивості, як автентичність, підзвітність, неспростовність і надійність. | Information security as an interdisciplinary field of knowledge and professional activity, which includes the practice of protecting information by reducing information risks. Properties such as authenticity, accountability, irrefutability and reliability may be involved. | |
| 128. | **Інфраструктурний домен гібридних загроз**<br><br>Основні засоби, послуги та обладнання, необхідні для функціонування громади, організації чи суспільства. Містить логістику, комунікаційну та транспортну інфраструктури, школи, лікарні, розподіл води та електроенергії, каналізацію, зрошення, географію тощо.<br><br>Один з 6-ти *ПМЕСІІ*-доменів. Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | **Infrastructure domain of hybrid threats**<br><br>The basic facilities, services, and installations needed for the functioning of a community, organisation, or society. Includes logistics, communications and transport infrastructures, schools, hospitals, water and power distribution, sewage, irrigation, geography, etc.<br><br>One of the 6 *PMESII*-domains. One of the 13 domains in the *Conceptual model of hybrid threats* | NATO (2013) – p.1-8<br><br>Cullen et al. (2021) – p.27 |
| 129. | **Інциденти**<br><br>сукупність дій в контексті протидії дезінформації (див. FIMI) з конкретними цілями, наприклад, змінити переконання, емоції або поведінку, можуть створюватися окремими особами, групами та організаціями. Інциденти описуються з використанням таких даних: час, місце впливу, відповідні індикатори, використані "Тактика, методи і процедури" (див. TTPs), оцінка впливу, запитані/вжиті заходи реагування, | **Incidents**<br><br>Sets of activity in the context of countering disinformation (see. FIMI) with specific objectives, e.g., to change beliefs, emotions, or behaviours, may created by individuals, groups, and organizations. Instances are described using data, such as time-related information, location of effect, related indicators, leveraged "Tactics, Techniques, and Procedures " (see. TTPs), impact assessment, response course of action requested/taken, source of the | STIX (2012). |

| № | UA | EN | Джерело |
|---|---|---|---|
| | джерело інформації про інцидент та журнал вжитих заходів. | incident information, and log of actions taken. | |

## К

| № | UA | EN | Джерело |
|---|---|---|---|
| 130. | **Кампанії впливу**<br><br>скоординована діяльність іноземних держав, включаючи використання оманливої або недостовірної інформації, для впливу на прийняття політичних та громадських рішень, громадську думку чи думки в іншій країні, що може негативно вплинути на суверенітет, цілі безпеки чи інші інтереси нашої країни.<br><br>До методів Кампаній Впливу відносяться: *Соціальні (Когнітивні) Злами, Оманливі Ідентичності, Технічне Використання, Дезінформація, Риторика Викривлення (Наклепу), Символічні Дії.*<br><br>Немає універсальної реакції на дії інформаційного впливу. Існує чотири категорії відповідей (оцінювати, інформувати, відстоювати і боронити), кожна з яких складається з декількох специфічних комунікативних прийомів. | **Influence Campaigns**<br><br>coordinated activities by foreign powers, including the use of misleading or inaccurate information, to influence political and public decision-making, public opinion, or opinions in another country, which may affect the sovereignty, the goals for the security or other interests negatively of our country.<br><br>Information influence techniques include: *Social (Cognitive) Hacking, Deceptive Identities, Technical Exploitation, Disinformation, Malign Rhetoric, Symbolic Actions.*<br><br>There is no one-size-fits-all response to information influence activities. There are four categories of response (assess, inform, advocate and defend), that each consist of several specific communicative techniques. | MSB (2018) – p.7, 35 |
| 131. | **Каскадна інформація**<br><br>явище, коли користувачі передають інформацію, розміщену їхніми близькими контактами, не обов'язково перевіряючи і навіть не замислюючись, чи ця інформація відповідає дійсності. Чим більше інформація поширюється, тим більше ми схильні їй довіряти і тим менше | **Cascading Information**<br><br>the phenomenon when users relay information posted by their close contacts without necessarily checking or even considering whether that information is true. The more the information is shared, the more we tend to trust it and the less we use critical thinking to assess it. | Vilmer et al. (2018) - p.42 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | використовуємо критичне мислення для її оцінки. | | |
| 132. | **"Катинська різанина" 1940**<br>один з наративів кремля,<br>"антикатинська" пропагандистська кампанія, яка змальовує цей військовий злочин (розстріли близько 22 000 польських військових і інтелігенції) як "справедливу історичну помсту" за фальшиві масові вбивства радянських військовополонених у Польщі під час польсько-радянської війни 1919 р. - 1921. На думку польських та російських істориків, основною причиною високої смертності серед радянських військовополонених були інфекційні хвороби, які забрали життя 16 000–20 000 (російська пропаганда наводить завищену цифру 100 000). | **"Katyń massacre" 1940**<br>one of the Kremlin narratives,<br>"anti-Katyń" propaganda campaign, that paints this war crime (executions of about 22,000 Polish military officers and intelligentsia) as a “just historical revenge” for the spurious mass killings of Soviet POWs in Poland during the Polish-Soviet war of 1919–1921. According to Polish and Russian historians, the main cause of high mortality among Soviet prisoners of war were infectious diseases that took the lives of 16,000–20,000 (while Russian propaganda most often cites the inflated number of 100,000). | Domańska (2019) – p.3 |
| 133. | **Квазі реальність**<br>частина стратегії гібридної війни, яка передбачає зміщення акцентів, подання напівправди, намагання відволікати увагу, здійснює вплив на прийняття рішень і спрямована на дипломатичне прикриття гібридної агресії. Вона є ключовою серед сукупних дій російської агресії, зокрема, - *Анексії Криму* та підтримки сепаратистів на Донбасі. | **Quasi reality**<br>the part of the hybrid war strategy, which provides for the shift of emphasis, releasing semitruths, striving for distracting attention; it affects decision making and aims at the diplomatic covering of the hybrid aggression. It is a key element of the Russian aggression, including the *Crimea Annexation* and support of separatists in Donbass. | Horbulin (2017) – p.159 |
| 134. | **Квантова технологія**<br>нова галузь фізики та техніки; використовує властивості квантових ефектів - взаємодії | **Quantum technology**<br>an emerging field of physics and engineering; it uses the properties of quantum effects – the interactions of | Thiele(b) (2020) – p.6 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | молекул, атомів і навіть менших частинок, відомих як квантові об'єкти - для створення практичних застосувань у багатьох різних сферах.<br><br>Одна з проривних технологій, яка активно використовується гібридними акторами (див.квантові науки) | molecules, atoms, and even smaller particles, known as quantum objects – to create practical applications in many different fields.<br><br>One of the breakthrough technologies actively used by hybrid actors (see quantum sciences) | |
| 135. | **Квантові науки**<br><br>нові технології, які дозволяють підвищити продуктивність електроніки понад законом Мура, який уже говорить, що ми можемо очікувати збільшення швидкості та можливостей комп'ютерів кожні два роки.<br><br>використовуючи квантові комп'ютери, функціональні можливості наявних звичайних технологій можна значно покращити з погляду чутливості, точності, швидкості або зручності для користувача.<br><br>Квантуум розвивається як прискорювач інших технологій, таких як нано, біо, IT та нейро, і, отже, значно зміцнює гібридних суб'єктів у своїй діяльності в *Сірій Зоні*. Зокрема, ми побачимо значно вдосконалені обчислювальні технології, комунікації, криптографію, навігацію та сенсорні можливості, які дозволять гібридним дійовим особам просунутись за межі гібридної агресії | **Quantum sciences**<br><br>new technologies which enable the performance of electronics to increase beyond Moore's Law, which already states that we can expect the speed and capability of computers to increase every couple of years<br><br>using quantum computers, the functionalities of already existing conventional technologies can be significantly improved in terms of sensitivity, accuracy, speed or user-friendliness<br><br>Quantum is evolve as an accelerator of other technologies such as nano, bio, IT, and neuro, and consequently strengthen hybrid actors significantly in their *Grey Zone* activities. In particular, we will see vastly improved computing, communication, cryptography, navigation, and sensing capabilities that will enable hybrid actors to push the envelope of hybrid aggression | Thiele(b) (2020) – p.6<br><br>Riekeles (2023)<br><br>Inglesant et al. (2016)<br><br>Thiele(b) (2020) – p.6 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 136. | **Квантові обчислення**<br>надшвидкі комп'ютери, які використовують відмінні від класичних алгоритми.<br>Приклади "гібридних" застосувань: злом кодів кібербезпеки з безпрецедентною швидкістю, що ускладнює кібербезпеку**.** | **Quantum computing**<br>super-fast computers that utilise different algorithms to classical computers<br>Examples of hybrid applications: Cracking cyber security codes with unprecedented speed, making cyber security even more difficult. | Bekkers et al. (2019) – p.26 |
| 137. | **Квід про кво**<br>(в перекладі з латини означає «щось за щось»)<br>це тип зловмисної атаки, що передбачає запит інформації в обмін на компенсацію. Наприклад: зловмисник запитує пароль жертви, називаючись дослідником, який проводить експеримент, в обмін на гроші. Атаки типу «послуга за послугу» відносно легко виявити, враховуючи асиметричну цінність інформації порівняно з компенсацією, тобто протилежну для зловмисника і жертви. У таких випадках найкращою протидією залишається доброчесність жертви та її здатність виявляти, ігнорувати та повідомляти про такі випадки. | **Quid Pro Quo**<br>"something for something" in Latin,<br>involves a request for information in exchange for a compensation. Example: the attacker asks the victim's password claiming to be a researcher doing an experiment, in exchange for money. Quid pro quo attacks are relatively easy to detect given the asymmetrical value of the information compared to the compensation, which is opposite for the attacker and the victim. In these cases the best countermeasure remains the victim integrity and ability to identify, ignore and report. | ENISA (n.d.) |
| 138. | **Китайська стратегічна культура**<br>Китайська стратегія гібридних впливів.<br>Основана на ідеї, що "війна — це обман", та передбачає мистецтво успішного зведення ворога зі шляху і, в ідеалі, - перемогу у війні без необхідності вдаватися до зброї. | **Chinese strategic culture**<br>The China's hybrid influence strategy.<br>Based on the idea of "war is deception" involving the art of successfullysuccessfully leading the enemy astray, and ideally winning the war without the need to resort to arms.<br>The ideologist of this strategy is Sun | Cullen et al. (2021) – p.20 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Ідеологом такої стратегії є Сунь Цзи, китайський мислитель 6 століття до н.е, автор трактату "Мистецтво війни". Китайська стратегія поєднує асиметричний підхід (див. *Асиметрія гібридних загроз*) та діалектичний погляд на стратегічне середовище: жодне поняття не є чітко визначеним та має динамічні самогенеруючі властивості (такі як "слабкість і сила", "таємні маневри та відкриті операції" тощо); а концепції є частинами конфігурацій, що постійно змінюються.<br>Теоретичне підгрунття цієї стратегії:<br>• традиції, розуміння та практика *Стратагем*;<br>• військова стратегія Китаю "*Три війни*" | Zu, a Chinese thinker from the sixth century BC, the author of the treatise "The Art of War". China's strategy combines asymmetric approach (see *Asymmetry of hybrid threats*) and a dialectic view of the strategic environment: any concept is not strictly defined, it has dynamic self-generating properties (such as “weakness and strength”, “clandestine manoeuvres and open operations” etc.); all concepts are parts of constantly changing configurations.<br>The theoretical basis of this strategy is:<br>• traditions, understanding and practice of *Stratagems*;<br>• China's military strategy "*Three Warfares*" | |
| 139. | **Китайський еволюціонуючий підхід до "інтегрованого стратегічного стримування"**<br>китайське розуміння *Крос-Доменного Стримування* включає "багатовимірну сукупність військових та невійськових можливостей, які в сукупності складають позицію "інтегрованого стратегічного стримування", необхідну для захисту інтересів національної безпеки Китаю".<br>Китайці думають про стримування в багатьох сферах, пояснюючи, що воно ґрунтується на поєднанні ядерних, звичайних, інформаційних, космічних та цивільних сил. | **China’s Evolving Approach to ‘Integrated Strategic Deterrence’**<br>Chinese understanding of *Cross Domain Deterrence* includes “a multidimensional set of military and non-military capabilities that combine to constitute the “integrated strategic deterrence” posture required to protect Chinese national security interests.”<br>Chinese thinking about deterrence across multiple domains, explaining that it rests upon a combination of nuclear, conventional, information, space, and civilian forces.<br>See also: *Cross Domain Deterrence* | Chase & Chan (2016) – p.3<br>Sweijs & Zilincik (2019) – p.14 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Див також: *Крос-Доменне Стримування* | | |
| 140. | **Кібератака**<br><br>1) сукупність кількох короткочасно узгоджених за метою і часом заходів інформаційно-технологічного впливу, спрямованих на деструктивні зміни визначеного об'єкта інформаційної інфраструктури.<br><br>2) відключення системи, починаючи від перезавантаження і закінчуючи "синіми екранами смерті" для силових установок, радарів, систем управління повітряним рухом та мереж управління та контролю, що впливають як на засекречені, так і на незасекречені системи. Перша категорія кібератак буде проведена в рамках більш широких зусиль з виведення з ладу озброєння цілі та зриву стратегічних / військових систем. Друга категорія кібератак буде спрямована на здатність та готовність цілі вести війну протягом тривалого періоду часу. | **Cyberattack**<br><br>1) the stand for the total of several brief measures for information and technological influence agreed in time and united by a single purpose to destroy the target object of information infrastructure.<br><br>2) system outages ranging from reboots to “blue screens of death” for propulsion systems, radar, air traffic control systems and command and control networks affecting both classified and unclassified systems. The first category of cyber-attacks would be conducted as part of a broader effort to disable the target’s weaponry and to disrupt strategic/military systems. The second category of cyber-attacks would be aimed at the target’s ability and willing- ness to wage war for an extended period of time. | Horbulin (2017) – p.156<br><br>Schroefl (2020) – p.3,5 |
| 141. | **Кібервійна**<br><br>нові високотехнічні форми ведення війни в епоху інформації, які засновані на широкому використанні комп’ютерів та програмного забезпечення, електронізації та мережах майже у всіх військових та цивільних галузях. Інтенсивність цих операцій, їхній "успіх" з погляду зриву та відмови в IT-послугах, | **Cyberwarfare**<br><br>new highly technical forms of warfare in the information age, which are based on the extensive use of computers and software, electronization and networking of almost all military and civilian areas. The intensity of these operations, their “success” in terms of the disruption and denial of IT services, computer programs and underlying | Schroefl (2020) – p.4 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | комп'ютерних програм та основних мереж, а також з точки зору дезінформації та викривлення, і, нарешті, їхні політичні та / або стратегічні цілі - все це вказує на їхню характеристику як кібервійни. | networks, as well as in terms of disinformation and defacement, and lastly their political and/or strategic goals point to their characterization as cyber "warfare". | |
| 142. | **Кібервійська**<br><br>команди, що мають належність до уряду, армії чи політичних партій, місія яких полягає у маніпулюванні громадською думкою за допомогою соціальних мереж. | **Cybertroops**<br><br>teams belonging to the government, the army, or political parties, whose mission is to manipulate public opinion via social media. | Bradshaw & Howard (2017) – p.3<br><br>Vilmer et al. (2018) - p.48 |
| 143. | **Кібердипломатія**<br><br>дипломатія в кіберпросторі або використання дипломатичних ресурсів і виконання дипломатичних функцій для захисту національних інтересів у кіберпросторі. Такі інтереси зазвичай виявляються в національних стратегіях кіберпростору або кібербезпеки, які часто містять посилання на дипломатичний порядок денний. Домінувальні питання в порядку денному кібердипломатії включають кібербезпеку, *Кіберзлочинність*, зміцнення довіри, свободу Інтернету та управління Інтернетом. | **Cyber-diplomacy**<br><br>can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance | Barrinha & Renard (2017) – p.355 |
| 144. | **Кіберзлочинність**<br><br>злочинні діяння, вчинені в онлайновому режимі з використанням електронних комунікаційних мереж та інформаційних систем | **Cybercrime**<br><br>consists of criminal acts committed online by using electronic communications networks and information systems | European Commission (2021) |

| № | UA | EN | Джерело |
|---|---|---|---|
| 145. | **Кіберпростір / Кібер домен**<br><br>Мережева інформаційна інфраструктура, яка є частиною *інформаційного простору*. Три рівні унікальні для кіберпростору:<br><br>• фізичний рівень мережі – апаратне забезпечення (комп'ютери, маршрутизатори, смартфони) і фізичні з'єднання між цими концентраторами (волоконно-оптичні кабелі). Дані виробляються, передаються, обробляються та зберігаються у фізичних частинах, а інформація проходить через фізичні компоненти різних мереж.<br><br>• логічний рівень, тобто програмне забезпечення та дані. Логічний рівень містить всі нематеріальні елементи, що проявляються в даних або коді («нулі та одиниці»), такі як операційні системи, протоколи, програми або інше програмне забезпечення та компоненти даних. Логічний рівень не може функціонувати без фізичного рівня мережі.<br><br>• віртуальна особа, яка є відображенням (груп) осіб у віртуальному вимірі. Віртуальна особа дозволяє реальним особам або організаціям отримувати доступ до кіберпростору через адресу електронної пошти або облікові записи на платформах соціальних мереж. Віртуальні особи дають доступ до логічного рівня. | **Cyberspace / Cyber domain**<br><br>the networked information infrastructure, is part of the *information environment*. The three layers unique to cyberspace are:<br><br>• the physical network layer – the hardware (computers, routers, smartphones) and the physical connections between these hubs (fibre optic cables). Data is produced, transmitted, processed and stored in physical parts and information flows through physical components of various networks.<br><br>• the logical layer i.e. the software and the data. The logical layer includes all non-tangible elements manifested in data or code ('zeros and ones'), such as operating systems, protocols, applications, or other software and data components. The logical layer cannot function without the physical network layer.<br><br>• the virtual persona which are the reflections of (groups of) persons in the virtual dimension.Virtual personas allow real persons or organisations to access cyberspace via e-mail address or accounts on social media platforms. The virtual personas enable access to the logical layer.<br><br>One of the 13 domains in the *Conceptual model of hybrid threats* | Pijpers & Ducheine (2020) – p.4<br><br>Mayer (2018) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | | |
| 146. | **Кіберстійкість**<br>здатність постійно досягати запланованого результату, незважаючи на несприятливі кіберподії. | **Cyber resilience**<br>the ability to continuously deliver the intended outcome despite adverse cyber events. | Lantto et al. (2019) |
| 147. | **Кібертерорист**<br>терорист, який використовує Інтернет, інформаційні та комунікаційні технології для здійснення своїх нападів. Він користується перевагами технологічних інструментів, наприклад здатністю негативно впливати на велику кількість людей за короткий проміжок часу, без особистого фізичного впливу, через власний компютер. | **Cyberterrorist**<br>a terrorist that uses the internet as well as information and communication technologies to perpetrate their attacks. He takes advantage of the benefits offered by technological tools, for example the ability to negatively impact a large number of people in a brief period of time without personally physically exposing oneself, but from the comfort of its own computer. | Mayer (2018) |
| 148. | **Кібершпигунство**<br>традиційні шпигунські операції, спрямовані на збір інформації для держави-замовника. Викрадена інформація, зібрана під час таких операцій, може або передаватися для впливу на суспільний дискурс та думку - стаючи тим самим важливою частиною інформаційної війни - або зберігатись в таємниці гібридного загрожувача для власних вигод. | **Cyber espionage**<br>is traditional espionage operations, aiming to gather information for the sponsored state. The stolen information collected during such operations can either be relayed to influence public discourse and opinion – thereby becoming an essential part of information warfare – or kept covert by the hybrid threatener for its own benefits. | Treverton et al. (2018) - p. 54 |
| 149. | **Когнітивна війна**<br>сукупність дій, які застосовують одночасно з іншими інструментами сили, щоб вплинути на ставлення і поведінку людей | **Cognitive Warfare**<br>the activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by | NATO (2023) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | шляхом впливу, захисту та/або руйнування індивідуальних і групових переконань з метою отримання переваги. Ці дії дуже різняться і можуть охоплювати позитивні або конфліктні культурні чи особистісні компоненти – соціальна психологія, теорія ігор та етичні норми – це ті фактори, які впливають на них. Однак, методи сучасної війни не обов'язково мають кінетичний компонент або безпосередньо реальні результати, такі як захоплення територій чи ресурсів – як і у випадку з іншими гібридними загрозами, супротивники ведуть когнітивну війну протягом усього конфлікту і прагнуть залишатися в «сірій зоні» нижче порогу збройного протистояння. Когнітивна війна поєднує в собі інструменти соціальної інженерії, а також кібернетичні, інформаційні та психологічні технології. | influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage. These activities vary greatly, and may encompass supporting or conflicting cultural or personalized components – social psychology, Game Theory, and ethics are all contributing factors. However, activities of modern warfare do not necessarily carry a kinetic component or directly tangible outcomes, such as territorial or resource acquisition – as with other hybrid threats, our adversaries conduct Cognitive Warfare throughout the continuum of conflict, and aim to stay in the 'Gray Zone' below the threshold of armed conflict. Cognitive Warfare integrates cyber, information, psychological, and social engineering capabilities. | |
| 150. | **Когнітивний злам** (або *Соціальний Злам*)<br><br>є одним із методів інформаційного впливу (див. *Кампанії Впливу*)<br><br>шкідлива діяльність, яка використовує способи функціонування соціальних відносин та процесів мислення. Це схоже на хакерство в тому сенсі, що ворожі суб'єкти прагнуть обдурити або "зламати" ці процеси. Наші передбачувані моделі поведінки можуть бути використані ворожими суб'єктами, які свідомо активують тригер-точки. | **Cognitive Hacking** (or *Social Hacking*)<br><br>is one of the information influence techniques (see *Influence Campaigns*)<br><br>malicious activities that exploit the ways that social relationships and thought-processes work. It is like hacking in the sense that hostile actors seek to cheat, or "hack", these processes. Our predictable patterns of behavior can be exploited by hostile actors who deliberately activate trigger-points. | MSB (2018) – p.19 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Серед інструментів таких зламів: *Темна реклама, Ефект приєднання до більшості, Спіраль мовчання, Луна-Камери, Бульбашка фільтрів* тощо. | it includes: *Dark Ads, Bandwagon-Effect, Spiral of Silence, Echo Chambers, Filter Bubbles* etc. | |
| 151. | **КозіБе та ФансіБе** (дослівно)<br>(англ - "Затишний ведмежа" та "Модний ведмежа")<br>хакерські групи, пов'язані з російським урядом, та із розвідувальними відомствами, які є принаймні конкурентами - ФСБ або СВР (федеральна служба безпеки, наступник Управління закордонних операцій КДБ) та ГРУ (головне управління розвідки, військова розвідка) відповідно. | **CozyBear and FancyBear**<br>the hacker groups,<br>are both tied to the Russian government but to intelligence agencies that are at least competitors — the FSB or SVR (the federal security service, successor to the KGB's foreign operations directorate), and the GRU (main intelligence directorate, military intelligence), respectively. | Treverton et al. (2018) - p. 17, 40 - 42 |
| 152. | **Кольорова революція**<br>ненасильницьке повалення урядів масовими протестами;<br>не військова війна | **Colour revolution**<br>the non-violent nature of the regime change resulting from mass protests;<br>non-military warfare | Bouchet (2016) – p.1 |
| 153. | **Командно-контрольна війна**<br>інтегроване використання військових можливостей, включаючи заходи із забезпечення прихованості операцій, введення в оману; психологічні операції; засоби ведення радіоелектронної боротьби та фізичне знищення, що підтримуються узагальненою розвідувальною інформацією, системами зв’язку та інформаційними системами. Всі ці заходи спрямовані на здійснення впливу, послаблення або знищення системи управління противника, з одночасним | **Command and control warfare (C2W)**<br>the integrated use of all military capabilities including operations security, deception, psychological operations, electronic warfare and physical destruction, supported by all-source intelligence and communication and information systems, to deny information to, influence, degrade or destroy an adversary's command and control capabilities while protecting friendly command and control capabilities against similar actions. | NSA (2013) – p. 2-C-9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | забезпеченням захисту власної системи управління від таких дій. | | |
| 154. | **Командно-контрольна комунікаційна система**<br>це система, яка забезпечує обмін інформацією між органами військового управління з метою здійснення оперативного управління військами. | **Command and control communication system (C2CS)**<br>a communication system which conveys information between military authorities for command and control purposes. | NSA (2013) – p. 2-C-9 |
| 155. | **Командно-контрольна система управління**<br>це сукупність обладнання, методів та процедур, за необхідності – особового складу, яка дозволяє командирам та їхнім штабам здійснювати оперативне управління. | **Command and control system (C2S)**<br>an assembly of equipment, methods and procedures and, if necessary, personnel, that enables commanders and their staffs to exercise command and control. | NSA (2013) – p. 2-C-9 |
| 156. | **Комп'ютерна пропаганда**<br>використання алгоритмів, автоматизації, аналізу великих даних та кураторства для маніпулювання громадським життям через соціальні мережі. | **Computational propaganda**<br>the use of algorithms, automation, big data analytics and human curation to manipulate public life over social media networks. | Neudert & Marchal (2019) – p.5 |
| 157. | **Компромат (як метод)**<br>компрометація цілі (жертви), яку таким чином можна контролювати та маніпулювати нею. | **"Kompromat" Method**<br>compromising a target who can thus be controlled and manipulated. | Vilmer et al. (2018) - p.160 |
| 158. | **Комунікація заради стримування**<br>Один із "*трьох С*" – *компонентів стримування*.<br>Означає двостороннє розуміння та сприйняття, що використовується обома сторонами для визначення витрат та вигід. | **Communication for deterrence**<br>One of the *'three Cs' of deterrence*.<br>means the two-way understanding and perception that informs cost-benefit calculations on both sides. | MCDC(a) (2019) – p.35 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 159. | **Конспірологічна теорія**<br><br>Див. *Теорія Змови* | **Conspiracy theory of society**<br><br>See*: conspiracy theory of society* | |
| 160. | **Контрзаходи**<br><br>комплек заходів, які вживаються для того, щоб послабити вплив небажаної дії чи ситуації або зробити її нешкідливою. Такий комплекс застосовують на противагу або у відповідь на якісь інші дії. Як загальна концепція, вона передбачає точність і є будь-яким технологічним або тактичним рішенням або системою, призначеною для запобігання небажаному результату. | **Countermeasures**<br><br>actions that are taken in order to weaken the effect of unwanted action or a situation, or to make it harmless. These are actions taken in opposition or retaliation against some other actions. As a general concept, it implies precision and is any technological or tactical solution or system designed to prevent an undesirable outcome. | Kalenský et al. (2024) |
| 161. | **Контроль за експортом зброї**<br><br>комплекс заходів, спрямованих на забезпечення процесу експорту озброєнь із суворим дотриманням вимог захисту інтересів національної оборони й економіки, суспільного спокою, внутрішньої і зовнішньої безпеки та дотриманням міжнародних зобов'язань держави, за яких держава створює правові інструменти, що забезпечують здійснення такого експортного контролю на своїй території. Діяльність щодо контролю за експортом зброї розвивається в контексті відносин між державами, які є частиною світової системи | **Control of arms exports**<br><br>(pt ) tal controlo poderá ser definido como sendo o conjunto das medidas tendentes a assegurar que aquelas exportações, incluídas pela Lei nas actividades de comércio de armamento, ocorram “em estrita subordinação à salvaguarda dos interesses da defesa e da economia nacionais, da tranquilidade pública, da segurança interna e externa e do respeito pelos compromissos internacionais do Estado português»; … «É o Estado que cria os instrumentos jurídicos que concretizam, no seu território...»… «... de controlo de exportações de armamento evoluem no contexto das relações entre os Estados integrantes do Sistema Internacional | Mira (2011) - p. 248-249, p.247, p.246 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 162. | **Концептуальна модель гібридних загроз**<br><br>Модель, яка фіксує складові гібридних загроз та демонструє зв'язки між ними. Аналітична структура моделі розроблена навколо чотирьох основних стовпів, які формують ландшафт гібридних загроз:<br>• Актори / гравці гібридних загроз та їх стратегічні цілі: 2 типа<br>• Домени гібридних загроз, на які вони спрямовані: 13 видів<br>• Інструменти сили, які використовує актор: більш ніж 40 видів<br>• Фази гібридних загроз: 4 вида<br><br>Концепція базується на тому, що головна мета гібридних впливів – підірвати здатність жертви до прийняття рішень. | **Hybrid threats conceptual model**<br><br>A model that identifies the components of hybrid threats and demonstrates the connections between them. The analytical framework of the model is developed around four main pillars that shape the landscape of hybrid threats:<br>• Actors of hybrid threats (and their strategic objectives): 2 types,<br>• Domains of hybrid threats that are targeted: 13 types<br>• Instruments of power applied by the actor: more than 40 types<br>• Phases: 4 types<br><br>The concept is based on the premise that the primary objective of hybrid influences is to undermine the victim's decision-making ability. | Cullen et al. (2021) – p.13 |
| 163. | **Корисні ідіоти**<br><br>особи, які несвідомо надихаються на розповсюдження дезінформації, і несвідомо сприяють діям гібридних акторів | **Useful Idiots**<br><br>persons who unconsciously inspired to proliferate disinformation and unknowingly contribute to the actions of hybrid actors | Vilmer et al. (2018) - p.71<br><br>Szwed (2016) – p.55<br><br>Cullen et al. (2021) – p.22 |
| 164. | **"Корупційний трикутник"**<br><br>є одним із способів концептуалізації корупції.<br><br>Основна ідея: щоб корупція мала місце, потрібні три ключові фактори:<br><br>- мотивація,<br>- можливість і | **'Corruption Triangle'**<br><br>is one way of conceptualising corruption.<br><br>Main idea: for corruption to take place requires three key factors to come together:<br><br>- motivation,<br>- an opportunity and | MCDC(b) (2019) – p.1 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | - раціоналізація тих, хто здійснює корупцію. | - a rationalisation by those carrying out the corruption. | |
| 165. | **Корупція**<br><br>зловживання довіреною владою з метою отримання приватної вигоди.<br><br>зловживання службовим становищем і неналежне функціонування державних установ, яке шкодить загальному благу.<br><br>є одним з видів гібридних озброєнь: 1) як ключовий фактор, що сприяє використанню іншої зброї в гібридному озброєнні; 2) як підсилювач впливу інших видів діяльності; 3) як потужна зброя масового руйнування; 4) як зброя масового відволікання.<br><br>Це нечесна чи шахрайська поведінка владних структур, як правило, пов'язана з підкупом.<br><br>Корупція має як фізичну, так і психологічну складову. Фізичний компонент зосереджується на втраті ресурсу там, куди ресурс спочатку був призначений. Це проявляється у можливостях, які коштують дорожче, ніж слід (корупційні "накладні витрати"), або в погіршенні продуктивності. Набагато згубнішою є психологічна складова корупції. Корупція як поняття тісно пов'язана в психіці людини з поняттями справедливості та несправедливості. | **Corruption**<br><br>the abuse of entrusted power for private gain.<br><br>the misuse of public institutions and office to the detriment of the common good.<br><br>is one of the hybrid weapons: 1) as a key enabler in the use of the other weapons in the hybrid armoury; 2) as an amplifier of the impact of other activities; 3) as a powerful weapon of mass disruption; 4) as a weapon of mass distraction.<br><br>Is the dishonest or fraudulent conduct by those in power, typically involving bribery.<br><br>Corruption has both a physical and a psychological component. The physical component centres on the loss of resource to the endeavour that the resource was originally intended for. This manifests in capabilities costing more than they should (the corruption 'overhead') or degraded performance. Far more pernicious is the psychological component of corruption. Corruption as a concept is closely linked in the human psyche to concepts of justice and injustice, fairness and unfairness. | Transparency International (a)<br><br>Lough & Dubrovskiy (2018) – p.4<br><br>MCDC(b) (2019) – p.1 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 166. | **Космічний домен гібридних загроз**<br><br>Це космічні послуги, які включають навігацію, геолокацію, зв'язок, дистанційне зондування, *PNT-послуги*, науку та дослідження.<br><br>Космічні технології є технологіями подвійного використання, тому військові та цивільні космічні служби непросто розділити. Це створює "сіру зону" невизначеності, яка сприяє гібридній активності. Тенденції, що посилюють вразливість космічного домену, – це комерціалізація та мілітарізація космосу. Напрями використання космічних технологій у гібридних впливах:<br><br>• шпигунська діяльність<br>• знищення або пошкодження космічної інфраструктури супротивника<br>• використання залежності супротивників від космічних систем (наприклад, через *РЕБ*)<br>• інформаційні впливи, які експлуатують тему космосу.<br><br>Один з 13-ти доменів у *Концептуальній моделі гібридних загроз*. | **Space domain of hybrid threats**<br><br>It`s space-based services which include navigation, geolocation, communications, remote sensing, *PNT- services*, science and exploration.<br><br>Space technologies are dual-use technologies, therefore military and civilian space services are not easily separated. This creates a "grey area" of uncertainty that favors hybrid activity. Trends increasing the vulnerability of the space domain are the commercialization and militarization of space. Areas of use of space technologies in hybrid effects:<br><br>• espionage activities<br>• destruction or damage to the enemy's space infrastructure<br>• using the dependence of opponents on space systems (for example, through *EW*)<br>• informational influences that exploit the theme of space.<br><br>One of the 13 domains in the *Conceptual model of hybrid threats* | Cullen et al. (2021) – p.19<br><br>DIA (2022) – p.IV |
| 167. | **Криза економічної моделі**<br><br>одно з явищ "кризи преси".<br><br>є результатом зменшення доходів від реклами в пресі через конкуренцію, із якою вона стикнулася спочатку після появи телебачення, а згодом і з винаходом Інтернету. Перехід до | **Crisis of the economic model**<br><br>one of "the crisis of the press" phenomenon.<br><br>the result of the decrease in press advertising revenues, due to the competition it first faced from the advent of television, and then later on with the invention of the internet. | Vilmer et al. (2018) - p.38, 187<br><br>Tworek (2018) – p.2 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | цифрових ЗМІ не забезпечив повноцінної компенсації: цифрова реклама менш прибуткова, ніж друк і телебачення. Багатьом агенціям та новинним організаціям доводилося звільняти журналістів, виплачувати вихідні виплати та припиняти певні інформаційні видання. Ця нестабільна ситуація робить пресу ще більш вразливою до маніпуляцій з інформацією, оскільки залишається менше людей і менше часу для їх виявлення, а також завдяки збільшення кількості, а не якості інформації.<br><br>Тим не менше, постійно з'являються нові економічні моделі, за якими сплачують підписку, та диверсифікація джерел доходів. | The shift over to digital media hardly provided compensation: digital publicity is less lucrative than both print and television. Many agencies and news organizations have had to lay off journalists, doll out severance payments and terminate certain news outlets. This precarious situation renders the press even more vulnerable to information manipulation, because there are less people and less time to detect them and because of the premium placed on quantity rather than quality.<br><br>Nevertheless, new economic models are constantly cropping up, and are paid for by subscriptions and the diversification of revenue sources. | |
| 168. | **Критична інфраструктура**<br><br>у своєму найширшому розумінні охоплює таку інфраструктуру, як: заводи, лікарні, електростанції, електромережа, аеропорти, порти, мости та дороги, логістичні мережі, а також мережі, що виробляють та передають інформацію, товари та гроші, тобто всі великі фізичні або віртуальні системи, що забезпечують сучасне суспільство тим, що йому потрібно для нормального повсякденного життя. | **Critical Infrastructure**<br><br>in its broadest sense, covers infrastructure such as factories, hospitals, power plants, electric grid, airports, ports, bridges and roads, but also logistics chains as well as networks that produce and transfer information, goods and money, i.e. all large physical or virtual systems that provide modern societies with what they need for normal daily life. | Savolainen (2019) – p.8 |
| 169. | **Критична інфраструктура ЄС**<br><br>активи, системи або їх частини, розташовані в державах-членах ЄС, що мають важливе значення для | **EU Critical Infrastructure**<br><br>asset, system or part thereof located in Member States which is essential for the maintenance of vital societal | European Council (2008). - 345/77 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | підтримання життєво важливих соціальних функцій, охорони здоров'я, збереження, безпеки, економічного чи соціального добробуту людей, і порушення або знищення яких матиме значний вплив на Державу-члена ЄС внаслідок неможливості зберегти ці функції | functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions | |
| 170. | **Критичні функції**<br><br>діяльність або операції, розподілені за політичним, військовим, економічним, соціальним, інформаційним, інфраструктурним (*ПМЕСІІ*) спектром, припинення роботи яких призведе до порушення служб, від яких залежить функційна система (наприклад, держава, суспільство або його складова).<br><br>Критичні функції можуть бути розбиті на комбінацію суб'єктів (наприклад, окремих осіб чи організацій), інфраструктури (наприклад, "критичні" національні електромережі) та процесів (наприклад, юридичних / юрисдикційних, технічних, політичних). | **Critical functions**<br><br>activities or operations distributed across the political, military, economic, social, information, infrastructure (*PMESII*) spectrum, the discontinuance of which would lead to the disruption of services that a working system (for example, a state, its society, or a subsection thereof) depends on.<br><br>Critical functions can be broken down into a combination of actors (for example, individuals or organizations), infrastructures (for example, 'critical' national power grids) and processes (for example, legal/jurisdictional, technical, political). | MCDC(a) (2019) – p.89<br><br>MCDC (2017) – p.11 |
| 171. | **Крос-доменне стримування**<br><br>використання загроз в одному домені (сфері) для протидії діяльності в інших доменах (сферах). | **Cross domain deterrence**<br><br>involves the use of threats in one domain to counter activities in other domains. | Sweijs & Zilincik (2019) – p. 12 |
| 172. | **Культурна дипломатія**<br><br>1) спосіб "демонстрації культури країни за допомогою концертів чи | **Cultural diplomacy**<br><br>1) a way for "showcasing a country's culture through concerts or | Williams S. (2021)<br><br>Ryniejska–Kiełdanowicz, |

| № | UA | EN | Джерело |
|---|---|---|---|
| | виставок» та інших креативних практик.<br><br>2) це обмін ідеями, інформацією, мистецтвом та іншими аспектами культури між країнами для сприяння та розвитку взаєморозуміння" (Концепція М. С. Каммінгса). | exhibitions» and other creative practices".<br><br>2) an exchange of ideas, information, art, and other aspects of culture between countries to facilitate mutual understanding" (Conception of M. C. Cummings). | M. (2009) – p.8 |
| 173. | **Культурна діяльність, товари та послуги**<br><br>діяльність, товари та послуги, які розглядаються як певний атрибут, використання чи мета, що втілюють або передають форми проявів культури, незалежно від їх комерційної цінності.<br><br>Культурна діяльність може бути самоціллю або сприяти виробництву культурних товарів та послуг | **Cultural activities, goods and services**<br><br>are the activities, goods and services, which at the time they are considered as a specific attribute, use or purpose, embody or convey cultural expressions, irrespective of the commercial value they may have.<br><br>Cultural activities may be an end in themselves, or they may contribute to the production of cultural goods and services | UNESCO (2019) – p.7 |
| 174. | **Культурна належність**<br><br>взаємовідносини спільної групової ідентичності, які можна простежити історично або доісторично між теперішньою та більш ранньою формою групи. В законодавстві США – це визначення використовується в контексті індіанських племен та корінних гавайських організацій. | **Cultural affiliation**<br><br>means that there is a relationship of shared group identity which can be reasonably traced historically or prehistorically between a present day tribe ….and an identifiable earlier group. In the USA Law this definition concerns Indian tribes and Native Hawaiian organization. | USA Congress (1990) |
| 175. | **Культурна спадщина**<br><br>це успадкована з минулого сукупність ресурсів, яку люди, незалежно від форм власності, визначають як відображення та вираження своїх цінностей, які | **Cultural heritage**<br><br>is a group of resources inherited from the past which people identify, independently of ownership, as a reflection and expression of their constantly evolving values, beliefs, knowledge and traditions. | COE (2005). – p.2 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | постійно еволюціонують, вірувань, знань та традицій.<br><br>Вона включає в себе всі аспекти навколишнього середовища, що є результатом взаємодії між людьми та місцевостями (місцями) у часі. | It includes all aspects of the environment resulting from the interaction between people and places through time. | |
| 176. | **Культурна травма -**<br><br>є культурно інтерпретованою раною самої культурної текстури суспільства.<br><br>Унаслідок стрімких, радикальних соціальних змін "подвійність культури" проявить себе у своєрідній формі: травматичні події, які самі по собі мають значення та наділенні смисловим навантаженням членами колективу, можуть порушити наявне семантичне поле.<br><br>Якщо виникає порушення, символи починають означати щось інше, ніж зазвичай; цінності нівелюються, або вимагають нездійсненних цілей; норми прописують дії, що не можливо втілити; жести та слова втрачають свої первинні значення; переконання спростовуються, віра нівелюється, довіру порушено; харизма руйнується, кумири (ідоли) зазнають краху.<br><br>Культурна травма включає такі симптоми: аномія, цивілізаційна некомпетентність, колективна вина, колективна ганьба, синдром недовіри, криза ідентичності, криза легітимності, культурне відставання та соціальна напруга. | **Cultural trauma** –<br><br>Is culturally interpreted wound to cultural tissue itself.<br><br>In the aftermath of rapid, radical social change the ‘duality of culture’ will manifest itself in a peculiar way: traumatizing events that are themselves meaningful, endowed with meaning by the members of the collectivity, may disturb the very same universe of meanings.<br><br>If a disturbance occurs, the symbols start to mean something other than they normally do; values become valueless, or demand unrealizable goals; norms prescribe unfeasible actions; gestures and words signify something different from what the meant before; belief are refuted, faith undermined, trust breached; charisma collapses, idols fall.<br><br>Cultural trauma includes the following symptoms: anomie, civilization incompetence, collective guilty, collective shame, distrust syndrome, crisis of identity, legitimation crisis, cultural lag and social friction. | Sztompka (2000) – p.458 - 459 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 177. | **Культурний геноцид**<br><br>підкатегорія або аспект геноциду - спроби системного та навмисного знищення групи - поряд із фізичним геноцидом та біологічним геноцидом. Він охоплює руйнування як матеріальних (наприклад, культові споруди), так і нематеріальних (наприклад, мова) культурних структур. | **Cultural genocide**<br><br>is a sub-category, or aspect, of genocide – the attempt to systemically and wilfully destroy a group – alongside physical genocide and biological genocide. It denoted the destruction of both tangible (such as places of worship) as well as intangible (such as language) cultural structures. | Bilsky & Klagsbrun (2018) – p.374 |
| 178. | **Культурний контент**<br><br>символічне значення, художній вимір та культурні цінності, що походять з культурних ідентичностей чи виражають їх. | **Cultural content**<br><br>the symbolic meaning, artistic dimension and cultural values that originate from or express cultural identities. | UNESCO (2019) – p.7 |
| 179. | **Культурні цінності**<br><br>**т**ермін, який охоплює три аспекти. Конвенція про захист культурних цінностей у разі збройного конфлікту (Гаага, 1954) визначають культурні цінності як:<br><br>(a) цінності, рухомі чи нерухомі, які мають велике значення для культурної спадщини кожного народу, такі як пам'ятники архітектури, мистецтва або історії, релігійні або світські, археологічні розташування, архітектурні ансамблі, визначені як такі, що представляють історичний або художній інтерес, твори мистецтва, рукописи, книги, інші предмети художнього, історичного чи археологічного значення, а також наукові колекції або важливі колекції книг, архівних матеріалів | **Cultural property**<br><br>the term includes three aspects. The Convention for the Protection of Cultural Property in the Event of Armed Conflict (The Hague, 1954) defines the cultural property as:<br><br>(a) movable or immovable property of great importance to the cultural heritage of every people, such as monuments of architecture, art or history, whether religious or secular; archaeological sites; groups of buildings which, as a whole, are of historical or artistic interest; works of art; manuscripts, books and other objects of artistic, historical or archaeological interest; as well as scientific collections and important collections of books or archives or of reproductions of the property defined above; | UNESCO (1954) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | або репродукцій цінностей, зазначених вище;<br><br>(b) будівлі, головним і дійсним призначенням яких є збереження або експонування рухомих культурних цінностей, зазначених у пункті (a), такі як музеї, великі бібліотеки, сховища архівів, а також укриття, призначені для збереження в разі збройного конфлікту рухомих культурних цінностей, зазначених у пункті (a);<br><br>(c) центри, в яких є значна кількість культурних цінностей, зазначених у пунктах (a) і (b), так звані «центри зосередження культурних цінностей». | (b) buildings whose main and effective purpose is to preserve or exhibit the movable cultural property defined in sub-paragraph (a) such as museums, large libraries and depositories of archives, and refuges intended to shelter, in the event of armed conflict, the movable cultural property defined in sub-paragraph (a);<br><br>(c) centers containing a large amount of cultural property as defined in sub-paragraphs (a) and (b), to be known as `centers containing monuments'. | |

## Л

| № | UA | EN | Джерело |
|---|---|---|---|
| 180. | **Лідери думок**<br><br>люди, які мають суттєвий вплив на думки чи поведінку інших у неформальних соціальних взаєминах. Визначальні характеристики змінюються відповідно до “теми” впливу та соціального оточення, однак у будь-якій ситуації такі люди, зазвичай, краще поінформовані й більше користуються мас-медіями та іншими джерелами, вони товариські, їх поважають ті, на кого вони впливають. | **Opinion leaders**<br><br>persons who influence the thinking or behaviour of others in informal social relationships. The identifying characteristics vary according to the ‘topic’ of influence and social setting, but the people concerned are generally better informed, make more use of mass media and other sources, are gregarious and are likely to be respected by those they influence. | McQuail's, D. (2010) – p. 565 |
| 181. | **Луна-камери**<br><br>явище, яке використовується для *Когнітивному Зламу*.<br><br>Органічно створені підгрупи, в яких люди спілкуються лише з людьми подібних думок. Луна-камери існують як в Інтернеті, так і в реальному житті. Наприклад, виборці політичної партії можуть звертатися до тієї самої газети за інформацією, спілкуватися переважно з однолітками з подібного походження та брати участь у розмовах на форумах з людьми подібної політичної орієнтації. Таким чином, вони рідко піддаються ідеологічно протилежним думкам. Це може бути використано для зміцнення та поширення певної інформації до певних груп людей.<br><br>Див. також *Бульбашки Фільтрів* | **Echo Chambers**<br><br>a phenomenon that is used in *Cognitive Hacking*.<br><br>Organically created sub-groups in which people only engage with others of similar opinions. Echo chambers exist both online and in real life. For example, voters for a political party may turn to the same newspaper for information, socialise predominately with peers from backgrounds like theirs, and engage in conversations on forums with people of a similar political orientation. Thus, they are rarely exposed to ideologically contradicting opinions. This can be exploited to reinforce and spread certain information to specific groups of people.<br><br>See also *Filter Bubbles* | MSB (2018) – p.19-20 |

## M

| № | UA | EN | Джерело |
|---|---|---|---|
| 182. | **Маніпуляція**<br><br>(1) у психології: це приховане управління людьми та їх поведінкою. Різновид соціального впливу, який використовується для зрушень у свідомості та волі людини, щоб впровадити в її психіку установки маніпулятора, які не збігаються з актуальними потребами цієї людини<br><br>(2) є одним із методів *Дезінформації*.<br><br>додавання, видалення або зміна змісту тексту, фото, відео чи аудіо для передачі іншого (зміненого) повідомлення. | **Manipulation**<br><br>(1) in Psychology: This is the covert control of people and their behavior. It is a type of social influence used to shift a person's consciousness and will, in order to implant the manipulator's attitudes into their psyche, which do not align with the actual needs of the person.<br><br>(2) is one of the *Disinformation* methods.<br><br>adding, removing or changing the content of text, photo, video or audio to communicate a different message. | MSB (2018) – p.19, 25 |
| 183. | **Маріонетка**<br><br>Є одним із інструментів *Технічного Використання*.<br><br>акаунти-самозванці, якими керує особа, що не розкриває свою справжню ідентичність чи наміри. Ці неправдиві дані використовуються для приєднання до Інтернет-спільнот та участі в дебатах та виступають як "фронти" для введення неправдивої або суперечливої інформації. Два або більше маріонетних акаунти можуть використовуватися разом для моделювання обох сторін дискусії. | **Sock Puppet**<br><br>Is one of the *Technical Exploitation* tools.<br><br>imposter accounts managed by a person who does not reveal their real identity or intentions. These false identities are used to join online communities and participate in debates, and act as ‘fronts’ for introducing false or controversial information. Two or more sockpuppet accounts can be used in conjunction to simulate both sides of a debate. | MSB (2018) – p.19, 23 |
| 184. | **Медіаграмотність** | **Media literacy** | |

| № | UA | EN | Джерело |
|---|---|---|---|
| | забезпечення гарантування того, що будь-яка особа, яка стикається з інформацією, може оцінити її достовірність (аргументи, докази) та її джерело (надійність, мотивації).<br><br>Це здатність до дій, зокрема:<br>- отримати доступ до відповідної та точної інформації за допомогою засобів масової інформації (далі – ЗМІ ) у різних формах;<br>- критично аналізувати контент ЗМІ та вплив їх різних форм;<br>- оцінити вичерпність, актуальність, достовірність, авторитет та точність інформації;<br>- приймати освічені (свідомі) рішення на основі інформації, отриманої із ЗМІ та цифрових джерел;<br>- використовувати різні форми технологій та цифрові інструменти;<br>- аналізувати як використання ЗМІ та технологій може вплинути на приватне та суспільне життя. | the idea is to ensure that any person faced with a piece of information can assess its validity (arguments, evidence) and its source (reliability, motivations).<br><br>The ability to the following actions:<br>- to access relevant and accurate information through media in a variety of forms;<br>- critically analyze media content and the influences of different forms of media;<br>- evaluate the comprehensiveness, relevance, credibility, authority, and accuracy of information;<br>- make educated decisions based on information obtained from media and digital sources;<br>- operate various forms of technology and digital tools;<br><br>and reflect on how the use of media and technology may affect private and public life. | Vilmer et al. (2018) - p.178<br><br>USA Congress (2019) – sec.3, # 5 |
| 185. | **Медіатизація**<br><br>концепція про необхідність пристосування політичної діяльності до логіки ЗМІ. | **Mediatisation**<br><br>the concept about the necessity to adjust political activity to media logic. | Szwed (2016) – p. 16 |
| 186. | **Меми**<br><br>оцифровані одиниці інформації (текст, зображення, фільм, звук), які копіюються, обробляються і в цій обробленій формі повторно публікуються в Інтернеті; інструмент *Гібридного Впливу*. | **Memes**<br><br>digitalized units of information (text, image, film, sound) that are copied, processed and in this processed form, re-published on the Internet; a *Hybrid Influence* tool. | Szwed (2016) – p.9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 187. | **Ментальне здоров'я**<br><br>це такий стан людини, який існує у складному континуумі, з переживаннями, що варіюються від оптимального стану благополуччя до виснажливих станів сильного страждання та емоційного болю. Ризики для психічного здоров'я та його захисні фактори у суспільстві проявляються на різних рівнях. Локальні загрози підвищують ризик для окремих осіб, родин та громад. Глобальні загрози підвищують ризик для цілих груп населення і можуть сповільнити світовий прогрес на шляху до покращення добробуту. У цьому контексті ключовими загрозами сьогодні є: економічні спади і соціальна поляризація; надзвичайні ситуації у сфері охорони здоров'я; широкомасштабні гуманітарні надзвичайні ситуації і вимушене переміщення населення; кліматична криза та інші. Захисні фактори психологічного здоров'я розвиваються протягом усього нашого життя і слугують для зміцненню життєстійкості особи. Вони включають наші індивідуальні соціальні та емоційні навички, якості, а також позитивні соціальні взаємодії, якісну освіту, гідну роботу, безпечні райони і згуртованість громади, тощо. | **Mental health**<br><br>is such a condition of a person that exists on a complex continuum, with experiences ranging from an optimal state of well-being to debilitating states of great suffering and emotional pain. Mental health risks and protective factors can be found in society at different scales. Local threats heighten risk for individuals, families and communities. Global threats heighten risk for whole populations and can slow worldwide progress towards improved well-being. In this context, key threats today include: economic downturns and social polarization; public health emergencies; idespread humanitarian emergencies and forced displacement; and the rowing climate crisis. Protective factors similarly occur throughout our lives and serve to strengthen resilience. They include our individual social and emotional skills and attributes as well as positive social interactions, quality education, decent work, safe neighbourhoods and community cohesion, etc. | WHO (2022) |
| 188. | **«Мертва вода»**<br><br>Приклад теорії змови, фундатори якої стверджують, що усі біди росії почалися з прийняттям | **"Dead Water" (or “Mertvaya voda”)**<br><br>The conspiracy theory, which argues that all Russia’s woes began with the adoption of Christianity, specifically, | Soldatov & Borogan (2022) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | християнства, а саме «іудейського християнства», нав'язаного євреями. | "Judaic Christianity", imposed by the Jews. | |
| 189. | **Мислення бойове**<br>стан мислення, що забезпечує виживання під час критичного інциденту. Він складається з кількох компонентів: усвідомлення ситуації, концентрації, передбачення, урівноваженості та збереження кмітливості. Суть бойового мислення - самоконтроль емоцій і тіла. Бойовий спосіб мислення також описується як «настрій виживання», «бойовий дух», «психічна міцність», «молитва в моменти небезпеки», «сталеві нерви» або «настрій переможця». | **Combat mindset**<br>a state of mind that ensures one's survival during a critical incident. It is composed of several components: situational awareness, concentration, anticipation, level headedness, and the maintenance of dexterity. The essence of a combat mindset is self-control of the emotions and of the body. A combat mindset is also described as a "survival mindset", "fighting spirit", "mental toughness", "grace under fire", "nerves of steel" or a "winning mindset". | Boe et al. (2020) |
| 190. | **Міжкультурність**<br>наявність та рівноправна взаємодія різноманітних культур та можливість генерувати спільні форми прояву культури шляхом діалогу та взаємоповаги | **Interculturality**<br>the existence and equitable interaction of diverse cultures and the possibility of generating shared cultural expressions through dialogue and mutual respect | UNESCO (2019) – p.8 |
| 191. | **Міжнародна безпека**<br>система міжнародних відносин, що заснована на дотриманні усіма державами загальновизнаних принципів і норм міжнародного права, виключає вирішення спірних питань і розбіжностей між ними за допомогою сили або загрози. | **International security**<br>the system of international relations, based on compliance with generally accepted international law principles and rules by all countries, which excludes settlement of disputable issues and disagreements between them using force or threat. | Horbulin (2017) – p.158 |
| 192. | **Міжнародна криза**<br>соціальна та культурна конструкція, яку створюють | **International crisis**<br>crises more generally, are social, and specifically cultural, constructions. ... | Weldes (1999) – p.37 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | державні чиновники в процесі формування та відтворення національної ідентичності (унаслідок чого можуть виникати непередбачувані ситуації, проявлятися нові або приховані раніше конфлікти на міжнародному рівні). | crises are social constructions that are forged by state officials in the course of producing and reproducing state identity. | |
| 193. | **Міжнародне гуманітарне право**<br>набір правил, спрямованих на обмеження наслідків збройного конфлікту з міркувань гуманності. Воно захищає осіб, які не беруть або більше не беруть участь у військових діях, і обмежує засоби та методи ведення війни. Сфера дії обмежена з точки зору матеріальних наслідків збройного конфлікту. | **International humanitarian law**<br>a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities, and restricts the means and methods of warfare. Its scope is, therefore, limited ratione materiae to situations of armed conflict. | UN (2011) – p.5 |
| 194. | **Міжнародне мовлення**<br>спроба актора керувати міжнародним середовищем за допомогою технологій радіо, телебачення та Інтернету для взаємодії з іноземними фігурантами. | **International broadcasting**<br>an actor's attempt to manage the international environment by using the technologies of radio, television and Internet to engage with foreign publics | Cull (2009) – p.21 |
| 195. | **Мікротаргетинг**<br>1) мікро-націлювання з підвищеною точністю, завдяки якій населення сегментоване на цільові групи.<br>Див. також: *Бульбашки Фільтрів, Інтернет-Кокон*<br>2) Поєднання кількох технологій (великі дані, IoT, мікророботи тощо) з метою відстеження та усунення (цільових) осіб. | **Micro-targeting**<br>1) the increased precision with which the population is segmented and targeted.<br>see also: *Filter Bubbles, Internet-Cocooning*<br>2) Micro-targeting: The combination of several technologies (Big Data, IoT, Micro-robots etc.) in order to track, trace and eliminate (target) individuals. | Vilmer et al. (2018) - p.39<br>Bekkers et al. (2019) – p.27 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Приклади "гібридних" застосувань: використання бойових роботів для усунення конкретних людей або груп. | Examples of hybrid applications: employing slaughter bots and use these to eliminate specific persons or groups. | |
| 196. | **Мова ненависті**<br>текст, який погрожує, ображає або нападає на людину чи групу на основі національного походження, етнічної приналежності, раси чи релігії. | **Hate Speech**<br>text that threatens, insults or attacks a person or group on the basis of national origin, ethnicity, race or religion. | Szwed (2016) – p.10 |
| 197. | **Модель CORE**<br>Модель комплексної екосистеми стійкості<br>це системне представлення демократичного суспільства в цілому. Вона використовується для аналізу і, зрештою, протидії гібридним загрозам, які прагнуть підірвати і завдати шкоди цілісності та функціонуванню демократій, змінити процеси прийняття рішень і створити каскадні ефекти. | **CORE model**<br>Comprehensive resilience ecosystem model<br>is a systemic representation of democratic society as a whole. It is used to analyse and ultimately counteract hybrid threats that seek to undermine and harm the integrity and functioning of democracies, change decision-making processes, and create cascading effects. | Jungwirth et al. (2023) – p.8 |
| 198. | **Моніторинг (як спосіб виявлення гібридних загроз)**<br>процес сканування навколишнього середовища на наявність "*Відомих Невідомих*" – зазвичай за допомогою індикаторів – для пошуку упередженої інформації про можливі гібридні атаки.<br>Спосіб управління проблемою "*Відомих Невідомих*" (на відміну від *Виявлення*). | **Monitoring (as a way to detect hybrid threats)**<br>a process of scanning the environment for "*Known Unknowns*" – usually with the aid of indicators – to look for a set of preconceived information about possible hybrid warfare attacks.<br>A way to manage the problem of "*Known Unknowns*" (by contrast of *Discovery*). | MCDC(a) (2019) – p.26 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 199. | **Моральна паніка**<br><br>уперше цей термін ужив криміналіст Джон Янґ стосовно раптових виявів часто ірраціональної масової тривоги та страху через гадані "хвилі злочинності" або інші нібито докази безладу і соціальних лих (наприклад, розпусту чи імміграцію). Медії розглядають у цьому контексті через їхню схильність посилювати ці страхи. Деколи вони самі є об'єктом такої паники, зокрема коли раптово наростає тривога щодо їхнього шкідливого впливу (наприклад, у вигляді хвиль злочинності, самовбивств або заколотів). Нові медії, зокрема комп'ютерні ігри та інтернет, схильні спричинювати деяку паніку стосовно шкоди, якої, як підозрюють, вони завдають своїм (юним) користувачам. | **Moral panic**<br><br>the term was first applied by the criminologist Jock Young to sudden expressions of often irrational mass anxiety and alarm directed at 'crime waves' or other supposed evidence of disorder and social breakdown (including promiscuity and immigration). The media are implicated through their tendency to amplify such 'panics'. They are also sometimes objects of moral panics, when alarm at their harmful effects suddenly gains currency (e.g. in the form of crime waves, suicides or rioting). New media, such as computer games and the Internet, tend to generate some degree of panic at alleged harm to their (young) users. | McQuail's (2010) – p. 564 |
| 200. | **М'яка сила**<br><br>здатність впливати на інших для досягнення бажаних результатів через залучення, а не примус чи оплату. | **Soft power**<br><br>the ability to affect others to obtain the outcomes one wants through attraction rather than coercion or payment. | Simons (2015) – p.2 |
| 201. | **МПЕСІ**<br><br>Це абревіатура, що поєднує спектр *інструментів сили*, які використовуються *акторами / гравцями гібридних загроз*:<br><br>• Мілітарні, тобто *військові інструменти гібридних загроз*<br><br>• *Політичні інструменти гібридних загроз* | **MPECI**<br><br>This is an acronym that combines the spectrum (set) of *Instruments of power* used by *actors of hybrid threats*:<br><br>• *Military instruments of hybrid threats*<br><br>• *Political instruments of hybrid threats* | MCDC (2017) – p.4, 9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | • *Економічні інструменти гібридних загроз*<br>• Соціальні, тобто *громадянські інструменти гібридних загроз*<br>• *Інформаційні інструменти гібридних загроз* | • *Economic instruments of hybrid threats*<br>• *Civil instruments of hybrid threats*<br>• *Information instruments of hybrid threats* | |

## Н

| № | UA | EN | Джерело |
|---|---|---|---|
| 202. | **Набір інструментів для кібердипломатії**<br><br>"Спільна дипломатична відповідь ЄС" як різноманітний пул крос-доменних варіантів для боротьби із "зловмисною кібердіяльністю різного розмаху, масштабу, тривалості, інтенсивності, складності, витонченості та впливу." | **Cyber diplomacy toolbox**<br><br>“joint EU diplomatic response” as a diverse pool of cross domain options to deal with “malicious cyber activities of varying in scope, scale, duration, intensity, complexity, sophistication and impact. | Council of the EU (2017) – p.3<br><br>Sweijs & Zilincik (2019) – p.21 |
| 203. | **Надлишок інформації**<br><br>явище, відоме як надмірна кількість інформації.<br><br>сприяє дезінформації, оскільки це призводить до зниження концентрації уваги, що послаблює нашу пильність і здатність обробляти контраргументи. | **Infobesity**<br><br>a phenomenon known as the overabundance of information<br><br>contributes to disinformation because it leads to decreased concentration, which weakens our vigilance and our ability to process counter-arguments | Vilmer et al. (2018) - p.39 |
| 204. | **Найгірший сценарій**<br><br>це концепція про найнеприємніше, що може статися в ситуації. Вона може стосуватися будь-якої ситуації або висновку; найгірш можливого результату. Це - також концепція у плануванні на випадок потенційних катастроф, що розглядає найгірший результат, який можна обґрунтовано спрогнозувати у конкретній ситуації. | **The worst-case scenario**<br><br>it is a concept about the most unpleasant thing that could happen in a situation. It can concern any situation or conclusion which could not be any worse; the worst possible outcome. It is a concept in planning for potential disasters, considers the most severe possible outcome that can reasonably be projected to occur in a given situation. | Kalenský et al., (2024) |
| 205. | **Напад**<br><br>один із методів *Риторики Викривлення*. | **Hijacking**<br><br>is one of the *Malign Rhetoric* methods. | MSB (2018) – p.19, 26 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Втручання в існуючу дискусію шляхом зміни її мети чи теми. Особливо ефективний при застосуванні хештегов, мемів, подій або контркультурних соціальних рухів. | Contributing to an existing debate by taking it over and changing the purpose or topic. Particularly effective when applied to hashtags, memes, events or counter-cultural social movements. | |
| 206. | **Національні інтереси**<br>життєво важливі потреби людини, суспільства та держави, реалізація яких забезпечує державний суверенітет та добробут держави, її прогресивний демократичний розвиток. | **National interests**<br>the vital needs of a person, society and state. Their implementation ensures state sovereignty and welfare of a state, it's progressive democratic development. | Horbulin (2017) – p.158 |
| 207. | **Національні цінності**<br>основоположні матеріальні, інтелектуальні та духовні надбання народу, визначальні умови існування та розвитку людини, суспільства та держави. | **National values**<br>the basic material, intellectual and cultural heritage of people, key conditions of existence and development of a person, society and state. | Horbulin (2017) – p.158 |
| 208. | **Небезпека у міжнародних відносинах**<br>наявність реальних загроз міжнародній безпеці, проти яких немає адекватних контрзаходів. | **dangers in international relations**<br>insecurity (threats against which no adequate countermeasures are available) | Buzan et al. (1998) - p.4 |
| 209. | **Невідомі невідомі**<br>змінні, які належать до способів гібридної атаки, про які ми навіть не обізнані щодо їх природи, нашої вразливості до них або навіть щодо нашого незнання загрози (на відміну від "*Відомі Невідомі*").<br>Цей тип інформації не піддається методології *Моніторингу*, який побудований на "сприйнятті того, що ми очікуємо сприймати" за допомогою шаблонів | **Unknown unknowns**<br>refer to modes of hybrid attack that we are not even aware of its nature, our vulnerability to it, or even of our own ignorance to the threat (by contrast " *Known Unknowns*").<br>This type of information is not amenable to a *Monitoring* methodology built upon 'perceiving what we expect to perceive' via either pattern recognition or the use of *Indicator* lists. This is because the | MCDC(a) (2019) – p.26 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | розпізнавання або використання набору *Індикаторів*. Це пов'язано з тим, що аналітик ніколи раніше не бачив цієї закономірності і не може мати набір індикаторів для того виду атаки, який раніше ніколи не мав місця або навіть не був уявним. | analyst has never seen this pattern before, and cannot be equipped with an indicator list for a type of attack that has never occurred or even been imagined before. | |
| 210. | **Невірне інформування**<br>ненавмисне поширення інформації, яка є повністю або частково неправдивою (на відміну від *Дезінформації*). | **Misinformation**<br>the unintentional dissemination of information that is wholly or partly false (as opposed to *Disinformation*). | Vilmer et al. (2018) - p.19 |
| 211. | **Невірне призначення**<br>є одним із методів Дезінформації.<br>Використання фактично коректного змісту, представленого в питанні, яке не належить до справи, для викривлення проблеми, події чи особи. Наприклад, у фальшивій новинній статті в якості доказу існування можуть бути використані зображення не пов'язаної з нею події. | **Misappropriation**<br>is one of the *Disinformation* methods.<br>The use of factually correct content presented on an unrelated matter to frame an issue, event or person in a deceptive way. For example, a false news article might use pictures from an unrelated event as proof of its existence. | MSB (2018) – p.19, 25 |
| 212. | **Недержавні актори гібридних загроз**<br>Суб'єкти, які відіграють важливу роль у міжнародних відносинах і мають достатню владу, щоб втручатися, впливати та спричиняти зміни без будь-якої приналежності до встановлених інститутів держави. До таких гравців можна віднести:<br>• транснаціональні загрозливі організації, зокрема, - джихадистські терористичні | **Non-state actors of hybrid threats**<br>Constitute entities that play a part in international relations and that exercise sufficient power to interfere, influence and cause change without any affiliation to the established institutions of a state. Such players include:<br>• transnational threat organizations, particularly jihadist terrorist groups—are actively competing against the United | Cullen et al. (2021) – p.22 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | групи, які активно змагаються проти США (такі як Хезболла, Аль-Каїда, ІДІЛ),<br>• проксі-актори,<br>• транснаціональні організовані злочинні синдикати,<br>• прибуткові «незалежні» актори<br>• ідеологічні рухи тощо.<br><br>Є одним з елементів *Концептуальної моделі гібридних загроз,* відносятся до групи *Актори / гравці гібридних загроз* | States (like Hezbollah, Al-Qaeda, and ISIL),<br>• proxy actors,<br>• transnational organized crime syndicates,<br>• profit-making “freelance” actors<br>• ideological movements etc.<br><br>Is one of the elements of the *Conceptual model of hybrid threats*, refers to a group *Actors of hybrid threats* | |
| 213. | **Нелетальні психологічні операції з використанням соціальних мереж**<br><br>формування суспільної поведінки за допомогою використання "динамічних наративів" для боротьби з політичною пропагандою яка поширюється терористичними організаціями. | **Non-lethal psychological operations using social networks**<br><br>shaping public behavior through the use of “dynamic narratives” to combat the political propaganda disseminated by terrorist organizations | Bradshaw & Howard (2017) – p.4 |
| 214. | **Нелінійність**<br><br>властивість, яка характеризує непередбачувані (які не є причинно-лінійними) наслідки атак гібридної війни. Вони (наслідки) є результатом синергетичної взаємодії гібридних атак, в яких ціле є більшим, ніж сума його частин. Нелінійні ефекти не завжди можуть бути передбачені зловмисником або захисником. | **Non-linearity**<br><br>a property that characterizes the unpredictable effects of hybrid warfare attacks that are not causally linear. They are the result of synergistic interactions of hybrid warfare attacks in which the whole is greater than the sum of their parts. Non-linear effects cannot always be predicted by the attacker or defender. | MCDC(a) (2019) – p.90 |
| 215. | **Неоднозначність**<br><br>властивість, що є характерною для ворожої гібридної дії, яку державі важко визначити за певною ознакою або публічно визначити як | **Ambiguity**<br><br>a characteristic of hostile hybrid action that is difficult for a state to identify attribute or publicly define as coercive uses of force. Ambiguity is | MCDC (2017) – p.31 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | умисне застосування сили. Використовується для ускладнення або підриву процесів прийняття рішень опонентом. Також використовується для ускладнення будь-якого типу відповіді. У військовій сфері розробляється таким чином, щоб знизитись за поріг війни та де-легітимізувати або зробити ірраціональною здатність відповідати із застосуванням військової сили. | used to complicate or undermine the decision-making processes of the opponent. It is tailored to make any type of response difficult. In military terms, it is designed to fall below the threshold of war and to delegitimize or render irrational the ability to respond with the use of military force. | |
| 216. | **Непрозорі алгоритми**<br><br>(в контексті штучного інтелекту)<br><br>Такий набір інструкцій та правил, які використовуються комп'ютерною програмою, але не дозволяє пояснити, чому ШІ прийшов до конкретного рішення<br><br>*штучний інтелект* у його нинішньому вигляді досі є досить вразливою технологією, схильною до отруєння та маніпуляцій з даними з боку зловмисників. Він цілком може зазнати невдачі, зіткнувшись із завданнями чи середовищами, відмінними від тих, для яких він навчався. | **Opaque algorithms**<br><br>(in the context of artificial intelligence)<br><br>Such a set of instructions and rules used by a computer program, but does not allow to explain why the AI came to a particular decision<br><br>*artificial intelligence* in its present shape is still a fairly vulnerable technology – susceptible to training data poisoning and manipulation by adversarial actors. It may well fail when confronted with tasks or environments different from those it was trained for. | Thiele (a) (2020) – p.11 |
| 217. | **Нова модель внутрішнього контролю над росією**<br><br>Ця модель є теоретичним підгрунттям *російського стратегічного мислення*. Автор моделі – Володимир Лепський.<br><br>Основою моделі є уточнення набору визначених цінностей та ідей, які були б розумними при зіткненні з викликами Заходу | **New model for controlling Russia internally**<br><br>This model is the theoretical basis for *Russian strategic thinking*. The author of the model is Vladimir Lepskiy.<br><br>The basis of the model is clarifying a set of specified values and ideas, which would be prudent in the face of challenges from the West | Cullen et al. (2021) – p.19 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | (економічними і технологічними), оскільки суб'єкти (населення) стануть єдиною масою із загальною свідомістю та баченням майбутнього розвитку. Концепти, на яких базується модель: *полісуб'єкт, російськість, антизахідництво, великодержавність* | (economic and technological), as the subjects (the population) would be a coherent mass with a shared mindset and vision of future development. Concepts on which the model is based: *polisubjekt, russianness, anti-westernism, greatpowerness* | |
| 218. | **Нові ЗМІ** (нові засоби масової інформації, нові мас медіа)<br>соціальні медіа, керовані "аматорами"; в кінцевому підсумку вони можуть виконувати ті самі функції, що й звичайні журналісти, але з більш особистою та менш регульованою відповідальністю (на відміну від *Традиційних Засобів Масової Інформації*). | **New Mass Media**<br>the social media run by 'amateurs' who ultimately may fulfil the same functions as regular journalists but with more personal and less regulated responsibility. (by contrast of the *Traditional Mass Media*). | Robbin & Buente (2008) – p.2214 – 2215 (p.5 – 6)<br>Szwed (2016) – p. 12 |

## О

| № | UA | EN | Джерело |
|---|---|---|---|
| 219. | **Обмеження рамками** – див. *Фреймінг* | **Framing** | |
| 220. | **Озлоблення**<br><br>один із способів поєднання методів інформаційного впливу (див. *Кампанії впливу*).<br><br>Ярість використовується у делікатних питаннях на публічних дебатах. Ця комбінація використовує *Когнітивний Злам*, *Оманливу Ідентичність* та *Риторику Викривлення* для залучення простих громадян, посилаючись на їх емоційне відношення до певної проблеми. | **Enraging**<br><br>one of the ways to combine of information influence techniques (see *Influence Campaigns*).<br><br>Enraging takes advantage of sensitive issues in public debate. This combination utilizes *Cognitive Hacking*, *Deceptive Identities* and *Malign Rhetoric* to engage ordinary citizens by invoking their emotional relationship to a specific issue. | MSB (2018) – p.29 |
| 221. | **Окупована територія**<br><br>територія, що фактично перебуває під владою ворожих іноземних збройних сил. Окупація поширюється лише на територію, де така влада встановлена і може здійснюватися. Тому територія держави може бути частково окупованою, і в цьому випадку закони та зобов'язання окупації застосовуються лише на території, яка фактично окупована. | **Occupied territory**<br><br>actually placed under the authority of the adverse foreign armed forces. The occupation extends only to the territory where such authority has been established and can be exercised. A State's territory may therefore be partially occupied, in which case the laws and obligations of occupation apply only in the territory that is actually occupied. | Bouvier (2020) - p. 28. |
| 222. | **Оманливі ідентичності**<br><br>є одним із методів інформаційного впливу (див. *Кампанії Впливу*)<br><br>Ми часто оцінюємо достовірність інформації, виходячи з її джерела. Хто зі мною розмовляє і чому? Що вони знають про цю проблему? | **Deceptive Identities**<br><br>is one of the information influence techniques (see *Influence Campaigns*)<br><br>We often evaluate the credibility of information by looking at its source. Who is talking to me and why? What | MSB (2018) – p.19, 21 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Вони - саме такі, якими видаються? Імітуючи законні джерела інформації (чи то особи, організації або платформи), учасники діяльності, що займаються інформаційним впливом, експлуатують довіру до месенджера, використовуючи оманливі ідентичності.<br><br>Сюди відносять*: Шиллінг, Імітатори та самозванці, Підробки, Потьомкінські села, Фейкові медіа* тощо. | do they know about the issue? Are they who they claim to be? By imitating legitimate sources of information (be it persons, organizations or platforms), actors engaged in information influence activities exploit trust in the messenger by utilizing deceptive identities.<br><br>it includes: *Shilling, Impersonators & Impostors, Forgeries, Potemkin Villages, Fake Media* etc. | |
| 223. | **Оперативна сумісність**<br><br>це здатність ефективно та результативно діяти разом із метою досягнення тактичних, оперативних та стратегічних цілей Північноатлантичного Аьянсу (НАТО). | **Interoperability**<br><br>the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives. | NSA (2013) – p. 2-I-8 |
| 224. | **Операції зі стабілізації**<br><br>різні військові місії, завдання і заходи, що проводяться для підтримки або відновлення безпечного і надійного середовища, забезпечення необхідних державних послуг, реконструкції критичної інфраструктури, а також гуманіторної допомоги. | **Stabilization operations**<br><br>the different military missions, actions and activities, undertaken to support or restore safety and stability, ensure the provision of essential public services and humanitarian aid, as well as reconstruction of critical infrastructure. | Horbulin (2017) – p.159 |
| 225. | **Опорність (резистентність)**<br><br>здатність системи чинити опір зовнішнім впливам або загрозам, функціонувати при підвищених навантаженнях. Одна зі складових *Стійкості* | **Resistance**<br><br>ability to resist external influences or threats and function under increased loads. One of the components of *Resilience* | Gryshko et al. (2024) |

| № | UA | EN | Джерело |
|---|---|---|---|
| 226. | **“Отруєння хештегами”**<br>використання хештегів, "поведінка" яких схожа на спам, щоб зруйнувати критику або інші небажані дискусії через потік не пов’язаних твітів | **“Hashtag Poisoning”**<br>using the spam trending hashtags to disrupt criticism or other unwanted conversations through a flood of unrelated tweets | Bradshaw & Howard (2017) – p.9 |

## П

| № | UA | EN | Джерело |
|---|---|---|---|
| 227. | **Пакети синхронізованих атак (SAPs)**<br><br>Конкретний МПЕСІ- набір інструментів сили (мілітарні, політичні, економічні, соціальні, інформаційні), який синхронізований та пристосований до конкретних вразливостей, які використовуються в атаках гібридної війни.<br><br>Див. також: *Синхронізація Засобів* | **Synchronized attack packages (SAPs)**<br><br>specific set MPECI-instruments of power (Military, Political, Economic, Civil, Information), means that are synchronized and tailored to specific vulnerabilities that are used in a hybrid warfare attack.<br><br>See also: *Synchronization of Means* | MCDC (2017) – p.32<br><br>MCDC(a) (2019) – p.90 |
| 228. | **Пакт Молотова – Ріббентропа про ненапад (Пакт Гітлера-Сталіна)**<br><br>Один з наративів кремля<br><br>пакт про ненапад між нацистською Німеччиною та СРСР (1939 р.), який розділяє Центрально-Східну Європу на німецьку та радянську зони впливу. Російська пропаганда представляє це як велике досягнення радянської дипломатії, яким росіяни можуть пишатися.<br><br>Подання вочевидь агресивного договору як виправданого оборонного заходу свідчить про те, що превентивне застосування сили проти інших держав можна розглядати як законний засіб переслідування національних інтересів та зміцнення власної безпеки.<br><br>Резолюція Європарламенту 2019 позначила Пакт Молотова – Ріббентропа як безпосередню | **Molotov–Ribbentrop Non-Aggression Pact (Hitler-Stalin Pact)**<br><br>one of the Kremlin narratives,<br><br>non-aggression pact between Nazi Germany and the USSR (1939), which dividing Central-Eastern Europe into German and Soviet zones of influence. Russian propaganda presents it as a great achievement of Soviet diplomacy which Russians can be proud of.<br><br>The depiction of a patently aggressive treaty as a justified defensive measure suggests that preventive use of force against other states can be regarded as a legitimate means of pursuing national interests and strengthening one's own security.<br><br>The 2019 European Parliament's resolution labelled the Molotov–Ribbentrop Pact as an immediate cause of the outbreak of the Second World War | Domańska (2019) – p.5<br><br>European Parliament (2019 ) – p.3 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | причину початку Другої світової війни | | |
| 229. | **Переконливість стримування**<br>воля здійснювати дії, які вимагають витрат від супротивника<br>Один із "*трьох С" – компонентів стримування*. | **Credibility of deterrence**<br>the will to carry out actions that impose costs on the adversary<br>One of the *'three Cs' of deterrence* | MCDC(a) (2019) – p.35 |
| 230. | **Перехід на особистості**<br>(лат. - "аргумент, спрямований на людину") - напад, дискредитація та висміювання особи, яка стоїть за аргументом, для примушення особи до мовчання, стримування чи знеохочення.<br>Один з методів *Риторики Викривлення.* | **Ad Hominem**<br>attacking, discrediting and ridiculing the person behind an argument to silence, deter or discourage.<br>Is one of the *Malign Rhetoric* methods. | MSB (2018) – p.19, 26 |
| 231. | **Підробки**<br>метод, який використовується в *Оманливих Ідентичностях*.<br>являє собою фабрикування офіційних документів.<br>Це ефективний спосіб зробити дезінформацію справжньою. Наприклад, підроблені заголовки листів, штампи чи підписи можуть бути використані для виготовлення підробленої документації. | **Forgeries**<br>a method that is used in *Deceptive Identities.*<br>Fabricating official documents is an effective way of making disinformation appear authentic. For example, fake letter heads, stamps or signatures can be used to produce forged documentation. | MSB (2018) – p.19, 20 |
| 232. | **Підтверджувальна упередженість**<br>психологічне явище: ми схильні надавати перевагу інформації, яка підтверджує наші пущення, підтримує наші позиції і не ображає наші відчуття. | **Confirmation Bias**<br>the psychological phenomenon: we tend to favor information that confirms our preexisting assumptions, supports our positions and does not offend our sensibilities. | Vilmer et al. (2018) - p.31 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 233. | **Планування на оперативному рівні**<br><br>це рівень управління, на якому кампанії та основні операції плануються, поводяться та підтримуються з метою досягнення стратегічних цілей в театрі або в районах проведення операцій.<br><br>Довідково: Найкращий англійський термін, що вживається для визначення поняття планування операцій на оперативному рівні – це «планування на оперативному рівні». Термін «оперативне планування» може бути сплутаний із терміном «планування операцій». | **Operational-level planning / operational planning**<br><br>level at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objective within theatres or areas of operations.<br><br>Note: The preferred English term to designate the planning of military operations at the operational level is “operational level planning”. The term “operational planning” is not to be used so as to prevent confusion with “operations planning”. | NSA (2013) – p. 2-O-3 |
| 234. | **"Плюралістичне невігластво"**<br><br>явище, коли люди мають хибне враження про те, що інші думають з різних питань. Явище виникає, коли люди невірно уявляють уподобання членів групи, до якої вони належать або прагнуть бути її частиною. Це може статися в ситуації дефіциту інформації - відсутності зв'язку між членами групи, коли у нас складається враження, що інші члени знають краще за нас і здатні використовувати суттєві аргументи в дискусії. У цій ситуації ми покладаємось на „їхні думки”, навіть якщо цих думок насправді не існує. | **‘Pluralistic Ignorance’**<br><br>a phenomenon of people having a false impression of what others think about various matters. The phenomenon occurs when people have an incorrect belief about the preferences of the members of a group they belong to or aspire to be part of. It may occur in a situation of information deficit – lack of communication between members of a group, when we have an impression that other members know better than us and are able to use substantive arguments in a discussion. In this situation, we rely on ‘their opinions’, even though those opinions do not actually exist. | Szwed (2016) – p. 39 |
| 235. | **Побудова інформації** | **Information Building** | Szwed (2016) – p.13 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | це метод і процес, за допомогою яких платні тролі намагаються створити позитивне висвітлення в Інтернеті та компенсувати негативне висвітлення відповідно до цілей інформаційної політики покровителя. | is the method and process by which paid trolls attempt to create positive coverage in the internet and offset negative coverage in line with the objectives of the patron's information policy. | |
| 236. | **"Побудова платформ"**<br><br>один із методів привнесення ідеологічного контенту.<br><br>Означає підключення кожного суб'єкта до того контенту, який бажано передати, за допомогою логічного зв'язку, наприклад: "варто пам'ятати, що ...", "це цікаві зауваження, однак, щоб розібратись в ситуації, потрібно пам'ятати, що..." тощо.<br><br>див. також *"Заїжджена Платівка"* | **'Building Platforms'**<br><br>is one of the methods of introducing ideological content.<br><br>means connecting every subject to the content one wants to communicate through the use of logical linkage between them, e.g. It is worth remembering that…, Those are interesting remarks, however, in order to understand the situation well, one has to remember that…, etc.<br><br>see also *'Broken Record'* | Szwed (2016) – p. 81 |
| 237. | **Повторення ключових наративів**<br><br>повторення раніше описаного наративу або посилення акценту на значенні тієї або іншої події. Повторення передбачає, що ЗМІ або пропагандисти розповідають про ту саму подію або наратив, але вже з новим змістом. Це один з найефективніших пропагандистських прийомів. Повторення надає правдивості інформації, незалежно від того, чи є вона насправді правдивою чи неправдивою. Використовується як один з методів привнесення ідеологічного контенту. Повторювані наративи легко перетворюються на стереотипи, | **Repetition of key narratives**<br><br>repetition of a previously described narrative, or add to, the emphasis on the meaning of that event. Mass media or propagandists recount the same event or narrative, yet the meaning may be new. It is one of the most effective propaganda techniques. Repetition makes information appear truer, regardless of whether it is actually true or false. Repeated narratives easily turn into stereotypes people may act upon. If one hears the same narrative several times and especially from different sources, they would be inclined to believe it no matter whether it's true or false. | Kalenský et al. (2024) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | якими люди можуть керуватися. Якщо людина чує один і той самий наратив кілька разів, особливо з різних джерел, вона буде схильна повірити в нього, незалежно від того, правдивий він чи неправдивий.<br><br>Див. також *Заїжджена платівка* | See also *Broken Record* | |
| 238. | **Полемічний аргумент**<br><br>аргумент, метою якого є успішне оскарження чужого аргументу, а не пошук істини. | **Eristic Argument**<br><br>an argument that aims to successfully dispute another's argument, rather than searching for truth. | Szwed (2016) – p. 44 |
| 239. | **Полісуб'єкт**<br><br>Базовий концепт *Нової моделі внутрішнього контролю над росією*.<br>Це саморегульована група людей, яка розглядається як цілісний організм, що має єдність через тісну взаємодію своїх суб'єктів та їхній рівномірний розвиток. Полісуб'єкт функціонує як єдине ціле, як єдиний організм, що заснований на єдності своїх суб'єктів та їх взаємодії, він здатний пристосовуватися (як одиниця) до різних обставин і взаємодіяти з іншими суб'єктами всередині спільноти, щоб слідувати спільному курсу розвитку. Зв'язуючим елементом російської полісуб'єктності є так звана *російськість*. Розробник концепту – В.Лепський | **Polisubjekt**<br><br>This is the basic concept of the model a *New model for controlling Russia internally*.<br>This is a self-regulating group as one comprehensive body, that has unity through the intimate interactions of its subjects and their uniform development. The polisubjekt functions as a single whole, as one organism based on the unity of its subjects and their interactions, capable of adapting (as a unit) to different circumstances and interacting with other subjects within the community to pursue the mutual course of development The so-called *russianness* is the connecting element of Russian polysubjectivity. Concept developer -– V.Lepskiy | Cullen et al. (2021) – p.19 |
| 240. | **Політика паспортизації**<br><br>неформальна політика кремля щодо надання російських | **Passportization policy**<br><br>Kremlin's informal policies to deliver Russian passports especially to the | Rotaru (2018) – p.7 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | паспортів, особливо населенню сепаратистських регіонів інших держав.<br>Ідеться про надання російського громадянства без здачі паспорта з рідної країни. | populations of secessionist regions of other states.<br>This involves granting Russian citizenship without the surrendering the passport from the home country. | |
| 241. | **Політичний домен гібридних загроз**<br>Будь-яке угруповання переважно громадянських суб'єктів, організацій та інституцій, як офіційних, так і неформальних, які здійснюють владу чи панують у певних географічних або організаційних межах шляхом застосування різних форм політичної влади та впливу. Він містить політичну систему, партії та головних акторів. Він має відображати культурні, історичні, демографічні та іноді релігійні чинники, які формують ідентичність суспільства. Один з 6-ти *ПМЕСІІ*-доменів. Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | **Political domain of hybrid threats**<br>Any grouping of primarily civil actors, organisations and institutions, both formal and informal, that exercises authority or rule within a specific geographic boundary or organisation through the application of various forms of political power and influence.<br>It includes the political system, parties and main actors. It must be representative of the cultural, historical, demographic and sometimes religious factors that form the identity of a society. One of the 6 *PMESII*-domains. One of the 13 domains in the *Conceptual model of hybrid threats* | NATO (2013) – p.1-8 |
| 242. | **Політичні інструменти гібридних загроз**<br>Політичний інструмент означає використання політичної влади, зокрема на дипломатичній арені, співпрацюючи з різними акторами, щоб вплинути на супротивника або створити вигідні умови. Один з 5-ти *МПЕСІ*-інструментів. Група інструментів у *Концептуальній моделі гібридних загроз* | **Political instruments of hybrid threats**<br>The political instrument refers to the use of political power, in particular in the diplomatic arena cooperating with various actors, to influence an adversary or to establish advantageous conditions. One of the 5 *MPECI*-instruments. A set of tools in the *Conceptual model of hybrid threats* | NATO (2013) – p.1-9 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 243. | **Поляризація**<br><br>один із способів поєднання методів інформаційного впливу (див. *Кампанії Впливу*).<br><br>Політичний, соціальний та ідеологічний поділ суспільств на чітко протилежні групи.<br><br>Поляризація підтримує дві протилежні крайності конкретної проблеми. Це досягається підтримкою вже існуючих розколів, використанням *Соціального Зламу, Оманливих Ідентичностей* та *Дезінформації*. Часто *Тролів* та *Ботів* використовують для подальшої поляризації дискусії. | **Polarisation**<br><br>one of the ways to combine of information influence techniques (see *Influence Campaigns*).<br><br>The political, social and ideological division of societies into distinctly opposed groups<br><br>Polarisation supports two opposing extremes of a specific issue. This is achieved by supporting pre-existing perspectives, using *Social Hacking, Deceptive Identities* online, and *Disinformation*. Often *Trolls* and *Bots* are used to further a polarised discussion. | MSB (2018) – p.29<br><br>Neudert & Marchal (2019) – p.6 |
| 244. | **Попередження конфлікту**<br><br>це комплекс операцій з підтримання миру, що включає застосування додаткових дипломатичних, цивільних та, за необхідності, військових засобів, яка проводиться з метою вивчення та визначення причин виникнення конфлікту, а також вчасного запобігання його виникненню, ескалації або відновленню військових дій. | **Conflict prevention**<br><br>a peace support operations employing complementary diplomatic, civil, and – when necessary – military means, to monitor and identify the causes of conflict, and take timely action to prevent the occurrence, escalation, or resumption of hostilities. | NSA (2013) – p. 2-C-12 |
| 245. | **Популізм**<br><br>показний політичний стиль, який використовує проти істеблішменту риторику, що викликає розкол та протиставляє "людей" та невловиму "еліту". | **Populism**<br><br>a performative political style that employs a divisive, anti-establishment rhetoric pitting 'the people' against an elusive 'elite'. | Neudert & Marchal (2019) – p.6 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 246. | **Поріг**<br><br>визначена величина або інтенсивність функціонального стану критичних функцій (наприклад, "рівень стресу"), які слід перевищити для досягнення конкретного статусу (наприклад, нормального чи кризового). Це рівень ворожості, з якого буде здійснюватися протидія.<br><br>Див. також: *Допорогові виклики* | **Threshold**<br><br>determining the magnitude or the intensity of a functional status (for example, the 'stress level') of one's critical functions to be exceeded to achieve a specific status (for example, normal or crisis). It is the the level of hostility at which counteraction will be taken.<br><br>See also: *Sub-Threshold Challenges* | MCDC(a) (2019) – p.90 |
| 247. | **Послуги позиціонування, навігації та часу / PNT-послуги**<br><br>Один із космічних сервісів, інструменти та вразливості якого використовуються у *космічному домені гібридних загроз*.<br><br>Містить космічні можливості для передачі сигналів часу для різних застосувань, включаючи повітряну, наземну, морську та космічну навігацію; відстеження активів та наведення високоточної зброї. PNT також підтримує громадський транспорт; точне землеробство; автономне керування транспортом; синхронізація часу для електричних мереж і банківських операцій; зв'язок через бездротовий Інтернет і екстрену медичну допомогу, пожежну службу та поліцію; а також навігаційні послуги для залізничних, автомобільних, повітряних і океанських вантажних операцій. | **Positioning, navigation, and timing / PNT-services**<br><br>One of the space-based services, whose tools and vulnerabilities are used in *space domain of hybrid threats*.<br><br>This contains space capabilities to transmit timing signals for various applications, including air, land, sea, and space navigation; asset tracking; and precision weapons guidance. PNT also supports civilian transportation; precision farming; autonomous vehicle guidance; time synchronization for electrical power grids and banking transactions; communications across wireless Internet and emergency medical, fire, and police services; as well as navigation services for rail, road, air, and ocean cargo operations. | DIA (2022) – p.2 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 248. | **Постконфліктна (деокупована) територія**<br><br>частина території, на якій відбувся збройний конфлікт і яка була звільнена. Для такої території характерні дестабілізація економічної ситуації, руйнування виробничої, транспортної, енергетичної, соціальної інфраструктури, житлового фонду, відтік населення, деурбанізація та знелюднення сіл, зниження рівня зайнятості та доходів населення. Для відновлення нормального функціонування такої території необхідне застосування спеціальних режимів господарської діяльності. Наразі в Україні це частина території Донецької та Луганської областей, на якій з вести 2014 року відбувся збройний конфлікт і яка була звільнена влітку 2014 року. | **Post-conflict (de-occupied) area**<br><br>the part of the area, where the military conflict occurred and which was liberated. This area features destabilized economic situation, ruined production, transport, energy and social infrastructure, housing, both urban and rural population decline, lower employment and income rate. The resumption of the post-conflict (de-occupied) area functioning requires special economic activity regimes. Currently in Ukraine this term refers to the part of Donetsk and Luhansk regions, where a military conflict had started in spring 2014 and which was liberated in summer 2014. | Horbulin (2017) – p.158 |
| 249. | **Потьомкінські села**<br><br>метод, який використовується в *Оманливих Ідентичностях*.<br><br>Гравці, які мають достатньо ресурсів, можуть створювати установи або навіть мережі установ, які служать для обману та введення в оману. Неправдиві компанії, науково-дослідні установи та аналітичні центри - це приклади так званих потьомкінських сіл, які можуть створювати та обґрунтовувати неправдиву інформацію. | **Potemkin Villages**<br><br>a method that is used in *Deceptive Identities.*<br><br>Actors with sufficient resources can set up institutions or even networks of institutions that serve to deceive and mislead. False companies, research institutions and think tanks are examples of so-called Potemkin villages which can create, and legitimate, false information. | MSB (2018) – p.19 – 20 |
| 250. | **Претекстинг** | **Pretexting** | ENISA (n.d.) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | це техніка використання претексту (приводу) – оманливого обґрунтування певного способу дій – для того, щоб завоювати довіру жертви та ввести її в оману. Наприклад, зловмисник стверджує, що працює в IT-підтримці, і просить пароль жертви для обслуговування. Щоб уникнути таких кібератак, необхідно запровадити належні процеси ідентифікації та автентифікації, політики та навчання. | this technique the use of a pretext - a false justification for a specific course of action - to gain trust and trick the victim. Example: the attacker claims to work for IT support and requests the target's password for maintenance purposes. Proper identification and authentication processes, policies and trainings should be in place to circumvent such attacks. | |
| 251. | **Прийняття рішень**<br><br>Це процес вибору якогось рішення, яке описує стан середовища в конкретній точці простору, серед альтернатив на основі визначеної системи цінностей. В Концептуальній моделі гібридних загроз прийняття рішень розглядається як головна ціль акторів / гравців гібридних загроз. Гібридні впливи спрямовані на те, щоб підірвати здатність жертви до незалежного прийняття рішень. | **Decision-Making**<br><br>This is the process of selecting a decision that describes the state of the environment at a specific point in space from among alternatives, based on a defined value system. In the Conceptual Model of Hybrid Threats, decision-making is considered the main target of actors of hybrid threats. Hybrid influences aim to undermine the victim's ability to make independent decisions. | Cullen et al. (2021) – p.13 |
| 252. | **Проксі-війна**<br><br>це підхід, прийнятий державами, які діють через *недержавних акторів* у ворожих цілях. Її ключовою ознакою є пряме чи опосередковане фінансування традиційних або нерегулярних сил третіх сторін, які перебувають поза межами конституційного ладу держав, а також у збройному конфлікті. Стратегічні цілі спонсорів передбачають поєднання примусу, руйнування (послаблення ворога) | **Proxy warfare**<br><br>The approach adopted by states acting through *non-state actors* for hostile purposes. Its key feature is the direct or indirect sponsorship of third-party conventional or irregular forces that lie outside of the constitutional order of states engaged in armed conflict. The strategic objectives of sponsors involve a combination of coercion, disruption (weakening an enemy), and/or transformation (engineering | Cullen et al. (2021) – p.22 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | та/або трансформації (створення фундаментальних політичних змін у цільовій державі). | a fundamental political transition in the target state). | |
| 253. | **Протидія агресії**<br>етап в Системі превентивних заходів НАТО, під час якого відбувається перехід від стадії підготовки та готовності до стадії санкціонованого застосування сил НАТО проти держави або кількох держав, а також проти сил, які проводять або активно підтримують агресію проти території та/або сил НАТО. | **Counter-aggression (CA)**<br>a stage of the NATO Precautionary System marking the transition from a condition of preparation and development of readiness to one of authorization for the employment of NATO forces against a nation, or nations, and against forces which are conducting or actively supporting aggression against NATO territory and/or forces. | NSA (2013) – p. 2-C-16 |
| 254. | **Пропаганда**<br>1) спроба вплинути на думку та поведінку суспільства з метою прийняття людиною тієї чи іншої думки та поведінки<br>2) Поширення інформації, фактів, аргументів, чуток, напівправди або брехні з метою впливу на думки, емоції, ставлення чи поведінку певної групи для отримання прямої чи опосередкованої вигоди замовником. | **Propaganda**<br>1) an attempt to influence the opinion and behavior of society in order for people to adopt a particular opinion and behavior<br>2) The spreading information, facts, arguments, gossip, half-truths or lies designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. | Vilmer et al. (2018) - p.19<br>Horbulin (2017) – p.159 |
| 255. | **Проросійські псевдо-ГО** (громадська організація)<br>ГО-подібні структури, які фінансує уряд росії.<br>спосіб інструменталізації громадянського суспільства кремлем.<br>багато з цих "ГО" імітують західні підходи, наприклад, звинувачуючи уряди колишніх радянських республік у серйозних порушеннях | **(pro)-Russian pseudo “NGOs”**<br>NGO-like structures financed by the Russian government.<br>way of instrumentalization of civil society by the Kremlin.<br>many of these “NGO”s mimic Western approaches, for example by accusing the governments of the former Soviet republics of serious human rights violations, especially toward Russian minorities; others | Rotaru (2018) – p.8 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | прав людини, особливо щодо російських меншин; інші по-різному пропагують російську мову та захищають російську інтерпретацію історії, демонізують угоди про асоціацію з ЄС як "форму окупації" та інструмент "заманювання держав у НАТО", пропагують консервативні цінності та православне християнство як ядро євразійської цивілізації в опозиції "чужих" європейських цінностей та мобілізації людей на вулиці для проросійських інтеграційних протестів та розпалення напруженості.<br><br>варіюються від асоціацій, що представляють російські меншини, проросійські молодіжні рухи, аналітичні центри, організації з моніторингу виборів та проросійські або сепаратистські установи. | variously promote the Russian language and defend the Russian interpretation of history, demonize EU association agreements as a “form of occupation” and an instrument to “lure states into NATO,” promote conservative values and Orthodox Christianity as the core of Eurasian civilization in opposition to “foreign” European values, and mobilize people onto the streets for pro-Russian integration protests and to stir up tensions.<br><br>range from associations representing Russian minorities, pro-Russian youth movements, think tanks, analytical centers, election-monitoring organizations, and proRussian or secessionist institutions. | |
| 256. | **Психологічна війна**<br><br>заходи, пов’язані із впливом на цінності та систему переконань цільової аудиторії, її сприйняття, емоції, мотиви, міркування та, в ідеалі, на їх поведінку.<br><br>Метою психологічної війни є послаблення морального духу опонента та зміцнення власного морального духу, створюючи атмосферу, в якій цільова аудиторія стає більш схильна до вселянь.<br><br>Є одним з 3-х елементів китайської стратегії "*Три війни*" | **Psychological Warfare**<br><br>those activities associated with influencing a target audience’s values and belief system, their perceptions, emotions, motives, reasoning, and, ideally, their behaviour.<br><br>The purpose of psychological warfare is to weaken the morale of the opponent and strengthen one’s own morale, creating an atmosphere in which the recipients of statements are more prone to suggestion.<br><br>Is one of the 3 elements of the Chinese strategy "Three Wars" | Szwed (2016) – p. 62<br><br>Nissen (2015) – p.67<br><br>Fokin (2016) – p.7<br><br>Cullen et al. (2021) – p.21 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 257. | **Публічна дипломатія**<br><br>є формою спілкування уряду з людьми (G2P) і, отже, відрізняється від традиційної дипломатії, яка є формою спілкування уряду з урядом (G2G). Публічна дипломатія містить зусилля урядів однієї нації надсилати повідомлення безпосередньо "людям" в іншій країні і є частиною м'якої сили.<br><br>Різні заходи, пов'язані з публічною демократією, включають: освітні обміни та програми для науковців та студентів, навчання / освіта мови та культури, програми для відвідувачів, культурні обміни та заходи, радіо- та телевізійне мовлення. | **Public Diplomacy**<br><br>is a form of government to people (G2P) communication and therefore differs from traditional diplomacy that is a form of government to government communication. Public diplomacy comprises the efforts of governments from one nation to send messages directly to the "people" in another country and is part of soft power.<br><br>Various activities associated with Public Diplomacy includes: educational exchanges and programmes for scholars and students, language and culture training/education, visitor programmes, cultural exchanges and events, radio and TV broadcasting. | Simons (2015) – p.2 |
| 258. | **ПЕСІ**<br><br>абревіатура, що поєднує набір невійськових *Інструментів сили*, які використовуються *акторами / гравцями гібридних загроз*: політичні, економічні, соціальні та міжнародні інструменти. | **PECI**<br><br>This is an acronym that combines the spectrum (set) of non-military *Instruments of power* used by *actors of hybrid threats*: political, economic, civil, international tools. | MCDC (2017) – p.4 |
| 259. | **ПМЕСІІ**<br><br>абревіатура, що поєднує спектр (набір, перелік) доменів гібридних загроз:<br>• *Політичний домен*<br>• *Військовий домен (мілітарний)*<br>• *Економічний домен*<br>• *Соціальний домен*<br>• *Інформаційний домен*<br>• *Інфраструктурний домен* | **PMESII**<br><br>This is an acronym that combines a spectrum (set, list) of domains of hybrid threats:<br>• *Political domain*<br>• *Military domain*<br>• *Economic domain*<br>• *Social domain*<br>• *Information domain*<br>• *Infrastructure domain* | MCDC (2017) – p.4 |

## Р

| № | UA | EN | Джерело |
|---|---|---|---|
| 260. | **Радіо-електронна боротьба (РЕБ) / Електронна війна**<br><br>Будь-яка дія, що передбачає використання електромагнітного спектру або спрямованої енергії для контролю такого спектру, нападу на противника або перешкоджання нападу противника.<br><br>Це - елемент технологічного аспекту стратегії та елемент бойової потужності збройних сил. Мета РЕБ – позбавити супротивника переваги електромагнітного спектру та забезпечити безперешкодний дружній доступ до нього.<br><br>РЕБ складається з трьох основних елементів: радіоелектронна атака (ЕА), електронний захист (ЕР) і радіоелектронна підтримка (ES). РЕБ містить використання *джамінгу* та *спуфінгу* для контролю електромагнітного спектру. Також тут використовуються наступні прийоми: сигнали для перехоплення, визначення місцезнаходження, ідентифікація, виявлення, порушення, обман, захист, аналіз та криптоаналіз тощо.<br><br>Складно відрізнити РЕБ від ненавмисного втручання. РЕБ сприяє успіху інформаційних, космічних операцій гібридної війни тощо | **Electronic warfare (EW)**<br><br>Any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or impede enemy assaults.<br><br>This is an element of the technological aspect of strategy and an element of the combat power of the armed forces. The purpose of electronic warfare is to deny the opponent the advantage of—and ensure friendly unimpeded access to—the electromagnetic spectrum.<br><br>Electronic warfare consists of three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). Electronic warfare includes using *jamming* and *spoofing* techniques to control the electro-magnetic spectrum. The following techniques are also used here: signals intercepting, locating, identifying, detecting, disrupting, deceiving, protecting, analyzing, and cryptanalyzing etc.<br><br>EW can be challenging to attribute and distinguish from unintentional interference. EW contributes to the success of information operations, space operations of hybrid warfare etc. | Gordon (2014)<br><br>CJCS (2007) - p. I-4<br><br>DIA (2022) – p. 44 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 261. | **Рефлексивний контроль**<br><br>Специфічний метод соціального контролю, який базується на *маніпуляції*. Передбачає маніпулювання індивідами та соціальними групами з метою зміни поведінки противника, коли він не здогадується, що його рішення не є добровільним. Рефлексивний контроль працює як *зворотня психологія*: опонентом маніпулюють, щоб переконати, що рішення було прийнято з його власної волі.<br>Цей підхід розроблений Георгієм Смоляном на основі теорії рефлексивних ігор В. Лефевра і є підгрунттям для *російського стратегічного мислення* | **Reflexive control**<br><br>A specific method of social control, який базується на *manipulation*. It involves manipulating individuals and social groups in order to change the behavior of the adversary when they are unaware that their decisions are not voluntary. Reflexive control works like *reverse psychology*: the opponent is manipulated into believing that the decision was made of his own free will.<br>This approach was developed by Georgii Smoljan, based on the theory of reflexive games of V. Lefebvre and is the basis for *Russian strategic thinking.* | Cullen et al. (2021) – p.19 |
| 262. | **Рецептивність, сприйнятливість**<br><br>уразливість цільової аудиторії до певних медійних засобів ведення психологічних операцій. | **Receptivity**<br><br>the vulnerability of a target audience to particular psychological operations media. | NSA (2013) – p. 2-R-4 |
| 263. | **Риторика викривлення (наклепу)**<br><br>є одним із методів інформаційного впливу (див. *Кампанії Впливу*).<br><br>Риторика - це визнана і природна частина демократичних дебатів, де кожен має право висловити свою думку та взяти участь у публічних обговореннях. Певна кількість риторики є прийнятною в публічних дебатах, тоді як наклепницька риторика – ні. Риторика наклепу часто має фрагментований характер розмов у сучасній публічній сфері, щоб скаламутити воду, обдурити та | **Malign Rhetoric**<br><br>is one of the information influence techniques (see *Influence Campaigns*).<br><br>Rhetoric is an accepted and natural part of democratic debate where everyone has the right to voice their opinions and engage in public deliberation. A certain amount of rhetoric is accepted in public debate whereas malign rhetoric is not. Malign rhetoric exploits the often-fragmented nature of conversations in the contemporary public sphere to muddy the waters, deceive and | MSB (2018) – p.19, 26 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | ввести в оману, а також знеохотити учасників брати участь у публічних дебатах. Поширеним засобом наклепницької риторики в Інтернеті є *Тролі*.<br><br>Це включає: *Перехід на особистості, Якщодоізм, Галоп Гіша, Солом'яне опудало, Напад* (чорна риторика) тощо. | mislead, and discourage actors and voices to participate in the public debate.<br><br>A common vehicle for online malign rhetoric is *Trolls*.<br><br>It includes: *Ad Hominem, Whataboutism, Gish-Gallop, Strawman, Hijacking* etc. | |
| 264. | **Розвинена стала загроза (загроза підвищеної складності)**<br><br>Актор, який володіє повним спектром технік збору розвідданих і переслідує конкретні цілі, а не просто шукає інформацію з фінансовою вигодою або з іншою метою, керуючись як наміром, так і можливостями, а саме здійснює атаки через скоординовані дії людей, а не за допомогою бездумних і автоматизованих шматків коду.<br><br>Злочинні групи, які займаються кіберзлочинністю, часто разом називають розвиненою сталою загрозою або загрозою підвищеної складності. Найбільш відомою є APT41, яка також носить назви Double Dragon або Cicada. Її прийнято вважати групою, спонсорованою китайською державою, що займається кібершпигунством від імені уряду, одночасно беручи участь у фінансово мотивованих кіберзлочинах для особистої вигоди. | **Advanced persistent threat**<br><br>An actor equipped with the full spectrum of intelligence-gathering techniques, pursuing specific objectives rather than just opportunistically<br>seeking information for financial or other gain, and guided by both intent and capability, namely executing attacks by coordinated human actions rather than mindless and automated pieces of code.<br><br>The opaque groups that engage in cyber crime are often collectively referred to as Advanced Persistent Threats (APT). Perhaps the most widely reported case is that of APT41, also known as Double Dragon or Cicada, which is generally assessed to be a Chinese state-sponsored group that engages in cyber espionage on behalf of the government, while simultaneously participating in financially motivated cybercrime for personal gain. | Jokinen et al., (2022) – p.15<br><br>Missiroli (2021) – p.11 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 265. | **Російська екосистема дезінформації та пропаганди**<br><br>сукупність офіційних, уповноважених (опосередкованих) каналів комунікації, а також платформ без зазначення такої приналежності, які росія використовує для створення та посилення фальшивих наративів. Екосистема складається з п'яти основних елементів:<br>- офіційні державні комунікації,<br>- фінансовані державою глобальні повідомлення,<br>- вирощування проксі-джерел,<br>- озброєння соціальних медіа,<br>- дезінформація за підтримки кібер-засобів. | **Russia's disinformation and propaganda ecosystem**<br><br>the collection of official, proxy, and unattributed communication channels and platforms that Russia uses to create and amplify false narratives. The ecosystem consists of five main pillars:<br>- official government communications,<br>- state-funded global messaging,<br>- cultivation of proxy sources,<br>- weaponization of social media,<br>- and cyber-enabled disinformation. | GEC (2020) – p.3 |
| 266. | **Російська політика пам'яті**<br><br>становить важливий елемент [російської ] державної пропаганди: історичні факти та їхні інтерпретації підпорядковують політичним інтересам тих, хто приймає рішення.<br><br>складається з ідей та практик, спрямованих на формування колективної пам'яті та історичного дискурсу в такий спосіб, що відповідає політичним інтересам [російської ]правлячої еліти. Її впроваджують державні установи, підконтрольні державі ЗМІ, частина наукових кіл та мережа соціальних організацій. Політика пам'яті має бути одним із інструментів легітимації авторитарного режиму. Її значення зростає, коли вплив інших | **Russia's politics of memory**<br><br>constitutes an important element of [Russian] state-sponsored propaganda: historical facts and their interpretations are subordinated to the political interests of decision makers.<br><br>consists of ideas and practices designed to shape collective memory and historical discourse in a way that serves the political interests of the [Russian] ruling elite. It is implemented by state agencies, state-controlled media outlets, a part of academia and a network of social organisations. The politics of memory is intended to be one of the tools for legitimising an authoritarian regime. Its significance grows whenever the impact of other legitimising factors (economic, | Domańska (2019) – p.1, 3 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | легітимізуючих факторів (економічних, політичних, соціальних та міжнародних) зменшується. | political, social and international) wanes. | |
| 267. | **Російське крос-доменне стримування**<br><br>стримування, яке складається з трьох взаємопов'язаних понять: традиційне ядерне стримування; неядерне (загальноприйняте) стримування, що покладається здебільшого на точні керовані ракети та спецназ; та інформаційне стримування в кібер просторі.<br><br>На практиці це призводить до "безперервного інформаційного стримування на всіх можливих фронтах проти всіх можливих аудиторій, що посилюється ядерною сигналізацією і доповнюється внутрішньо-військовим примусом".<br><br>Кінцевою метою такого виду стримування є "деескалація або відгородження противника від агресії та нав'язування волі агресора, бажано з мінімальним насильством"<br><br>Див також: *Крос-Доменне Стримування* | **Russian cross-domain deterrence**<br><br>deterrence that being composed of three intertwined concepts: traditional nuclear deterrence; non-nuclear (conventional) deterrence relying mostly on precision-guided missiles and special forces; and informational deterrence in cyber space.<br><br>In practice, this results in “uninterrupted informational deterrence waged on all possible fronts against all possible audiences, augmented by nuclear signaling, and supplemented by intrawar coercion”<br><br>The ultimate purpose of this kind of deterrence is “to deescalate, or dissuade the adversary from aggression, and impose the aggressor’s will, preferably with minimal violence.”<br><br>See also: *Cross Domain Deterrence* | Adamsky (2015) – p. 37<br><br>Sweijs & Zilincik (2019) – p.14 |
| 268. | **Російське стратегічне мислення**<br><br>Російська стратегія гібридних впливів.<br><br>Вона побудована так, що окремі актори мають власну зацікавленість та переслідують незалежні цілі, які відповідають стратегічним цілям кремля. Тому | **Russian strategic thinking**<br><br>Russian hybrid influence strategy.<br><br>t's built in a way that individual actors have their own stake in the operation and want to pursue independent goals, which are in line with Kremlin’s overall strategic objectives… Therefore the Russian leadership | Cullen et al. (2021) – p.18 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | російське керівництво не зобов'язане дотримуватися якихось жорстких, деталізованих планів, а може смикати за ниточки виходячи з потреб і можливостей. Теоретичне підгрунтя цієї стратегії:<br>• *Нова модель внутрішнього контролю над росією*<br>• *Рефлексивний контроль* | does not have to stick to any rigid, detailed plans, but may pull the strings according to the actual needs and possibilities. The theoretical basis of this strategy:<br>• *A new model for controlling Russia internally*<br>• *Reflexive control* | |
| 269. | **Російськість**<br><br>Це – сполучний елемент для створення російського *полісуб'єкту*, який прив'язує всіх росіян до забезпечення російського національного стратегічного інтересу та стратегічних завдань, поставлених вищим керівництвом. В *російському стратегічному мисленні* це подається як "цивілізаційна унікальність" та "російська цивілізаційна перевага".<br><br>Формується в двох напрямках: *великодержавність* та *антизахідництво*. Обидві теми надали російській політичній еліті інструменти для пошуку тих, хто готовий просувати стратегічні інтереси російського режиму. | **Russianness**<br><br>This is the connecting element for the creation of a Russian *polysubject*, which ties all Russians to securing the Russian national strategic interest and strategic objectives given by the top leadership. In *Russian strategic thinking* this is presented as "civilizational uniqueness" та "russian civilizational superiority".<br><br>It is formed in two directions: *greatpowerness* and *anti-westernism*. Both themes have given tools for Russian political elite to find those that are ready to push forward the strategic interests that today's Russian regime has. | Cullen et al. (2021) – p.19 |
| 270. | **Російськомовні громади**<br><br>складова "*руського миру*", що є основою російської мережі за кордоном. Основна ідея: "якщо вирощувати проросійське мислення за кордоном, важливо | **Russian-Speaking Communities**<br><br>component of the *Russkiy Mir*, which form the bedrock of Russia's network abroad. Main idea: "if a pro-Russian way of thinking is to be nurtured abroad, it is crucial to invest in the | Lutsevych (2016) – p.14, 16 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | вкладати кошти у посилення російської мови".<br><br>Але законні зусилля з просування російської мови використовують із підривною метою:<br><br>- отримання лояльності "російськомовних" (фінансуючи проєкти, що просувають російську мову),<br><br>- "захист прав" російськомовного населення (в Україні та інших країнах),<br><br>- розпалювання напруженості та сепаратистських настроїв в Україні (підтримуючи маргинальні сепаратистські крила слов'янофільських та русофільських організацій).<br><br>"Руський мир всюди, де говорять російською" | reinforcement of the Russian language".<br><br>But legitimate efforts to promote the Russian language is used for subversive purposes:<br><br>- to buy the loyalty of Russian-speakers (by financing projects promoting the Russian language),<br><br>- to "defend rights" of Russian-speaking population (in Ukraine and other countries),<br><br>- to foment tensions and separatist sentiments in Ukraine (by supporting the fringe separatist wings of Slavophile and Russophile organizations).<br><br>"the Russian World is everywhere where the Russian language is spoken" | |
| 271. | **Роскомнадзор**<br><br>Російське державне агентство, яке здійснює нагляд за ЗМІ;<br>інструмент гібридного впливу | **Roskomnadzor**<br><br>The Russian state agency that oversees mass media; a hybrid influence tool | GEC (2020) – p.31 |
| 272. | **Россотрудничество**<br><br>російське державне агентство, завданням якого є посилення впливу росії за кордоном, особливо в країнах СНД.<br><br>Створене в 2008 році, діє як парасолькова організація для мережі російських співвітчизників та фінансує різні проєкти "державної дипломатії". Россотрудничество відіграє активну політичну роль у зовнішній | **Rossotrudnichestvo**<br><br>Russian public agencie, whose mission is to further Russian influence abroad, especially in CIS countries.<br><br>Established in 2008, it acts as an umbrella organization for a network of Russian compatriots and funds various 'public diplomacy' projects. Rossotrudnichestvo plays an active political role in Russia's foreign policy by consolidating the activities of pro- | Vilmer et al. (2018) - p.70<br><br>Lutsevych (2016) – p.9<br><br>Rotaru (2018) – p.3 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | політиці росії, консолідуючи діяльність проросійських гравців у пострадянському регіоні та розповсюджуючи нарратив кремля. Відповідно до нової Концепції сприяння міжнародному розвитку, яка була підписана путіним у 2014 році, Россотрудничество офіційно отримало провідну роль у розвитку м'якої сили росії, яку в офіційних документах часто називають як "гуманітарний вимір зовнішньої політики". | Russian players in the post-Soviet region and in disseminating the Kremlin's narrative. In line with the new Concept of International Development Assistance, which was signed by Putin in 2014, Rossotrudnichestvo was officially given a flagship role in developing Russia's soft power, often referred to in official documents as the 'humanitarian dimension of foreign policy'. | |
| 273. | **Руйнівні технології**<br><br>специфічні технології, які можуть принципово змінити не тільки усталені технології, але також правила та бізнес-моделі певного ринку, а часто бізнесу та суспільства загалом. | **Disruptive technologies**<br><br>a specific technology that can fundamentally change not only established technologies but also the rules and business models of a given market, and often business and society overall. | Doyle (2011) |
| 274. | **"Руський Мир"**<br><br>1) російська **псевдо-ГО** (громадська організація), що фінансується російською державою і тісно співпрацює з нею, створена в 2007 році для просування російської мови та культури за кордоном і яка насправді служить мостом між урядом та важелями впливу за кордоном<br><br>2) **концепція** "Руського миру" є геополітичним інструментом для формування російської легітимності та впливу в регіоні, а також ключовою структурою для її проксі-груп. Як визначив путін у 2014 році, руський мир - це | **"Russkiy Mir"**<br><br>1) russian **pseudo-NGO**, financed by the russian State and working closely with itcreated in 2007 to promote Russian language and culture abroad and which serves in reality as a bridge between the government and relays of influence abroad<br><br>2) **the concept** of the Russian World (Russkiy Mir) is a geopolitical tool for building up Russian legitimacy and influence in the region, and a key framework for its proxy groups. As defined by Putin in 2014, the Russian World is a civilization that includes people who feel culturally close to | Vilmer et al. (2018) - p.70<br><br>Lutsevych (2016) – p.3, 8<br><br>Rotaru (2018) – p.5<br><br>Laruelle (2015) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | цивілізація, яка включає людей, які почуваються культурно близькими до росії. Тому руський мир має гнучку географію для своїх прихильників. Нинішній наратив руського миру охоплює:<br>- мова (*Російськомовні Громади*)<br>- культура (євразійська православна ідентичність),<br>- історія (росіяни та українці були «одним народом», «Велика Вітчизняна війна» тощо),<br>- спільна спадщина (радянський історичний нарратив),<br>- економічні зв'язки (Євразійський економічний союз, ЄАЕС; Євразійський митний союз),<br>- релігія (російська православна церква, «православні олігархи», православний союз молоді, східно-православна цивілізація…),<br>- консервативні цінності (на противагу західним цінностям лібералізму та прав людини).<br><br>Руський мир зображує колишній СРСР як єдиний всесвіт російської мови та культури, закріплений загальним історичним досвідом, включаючи братство зброї під час *Великої Вітчизняної війни*. Україна та Білорусь відіграють особливу роль у проекті “Руський мир” як частини “триєдиної російської нації”, пов’язані “вічними” зв’язками з росією (ці країни, таким чином, не розглядаються як повністю суверенні). | Russia.The Russian World thus has a fluid geography for its advocates. The current narrative of the Russian World encompasses:<br>- language (*Russian-Speaking Communities*)<br>- culture (EurasianOrthodox identity),<br>- history (Russians and Ukrainians were ‘one people’, ‘the Great Patriotic War‘ etc),<br>- shared heritage (the Soviet historical narrative),<br>- economic links (The Eurasian Economic Union, EAEU; the Eurasian Customs Union),<br>- religion (The Russian Orthodox Church, 'Orthodox oligarchs’, the Orthodox Union of Youth, the Eastern Orthodox civilization…),<br>- conservative values (in opposition to Western values of liberalism and individual human rights).<br><br>The "Russian world" portrays the former USSR as a single universe of Russian language and culture, cemented by common historical experience, including the brotherhood of arms during the *Great Patriotic War*. Ukraine and Belarus play a special role in the “Russian world” project as parts of the "triune Russian nation", connected by "eternal" ties with Russia (these countries are thus not viewed as fully sovereign). | Domańska (2019) – p.7 |

## С

| № | UA | EN | Джерело |
|---|---|---|---|
| 275. | **Самооцінка гібридної війни**<br><br>постійний національний процес для виявлення критичних функцій та пошуку вразливостей у *ПМЕСІІ*-спектрі. | **Hybrid warfare self-assessment**<br><br>a continuous national process to identify critical functions and find vulnerabilities within the *PMESII* spectrum | MCDC(a) (2019) – p.89 |
| 276. | **Сатира та пародія**<br><br>є одним із методів *Дезінформації*.<br><br>Висміювання, викриття та критика людей, розповіді чи думки з використанням гумору та перебільшення. Хоча найчастіше нешкідливе, це може бути використано агресивно в рамках більш широких зусиль з дезінформації. Гумор також дуже ефективний для легітимації суперечливих думок. | **Satire And Parody**<br><br>is one of the *Disinformation* methods.<br><br>Ridicule, exposure and critique of individuals, narratives or opinions using humour and exaggeration. Though often harmless, this can be used aggressively within the framework of broader disinformation efforts. Humour is also very effective for legitimising controversial opinions. | MSB (2018) – p.19, 25 |
| 277. | **Сендворм**<br><br>Також відомі як: Quedagh, VOODOO BEAR, TEMP.Noble, IRON VIKING, G0034, ELECTRUM, TeleBots, IRIDIUM, Blue Echidna, FROZENBARENTS.<br><br>Група "патріотичних" російських хакерів, напряму пов'язана з російською військовою розвідкою, а саме Головним центром спеціальних технологій ГРУ, ГЦСТ, також відомим за своїм польовим поштовим номером 74455.<br><br>Цей гібридний актор (розвинена стала загроза) атакує промислові системи управління, використовуючи інструмент під | **Sandworm**<br><br>aka: Quedagh, VOODOO BEAR, TEMP.Noble, IRON VIKING, G0034, ELECTRUM, TeleBots, IRIDIUM, Blue Echidna, FROZENBARENTS<br><br>“Patriotic” Russian hackers, a group directly linked to Russian military intelligence, namely, GRU’s Main Centre for Special Technologies, GTsST also known by its field post number 744550.<br><br>This threat actor targets industrial control systems, using a tool called Black Energy, associated with electricity and power generation for espionage, denial of service, and data destruction purposes. Believed to be | Praks (2024)<br><br>UK Government (2020)<br><br>Malpedia (a). (n.d.)<br><br>Malpedia (b). (n.d.)<br><br>Google (2023) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | назвою Black Energy, пов'язаний з виробництвом електрики та електроенергії, з метою шпигунства, відмови в обслуговуванні та знищення даних. Вважається відповідальним за DDoS-атаки 2008 року в Грузії, відключення електроенергії в Україні 2015 року та вірус NotlPetya. | responsible for the 2008 DDoS attacks in Georgia, the 2015 Ukraine power grid outage and NotPetya virus. | |
| 278. | **Сигнали (у гібридних загрозах)**<br>неявні попередження, спричинені зміною статусу сили або позиції готовності, занепокоєнням щодо поведінки опонента, розвитком неявного розуміння "червоних ліній" та порогових значень, неявним чи явним розумінням потенційних опонентів та публічних заяв про наміри. | **Signals (in hybrid threats)**<br>implicit warnings created by changes in force status or readiness posture, concern over opponent behavior, by developing tacit understandings on 'redlines' and thresholds, by implicit or explicit understandings among potential opponents, and by public statements about intentions. | Sweijs & Zilincik (2019) – p. 17<br>Denning (2015) - p.15 |
| 279. | **Сигналізація (у гібридних загрозах)**<br>життєво важливий компонент стримування, завдяки якому суб'єкти можуть продемонструвати свою здатність, а також готовність виконати стримуючу загрозу, що, у свою чергу, дозволяє виробити правила, які формують взаємодію між учасниками.<br>Сигналізація може здійснюватися за допомогою широкого спектру засобів та містить як слова, так і дії. | **Signaling (in hybrid threats)**<br>a vital component of deterrence through which actors are able to convey their ability as well as their willingness to execute a deterrent threat, which in turn allows for the development of the rules that shape the interaction between the participants.<br>Signaling can be done through a wide spectrum of means and involves both words and actions. | Sweijs & Zilincik (2019) – p. 23 |
| 280. | **Сила** (в контексті гібридних загроз)<br>Здатність держави досягати своїх політичних цілей за допомогою різних *інструментів сили*. | **Power** (in the context of hybrid threats)<br>The ability of a State to achieve its political goals using different *instruments of power*. | Van Haaster (2019) – p.31 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Існує два підходи до формування сили держави:<br>• Підхід «влада як ресурс»: сила держави визначається факторами, які легко виміряти – територія, багатство, армії та флоти.<br>• Підхід «влада на відносинах»: влада розглядається як фактичні чи потенційні відносини між двома чи більше суб'єктами (особами, державами, групами тощо), а не властивість будь-кого з них. | There are two approaches to the formation of state power:<br>• The 'power as resource approach': the power of States is deemed to be easily measurable factors - territory, wealth, armies and navies.<br>• The 'relational power approach': power is conceived to be an actual or potential relationship between two or more actors (persons, states, groups, etc.) rather than a property of any one of them. | |
| 281. | **Сила слабких**<br>навички ведення переговорів та ведення торгів, вміння правильно визначати час (наприклад, провокації та / або заподіяння шкоди репутації) та видимість узгодженості (на відміну від військової та економічної сили). | **The power of the weak**<br>negotiation and bargaining skills, being able to time action correctly (for example provocations and/or inflict damage on reputation) and appearance of coherence (by contrast of military and economic power). | Smith (2017) – p. 5 |
| 282. | **Символічні дії**<br>є одним із методів інформаційного впливу (див. *Кампанії Впливу*).<br>Дії значать більше, ніж слова. Іноді дії розраховані на те, щоб щось сигналізувати, а не на досягнення мети самої дії. В цьому випадку діяльність є символічною дією. На відміну від звичайних дій, символічні дії мотивовані комунікативною логікою та стратегічною обстановкою. Це можна зробити дуже грубо, наприклад, граючи на загальнолюдських страхах випадкового насильства, | **Symbolic Actions**<br>is one of the information influence techniques (see *Influence Campaigns*).<br>Actions speak louder than words. Sometimes actions are calculated to signal something, rather than to achieve the objective of the action itself. When this is the case, the action is a symbolic action. In contrast to any ordinary action, symbolic actions are motivated by a communicative logic and a strategic setting. This can be done very crudely, for by example playing on universally shared fears of random | MSB (2018) – p.19, 27 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | наприклад, в терористичній діяльності. Також це можна зробити вишукано, посилаючись на точні культурні символи, які стосуються лише певної цільової аудиторії.<br><br>Це містить: *Витоки, Хакінг, Громадські Демонстрації* тощо | violence such as in terrorist activities. It can also be conducted in a sophisticated manner by relating to precise cultural symbols relevant only to a specific target audience.<br><br>It includes: *Leaking, Hackning, Public Demonstrations* etc | |
| 283. | **Синхронізація засобів**<br><br>здатність учасника гібридної війни ефективно координувати *інструменти сили МПЕСІ* для досягнення бажаних ефектів як горизонтальним, так і вертикальним способом.<br><br>Див. також: *Горизонтальна Ескалація, Вертикальна Ескалація* | **Synchronization of means**<br><br>the ability of a hybrid warfare actor to effectively coordinate of the *instruments of power MPECI* to achieve the desired effects in both horizontal and vertical ways.<br><br>See also: *Horizontal Escalation, Vertical Escalation* | MCDC(a) (2019) – p.90 |
| 284. | **Система цінностей** (в прийнятті рішень)<br><br>це набір параметрів та критеріїв (правил) за якими відбувається прийняття рішень. Є невід'ємним елементом прийняття рішень, а тому - потенційною ціллю акторів / гравців гібридних загроз. | **Value System** (in decision-making)<br><br>This is a set of parameters and criteria (rules) by which decisions are made. It is an integral element of decision-making and, therefore, a potential target for actors of hybrid threats. | Методика навчання в умовах гібридних загроз (2023) |
| 285. | **Ситуаційна обізнаність (SA)**<br><br>1) у широкому сенсі:<br><br>а) це сприйняття людиною всіх доступних елементів інформації стосовно конкретної ситуації, що дозволяє більш цілісно та обґрунтовано тлумачити дійсність;<br><br>б) це сприйняття людиною елементів навколишнього середовища в обсязі часу і простору, усвідомлення їх | **Situational Awareness (SA)**<br><br>1) in the broad sense:<br><br>a) is the human perception of all available elements of information in relation to a specific situation that allows for a more holistic and informed interpretation of reality;<br><br>b) a person`s perception of the elements of the environment within a volume of time and space, the comprehension of their meaning and | NATO (2013) – p.2-5<br><br>Endsley (1995) - p.36<br><br>Yang et al. (2018) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | значення та прогнозування їх стану в найближчому майбутньому;<br><br>2) в IT-сфері: це інтегрована система обслуговування програмного забезпечення, що аналізує поведінку користувача. Вона забезпечує користувача відповідною інформацією або послугами, налаштовує обмін інформацією між користувачем і ситуацією шляхом обґрунтованого застосування ситуаційної інформації. Ситуаційна обізнаність спирається на фактичну ситуацію з боку користувачів, і у той же час автоматично адаптується до навколишнього середовища. | the projection of their status in the near future;<br><br>2) in IT: is an integrated software service system. A system that intelligently judges user behavior and its purpose is to actively provide relevant information or services for the user, humanized adjustment the mutual exchange way and content between human and situation by reasonable application situational information. Situational awareness is mainly based on the actual situation of users, on the one hand, automatically adapt to the environment, on the other hand. | |
| 286. | **"Сіра зона"**<br><br>(1) (в прийнятті рішень) – множина потенційно неправильних рішень, зона плутанини та вразливості<br><br>(2) неоднозначна нейтральність між миром та війною, що відображає різновиди агресивних, наполегливих, рішучих кампаній, характерних для війни, але без явного використання військової сили.<br><br>(3) Війна, яка не відповідає або виходить за межі традиційного розуміння "війни". | **'Gray Zone' / 'Grey Zone'**<br><br>(1) (in decision-making) – a set of potentially wrong decisions, a zone of confusion and vulnerability.<br><br>(2) the ambiguous no-man's-land between peace and war, reflecting the sort of aggressive, persistent, determined campaigns characteristic of warfare but without the overt use of military force.<br><br>(3) Warfare that falls short of, or outside of, our traditional understanding of 'warfare' | Kaikova et al. (2022)<br><br>Mazarr (2015) – p.2<br><br>MCDC(a) (2019) – p.31<br><br>Takahashi (2018) – p.787 |
| 287. | **Сірий носоріг**<br><br>Ймовірна подія зі значним впливом. Ми бачимо ці ризики десь на відстані, але ми не чітко усвідомлюємо їхній повний вимір. Серед сірих носорогів на глобальному радарі є ризик | **Gray rhino**<br><br>Probable event with high impact. We see these risks out there in the distance, but we don't clearly perceive their full dimensions. Among the gray rhinos on the global radar is the risk of regional conflicts | Grant et al. (2023) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | ескалації регіональних конфліктів в Азії на тлі ширшої стратегічної конкуренції. Інші приклади можуть включати серйозну ескалацію на Близькому Сході з охолодженням відносин і міжнародним і внутрішнім тиском на певні режими, які спричиняють сплеск прямого або проксі-конфлікту. | in Asia escalating amid broader strategic competition. Other imminently charging rhinos may include a major escalation in the Middle East, with cooling relationships and international and domestic pressure against specific regimes that cause an uptick in direct or proxy conflict. | |
| 288. | **"Смерть від тисячі порізів"**<br>ключовий аспект потенційних наслідків гібридної війни, спричинений низкою синхронізованих, мало спостережуваних або неспостережуваних подій, що діють нижче порогу того, що зазвичай являє собою "війну". | **'Death by a Thousand Cuts'**<br>a key aspect of the potential effects of hybrid warfare, caused by a series of synchronized, low-observable or unobserved events operating below the threshold of what would normally constitute 'war'. | MCDC (2017) – p.15 |
| 289. | **Солом'яне опудало**<br>Один з методів *Риторики Викривлення.*<br>дискредитувати супротивників, приписуючи позиції або аргументи, яких вони не дотримуються, а потім виступати проти цих позицій. | **Strawman**<br>is one of the *Malign Rhetoric* methods.<br>Discredit an adversary by attributing positions or arguments that they do not hold and then arguing against those positions. | MSB (2018) – p.19, 26 |
| 290. | **Соціальна інженерія (в контексті інформаційної безпеки)**<br>це психологічне маніпулювання людьми, спрямоване на те, щоб переконати жертву розкрити певну інформацію або виконати певну нелегітимну дію. Хоча така форма шахрайства існувала завжди, вона значно еволюціонувала з розвитком ІКТ-технологій. У цьому новому контексті методи соціальної інженерії в ІТ можна | **Social engineering (in Information Security)**<br>refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons. Though such form of trickery has always existed, it has significantly evolved with ICT technologies. In this new context, social engineering techniques in IT can be looked at from two different angles: | ENISA (n.d.) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | розглядати під двома різними кутами зору:<br><br>або використання психологічних маніпуляцій для отримання подальшого доступу до IT-системи, фактичної мети шахрая, наприклад, видавання себе за важливого клієнта за допомогою телефонного дзвінка, щоб заманити жертву на вірусний веб-сайт і інфікувати її систему;<br><br>або використання IT-технологій для підтримки методів психологічних маніпуляцій для досягнення мети поза межами IT-сфери, наприклад, отримання банківських даних за допомогою фішингової атаки з метою крадіжки грошей жертви. Зростаюче використання IT-технологій природно призвело до збільшення використання таких методів, а також їх комбінування, до такої міри, що більшість кібератак сьогодні включають в себе ту чи іншу форму соціальної інженерії. | either by using psychological manipulation to get further access to an IT system where the actual objective of the scammer resides, e.g. impersonating an important client via a phone call to lure the target into browsing a malicious website to infect the target's workstation;<br><br>or using IT technologies as support to psychological manipulation techniques to achieve an objective outside the IT realm, e.g. obtaining banking credentials via a phishing attack to then steal the target's money. The increasing use of IT technologies has naturally led to an increase in the use of such techniques, as well as to their combination, to such a point that most cyber attacks nowadays include some form of social engineering | |
| 291. | **Соціальна мережа** - див. *Цифрова Платформа, Нові ЗМІ* | **Social Network** – see *Digital Platform, New Mass Media* | |
| 292. | **Соціальний домен гібридних загроз**<br><br>Взаємозалежна мережа соціальних інститутів, які підтримують, сприяють і розвивають індивідів, а також надають можливості участі для досягнення особистих очікувань і життєвих цілей у спадкових і | **Social domain of hybrid threats**<br><br>The interdependent network of social institutions that support, enable and acculturate individuals and provide participatory opportunities to achieve personal expectations and life-goals within hereditary and nonhereditary groups, in either stable or unstable environments. | NATO (2013) – p.1-8 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | неспадкових групах, у стабільному чи нестабільному середовищі.<br><br>Він охоплює такі соціальні аспекти, як релігія, структура суспільства, правова та судова система, поліцейська та допоміжна інфраструктура, гуманітарна справа тощо.<br><br>Один з 6-ти *ПМЕСІІ*-доменів. Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | It covers the social aspects such as religion, a society's structure, the legal and judicial system, policing and supporting infrastructure, humanitarian, etc.<br><br>One of the *6 PMESII*-domains. One of the 13 domains in the *Conceptual model of hybrid threats* | |
| 293. | **Соціальний злам** - див. *Когнітивний Злам* | **Social Hacking** - see *Cognitive Hacking* | |
| 294. | **Соціальні медіа**<br><br>*цифрові платформи*, що сприяють створенню та обміну інформацією в мережевих спільнотах. | **Social media**<br><br>*digital platforms* that facilitate the creation and sharing of information in networked communities. | Neudert & Marchal (2019) – p.6 |
| 295. | **Соціокультурна система**<br><br>система, до складу якої входять три типи явищ: матеріальні, структурні та ідеаційні.<br><br>Перший тип явищ має фізичне втілення, яке можна легко спостерігати (навколишнє середовище, населення, його характеристики: розмір, вік, народження тощо) та технології, що використовуються у суспільстві. Другий тип стосується соціальних груп та їхньої організації (уряд, сімейна система тощо). Третій тип явищ охоплює ідеології, релігії, норми, цінності тощо. | **Sociocultural system**<br><br>the system, which consist of three types of phenomena: material, structural and ideational.<br><br>The first ones have a physical presence, which can be readily observed (environment, population, its characteristics (size, age, birth etc.) and technologies, used in the society. The second ones deal with the social groups and their organization (government, family system etc). The third ones refer to ideologies, religion, norms, values etc". | Elwell (2013) – p.13 |
| 296. | **"Співвітчизники" (соотєчєствєннікі)** | **"Russian Compatriots" (sootechestvenniki)** | Rotaru (2018) – p.7 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | одна з концепцій, що окреслює сфери інтересів кремля,<br><br>Це визначення функціонує концентрично: від громадянського ядра (громадяни-емігранти) до більш широкого кола, яке включає людей, які культурно та духовно орієнтовані на росію (наприклад, сепаратисти Придністров'я, Донецька та Луганська), потім до ще більшої групи всіх колишніх радянських народів та людей, що входили до Царської імперії (таким чином, навіть поляки та фіни могли б бути співвітчизниками!), і нарешті, останнє коло є найширшим та включає людей, які говорять російською мовою та відчувають спорідненість із російською культурою та духовністю. | one of the concepts that outline the Kremlin's spheres of interest<br><br>This definition functions in a concentric way: from a civic core (expatriate citizens) to a broader circle that includes people who are culturally and spiritually oriented toward Russia (for example the separatists of Transnistria or the insurgents from Donetsk and Luhansk), then to an even larger group of all former Soviet peoples and people who were part of the Tsarist Empire (thus, even Poles and Finns could be compatriots!), and finally, the last circle is the broadest one and includes people who speak Russian and who feel an affinity for Russian culture and spirituality. | |
| 297. | **Спільне радянське минуле (спільна історія)**<br><br>є не лише джерелом м'якої сили для кремля, але й важливим елементом для створення спільної ідентичності на пострадянському просторі. | **The shared Soviet past (Common history)**<br><br>is not only a source of soft power for the Kremlin but also an essential element for the creation of a shared identity in the post-Soviet space. | Rotaru (2018) – p.7 |
| 298. | **Спін-доктор / політтехнолог**<br><br>усі, хто професійно керує представленням інформації чи ідей громадськості (зокрема від імені політиків) з максимальною для своїх клієнтів вигодою. Їхня робота призводить до маніпуляції новинами, вона пов'язана зі зв'язками з громадськістю і пропагандою. | **Spin doctor**<br><br>all those who have the job of managing (or massaging) the public presentation of information or ideas (especially on behalf of politicians) to maximum advantage. Their work results in the manipulation of news and is related to public relations and propaganda | McQuail's, D. (2010) – p. 571 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 299. | **"Спіраль мовчання"**<br><br>явище, коли ми мовчимо, боячись думки більшості, не бажаючи їхньої критики.<br><br>Інтернет-користувачі, як правило, не діляться своїми поглядами, якщо вони суперечать панівній думці форуму. Таким чином, декілька тролів можуть, розмістивши ряд коментарів, створити враження думки більшості, та навіть коли це зовсім не так – цього достатньо, щоб мати паралізувальний вплив на інших.<br><br>Дивіться також *Астротурфінг*<br><br>явище, яке використовується в *Когнітивному Зламі.*<br><br>Люди, які відчувають себе частиною меншини, рідше висловлюють свої думки. За сценарієм, подібним *Ефекту Приєднання до Більшості*, поява соціальної згоди навколо проблеми може змусити людей із протилежними думками мовчати. Це апелює до побоювань бути виключеними чи відокремленими через непопулярну думку. | **'Spiral of Silence'**<br><br>a phenomenon when we keep quiet in fear of the majority's opinion, not wanting to be criticized by them.<br><br>Internet surfers tend not to share their viewpoints if these viewpoints go against the dominant opinion of the forum. In this way, a few trolls can, by posting a number of comments, give the impression of a majority opinion even when it is not at all the case—it is enough to have a paralyzing effect on others.<br><br>See also *Astroturfing*<br><br>a phenomenon that is used in *Cognitive Hacking.*<br><br>People who feel like part of the minority are less likely to air their opinions. In a similar scenario to the *Bandwagon Effect*, the appearance of social conformity around an issue can cause people with contradictory opinions to remain silent. This appeals to fears of being excluded or singled-out because of an unpopular opinion. | Szwed (2016) – p.40<br><br>Vilmer et al. (2018) - p.87<br><br>MSB (2018) – p.19-20 |
| 300. | **Спіраль цинізму**<br><br>гіпотетичний процес, подібний до "спіралі мовчання", за якого створюється клімат, де зменшується довіра і бажання брати участь у демократичних процесах через систематично негативне висвітлення медіями політичних кампаній і політиків, особливо коли наголошується на | **Spiral of cynicism**<br><br>a hypothetical process, similar to the spiral of silence, whereby persistently negative media coverage of a political campaign and politicians, especially where this emphasizes insincerity, corruption, dirty tricks, personal ambition and ignores substance and honest intention, is thought to create a | McQuail's, D. (2010) – p. 571 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | нещирості, корупції, брудних прийомах, особистих амбіціях, та ігноруються справжня суть та чесні наміри. По-суті, стверджується, чим більший вплив на медії, тим менше буде громадської довіри та участі. Причини криються в процесі медіатизації та пов'язані із медіа-логікою. | climate in which trust and the wish to participate in the democratic process is diminished. In effect, the thesis holds that the more exposure to the media, the less there will be public trust and participation. The causes are held to lie especially in the process of mediatization and are also linked to media logic. | |
| 301. | **Спроможніть до стримування**<br>спроможність або технічна здатність здійснювати дії, що нав'язують витрати супротивнику.<br>Один із "*трьох С*" – *компонентів стримування*. | **Capability of deterrence**<br>the ability or technical capacity to carry out actions that impose costs on the adversary.<br>One of the *'three Cs' of deterrence*. | MCDC(a) (2019) – p.35 |
| 302. | **Спуфінг / Підміна**<br>Це методи *РЕБ*, які вводять в оману електромагнітний приймач, підміняючи сигнал на фальшивий, з помилковою інформацією. | **Spoofing**<br>It`s *EW*-techniques which deceive the receiver by introducing a fake signal with erroneous information. | DIA (2022) – p. 44 |
| 303. | **Стакснет**<br>атака, що спрямована на суспільство (інфраструктуру) – фінансовий сектор, водопостачання та інші інфраструктурні об'єкти. Стакснет – комп'ютерний хробак, який використовують для диверсій в автоматизованих системах контролю промислових підприємств, електростанцій, аеропортів тощо. | **Stutznet / Stuxnet**<br>attacks aimed specifically at society (infrastructure) – at finance, water, power or other infrastructure. Stuxnet is a computer worm, which could be used for sabotage in automated control systems of industrial enterprises, power plants, airports, etc. | Treverton et al. (2018) - p. 54 |
| 304. | **Стандарт оборонного планування**<br>набір суджень і директив для перетворення стратегічної політики в конкретні керівні | **Defense planning standard**<br>a set of judgments and directives for translating strategic policy into concrete guidelines for preparing | Binnendijk & Kugler (2001) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | принципи для підготовки військових сил. Стандарт має три пов'язані між собою функції: визначати чисельність сил та їхні основні завдання; встановити програмні та бюджетні пріоритети; а також інформувати уряд і громадськість про обґрунтування оборонної стратегії та позиції сил. | military forces. This standard has three associated roles: to determine the size of forces and their main missions; to establish program and budgetary priorities; and to inform the government and the public of the rationale behind the defense strategy and force posture. | |
| 305. | **Стандартизація**<br><br>розробка та втілення концепцій, доктрин, процедур і планів із метою досягнення та підтримання сумісності, взаємозамінності або спільності, які необхідні для досягнення належного рівня взаємодії й оптимізації використання ресурсів у сфері проведення операцій, матеріально-технічного забезпечення та управління. | **Standardization**<br><br>the development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability or commonality which are necessary to attain the required level of interoperability, or to optimise the use of resources, in the fields of operations, materiel and administration. | NSA (2013) – p. 2-S-10 |
| 306. | **Стійкість / резильєнтність**<br><br>1. Базове визначення: це здатність відновлюватись після порушень<br><br>2. Для складних систем: властивість для захисту системи від структурних порушень, які змінюють самі чинники розвитку (на відміну від Надійності). Складається з комбінації Опорності (резистентності) та Відновлюваності. Містить наступне: здатність уникати аварій завдяки передбаченню, виживати під час порушень завдяки відновленню, та зростати через адаптацію.<br><br>3. В контексті гібридних загроз: | **Resilience**<br><br>1. Basic definition: the ability to recover after disturbances<br><br>2. For complex systems: the property for protecting the system from structural disturbances that alter the very factors of development (by contrast "Robustness"); is a combination of Resistance and Recovery. Contains the following: the ability to circumvent accidents through anticipation, survive disruptions through recovery, and grow through adaptation.<br><br>3. In the hybrid threats context:<br><br>• the ability of society and government to absorb, withstand | MCDC(a) (2019) – p.90<br><br>Gryshko et al. (2024)<br><br>Jungwirth et al. (2024) - p.27 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | • здатність суспільства та уряду долати порушення та зовнішні потрясіння, протистояти їм та відновлюватись. Заходи щодо підвищення стійкості сприяють *Стримуванню Шляхом Заперечення*.<br>• здатність не тільки протистояти викликам і справлятися з ними, але й проходити перехідний період у стійкий, справедливий і демократичний спосіб. Це - ключова властивість для протидії гібридним загрозам | and recover from disruption and external shocks. Measures to increase resilience contribute to *Deterrence By Denial.*<br>• the ability not only to withstand and cope with challenges but also to undergo transitions in a sustainable, fair, and democratic manner. This is a key feature for countering hybrid threats. | |
| 307. | **Стійкість критичної інфраструктури**<br>спроможність *Критичної Інфраструктури* надійно функціонувати в нормальному режимі, адаптовуватись до умов, що постійно змінюються, протистояти та швидко відновлюватись після аварій та технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ. | **Critical infrastructure resilience.**<br>The ability of the *Critical Infrastructure* to function reliably in the normal mode, adapt to continuously changeable conditions, resist and promptly recover after accidents and technical failures, malicious actions, natural disasters and hazardous natural phenomena. | Horbulin (2017) – p.156 |
| 308. | **Стратегічне командування**<br>командна організація на найвищому рівні структури військового командування НАТО. Довідково: Існує два стратегічних командування, а саме: командування ОЗС НАТО з питань операцій та командування ОЗС НАТО з питань трансформацій. | **Strategic command / SC**<br>the command organization at the highest level of the NATO military command structure. Note: There are two strategic commands, namely, Allied Command Operations and Allied Command Transformation. | NSA (2013) – p. 2-S-12 |
| 309. | **Стратегічні комунікації / СтратКом**<br>скоординоване та належне використання комунікаційних | **Strategic communications**<br>the mean coordinated and proper use of state communication | Horbulin (2017) – p.159 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | можливостей держави - публічної дипломатії, зв'язків із громадськістю, військових зв'язків із громадськістю, інформаційно-психологічних операцій, заходів, спрямованих на просування завдань держави. | capacities – public diplomacy, public relations, military public relations, information and psychological operations, events designed to facilitate and meet the targets of the country. | |
| 310. | **Стратегічні цілі**<br>цілі стратегії протидії гібридній війні. Стратегічні цілі відображають рівень амбіцій захисника. | **Strategic goals**<br>the aims of the strategy to counter hybrid warfare. Strategic goals reflect the level of ambition of the defending actor. | MCDC(a) (2019) – p.90 |
| 311. | **Стратегія клину**<br>тип державної стратегії, спрямований на запобігання утворенню ворожих альянсів або на роз'єднання тих, що вже утворилися. Ці стратегії можуть спричинити розстановку сил, яка в іншому випадку була б малоймовірною, і, таким чином, мати значні наслідки для міжнародної політики. | **Wedge Strategy**<br>the type of state strategy to prevent hostile alliances from forming or to disperse those that have formed. These strategies can cause power alignments that are otherwise unlikely to occur, and thus have significant consequences for international politics. | Wigell (2019) |
| 312. | **Стратегія "цільового зміцнення"**<br>термін, який використовують поліцейські, працівники охорони та військові; передбачає посилення безпеки будівлі чи споруди з метою її захисту у випадку нападу або зменшення ризику крадіжки. Вважається, що "сильний, видимий захист стримуватиме або затримуватиме атаку". | **"Target hardening" strategy**<br>a term used by police officers, those working in security, and the military referring to the strengthening of the security of a building or installation in order to protect it in the event of attack or reduce the risk of theft. It is believed that a "strong, visible defence will deter or delay an attack" | Falk (2020) – p. 3 |
| 313. | **Стримування**<br>один зі способів перешкоджання діяльності, яка суперечить інтересам держави або | **Deterrence**<br>the discouraging activities that conflict with the interests of the State or the international rule of law by | Van Haaster (2019) – p.48 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | міжнародному верховенству права, через створення перспективи "заходів у відповідь". | holding out the prospect of retaliatory measures. | |
| 314. | **Стримування шляхом заперечення**<br><br>Одна із стратегій стримування як інструмент протидії гібридній війні.<br><br>Покликане підірвати здатність супротивника досягти своєї мети, в першу чергу шляхом, наприклад, "загартовування" цілі. | **Deterrence by denial**<br><br>One of the deterrence strategy as a tool for countering hybrid warfare.<br><br>Aims to undermine the ability of the adversary to achieve their objective in the first instance through, for example, 'hardening' the target. | MCDC(a) (2019) – p.35, 89 |
| 315. | **Стримування шляхом покарання**<br><br>Одна із стратегій стримування як інструмент протидії гібридній війні.<br><br>Має на меті переконати противника в тому, що витрати на досягнення його мети будуть занадто високими. | **Deterrence by punishment**<br><br>One of the deterrence strategy as a tool for countering hybrid warfare.<br><br>Aims to persuade the adversary the costs of achieving their objective will be prohibitive by threatening retaliation to aggressive action. | MCDC(a) (2019) – p.36, 89 |
| 316. | **САПс** – див. *Пакети Синхронізованих Атак* | **SAPs** - see *Synchronized Attack Packages* | |

## T

| № | UA | EN | Джерело |
|---|---|---|---|
| 317. | **Тактичний рівень штучного інтелекту**<br><br>На тактичному рівні *Штучний Інтелект* може забезпечити поліпшене та більш швидке усвідомлення ситуації екіпажами бойових машин. Він може автоматизувати виявлення загроз за допомогою розпізнавання людей або типів об'єктів, а також за допомогою розпізнавання потенційно небезпечної поведінки. І навпаки, система може використовувати ШІ для запису інформації у формі природного мовлення, оцифрування та надання доступу до системи в попередньо обробленій формі, тим самим значно підвищуючи ефективність. Технології на базі ШІ, швидше за все, полегшать логістичне навантаження, забезпечать військово-технологічну перевагу та збільшать час бойового реагування. | **AI Tactical level**<br><br>At the tactical level, *Artificial Intelligence* may provide improved and faster situational awareness for the crews of combat vehicles. It can automate threat detection by recognizing persons or object types, but also by recognizing potentially dangerous behaviours. Conversely, the system can use Artificial intelligence to record information in the form of natural speech, digitize it, and make it available to the system in a pre-processed form, thereby significantly increasing efficiency. Artificial intelligence enabled technologies will likely ease logistical burdens, ensure military-technological superiority and enhance combat reaction times. | Thiele (a) (2020) – p.10<br><br>Horowitz (2018) |
| 318. | **Тейлгейтинг (переслідування)**<br><br>це стеження за авторизованою особою в зоні або системі з обмеженим доступом. Приклад: зловмисник, одягнений як співробітник, несе велику коробку і переконує жертву, яка є уповноваженим співробітником та заходить одночасно із зловмисником, відкрити двері дата-центру за допомогою перепустки жертви. Доступ до закритих зон повинен контролюватися політикою доступу | **Tailgating**<br><br>is the act of following an authorised person into a restricted area or system. Example: the attacker, dressed as an employee, carries a large box and convinces the victim, who is an authorised employee entering at the same time, to open the door of the data-centre using the victim's RFID pass. Access to non public areas should be controlled by access policies and/or the use of access control technologies, the more sensitive the area the stricter the | ENISA (n.d.) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | та/або використанням технологій контролю доступу, при цьому, чим важливіша зона, тим суворіша комбінація кодів. Обов'язок носити бейдж, присутність охоронця та власне протизламні двері, такі як двері-пастки з радіочастотним контролем доступу, зазвичай достатньо для запобігання проникненню зловмисників. | combination. The obligation to wear a badge, the presence of a guard and actual anti-tailgating doors such as mantraps with RFID access control should be sufficient to deter most attackers. | |
| 319. | **Темна реклама**<br><br>є одним із методів *Когнітивного Зламу*<br><br>це повідомлення, які побудовані на основі психографічного профілю людини. Великі дані можуть бути використані для створення бази даних про людей зі схожою ідеологічною позицією та рисами особистості. Придбані рекламні оголошення, які можуть бачити лише відповідні люди, можуть містити повідомлення, що апелюють до їх психологічних схильностей та спонукають до певної форми поведінки чи дій. | **Dark Ads**<br><br>is one of the *Cognitive Hacking* methods<br><br>is messages, which are tailored based upon an individuals' psychographic profile. Big data can be used to create a database of individuals with a similar ideological stance and personality traits. Purchased advertisements that only they can see could include messages that appeal to their psychological leanings and encourage a certain form of behaviour or action. | MSB (2018) – p.19-20 |
| 320. | **Теорія економічного стримування**<br><br>теорія, згідно якої платнику податків потрібні економічні фактори, щоб мати можливість вирішити чи виконувати податкові зобов'язання. Дії платників податків залежать від очікуваних вигод. Найбільш відомим підходом стримування, який змушує платників податків виконувати зобов'язання, є загальний підхід стримування, який пов'язаний з ефектом можливих санкцій і покарань. Центральним | **Economic deterrence theory**<br><br>theory advocates that taxpayer need economic factors to be able to decide whether to comply with tax obligations. The action taken by taxpayers on whether to comply is dependent on the likelihood of the expected utilities. The most well-known deterrence approach that makes taxpayers comply is the general deterrence approach, which is related to the effect of likely sanctions and punishment. The central argument of the deterrence | Ya'u et al. (2023) – p. 292 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | аргументом теорії стримування є те, що такі змінні, як податкова ставка, штраф і ймовірність виявлення, є функцією поведінки платників податків при прийнятті рішень. | theory is that variables, such as tax rate, penalty, and detection probability, are the function of taxpayers' decision-making behavior. | |
| 321. | **Теорія залежності від ресурсів**<br>теорія, що розглядає організацію як соціальну систему, боротьбу організацій на основі організаційних відносин і зв'язків із середовищем, і намагається пояснити баланс сил і рівнів залежності на етапі отримання ресурсів, необхідних для виживання. | **Resource dependence theory**<br>a theory that sees an organization as a social system, deals with the struggles of organizations on the basis of organizational and environmental relations, and tries to explain the balance of power and dependence levels at the point of obtaining the resources necessary for their survival. | Ilhan (2020) – p.177 |
| 322. | **Теорія змови (Конспірологічна теорія)**<br>теорія, згідно з якою пояснення будь-якого соціального явища полягає у з'ясуванні того, хто зацікавлений у появі цього явища. Звичайно, ця точка зору випливає з помилкової теорії, згідно з якою все, що трапляється в суспільстві - особливо такі події, як війна, безробіття, бідність, дефіцит, які люди, як правило, не люблять, - це прямий задум деяких впливових осіб та груп. | **Conspiracy theory of society**<br>"there is a view, which I shall call the conspiracy theory, which holds that the explanation of any social phenomenon consists in finding out who is interested in the occurrence of this phenomenon. This view arises, of course, from the mistaken theory that, whatever happens in society—especially happenings such as war, unemployment, poverty, shortages, which people as a rule dislike—is the direct design by some powerful individuals and groups." | Popper, K. (2020) – p.306<br>Vilmer et al. (2018) - p.35 |
| 323. | **Тероризм внутрішній**<br>діяльність, пов'язана з діями, небезпечними для життя людини, що є порушенням кримінального законодавства країни; має на меті залякування або примус цивільного населення; вплив на політику уряду шляхом | **Domestic terrorism**<br>activities that involve acts dangerous to human life that are a violation of the criminal laws of the country; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to | United States Code (2010) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | залякування чи примусу; або вплив на поведінку уряду шляхом масового знищення, убивства чи викрадення; і відбувається переважно у межах територіальної юрисдикції країни. | affect the conduct of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the country. | |
| 324. | **Тероризм міжнародний**<br><br>діяльність, що передбачає насильницькі дії або дії, небезпечні для життя людини, і є порушенням кримінального законодавства країни; має на меті залякування або примус цивільного населення до певних дій; вплив на політику уряду шляхом залякування чи примусу; або вплив на поведінку уряду шляхом масового знищення, вбивства чи викрадення; виходить за рамки національних кордонів з точки зору засобів, за допомогою яких вони здійснюються, осіб, яких вони мають на меті залякати чи примусити до певних дій, або місць, де злочинці діють або шукають собі притулку. | **International terrorism**<br><br>activities that involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the country; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping; and transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum. | United States Code (2010) |
| 325. | **Технічне використання**<br><br>є одним із методів інформаційного впливу (див. *Кампанії Впливу*)<br><br>Діяльність інформаційного впливу часто використовує нові інформаційні технології. Використовуючи більш досконалі технічні навички, ніж ті, якими володіє більшість людей, вони можуть маніпулювати потоками інформації в Інтернет. Маніпуляції проводять окремі особи, автоматизовані профілі або алгоритми, а також комбінації | **Technical exploitation**<br><br>is one of the information influence techniques (see *Influence Campaigns*)<br><br>Information influence activities often make use of, and exploit, new technologies. By using more advanced technical skills than most individuals possess, they can manipulate flows of information online. Manipulation can be conducted by individuals, by automated accounts or algorithms, and by combinations of people and | MSB (2018) – p.19, 23 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | людей та автоматизації. Слід зазначити, що Технічне Використання часто застосовує технологічну перевагу для здійснення цілком традиційних методів інформаційного впливу, таких як *Оманливі Ідентичності*, *Дезінформація* та підробка.<br><br>Сюди відносимо: *Боти, Маріонетка, Діпфейки, Фішинг* тощо. | automation. It should be noted that technical exploitation often uses a technological advantage to perform quite traditional information influence techniques such as *Deceptive Identities, Disinformation* and forgery.<br><br>it includes: *Bots, Sock Puppet, Deep Fakes, Phishing* etc. | |
| 326. | **Торгова війна**<br><br>конфлікт двох або кілької країн у сфері зовнішньоторговельних відносин, супроводжуваний застосуванням дискримінаційних умов торгівлі та реалізований тарифними і нетарифними методами. Застосовується як у межах чинних міжнародних та національних норм, так і поза ними, з метою отримання економічних та політичних переваг над іншою країною-супротивноким. Може бути спрямована на захоплення ринків інших країн, а також на захист національного ринку. Є різновидом економічних війн (як-от валютна, енергетична, продовольча війни тощо). | **Trade war**<br><br>the international trade conflict between two or more states accompanied by the use of discriminatory rules of trade. It is realized by tariff and non-tariff trade defense methods. TW is used both in and out of the existing international and national regulations with aim to gain economic and political advantages at the expenses of the rival country. TW can be directed to the expansion on the other countries' markets as well as to national markets protection. TW is one of the type of economic war (such as currency, energy, food wars, etc.). | Horbulin (2017) – p.159 |
| 327. | **Традиційні ЗМІ**<br><br>засоби масової інформації, що керуються професіоналами (на відміну від *Нових ЗМІ*) | **Traditional Mass Media**<br><br>the media which operated by professionals (by contrast of the *New Mass Media*) | Robbin & Buente (2008) – p.2214 – 2215 (p.5 – 6)<br><br>Szwed (2016) – p.12 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 328. | **Транс-культурна (етнічна) дифузія**<br>розповсюдження культурних елементів, як-от ідеї, стилі, релігії, технології, мови тощо між людьми, в межах однієї культури або від однієї культури до іншої. | **Trans-cultural diffusion**<br>the spread of cultural items—such as ideas, styles, religions, technologies, languages etc.—between individuals, whether within a single culture or from one culture to another. | Hume & Hume (2014) |
| 329. | **«Три С» стримування**<br>основні принципи стримування, як важливого інструменту протидії гібридній війні: Переконливість стримування, *Спроможність до стимування, Комунікація заради стримування*. | **'Three Cs' of Deterrence**<br>basic principles of deterrence as an important tool for countering hybrid warfare: *Credibility of deterrence*, *Capability of deterrence, Communication for deterrence.* | MCDC(a) (2019) – p.35 |
| 330. | **"Три війни"**<br>військова стратегія Китаю: Як у мирний, так і у воєнний час застосування трьох видів війни (*війна за громадську думку, психологічна війна, юридична війна*) має на меті контролювати переважаючі дискурси та впливати на сприйняття таким чином, щоб просунути інтереси Китаю, одночасно ставлячи під загрозу можливості опонентів відповідати. | **"Three Warfares"**<br>the China's military strategy: in peacetime and wartime alike, the application of the three warfares (*public opinion warfare, psychological warfare, legal warfare*) is intended to control the prevailing discourse and influence perceptions in a way that advances China's interests, while compromising the capability of opponents to respond. | Vilmer et al. (2018) - p.60<br>Kania (2016)<br>Cullen et al. (2021) – p.19 |
| 331. | **Тролі**<br>особи, які поширюють інформацію, насичують певні веб-сайти коментарями та / або переслідують інші.<br>користувач акаунту в соціальних мережах, який навмисно викликає незадоволення в інших користувачів своїми коментарями та поведінкою, що сприяє | **Trolls**<br>individuals who spread information, saturate certain websites with comments, and/or harass others.<br>a user of a social media account who deliberately antagonises other users through their comments and behaviour. This contributes to increased polarization, silences | Vilmer et al. (2018) - p.84<br>MSB (2018) – p.19, 25 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | посиленню поляризації, замовчує суперечливі думки та заглушує законну дискусію. Троль керується або особистими спонуканнями, або, як у випадку з гібридними тролями, діє під керівництвом когось іншого. | dissenting opinions, and drowns out legitimate discussion. The troll is governed either by personal motivations or, as in the case of hybrid trolls, operates under the direction of someone else | |
| 332. | **Тролінг**<br><br>така поведінка, як публікація провокаційних коментарів в Інтернеті з метою викликати конфлікт.<br><br>Як правило, протікає у три фази: заманювання, захоплення приманки та витягування. | **Trolling**<br><br>behaviour such as publishing provocative comments on the internet with the intention of causing conflict.<br><br>Generally proceeds in three phases: luring, taking the bait and hauling in. | Vilmer et al. (2018) - p.86<br><br>Szwed (2016) – p.7, 54 |
| 333. | **ТТП(с)**<br><br>абревіатура, яка розшифровується як "Тактика, методи і процедури" (англ.), є ключовим поняттям у кібербезпеці та розвідці загроз. Це підхід до визначення моделей поведінки, що можуть бути використані для захисту від конкретних стратегій і векторів загроз, що використовуються зловмисниками:<br><br>• Тактика - це найвищий рівень опису такої поведінки, і це діяльність, яку суб'єкт (що здійснює інцидент FIMI), найімовірніше, буде використовувати.<br>• Методи дають більш детальний опис поведінки в контексті тактики і показують, як суб'єкт може застосовувати тактику (тактики). | **TTP(s)**<br><br>is an acronym that stands for "Tactics, Techniques, and Procedures", a key concept in cybersecurity and threat intelligence. The purpose is to identify patterns of behaviour which can be used to defend against specific strategies and threat vectors used by malicious actors.<br><br>• A tactic is the highest-level description of this behaviour and is the activity that an actor (conducting a FIMI incident) is likely to use.<br>• Techniques give a more detailed description of behaviour in the context of a tactic and are how an actor might conduct the tactic(s).<br>• Procedures are an even lower-level, highly detailed description in the context of a technique and are the detailed steps that | Johnson et al. (2016) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | • Процедури - це ще більш низький рівень, дуже детальний опис в контексті методу і є детальними кроками, які визначають, як виконувати конкретні завдання. | prescribe how to perform specific tasks. | |
| 334. | **"Туман війни"**<br>відсутність інформації у командира на багатьох рівнях - від тактичного до великого стратегічного | **'Fog of war'**<br>the absence of information a commander has across a multitude of levels, from the tactical to the grand strategic | Mumford (2020) – p. 4 |

## У

| № | UA | EN | Джерело |
|---|---|---|---|
| 335. | **Угода про стандартизацію НАТО**<br>нормативний документ, що представляє собою угоду між кількома або всіма країнами-членами НАТО, який був ратифікований на рівні урядів держав із метою втілення певних стандартів повністю або частково. | **NATO standardization agreement (STANAG)**<br>a normative document, recording an agreement among several or all NATO member nations, that has been ratified at the authorized national level, to implement a standard, in whole or in part, with or without reservation. | NSA (2013) – p. 2-N-2 |
| 336. | **Українська "Революція гідності"** (Євромайдан)<br>Див. *Євромайдан* | **Ukraine's "Revolution of Dignity"** (the Euromaidan)<br>See *Euromaidan* | |
| 337. | **Управління кіберзагрозами**<br>практика керування кіберзагрозами, що виходить за рамки базової оцінки ризиків в Системі управління інформаційною безпекою. Воно забезпечує раннє виявлення загроз, ситуаційну обізнаність на основі даних, точне прийняття рішень та своєчасні дії щодо пом'якшення загроз. | **Cyber Threat Management (CTM)**<br>the practice for managing cyber threats beyond the basic risk assessment found in Information Security Management System (ISMS). It enables early identification of threats, data-driven situational awareness, accurate decision-making, and timely threat mitigating actions. | EE-ISAC (2020) – p.7 |
| 338. | **Урядовість**<br>форма знання й практичної політики, заснована на логіці ринкової та ліберальної політичної економії. Вона діє через стимули (само)регулювання та передбачає оцінку ризиків, обчислення, просування найкращих практик, сприяння конкурентоспроможності через індексацію, бенчмаркінг країни, | **Governmentality**<br>a form of both knowledge and practical politics, based on the logics of market and liberal political economy. It operates through (self-)regulative incentives and implies risk assessment, calculation, best practices promotion, fostering of competitiveness through indexing, country benchmarking, various empowerment techniques. | Wallenstein (2013) – p. 28. |

| № | UA | EN | Джерело |
|---|---|---|---|
| | різні методи розширення повноважень. | | |
| 339. | **Ухил / Упередженість**<br><br>Будь-яка тенденція ухилятися в новинах від точного, нейтрального, збалансованого та неупередженого зображення “реальності” подій і соціального світу відповідно до визначених критеріїв. Зазвичай розрізняють умисний і неумисний ухил. Перший пов’язаний з прихильністю, уподобаннями й ідеологічною заангажованістю медій або джерел інформації. Другий загалом стосується організаційних та рутинних чинників у доборі та опрацюванні новин. | **Bias**<br><br>Any tendency in a news report to deviate from an accurate, neutral, balanced and impartial representation of the ‘reality’ of events and social world according to stated criteria. A distinction is usually made between intended and unintended bias. The former stems mainly from partisanship, advocacy and the ideological standpoint of the medium or source. The latter is generally attributed to organizational and routine factors in selection and processing of news. | McQuail's, D. (2010) – p. 549 |

## Ф

| № | UA | EN | Джерело |
|---|---|---|---|
| 340. | **Фабрикація**<br><br>один із методів *Дезінформації*.<br><br>Інформація, що не має фактичної основи, опублікована у стилі, який вводить аудиторію в оману, змушуючи повірити в її достовірність. Наприклад, фальшивий мейл від політика може бути надрукований і переданий у пресу, щоб підірвати довіру до цього політика. | **Fabrication**<br><br>is one of the *Disinformation* methods.<br><br>Information with no factual basis published in a style that misleads the audience to believe it to be legitimate. For example, a fake e-mail from a politician might be produced and leaked to the press to undermine that politician's credibility. | MSB (2018) – p.19, 25 |
| 341. | **Фейковий аккаунт**<br><br>або обліковий запис (профіль), яким керує хтось, хто видає себе за когось іншого,<br><br>або облікові записи, якими керують не люди, а автоматизовані (боти).<br><br>Фейкові акаунти в соціальних мережах – "піхота в цій формі війни". Вони працюють, щоб посилити повідомлення, ввести хештеги та залякати або заблокувати інших користувачів. | **Fake Account**<br><br>either an account that is managed by someone pretending to be someone else or accounts that are not managed by people, but are automated (bots).<br><br>The fake accounts on social media are "the foot soldiers in this form of warfare." They work to amplify the message, introduce hashtags and intimidate or block other users. | Vilmer et al. (2018) - p.81<br><br>Parliament Of Singapore (2018) - p. 15 (# 71)<br><br>Nimmo, B. (2018) – p.6 (# 33) |
| 342. | **Фейкові медіа**<br><br>метод, який використовується в *Оманливих Ідентичностях*.<br><br>Дезінформація може розповсюджуватися шляхом створення підроблених медіа платформ, які виглядають або мають веб-адресу, як справжні сайти новин. | **Fake Media**<br><br>a method that is used in *Deceptive Identities*.<br><br>Disinformation can be circulated by creating fake media platforms that look like, or that have a web address similar to, a real news site. | MSB (2018) – p.19-20 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 343. | **Фейкові новини**<br><br>Поняття фейкових (підроблених, фальшивих) новин включає як спотворення об'єктивних істин, так і оманливі історії.<br><br>Крім того, розповсюдження фальшивих новин забезпечується соціальними мережами, які загалом не вимагають перевірки опублікованих матеріалів, а також забезпечують зручну платформу для охоплення аудиторії.<br><br>Див. також *Нові ЗМІ* | **Fake News**<br><br>Fake news, a concept, includes both distortions of objective truths as well as misleading stories.<br><br>Furthermore, spreading fake news is enabled by social media, which in general does not require verification of published posts and also provides a handy platform to reach audiences.<br><br>See also: *New Mass Media* | Treverton et al. (2018) - p.57 |
| 344. | **Фільтрування**<br><br>загальний термін, яким позначають роль в інформаційних організаціях початкового добору та пізнішого редакторського опрацювання повідомлень про події. Працівники новинних медій мають вирішувати, які "події" пропустити через медійні "ворота", зважаючи на те, наскільки вони "вартують" бути новинами, та на інші критерії. Найважливіші питання стосуються критеріїв добору і систематичного упередження, які виявляються у процесі фільтрування. | **Gatekeeping**<br><br>general term for the role of initial selection and later editorial processing of event reports in news organizations. News media have to decide what 'events' to admit through the 'gates' of the media on grounds of their 'newsworthiness' and other criteria. Key questions concern the criteria applied and the systematic bias that has been discerned in the exercise of the role. | McQuail's, D. (2010) – p. 558 |
| 345. | **Фінансовані урядом аккаунти, веб-сторінки чи програми**<br><br>власні акаунти, веб-сайти та додатки, які фінансує уряд, та призначені для поширення політичної пропаганди. Ці облікові записи та зміст, що надходить з них, чітко позначені як урядові. | **Government-sponsored accounts, web pages or applications**<br><br>own government-sponsored accounts, websites and applications designed to spread political propaganda. These accounts and the content that comes out of them are | Bradshaw & Howard (2017) – p.10 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | | clearly marked as government operated. | |
| 346. | **Фінансування організацій**<br>Забезпечення організацій коштами для виконання їх статутних задач.<br>Багато урядів прагнуть фінансувати організації чи аналітичні центри, які просувають погляди, що відповідають їхнім інтересам. Просування ідей, що сприяють розвитку інтересів країни, є одним із найдавніших інструментів політичного та соціального впливу. | **Funding of Organizations**<br>Providing organizations with funds to fulfill their statutory tasks.<br>many countries seek to fund organizations or think-tanks that promote views friendly to their interests. Promoting ideas that further a country's interest is one of the oldest tools of political and social influence. | Treverton et al. (2018) - p.58 |
| 347. | **Фішинг**<br>є одним із інструментів *Технічного Використання*<br>Ці підходи намагаються оманою змусити користувачів розкрити паролі та іншу конфіденційну інформацію. Фішинг містить автоматичне розсилання імейл-спаму, яке виглядає законним, але веде до фальшивих веб-сайтів, які можуть збирати будь-яку введену особисту інформацію користувачів.<br>Цільовий фішинг передбачає більш складне націлювання на користувачів для отримання доступу, наприклад, до захищеної комп'ютерної системи роботодавця. | **Phishing**<br>Is one of the *Technical Exploitation* tools.<br>These approaches attempt to trick users into revealing passwords and other sensitive information. Phishing involves automated spamming of emails that look legitimate but that lead to fake websites which can then harvest any personal information entered.<br>Spear phishing involve the more sophisticated targeting of individuals to gain access to e.g. their employer's secure computer system. | MSB (2018) – p.19, 23 |
| 348. | **Флуд**<br>один із способів поєднання методів інформаційного впливу (див. *Кампанії Впливу*). | **Flooding**<br>one of the ways to combine of information influence techniques (see *Influence Campaigns*). | MSB (2018) – p.29 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Флуд створює плутанину, перевантажуючи аудиторію будь-якою інформацією: позитивною, негативною чи неактуальною.<br><br>Це робиться за допомогою спаму та *Тролінгу* в соціальних мережах або шляхом поширення дезінформації до правомірних джерел ЗМІ. Флуд витісняє легітимну інформацію. | Flooding creates confusion by overloading audiences with information, either positive, negative or irrelevant.<br><br>This can be done by spamming and *Trolling* on social media, or by disseminating disinformation to legitimate media sources. Flooding crowds out legitimate information. | |
| 349. | **Фреймінг** (або **Обмеження рамками**)<br><br>(для медійних зображень об'єктів, подій, особистостей або груп)<br><br>механізм, який може бути використаний для пояснення фактичного впливу стверджень на аудиторію. Фреймінг пояснює процес, за допомогою якого ЗМІ вирішують, про що люди повинні думати і яким чином, хоча вони не говорять їм, що саме думати.<br><br>Фреймінг введено до галузі соціального аналізу Ервінгом Гофманом, який розумів рамки (фрейми) як схеми інтерпретації, які дозволяють людям знаходити, помічати, ідентифікувати та надавати значення подіям, що відбуваються в їхньому особистому житті, а також у навколишньому світі. Завдяки фреймам деякі випадкові, незв'язані елементи або події будують єдине ціле, відповідаючи на питання "Що тут відбувається?" | **Framing**<br><br>(for media representations of objects, events, personalities or groups)<br><br>a mechanism that can be used to explain the actual influence of statements on recipients. Framing explains the process by which media decide what people should be thinking about and in what way, even though they do not tell them exactly what to think.<br><br>Framing was brought into the field of social analysis by Erving Goffman who understood frames as blueprints of interpretation which enable individuals to locate, notice, identify and give meaning to events taking place in their personal lives, as well as in the world around them. Thanks to frames some coincidental, loose elements or events construct a coherent whole, answering the question "What is going on here?" | Szwed (2016) – p.14-15<br><br>Goffman (1986) – p.8-10<br><br>Benford & Snow (2000) – p.614 |

## X

| № | UA | EN | Джерело |
|---|---|---|---|
| 350. | **Хакінг** (дослівно - злам)<br><br>злам означає отримання несанкціонованого доступу до комп'ютера або мережі та є злочином.<br><br>є одним із методів *Символічних Дій*.<br><br>Разом з інформаційним впливом хакерство може слугувати символічною дією, повідомляючи, що такі організації можуть бути скомпрометовані, що платформа не захищена або відкрита для шантажу. | **Hackning**<br><br>hacking means to gain unauthorized access to a computer or a network and is a crime.<br><br>is one of the *Symbolic Actions* methods.<br><br>In information influence activities, hacking can serve as a symbolic action by communicating that an organization's data can be compromised, that a platform lacks security, or to open for blackmail. | MSB (2018) – p.19, 27 |
| 351. | **ХБРЯв-подія**<br><br>абревіатура ХБРЯв означає: хімічне, біологічне, радіологічне, ядерне та вибухове.<br><br>Надзвичайна ситуація, пов'язана з хімічними, біологічними, радіологічними або ядерними матеріалами, можливо, у поєднанні з вибуховими речовинами (для поширення цих речовин). Це може відбутись через:<br><br>• нещасний випадок або вимушену подія (транспортний інцидент, пандемія тощо);<br>• зловмисну подію (злочин, терористичний акт тощо);<br>• використання або присутність військового обладнання, установок або агентів, що вимагає міждисциплінарного | **CBRNE incident**<br><br>the abbreviation CBRNE means Chemical, biological, radiological, nuclear, and explosive.<br><br>An emergency involving chemical, biological, radiological, or nuclear materials, possibly combined with explosives (to spread these materials). This may be due to:<br><br>• an accident or an involuntary event, for example, a transport incident or a pandemic;<br>• a malicious event, such as a crime or terrorist attack;<br>• the use or presence of military equipment, installations, or agents requiring multidisciplinary management and/or coordination at the national level. | Belgium National Crisis Center (n.d.) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | управління та/або координації на національному рівні. | | |

# Ц

| № | UA | EN | Джерело |
|---|---|---|---|
| 352. | **Центр дослідження асиметричних загроз (CATS)**<br><br>національний центр в Шведському університеті оборони, на який покладено завдання розробляти та поширювати знання про асиметричні загрози в контексті соціальної безпеки та стійкості | **Center for Asymmetric Threat Studies (CATS)**<br><br>a national centre within the Swedish Defence University tasked with developing and disseminating knowledge about asymmetric threats within the context of societal security and resilience | Treverton et al. (2018) - p. 93<br><br>Swedish Defence University (n.d.) |
| 353. | **Цивільні аспекти кризового менеджменту в Спільній зовнішній політиці і політиці безпеки Європейського Союзу**<br><br>кризовий менеджмент, який часто відбувається у постконфліктний період і характеризується гострою нестачею потенціалу, необхідного для забезпечення стійкого миру. У цей період ключове значення має швидке виявлення та своєчасне залучення цивільних фахівців. Консультативний орган ЄС, що займається цивільними аспектами кризового менеджменту – Комітет із цивільних аспектів кризового менеджменту (CFSP) | **Civilian Aspects of Crisis Management in The Common Foreign and Security Policy (CFSP) of the European Union**<br><br>the civilian crisis management takes often place in the post-conflict period, which is often characterized by a critical shortage of capacity needed to secure a sustainable peace environment. In this period the prompt identification and the timely deployment of civilian expertise is of key importance. The Committee for Civilian Aspects of Crisis Management (CivCom) is an advisory body within the European Union dealing with civilian aspects of crisis management. | Stevens (2011) – p.37 |
| 354. | **Цифрова грамотність**<br><br>Компонент *Медіаграмотності*, який описує здатність людей знаходити, орієнтуватися та критично оцінювати інформацію, знайдену в цифрових середовищах. | **Digital literacy**<br><br>A component of *Media Literacy* that describes individuals' capacity to locate, navigate and critically evaluate information found in digital environments. | Neudert & Marchal (2019) – p.5 |

| № | UA | EN | Джерело |
|---|---|---|---|
| 355. | **Цифрова екосистема**<br><br>соціально-технічні мережі взаємозалежних цифрових технологій і відповідних суб'єктів, які зв'язані між собою певним контекстом їхнього використання. | **Digital ecosystem**<br><br>sociotechnical networks of interdependent digital technologies and associated actors that are related based on a specific context of use. | Skog et al. (2018) |
| 356. | **Цифрова платформа** (включно з *Соціальною Мережею*)<br><br>(1) в контексті французької національної стратегії цифрової безпеки<br><br>"Цифрові платформи, включаючи соціальні мережі, можуть більш підступно формувати думку і часто є векторами цінностей, які не належать Французькій Республіці. У певних випадках вони можуть бути використані для цілей дезінформації та поширення пропаганди серед громадян Франції, особливо серед наймолодших. Поширені таким чином думки суперечать фундаментальним інтересам Франції і є нападом на оборону та національну безпеку, що підпадає під регулювання законом".<br><br>(2) в IT-контексті<br><br>сервіс, який виступає посередником для доступу до інформації, контенту, послуг чи активів, що редагують або надають треті сторони. За допомогою алгоритмів, які використовують ці сайти, платформи класифікують контент і встановлюють умови для розповсюдження цього контенту, | **Digital Platform** (*including Social Network*)-<br><br>(1) in the context of the French national digital security strategy<br><br>"Digital platforms, including social networks, can shape opinion more insidiously and are often vectors of values that are not those of the French Republic. In certain cases, they can be used for the purposes of disinformation and spreading propaganda to French citizens, particularly to the youngest ones. The opinions that are disseminated are therefore against France's fundamental interests and are an attack on defense and national security which is sanctioned by law."<br><br>(2) in the IT context<br><br>a service that acts as an intermediary by which to access information, content, services or assets that are edited or provided for by third parties. Through the algorithms that these sites use, the platforms rank content and set the conditions for the diffusion of that content, which is then shared and published. | SGDSN (2015) – p.20<br><br>Vilmer et al. (2018) - p.80 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | який потім надається спільно та публікується. | | |
| 357. | **Цифровий авторитаризм**<br>використання цифрових інформаційних технологій авторитарними режимами для спостереження, репресій та маніпулювання населенням всередені країни та за кордоном, що змінює баланс сил між демократіями та автократіями. | **Digital Authoritarianism**<br>the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations — is reshaping the power balance between democracies and autocracies. | Polyakova & Meserole (2019) – p.1 |
| 358. | **Цифровий збій**<br>тип турбулентності зовнішнього середовища, спричинений цифровими інноваціями, що призводить до розмивання кордонів і підходів, які раніше служили основою для організації виробництва та фіксації вартості. | **Digital disruption**<br>a type of environmental turbulence induced by digital innovation that leads to the erosion of boundaries and approaches that previously served as foundations for organizing the production and capture of value. | Skog et al. (2018) |

## Ч

| № | UA | EN | Джерело |
|---|---|---|---|
| 359. | **"Четверта хвиля" теорії стримування**<br><br>новий напрямок роботи щодо стримування, який почав з'являтися після закінчення холодної війни і набрав обертів після терактів 11 вересня.<br><br>Характеризується двома ключовими елементами, які мають значення для гібридної війни. По-перше, відхід від відносно симетричного взаємного стримування державних суб'єктів у бік стримування "асиметричних" загроз із боку недержавних та псевдодержавних суб'єктів. По-друге, визнання більш широкої концепції стримування, яка виходить за рамки військових засобів. | **'Fourth Wave' Of Deterrence Theory**<br><br>a new line of work on deterrence, which began emerging after the end of the Cold War and gained momentum after the September 11 terrorist attacks.<br><br>Is characterized by two key elements that are relevant to hybrid warfare. First, a shift away from the relatively symmetrical mutual deterrence of state-actors towards deterring 'asymmetric' threats from non-state and pseudo-state actors. Second, the recognition of a broader concept of deterrence that goes beyond military means. | MCDC(a) (2019) – p.38<br><br>Jervis (1979)<br><br>Knopf (2010) |
| 360. | **Чорний лебідь**<br><br>Непередбачувана подія з великим впливом. Незважаючи на відкрите нарощування військової сили росією у 2021 році, її перехід до повномасштабного вторгнення в Україну був, мабуть, основним прикладом цього поняття у 2022 році. Хоча чорні лебеді за своєю суттю непередбачувані, налаштувати своє мислення на передбачення якомога більшого спектру можливих сценаріїв є критично важливим для належного планування та підготовки. Потенційні чорні лебеді можуть охопити весь спектр | **Black swan**<br><br>An unpredictable event with high impact. Notwithstanding Russia's overt military buildup in 2021, its proceeding to a full-scale invasion of Ukraine was arguably the core case study in 2022. While black swans are inherently unpredictable, pushing one's thinking to anticipate as wide a range of scenarios as possible is critical for sound planning and preparedness. Potential black swans could run the gamut from the political implosion of a major economy; the forcible removal of a leader or a government; a significant regional military conflict; an | Grant et al. (2023)<br><br>Ducaru et al., (2019) |

| № | UA | EN | Джерело |
|---|---|---|---|
| | від політичного колапсу великих економік; примусового усунення лідера чи уряду; значного регіонального військового конфлікту; безпрецедентної кліматичної події, яка призведе до масових жертв, хвиль міграції та голоду до чергової пандемії.<br><br>Подія виняткового або екстраординарного характеру, яка є несподіванкою для спостерігача; подія, яка має широкий вплив і підкреслює те, чим спостерігачі знехтували, не розуміючи, що було критичним у їхній системі, процедурі чи підрозділі. | unprecedented climate event that results in mass casualties, waves of migration, and famine; to another pandemic.<br><br>An event with an exceptional or extraordinary character representing a surprise for the observer; one which has a wide impact and highlights something that has been neglected by observers in understanding what was critical in their system, procedure or unit. | |
| 361. | «**Чорний рахунок» (чорна каса)**<br><br>фінансові перекази прихованих грошей, які важко простежити. | **'black account' (chernaya kassa)**<br><br>financial transfers of hidden money, which are much harder to trace. | Galeotti (2020) – p.7 |

## Ш

| № | UA | EN | Джерело |
|---|---|---|---|
| 362. | **Шиллінг**<br><br>метод, який використовується в *Оманливих Ідентичностях*.<br><br>Шилл - це людина, яка створює враження незалежності, але яка насправді працює у партнерстві з кимось іншим. Прикладом можуть бути платні рецензенти товарів на веб-сайтах покупок, члени аудиторії, зайняті аплодуванням оратору під час публічних зборів, або група інтернет-тролів, яким платять за негативні коментарі. | **Shilling**<br><br>a method that is used in *Deceptive Identities*.<br><br>A shill is a person who gives the impression of being independent, but who is in reality working in partnership with somebody else. Examples include paid reviewers of products on shopping websites, audience members employed to applaud a speaker during a public meeting, or a group of online trolls paid to write negative comments. | MSB (2018) – p.19 - 20 |
| 363. | **Шкідливе програмне забезпечення**<br><br>програмне забезпечення, яке використовується для зриву роботи комп'ютерних систем, збору конфіденційних даних або отримання доступу до приватних комп'ютерних систем.<br><br>Приклади "гібридних" застосувань: маніпулювання системами управління повітряним рухом, що призводить до того, що оператори діють на основі хибних даних і видають неправильні вказівки пілотам та літакам, що призводить до різного роду небезпечних ситуацій. | **Malware**<br><br>software that is used to disrupt computer systems, to collect sensitive data or to get access to private computer systems.<br><br>Examples of hybrid applications: Manipulating air traffic control systems, resulting in operators who act upon false data and will issue wrong directions to pilots and aircraft, resulting in all kinds of dangerous situations. | Bekkers et al. (2019) – p.27 |
| 364. | **Штучний інтелект (ШІ)**<br><br>Інтелект, продемонстрований машинами та / або (напів-) автономними системами; | **Artificial intelligence (AI)**<br><br>Intelligence demonstrated by machines and/or (semi-) autonomous systems; | Bekkers et al. (2019) – p.26 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | це загальний термін, що охоплює методи, спрямовані на автоматизацію процесів прийняття рішень, які традиційно вимагають використання людського інтелекту, наприклад, розпізнавання закономірностей, навчання на досвіді, формування висновків, прогнозування чи вжиття заходів. Підживлюваний датчиками, оцифруванням даних та постійно зростаючим зв'язком, ШІ фільтрує, об'єднує, визначає пріоритети, класифікує, вимірює та прогнозує результати, тим самим забезпечуючи більш інформовані рішення на основі даних.<br><br>Приклади "гібридних" застосувань: використання (напів-) автономних систем (безпілотні літальні апарати, кіберзброя тощо) для всіх видів завдань і місій, таких як шпигунство, порушення електромагнітного спектру (радари, радіостанції), а також для вбивства або нейтралізації людей та платформ. За допомогою ШІ ці системи можуть виконувати призначене завдання або місію самостійно, при цьому здатні адаптуватися до нових ситуацій. Також стає важко визначити, хто за цим стоїть. | is an umbrella term that covers methods that aim to automate decision-making processes that traditionally require the use of human intelligence, such as recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action. Fuelled by sensors, data digitization, and ever-increasing connectedness, AI filters, associates, prioritizes, classifies, measures, and predicts outcomes, thereby enabling better-informed, data-driven decisions.<br><br>Examples of hybrid applications: Employing (semi-)autonomous systems (drones, cyber weapons, etc.) for all kinds of tasks and missions, such as spying, disrupting the EM spectrum (radars, radios), but also to kill or neutralise persons and platforms. By using AI these systems can execute the assigned task or mission on their own, while being capable of adapting to new situations. Also, the attribution of responsibility, the who-is-behind-it, becomes difficult to determine. | Thiele (a) (2020) – p.6 |

## Ю

| № | UA | EN | Джерело |
|---|---|---|---|
| 365. | **Ю-есес-мен**<br><br>кліше російської інтернет-пропаганди.<br><br>це гра слів, що зв'язує есесівців (SS, нацистська Німеччина) та американців (USA, США). | **USS-Men**<br><br>a clichés of Russia's internet propaganda.<br><br>is a play on words to link SS-men (Nazi Germany) and US-men (United States). | Szwed (2016) – p.47 |
| 366. | **Юридична війна**<br><br>Техніка маневрування для досягнення юридичної переваги шляхом використання або зміни національного та міжнародного права для отримання політичної ініціативи чи військової переваги. Замість того, щоб розглядати закон як метод раціонального встановлення порядку, юридична війна шукає способи використання правової переваги для впливу на цілі, забезпечуючи ефект поразки, стримування чи захисту за допомогою законних засобів, у тому числі через національний або міжнародний арбітраж.<br>Є одним з 3-х елементів китайської стратегії "*Три війни*" | **Legal Warfare**<br><br>The technique of maneuvering to gain legal superiority by using or modifying domestic and international law to gain political initiative or military advantage. Rather than viewing law as a method of rational order-making, legal warfare looks for ways to use the legal advantage to influence targets by delivering the effects of defeat, deterrence, or defense via legal means, including through national or international arbitration.<br>Is one of the 3 elements of the Chinese strategy *"Three Wars"* | Cullen et al. (2021) – p.22 |
| 367. | **Юридичний / правовий домен гібридних загроз**<br><br>Сукупність правових норм, дій, процесів та інститутів, включаючи як їх нормативний, так і фізичний прояв, які використовуються або можуть бути використані для досягнення юридичних або неправових наслідків у контексті кампаній гібридного впливу. | **legal domain of hybrid threats**<br><br>The aggregate of legal rules, actions, processes, and institutions, including both their normative and physical manifestation, that is or may be utilized to achieve legal or non-legal effects in the context of a hybrid threat campaign.<br>One of the 13 domains in the *Conceptual model of hybrid threats* | Cullen et al. (2021) – p.30 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | Один з 13-ти доменів у *Концептуальній моделі гібридних загроз* | | |

## Я

| № | UA | EN | Джерело |
|---|---|---|---|
| 368. | **Якщодоізм**<br><br>один з методів *Риторики Викривлення (наклепу)*.<br><br>відхилення аргументу через привернення уваги до подібного явища, якому не приділяється стільки уваги. | **Whataboutism**<br><br>one of the *Malign Rhetoric* methods.<br><br>deflecting an argument by drawing attention to a similar phenomenon which does not get as much attention. | MSB (2018) – p.19, 26 |
| 369. | **«Ялтинський порядок» 1945**<br><br>ознаменував апогей статусу великої держави росії та СРСР. Нинішні геополітичні амбіції москви базуються на двох основних елементах цього порядку.<br><br>Перший - поділ Європи на зони впливу та доручення великим державам підтримувати ці зони стабільними; нині ця ідея означала б визнання пострадянського простору сферою виключного впливу поряд із привілейованими інтересами росії.<br><br>Інший - концепція "нерівного суверенітету", де лише великі держави з потужним військовим потенціалом мають повний суверенітет, тоді як незалежність інших держав обмежена за визначенням: вони, як очікується, будуть враховувати інтереси могутніх міжнародних суб'єктів як головний орієнтир для їхньої зовнішньої та внутрішньої політики. За цією логікою, країни Центральної та Східної Європи, імовірно, втілюють інтереси | **the “Yalta order” 1945**<br><br>marked the apogee of Russia-USSR great power status. Moscow’s current geopolitical ambitions build upon two main elements of this order.<br><br>The first one is the division of Europe into zones of influence and entrusting great powers with keeping these zones stable; nowadays, this idea would imply the recognition of the post-Soviet area as a sphere of exclusive influence, alongside the privileged interests of Russia.<br><br>The other is the concept of "non-equal sovereignty", where only great powers with strong military potential enjoy full sovereignty, while the independence of other states is limited by definition: they are expected to consider the interests of the powerful international actors as the main guideline for their foreign and domestic policies. By this logic, Central and East European countries are expected to embody Russian security interests rather than their own, which would be tantamount to | Domańska (2019) – p.6 |

| № | UA | EN | Джерело |
|---|---|---|---|
| | російської безпеки, а не свої, що було б рівнозначно створенню в цьому регіоні своєрідної буферної зони. | the creation of a sort of security buffer zone in this region. | |

## Абревіатури

| № | UA | EN | Джерело |
|---|---|---|---|
| 370. | **AMITT (тепер DISARM)** це абревіатура, яка розшифровується як "Тактика і методи ворожої дезінформації та впливу" (англ.), шаблон для опису інцидентів, пов'язаних з дезінформацією. Містить тактику, методи і процедури - TTP(s) й контрзаходи. | **AMITT (now DISARM)** is an acronym that stands for “Adversarial Misinformation and Influence Tactics and Techniques", a framework for describing disinformation incidents. Includes Tactics, Techniques, and Procedures - TTPs and countermeasures. | Newman (2022) |
| 371. | **DISARM (раніше AMITT**) це абревіатура, яка розшифровується як "Аналіз дезінформації та управління ризиками" (англ.), відкрита платформа з відкритим вихідним кодом для боротьби з дезінформацією шляхом координації ефективних дій. | **DISARM (formerly AMITT)** is an acronym that stands for “DISinformation Analysis & Risk Management (formerly AMITT), the open-source, master framework for fighting disinformation through the coordination of effective action. | Newman (2022) |
| 372. | **FIMI** абревіатура, яка розшифровується як "Зовнішнє інформаційне маніпулювання та втручання" (англ.), часто позначається як "дезінформація " | **FIMI** is an acronym that stands for "Foreign information manipulation and interference", often labelled as ‘disinformation’. | EEAS (2021) |
| 373. | **MISP** це абревіатура, яка розшифровується як "платформа обміну інформацією про шкідливе програмне забезпечення", програмне рішення з відкритим вихідним кодом для збору, зберігання, розповсюдження та обміну індикаторами та загрозами кібербезпеки. | **MISP** is an acronym that stands for "The Malware Information Sharing Platform", an open-source software solution for collecting, storing, distributing, and sharing cybersecurity indicators and threats. | MISP (n.d.) |

| № | UA | EN | Джерело |
|---|---|---|---|
| 374. | **STIX**<br><br>це абревіатура, яка розшифровується як "Структурований вираз інформації про загрози" (англ.), мова, яка розробляється у співпраці з усіма зацікавленими сторонами для специфікації, рбору, опису та передачі стандартизованої інформації про кіберзагрози. Це робиться у структурований спосіб для підтримки більш ефективних процесів управління кіберзагрозами.<br><br>STIX дозволяє аналітикам обмінюватися інформацією про загрози. STIX забезпечує об'єднуючу архітектуру, що зв'язує воєдино різноманітний набір інформації про кіберзагрози, включаючи:<br><br>• кібер-спостережувані дані;<br>• індикатори;<br>• інциденти (події);<br>• тактика, методи та процедури противника (включаючи шаблони атак, шкідливе програмне забезпечення, експлойти, ланцюжки вбивств, інструменти, інфраструктура, таргетинг тощо);<br>• об'єкти атаки (наприклад, вразливості та слабкі місця);<br>• курси дій (наприклад, реагування на інциденти або засоби усунення вразливостей/слабких місць);<br>• кампанії кібератак;<br>• суб'єкти кіберзагроз. | **STIX**<br><br>is an acronym that stands for "Structured Threat Information eXpression", a language being developed in collaboration with any and all interested parties for the specification, capture, characterization, and communication of standardized cyber threat information. It does so in a structured fashion to support more effective cyber threat management processes and application of automation.<br><br>STIX enables analysts to exchange threat information. STIX provides a unifying architecture tying together a diverse set of cyber threat information including:<br><br>• Cyber Observables<br>• Indicators<br>• Incidents<br>• Adversary Tactics, Techniques, and Procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, targeting, etc.)<br>• Exploit Targets (e.g., vulnerabilities and weaknesses)<br>• Courses of Action (e.g., incident response or vulnerability/weakness remedies)<br>• Cyber Attack Campaigns<br>• Cyber Threat Actors | Barnum (2014) |

| № | UA | EN | Джерело |
|---|---|---|---|
| 375. | **TAXII**<br><br>це абревіатура, яка розшифровується як "Довірений автоматизований обмін розвідувальною інформацією " (англ.), "транспортний механізм для обміну розвідувальною інформацією про кіберзагрози". Це протокол, який дозволяє обмінюватися інформацією про кіберзагрози через протокол HTTPS. | **TAXII**<br><br>**i**s an acronym that stands for “Trahe Trusted Automated Exchange of Intelligence Information”, the “transport mechanism for sharing cyber threat intelligence”. It is a protocol that enables the sharing of cyber threat information over HTTPS protocol. | Cyber Threat Intelligence Technical Committee (n.d.) |

## 5 Перелік джерел посилань / References

1. Adamsky D. (2015). Cross-domain coercion: the current Russian art of strategy. IFRI Security Studies Center. 45 p. https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf
2. Barbero, J. M., Taylor, D., & Canclini, N. G. (2006). Cultural agency in the Americas. Duke University Press. – 392 p. ISBN 0822387484
3. Barnum S. (2014). Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). MITRE, 1-22. https://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf
4. Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 3(4-5), 353-364. https://doi.org/10.1080/23340460.2017.1414924
5. Bekkers, F., Meessen, R., & Lassche, D. (2019). Hybrid conflicts: the new normal?. Den Haag: TNO. – 17 p. https://www.tno.nl/publish/pages/7427/tno-2019-hybride.pdf
6. Belgium National Crisis Center (n.d.). CBRNe. https://crisiscenter.be/en/risks-belgium/security-risks/cbrne
7. Bellingcat (n.d.) Who We Are. https://www.bellingcat.com/about/who-we-are/
8. Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual review of sociology*, *26*(1)ю – P. 611-639. https://doi.org/10.1146/annurev.soc.26.1.611
9. Bilsky, L., & Klagsbrun, R. (2018). The Return of Cultural Genocide?. European Journal of International Law, 29(2), 373-396. https://doi.org/10.1093/ejil/chy025
10. Binnendijk, H., Kugler, R.L. (2001). Revising the Two-Major Theater War Standard. Strategic Forum. No. 179. https://apps.dtic.mil/sti/pdfs/ADA404809.pdf
11. Boe, O., Torgersen, G.-E., Skoglund, T. H. (2020). Does the Norwegian Police Force Need a Well-Functioning Combat Mindset? Front. Psychol., 2020, Volume 11 p. 4. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01075/full
12. Bouchet, N. (2016). Russia's "militarization" of colour revolutions. CSS Policy Perspectives, 4(2). – p.1-4. https://doi.org/10.3929/ethz-a-010682969

13. Bouvier A. A. (2020). International Humanitarian Law and the Law of Armed Conflict. USA: Williamsburg, Peace Operations Training Institute, 42 p. https://cdn.peaceopstraining.org/course_promos/international_humanitarian_law/international_humanitarian_law_english.pdf

14. Bradshaw, S., Howard, Ph.N. (2017) Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project, Working paper no. 2017.12. University of Oxford. 37 p. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

15. Brown, A. (2019). The myth of Eurabia: how a far-right conspiracy theory went mainstream. *The Guardian*, 16. https://www.theguardian.com/world/2019/aug/16/the-myth-of-eurabia-how-a-far-right-conspiracy-theory-went-mainstream

16. Butfoy, A. (1997). Common Security. Common Security and Strategic Reform. Palgrave Macmillan, London. https://doi.org/10.1007/978-1-349-25531-3_1

17. Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers, 1998. – 239 p. ISBN 1555877842

18. Całus K. (2023). Hybrid CoE Working Paper 23. The Russian hybrid threat toolbox in Moldova: economic, political and social dimensions, p.6. Helsinki: The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230413-Hybrid-CoE-Working_Paper-23-Moldova-WEB.pdf

19. Cantekin, A. (2016). Ripeness and readiness theories in international conflict resolution. Journal of Mediation and Applied Conflict Analysis, Vol. 3, No. 2, p. 414 - 428. https://mural.maynoothuniversity.ie/7917/7/AC-Ripeness-2016.pdf

20. Chase, M. S., & Chan, A. (2016). China's Evolving Approach to "Integrated Strategic Deterrence". Rand Corporation. 64 p. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1366/RAND_RR1366.pdf

21. Chirkov, V. (2009). Critical psychology of acculturation: what do we study and how do we study it, when we investigate acculturation? Int. J. Intercult. Relat. 33, p. 94 – 105. doi: 10.1016/j.ijintrel.2008.12.004

22. Chivvis, Ch. S. (2017). Understanding Russian 'Hybrid Warfare' And What Can Be Done About it. RAND, March 22, 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

23. CJCS (Chairman of the Joint Chiefs of Staff, 2007). Joint Publication 3-13.1 Electronic Warfare. CJCS: Armed Forces of the United States of America, 144 p. https://info.publicintelligence.net/JCS-EW.pdf

24. COE (Council of Europe, 2005). Council of Europe Framework Convention on the value of cultural heritage for society, Faro, 27.10.2005. Council of Europe Treaty Series, No. 199. 9 p. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680083746

25. Collins English Dictionary (n.d.). Available at https://www.collinsdictionary.com/dictionary/english/perfect-storm

26. Council of the EU (Council of the European Union, June 2017) 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities'. – 5 p. https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

27. CSIS (Center for Strategic and International Studies, 2018), What Works: Countering Gray Zone Coercion. https://www.csis.org/analysis/what-works-countering-gray-zone-coercion

28. Cull, N. J. (2009). Public Diplomacy: Lessons from the Past. Los Angeles: University of Southern Californi, 62 p. http://kamudiplomasisi.org/pdf/kitaplar/PDPerspectivesLessons.pdf

29. Cullen P. (2018). Hybrid threats as a new 'wicked problem' for early warning. Helsinki: The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-2018-8-Cullen.pdf

30. Cullen P., Juola C., Karagiannis G., Kivisoo K., Normark M., Rácz A., Schmid J. & Schroefl J. (2021) The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. https://www.hybridcoe.fi/wp-

content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

31. Cyber Threat Intelligence Technical Committee (n.d.). https://oasis-open.github.io/cti-documentation/.

32. Deflem, M. (2018) Anomie, Strain, and Opportunity Structure: Robert K. Merton's Paradigm of Deviant Behavior. *The Handbook of the History and Philosophy of Criminology*, edited by Ruth A. Triplett. Malden, MA: Wiley-Blackwell. P. 140-155. https://doi.org/10.1016/B978-0-08-097086-8.03067-1

33. Denning, D. E. (2015). Rethinking the cyber domain and deterrence. Joint Force Quarterly 7, no. 2 (2015) – p. 8-15 http://faculty.nps.edu/dedennin/publications/Rethinking%20the%20Cyber%20Domain%20and%20Deterrence%20-%20jfq-77_8-15.pdf

34. DIA (2022). Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion. Defense Intelligence Agency. ISBN-13: 979-8838314291

35. Domańska, M. (2019). The myth of the Great Patriotic War as a tool of the Kremlin's great power policy. OSW Commentary. - № 316, 31.12. 2019. https://www.osw.waw.pl/en/publikacje/osw-commentary/2019-12-31/myth-great-patriotic-war-a-tool-kremlins-great-power-policy

36. Doyle, C. (2011) Dictionary of marketing (3 ed). - Oxford University Press, 2011. ISBN-13 9780199590230. - https://www.oxfordreference.com/view/10.1093/acref/9780199590230.001.0001/acref-9780199590230-e-0575

37. DRDC CSS (2013). Maritime Domain Awareness in the Canadian Safety and Security Program. Scientific Brief. – 10 p. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc152/p538602_A1b.pdf

38. Ducaru, S., Nițu, I., & Margvelashvili, M. (Eds.). (2019). Black Swan Events on NATO's Eastern Flank (Vol. 143). IOS Press.

39. EEAS (European External Action Service, 2021). Tackling Disinformation, Foreign Information Manipulation & Interference. Stratcom Activity Report. 16 p. https://www.eeas.europa.eu/sites/default/files/documents/Report%20Stratcom%20activities%202021.pdf

40. EE-ISAC (2020) European Energy Information Sharing and Analysis Centre. Threat Intelligence Management. An EE-ISAC White Paper. – 30 p. https://www.ee-isac.eu/threat-intelligence-management-white-paper/

41. Endsley, M.R. (1995). Measurement of situation awareness in dynamic systems. *Human factors*, 37(1), 65-84. https://doi.org/10.1518/001872095779049499

42. ENISA (European Union Agency for Cybersecurity, n.d.). Glossary: What is "Social Engineering"? https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

43. European Commission (2021). Cybercrime. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

44. European Commission (2020). Communication on tackling online disinformation. https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

45. European Commission (2018). A Multi-Dimensional Approach to Disinformation. https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en

46. European Commission (2017). Joint report to the European Parliament and the Council on the implementation of the Joint Framework on Countering Hybrid Threats - a European Union Response. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0030&from=EN

47. European Council (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. – L 345/75 - 345/82. - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

48. European Parliament (2019). European Parliament resolution on the 80th anniversary of the start of the Second World War and the importance of European remembrance for the future of Europe (2019/2819(RSP)). – 7p. https://www.europarl.europa.eu/doceo/document/B-9-2019-0098_EN.pdf

49. Elwell, F.L. (2013) Sociocultural systems: Principles of structure and change. Athabasca University Press, 2013. https://www.aupress.ca/app/uploads/120219_99Z_Elwell_2013-Sociocultural_Systems.pdf

50. Facon, N. M., Mazzucchi, N., Patry, J. (2018). Countering hybrid threats: EU and the Western Balkans case. European Parliament's Sub-committee on Security and Defence, Brussels. – 46 p. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/603851/EXPO_STU(2018)603851_EN.pdf

51. Falk, B.J. (2020) Strategic citizens: Civil society as a battlespace in the era of hybrid threats. Hybrid CoE Strategic Analysis № 25. – 8 p. - https://www.hybridcoe.fi/wp-content/uploads/2020/11/SA25_Strategic-Citizen.pdf

52. Fokin, A. (2016). Internet trolling as a tool of hybrid warfare: the case of latvia. - NATO STRATCOM COE , Latvia, Riga. – 106 p. https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

53. Freedman L. (2014) Ukraine And The Art Of Limited War. War on the Rocks, October 8, 2014. https://warontherocks.com/2014/10/ukraine-and-the-art-of-limited-war/

54. Fridman, O. (2017). The Russian Perspective on Information Warfare: Conceptual Roots and Politisation in Russian Academic, Political, and Public Discourse. Defence Strategic Communications. The official journal of the NATO Strategic Communications Centre of Excellence. Vol. 2. https://stratcomcoe.org/cuploads/pfiles/web_fridman.pdf

55. Galeotti, M. (2015) Time To Think About “Hybrid Defense”. War on the Rocks, July 30, 2015. https://warontherocks.com/2015/07/time-to-think-about-hybrid-defense/

56. Galeotti, M. (2020) The Navalny poisoning case through the hybrid warfare lens. - Hybrid CoE Paper 4. – 12 p. ISBN 978-952-7282-41-0 https://www.hybridcoe.fi/wp-content/uploads/2020/10/202010_Hybrid-CoE-Paper4_Navalny-case-through-a-hybrid-lens.pdf

57. Gerasimov, V. (2016) The Value of Science Is in the Foresight (originally published in Military-Industrial Kurier, 27 February 2013, translated from Russian by Robert Coalson). *US Army Military Review*, January-February 2016 - p. 23 – 29. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art001.pdf

58. GEC (Global Engagement Center at the U.S. Department, 2020) GEC’s Special Report: Pillars of Russia’s Disinformation and Propaganda Ecosystem. 77p.

https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

59. Google. (2023). Fog of War. How the Ukraine Conflict Transformed the Cyber Threat Landscape. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

60. Grant A., Haider Z., Raufuss A. (2023). Black swans, gray rhinos, and silver linings: Anticipating geopolitical risks (and openings). McKinsey. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/black-swans-gray-rhinos-and-silver-linings-anticipating-geopolitical-risks-and-openings

61. Grigas, A. (2016). Beyond Crimea: the new Russian empire. Yale University Press. – 352 p. ISBN 0300220766

62. Goffman, E. (1986). Frame Analysis. An Essay on the Organization of Experience. Boston: Northeastern University Press. 600 p. ISBN-13 : 978-0930350918

63. Gorbis, M., Frauenfelder, M., Joseff, K. & Pescovitz, D. (2019) Building a healthy cognitive immune system: defending democracy in the disinformation age. - Institute for the Future. https://www.iftf.org/projects/building-a-healthy-cognitive-immune-system/

64. Gordon, D.E. (2014). Electronic Warfare. Element of Strategy and Multiplier of Combat Power. Pergamon, 192 p. https://doi.org/10.1016/B978-1-4831-9722-7.50004-2

65. Gryshko, S., Terziyan, V., & Golovianko, M. (2024, submitted). Resilience Training in Higher Education: AI-Assisted Collaborative Learning. In: Proceedings of the 27th International Conference on Interactive Collaborative Learning. Lecture Notes in Networks and Systems. Springer.

66. Guillaume, M. (2019) Combating the manipulation of information – a French case. Hybrid CoE Strategic Analysis 16, May 3, 2019. – 9 p. https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_16_manipulation-of-information_.pdf

67. Harjanne A., Muilu E., Pääkkönen J., Smith H. (2018) Helsinki in the era of hybrid threats – Hybrid influencing and the city. – 32 p. ISBN 978-952-331-475-7 https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_020818_netti.pdf

68. Horbulin, V. P. (2017). The World Hybrid War: Ukrainian Forefront. – Kharkiv: Folio, 2017. — 158 p. ISBN 978-966-554-273-5 https://niss.gov.ua/sites/default/files/2017-01/GW_engl_site.pdf

69. Horowitz, M. C. (2018). The promise and peril of military applications of artificial intelligence. Bulletin of the Atomic Scientists, 23. https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/

70. Hosaka, S. (2021) Enough with Donbas "Civil War" Narratives? Identifying the Main Combatant Leading "the Bulk of the Fighting". Civil War? Interstate War? Hybrid War? Dimensions and Interpretations of the Donbas Conflict in 2014–2020. Ed. Hauter, J. Stuttgart.

71. Hristov, N. H. (2017). Modern War and its Asymmetric Nature. IJASOS-International E-journal of Advances in Social Sciences, 3(8), 467-472. http://ijasos.ocerintjournals.org/en/download/article-file/339251

72. Hume, C., & Hume, M. (2014). Augmenting transcultural diffusion through knowledge management: the critical role of internal marketing. In *Handbook of Research on Effective Marketing in Contemporary Globalism* (pp. 104-127). IGI Global. DOI: 10.4018/978-1-4666-6220-9.ch006

73. Hybrid CoE(a) (n.d.). Hybrid Threats https://www.hybridcoe.fi/hybrid-threats/

74. Hybrid CoE(b) (n.d.). What is Hybrid CoE https://www.hybridcoe.fi/who-what-and-how/

75. Ilhan A. (2020). An Evaluation of the Changing Nature of Power-Dependence Relations in Organizations Within the Context of the Resource Dependence Theory. International Review of Management and Business Research, Vol. 9, Is. 4, Part 2, p. 165 – 179. https://www.irmbrjournal.com/papers/1607856549.pdf

76. Inglesant, P., Jirotka, M., & Hartswood, M. (2016) Responsible Innovation in Quantum Technologies applied to Defence and National Security. Oxford 2016. https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2018-11/Responsible%20Innovation%20in%20Quantum%20Technologies%20applied%20to%20Defence%20and%20National%20Security%20PDFNov18.pdf

77. ISO/IEC 27000:2009 (E), Information technology – Security techniques – Information security management systems – Overview and vocabulary (2009). https://www.foo.be/docs/iso/ISO_IEC_27000_2009.pdf

78. Jauhiainen, J. S,. Erbsen, H. A., Lysa, O., Espenberg, K. (2022). Temporary Protected Ukrainians and other Ukrainians in Estonia. Turku: University of Turku, 142 p. https://skytte.ut.ee/sites/default/files/2022-12/Jauhiainen%20et%20al._Temporary%20protected%20Ukrainians%20in%20Estonia%2C%202022.pdf

79. Jervis, R. (1979). Deterrence Theory Revisited. *World Politics*, 31(2), 289-324. DOI: https://doi.org/10.2307/2009945

80. Jokinen, J., Normark, M., Fredholm, M. (2022) Hybrid CoE Research Report 6: Hybrid threats from non-state actors: A taxonomy. 36 p. https://www.hybridcoe.fi/wp-content/uploads/2022/06/Hybrid-Coe-Research-Report-6-WEB-EDS-20221121.pdf

81. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. (2023) Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 124 p. doi:10.2760/37899. https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf

82. Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., & Titova, L. (2022). Hybrid Threats against Industry 4.0 : Adversarial Training of Resilience. In R. Absi, & I. El Abbassi (Eds.), *EVF'2021 : 8th International Conference on Energy and City of the Future* (Article 03004). EDP Sciences. E3S Web of Conferences, 353. https://doi.org/10.1051/e3sconf/202235303004. https://jyx.jyu.fi/handle/123456789/82376

83. Kalenský, Jakub & Osadchuk, Roman (January 2024). How Ukraine fights Russian disinformation: Beehive vs mammoth. Hybrid CoE Research Report 11. URL: https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

84. Kania, E. (2016). The PLA's Latest Strategic Thinking on the Three Warfares. China Brief, XVI:13, August 2016, p. 10-14. http://cimsec.org/plas-latest-strategic-thinking-three-warfares/27468

85. Karlén, N., Rauta, V., Salehyan, I., Mumford, A., San-Akca, B., Stark, A., ... & Spatafora, G. (2021). Conflict Delegation in Civil Wars. International Studies Review, 23(4), 2048-2078. https://doi.org/10.1093/isr/viab053

86. Knopf, J. W. (2010). The fourth wave in deterrence research. *Contemporary Security Policy*, 31(1), p. 1-33. https://doi.org/10.1080/13523261003640819

87. Kumar, V. A. (2012). Money Laundering: Concept, Significance and its Impact. European Journal of Business and Management, Vol 4, No.2. 113 – 119.

88. Jaegher, K. D. (2022). Threat of Sabotage as a Driver of Collective Action. The Economic Journal, Volume 132, Issue 647, October 2022, Pages 2339–2365, https://doi.org/10.1093/ej/ueac023

89. Johnson Ch., Badger L., Waltermire D., Snyder J., Skorupka C. (2016). Guide to Cyber Threat Information Sharing. *National Institute of Standards and Technology*, 43 p. http://dx.doi.org/10.6028/NIST.SP.800-150

90. Lantto, H., Åkesson, B., Suojanen, M., Tuukkanen, T., Huopio, S., Nikkarila, Ristolainen, J.-P. M. (2019). Wargaming the cyber resilience of structurally and technologically different networks. Security and Defence Quarterly.;24(2):51-64. DOI: https://doi.org/10.35467/sdq/103346

91. Laruelle, M. (2015). The "Russian World": Russia's soft power and geopolitical imagination. Center on Global Interests. – 30p. https://www.academia.edu/12469030/_The_Russian_World_Russias_Soft_Power_and_Geopolitical_Imagination_Center_for_Global_Interests_May_2015

92. Lough, J., & Dubrovskiy, V. (2018). Are Ukraine's Anti-Corruption Reforms Working? Chatham House. - 46p. - https://www.chathamhouse.org/sites/default/files/publications/research/2018-11-19-ukraine-anti-corruption-reforms-lough-dubrovskiy.pdf

93. Lutsevych, O. (2016). Agents of the Russian World: Proxy Groups in the Contested Neighbourhood, Chatham House. – 44 p. https://www.chathamhouse.org/sites/default/files/publications/research/2016-04-14-agents-russian-world-lutsevych.pdf

94. MacFarlane S. N.(2009). Frozen Conflicts in the Former Soviet Union – The Case of Georgia/South Ossetia. IFSH (ed.), OSCE Yearbook, Baden-Baden, p. 23 – 33. https://ifsh.de/file-CORE/documents/yearbook/english/08/MacFarlane-en.pdf

95. Maehler, D. B., Weinmann, M., & Hanke, K. (2019). Acculturation and naturalization: Insights from representative and longitudinal migration studies in Germany. Frontiers in psychology, 10, 1160. https://doi.org/10.3389/fpsyg.2019.01160

96. Malpedia (a) (n.d.). Sandworm. https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm

97. Malpedia (b) (n.d.). EternalPetya. https://malpedia.caad.fkie.fraunhofer.de/details/win.eternal_petya

98. Mayer Lux, L. (2018). Defining cyberterrorism. Revista Chilena De Derecho Y Tecnología,Vol. 7(2), pp. 5–25. https://rchdt.uchile.cl/index.php/RCHDT/article/view/51028/54675

99. McQuail's, D. (2010) Mass Communication Theory, 6th Edition, SAGE, 2010. - 632 p. ISBN-10: 1849202923

100. Mumford, A. (2020). Ambiguity in hybrid warfare. - Hybrid CoE Strategic Analysis, 24, September 2020. – 8p. https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf

101. Mazarr, M. J. (2015). Mastering the gray zone: understanding a changing era of conflict. US Army War College Carlisle. 158 p. https://apps.dtic.mil/sti/pdfs/AD1000186.pdf

102. MCDC (Multinational Capability Development Campaign project, 2017). Countering hybrid warfare project: Understanding hybrid warfare. Great Britain, London. 34 p. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

103. MCDC(a) (Multinational Capability Development Campaign project, 2019). Countering hybrid warfare project: Countering hybrid warfare. 93 p. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

104. MCDC(b) (Multinational Capability Development Campaign project, 2019). Information Note, 'A deadlier peril': The Role of Corruption in Hybrid Warfare. 3p. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795222/20190318-MCDC_CHW_Info_note_7.pdf

105. Milton, M., Schmidt A., Kuerbis B. (2013) Internet Security and Networked Governance in International Relations, *International Studies Review*, Volume 15, Issue 1, March 2013, Pages 86–104. https://doi.org/10.1111/misr.12024

106. Mira, J. C. (2011). O controlo de exportações de armamentos como meio de prevenção de conflitos armados. Nação e Defesa, 2011. № 129-5. P. 237-262. http://comum.rcaap.pt/handle/10400.26/7635

107. Missiroli, A. (2021) Hybrid CoE Paper 7: Geopolitics and strategies in cyberspace: Actors, actions, structures and responses. Helsinki: The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622_Hybrid_CoE_Paper_7_Geopolitics_and_strategies_in_cyberspace_WEB.pdf

108. MSB (Swedish Civil Contingencies Agency, 2018) Countering information influence activities: A handbook for communicators. Sweden, Karlstad. 48 p. https://mycourses.aalto.fi/pluginfile.php/1705039/mod_resource/content/1/countering%20information%20influence%20activities%20handbook.pdf

109. MISP (n.d.). MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. https://www.misp-project.org/.

110. NATO (2010) Capstone Concept for the Military Contribution to Countering Hybrid Threats. Brussels: NATO Military Committee. – 18 p.

111. NATO (2013) Allied Command Operations Comprehensive Operations Planning Directive Interim V2.0. Belgium: North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe. 444 p. https://cmdrcoe.org/download.cgf.php?id=9

112. NATO (2023) Cognitive Warfare: Strengthening and Defending the Mind. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

113. Neudert, L. M., & Marchal, N. (2019). Polarisation and the use of technology in political campaigns and communication. European Parliament. – 57 p. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf

114. Newman H. (2022). Foreign information manipulation and interference defense standards: Test for rapid adoption of the common language and framework 'DISARM'. Hybrid CoE Research Report 7, November 2022. 60 p. https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf

115. Nimmo, B. (2018) Deliberate online falsehoods - methods and responses (In his hearing before the Singaporean committee, 22 February 2018, Written

Representation 36). – 10 p. https://www.parliament.gov.sg/docs/default-source/sconlinefalsehoods/written-representation-36.pdf

116. Nissen T. E. (2015). Weaponization of Social Media. Characteristics of Contemporary Conflicts. Copenhagen: Royal Danish Defence System. – 148 p. ISBN 8771470972, 9788771470970

117. NSA (NATO Standardization Agency, 2013). Nato Glossary Of Terms And Definitions. AAP-06, Edition 2013. 439p. https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf#:~:text=for%20NATO%20glossaries%20prescribed%20by%20C-M(2007)0023,%20Guidance%20for

118. Pariser, E. (2011). The filter bubble: What the Internet is hiding from you. Penguin UK. 304 p.

119. Parliament Of Singapore (2018) Report Of The Select Committee On Deliberate Online Falsehoods – Causes, Consequences And Countermeasures, Thirteenth Parliament Of Singapore, 19 September 2018. – 279 p.

120. Pawlak, P. (2017). Countering hybrid threats: EU-NATO cooperation. European Parliamentary Research Service. – 12 p. https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf

121. Pijpers P., & Ducheine, P.A.L., (2020, Sept. 24). Influence Operations in Cyberspace – How They Really Work. Amsterdam Law School Research Paper. No. 2020-61. Amsterdam Center for International Law No. 2020-31, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3698642

122. Polyakova, A.; Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Policy Brief, Democracy and Disorder Series*. Washington, DC: Brookings. 22p. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

123. Popper, K. (2020) Open Society and Its Enemies (5th ed.). USA, Princeton University Press. 808 p.

124. Praks, H. (2024). Hybrid CoE Working Paper 32. Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage. Helsinki: The European Centre of Excellence for Countering Hybrid Threats. Available at:

https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf

125. Riekeles, G. E. (2023). Quantum technologies and value chains: Why and how Europe must act now. Discussion Paper Europe's Political Economy Programme. – 20 p. https://www.epc.eu/content/PDF/2023/Quantum_Technologies_DP.pdf

126. Ritchey, T. (2013). Wicked problems. Acta morphologica generalis, 2(1). https://www.swemorph.com/pdf/amg-2-1-2013.pdf

127. Robbin, A., & Buente, W. (2008). Internet information and communication behavior during a political moment: The Iraq war, March 2003. *Journal of the American Society for Information Science and Technology*, 59(14), 2210-2231. https://repository.arizona.edu/bitstream/handle/10150/105527/RobbinIraqWar_2008Jun2-EntirePaper.pdf?sequence=1

128. Rotaru, V. (2018). Forced attraction? How Russia is instrumentalizing its soft power sources in the "near abroad". *Problems of Post-Communism*, 65(1), 37-48. https://doi.org/10.1080/10758216.2016.1276400

129. Ryniejska–Kiełdanowicz, M. (2009). Cultural diplomacy as a form of international communication. Institute for Public Relations. https://interarts.net/descargas/interarts664.pdf

130. Sari A. (2023) Hybrid CoE Paper 17: Instrumentalized migration and the Belarus crisis: Strategies of legal coercion https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230425-Hybrid-CoE-Paper-17-Instrumentalized-migration-and-Belarus-WEB.pdf

131. Sazonov, V., Mölder, H., Müür, K., Pruulmann-Vengerfeldt, P., Kopõtin, I., Ermus, A., Salum, K., Šlabovitš, A., Veebel, V., Värk, R. (2016). Russian Information Campaign against the Ukrainian State and Defence Force. Combined Analysis. Tartu, NATO Strategic Communications Centre of Excellence, Estonian National Defence College, https://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf

132. Savolainen, J. (2019) Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)? - Hybrid CoE Working Paper 4. – 22 p. https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Working-paper_WMDivers_2019_rgb.pdf

133. Schroefl, J. (2020). Cyber power is changing the concept of war. - Hybrid CoE Strategic Analysis 21, March 16, 2020. – 8 p. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis_21_Cyber-Power.pdf

134. SGDSN (Secretariat-General for National Defence and Security, France, 2015). French National Digital Security Strategy. 42 p. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf

135. Simons, G. (2015). Perception of Russia's soft power and influence in the Baltic States. Public Relations Review, 41(1), 1-13. https://doi.org/10.1016/j.pubrev.2014.10.019

136. Skog, D.A., Wimelius, H. & Sandberg, J. Digital Disruption. (2018). Business & Information Systems Engineering, Vol. 60, pp. 431–437. https://doi.org/10.1007/s12599-018-0550-4

137. Smith, H. (2017) In the era of hybrid threats: Power of the powerful or power of the “weak”? - Hybrid CoE Strategic Analysis 1. – 8 p. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-1-Smith.pdf

138. Soldatov A., & Borogan I. (2022). Dead Water: How the Russian Security Services’ Paranoid Mindset Justifies the War. SCEEUS Guest Report, No.5, 12 p. https://www.ui.se/globalassets/ui.se-eng/publications/sceeus/soldatov-borogan.pdf

139. Sommer, D. (2021). Cultural Agents.The Hemispheric Institute. https://hemisphericinstitute.org/en/enc07-work-groups/item/1072-enc07-cultural-agents.html

140. Spencer, M., Lalgee, R. (2008) Anomie Theory. *Encyclopedia of Violence, Peace, & Conflict (Second Edition). Sociological Studies, Overview*. Elsevier. P. 1970-1982. https://doi.org/10.1016/B978-012373985-8.00165-3 https://www.sciencedirect.com/topics/social-sciences/anomie

141. Stevens, W. (2011). Crisis management and planning. Nação e Defesa. 2011. № 129-5. P. 31-40. http://comum.rcaap.pt/handle/10400.26/7623

142. STIX (2012). Standardizing cyber threat intelligence information with the structured threat information expression. Mitre Corporation, 22 p. https://www.mitre.org/sites/default/files/publications/stix.pdf

143. Swedish Defence University (n.d.). https://www.fhs.se/en/centre-for-societal-security/about-ctss

144. Sweijs, T., & Zilincik, S. (2019). Cross Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p. https://hcss.nl/wp-content/uploads/2021/01/Cross-Domain-Deterrence-Final_0.pdf

145. Sztompka, P. (2000). Cultural trauma: The other face of social change. *European journal of social theory*, 3(4), 449-466. https://doi.org/10.1177/136843100003004004

146. Szwed, R. (2016) Framing of the Ukraine-Russia Conflict in Online and Social Media. NATO Strategic Communications Centre of Excellence. Latvia, Riga. 131 p. https://www.stratcomcoe.org/framing-ukraine-russia-conflict-online-and-social-media

147. Takahashi, S. (2018). Development of gray-zone deterrence: concept building and lessons from Japan's experience. The Pacific Review, 31(6), P. 787-810. https://doi.org/10.1080/09512748.2018.1513551

148. Tworek, H. (2018). Responsible Reporting in an Age of Irresponsible Information. Alliance for Securing Democracy (GMF) Brief 2018 No. 009, March 2018, - 10 p. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Responsible-Reporting_ASD_2_Final.pdf

149. Thiele, R. (a) (2020). Artificial Intelligence – A key enabler of hybrid warfare. Hybrid CoE Working Paper 6, March 2020. – 14 p. https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf

150. Thiele, R. (b) (2020). Quantum Sciences – Disruptive Innovation in Hybrid Warfare. Hybrid CoE Working Paper 7, March 19, 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Working-Paper-7_2020.pdf

151. Transparency International (a) (n.d.). Corruptionary A-Z: Corruption. https://www.transparency.org/en/what-is-corruption

152. Transparency International (b) (n.d.). Corruptionary A-Z: Integrity. https://www.transparency.org/en/corruptionary/integrity

153. Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. - Swedish Defence University. – 93 p. ISBN 978-91-86137-73-1

https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf

154. UK Government. (2020). Press release. UK exposes series of Russian cyber attacks against Olympic and Paralympic Games Foreign Secretary Dominic Raab condemns malicious cyber activity by Russia's GRU. Available at: https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

155. UN (United Nations, 2011) International Legal Protection of Human Rights in Armed Conflict. New York and Geneva, United Nations Publication, 124 p. https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict.pdf

156. UNESCO (United Nations Educational, Scientific and Cultural Organization, 2019). Basic Texts of the 2005 Convention on the Protection and Promotion of the Diversity of Cultural Expressions, 2019 edition. France, Paris. 131 p. https://unesdoc.unesco.org/ark:/48223/pf0000370521

157. UNESCO (United Nations Educational, Scientific and Cultural Organization, 1954). The Convention for the Protection of Cultural Property in the Event of Armed Conflict. (1954). UNESCO. 25 p. https://en.unesco.org/sites/default/files/1954_Convention_EN_2020.pdf

158. United States Code. (2010). Crimes and Criminal Procedure. Edition , Supplement 4. United States, Title 18, Sec. 2331. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2331&num=0&edition=prelim

159. USA Congress (1990). Public law 101-601—Nov. 16, 1990. Sec. 2. Definitions. https://www.congress.gov/101/statute/STATUTE-104/STATUTE-104-Pg3048.pdf

160. USA Congress (2019) Bill H.R.4668. Digital Citizenship and Media Literacy Act (Rep. Slotkin, Elissa). https://www.congress.gov/bill/116th-congress/house-bill/4668/text?q=%7B%22search%22%3A%5B%22media+literacy%22%5D%7D&r=1&s=3

161. Van Haaster, J. (2019). On cyber: The utility of military cyber operations during armed conflict. [Thesis, fully internal, Universiteit van Amsterdam] https://pure.uva.nl/ws/files/37093787/Thesis.pdf

162. Vilmer, J.-B. Jeangène, Escorcia, A., Guillaume, M., Herrera, J. (2018) Information Manipulation: A Challenge for Our Democracies, the report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces. France, Paris. 208 p. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

163. Wallenstein, S.-O. (2013). Introduction: Foucault, Biopolitics, and Governmentality. Foucault, Biopolitics, and Governmentality (eds. J. Nilsson, S.-O. Wallenstein), Stockholm: Södertörn University, 206 p.. https://www.diva-portal.org/smash/get/diva2:615362/FULLTEXT03.pdf

164. Wardle C., Derakhshan H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe report, DGI(2017)09. 110p. https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

165. Walt, S. M. (1991). The renaissance of security studies. International studies quarterly, 35(2), 211-239. https://doi.org/10.2307/2600471 http://users.metu.edu.tr/utuba/Walt%20Renais.pdf

166. Weldes, J. (1999). The cultural production of crises: US identity and missiles in Cuba. *Cultures of insecurity: States, communities, and the production of danger*, 35-62. https://sites.middlebury.edu/coldwarculture/files/2013/10/weldes_cultural_prod_of_crises.pdf

167. WHO (World Health Organisation, 2022) World mental health report: transforming mental health for all. P. xvi https://www.who.int/publications/i/item/9789240049338

168. Wigell M. (2019). Hybrid Interference as a Wedge Srategy: A Theory of Exernal Interference in Liberal Democracy. *International Affairs,* Volume 95, Issue *2*: 255–275. https://doi.org/10.1093/ia/iiz018

169. Williams S. (2021) Introduction to cultural relations and cultural diplomacy. The Culture and Creativity website. https://www.culturepartnership.eu/en/publishing/cultural-diplomacy/lecture-18-1

170. Yang, A.-M., Li, S.-S., Ren, C.-H., Liu H.-X., Han, Y., Liu, L. (2018). Situational Awareness System in the Smart Campus. IEEE Access, Vol. 6, pp. 63976-63986, doi: 10.1109/ACCESS.2018.2877428

171. Ya'u, A., Miraz, M. H., Saad, N., Bala, H., Rangasamy, D., Olaniyi, O. N., & Mustapha, U. A. (2023). Effects of Economic Deterrence Theory and Environmental Regulation on Tax Evasion: Evidence from Energy Sector. International Journal of Energy Economics and Policy, No 13(5), p. 289 – 302. https://doi.org/10.32479/ijeep.14736

172. Методика навчання в умовах гібридних загроз: посібник / Е. Балашов, М. Білоконь, Т. Борозенцева, М. Головянко, С. Гришко, Т. Жовтенко та ін. – Харків: ТОВ "ТЕХНОЛОГІЧНИЙ ЦЕНТР ГРУП", 2023. – 84 с. DOI: https://doi.org/10.62067/978-617-8242-02-2