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

Hybrid Threats Glossary / Глосарій з гібридних загроз

Deliverable 5.5 "WARN environment"

Результат 5.5 "WARN-середовище"

VERSIONING AND CONTRIBUTION HISTORY

Version	Date	Revision Description	Responsible Partner
01		Creation of document	NURE (Svitlana Gryshko)

This project has been funded with support from the European Commission.
This publication reflects the views only of the author,
and the Commission cannot be held responsible
for any use which may be made of the information contained therein.

Головний редактор:

Світлана Гришко

(ХНУРЕ, Харківський національний університет радіоелектроніки)

Упорядники:

Світлана Гришко, Марія Головянко

(ХНУРЕ, Харківський національний університет радіоелектроніки)

Марія Титаренко, Мирослава Чех, Оксана Василиця, Євген Ланюк, Валентина Засадко

(УКУ, Український католицький університет)

Оксана Карпенко, Валерій Завгородній

(ДУІТ, Державний університет інфраструктури та технологій)

Едуард Балашов

(НУОА, Національний університет "Острозька академія")

Тетяна Рева, Ольга Копієвська

(НАКККіМ, Національна академія керівних кадрів культури і мистецтва)

Михайло Білоконь, Величко Лариса

(ХРІДУ НАДУ, Харківський регіональний інститут державного управління НАДУ при Президентові України)

Галина Докашенко, Вікторія Концур, Іван Наумов

(ГІІМ ДВНЗ ДДПУ, Горлівський інститут іноземних мов Державного вищого навчального закладу "Донбаський державний педагогічний університет")

Editor

Svitlana Gryshko

(Kharkiv National University of Radio Electronics, NURE)

Compilers

Svitlana Gryshko and Mariia Golovianko

(Kharkiv National University of Radio Electronics, NURE)

Mariia Tytarenko, Myroslava Chekh, Oksana Vasylytsia, Yevhen Laniuk and Valentyna Zasadko

(Ukrainian Catholic University, UCU)

Oksana Karpenko and Valerii Zavhorodnii

(State University of Infrastructure and Technology, SUIT)

Eduard Balashov

(National University of Ostroh Academy, NUOA)

Tetiana Reva and Olha Kopiievska

(National Academy of Culture and Arts Management, NAMSCA)

Mykhailo Bilokon and Larysa Velychko

(Kharkiv Regional Institute of Public Administration of the National Academy of Public Administration under the President of Ukraine, KRI NAPA)

Halyna Dokashenko, Viktoriia Kontsur and Ivan Naymov

(Horlivka Institute for Foreign Languages of the State Higher Education Institution “Donbas State Pedagogical University”, HIFL SHEI DSPU)

Глосарій пройшов внутрішню процедуру забезпечення якості з 16.03.2021 по 9.04.2021 та отримав рекомендацію до оприлюдення від Ради якості WARN-проєкту в складі: Олена Кайкова (JYU), Марія Головянко (ХНУРЕ), Валентина Засадко (УКУ), Оксана Карпенко (ДУІТ), Віталій Лебедюк (НУОА), Тетяна Рева (НАКККіМ), Вячеслав Дзюндзюк (ХРІДУ НАДУ), Вікторія Концур (ГІІМ ДВНЗ ДДПУ), Катерина Супрун (МОН).

The glossary was accepted through the internal quality assurance procedure (conducted from 16.03.2021 to 9.04.2021) and was recommended to publish by Quality Assurance Board of the WARN-project consists of: Olena Kaikova (JYU), Mariia Golovianko (NURE), Valentyna Zasadko (UCU), Oksana Karpenko (SUIT), Vitalii Lebediuk (NUOA), Tetiana Reva (NAMSCA), Viacheslav Dziundziuk (KRI NAPA), Viktoriia Kontsur (HIFL SHEI DSPU), Kateryna Suprun (MESU).

ЗМІСТ / CONTENTS

1 ПЕРЕДМОВА

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.

Ми маємо намір оновлювати глосарій протягом проєкту, оприлюднюючи його подальші версії. А поки що із задоволенням ділимось із спільнотою його першою версією. The journey continues.

1. INTRODUCTION

> *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 Counteraction 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 incorrect 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 in our environments. 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, 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 an 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 the headquarters in Helsinki, Finland, and offices in many EU capitals. The EU approach to sustainability is based on providing timely and accurate information to citizens and decision-makers, on developing 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 the overall societal security was chosen as a fundamental one for the project and, consequently, to 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.

We intend to update the glossary throughout the project, publishing a version after a version. In the meantime, we gladly share the first issue with you. The journey continues.

2 ГІБРИДНІ ЗАГРОЗИ: ЗАГАЛЬНИЙ ВИМІР

2 HYBRID THREATS IN GENERAL

№	UA	EN	Джерело
1.	**Аналіз загрози гібридної війни** аналіз / процес, призначений для врахування всіх інструментів гібридної війни *MPECI*. В той час, як військові зосереджуються на M (мілітарному – військовому компоненті), експертів з цивільних питань та приватний сектор залучають для надання допомоги в аналізі нетрадиційних загроз, а саме інструментів гібридної війни PECI (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 PMESII.	**Hybrid warfare threat analysis** an analysis/process designed to account for the all MPECI instruments of a hybrid warfare threat. While the military focuses on the M (military), civilian subject matter experts and private sector are brought in to assist non-traditional threat analysis of PECI (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
2.	**Аналіз центру ваги** методологія військового планування, що походить з книги Карла фон Клаузевіца "Про війну", для виявлення "джерела" чи "центру" влади в системі.	**Centre of gravity analysis** 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
3.	**Асиметрія гібридних загроз** властивість гібридних загроз. Асиметричні загрози не потребують еквівалентних можливостей чи цілей, і тому дуже приваблюють: - як недержавних суб'єктів, які прагнуть досягти політичної або кримінальної мету, - так і державних діячів, які прагнуть досягти цілей	**Asymmetry of hybrid threat** a property (strength) of the hybrid threat. 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

	переконливими засобами заперечення.		
4.	**Астротурфінг** (посилання на бренд штучного газону "AstroTurf"). явище, при якому особистість замовника або організації виставляється як масова активність через фальшиві акаунти. Техніка полягає в тому, щоб створити видимість популярності. Див. також: *Боти*	**Astroturfing** (a reference to a brand of artificial turf "AstroTurf"). 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. This technique creates an artificial sense of popularity. see also: *Bots*	Bradshaw & Howard (2017) – p.11 Vilmer et al. (2018) - p.87
5.	**Базова лінія** 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** a reference point to allow for the identification of indicators and events as well as 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
6.	**Біо-хакінг** Секвенування та синтезування ДНК, а також зловживання цим. Приклади "гібридного" застосування: Створення нової біологічної зброї на основі технології синтетичної біології, наприклад, вірусів.	**Bio-hacking** DNA sequencing and synthesis and the misuse of this. Examples of hybrid applications: Creation of new biological weapons based on synthetic biology technology, such as viruses.	Bekkers et al. (2019) – p.27
7.	**Вертикальна ескалація** посилене використання одного конкретного засобу *MPECI*	**Vertical escalation** the intensified use of one specific means (*MPECI*)	MCDC(a) (2019) – p.90
8.	**Виклики сірої зони** див. *Допорогові Виклики*	**Gray Zone Challenges** see *Sub-Threshold Challenges*	

9.	**Витік** є одним із методів "*Символічних Дій*" оприлюднення інформації, отриманої неправомірними способами. Має символічне значення, оскільки, як правило, розкриває злочини та укриття фактів, не призначені для очей громадськості. Якщо витік використовується для інформаційного впливу, , інформація вириває ться з контексту і використовується для делегітимізації суб'єктів, а також спотворення інформаційного середовища. Витік інформації іноді відбувається внаслідок злому IT-систем або крадіжки. Наслідки цих витоків варіюються від пошкодження оперативної безпеки (збору розвідданих) до підриву довіри до політичної системи країни та її керівництва. Див. також "*Витік Макрона*"	**Leaking** is one of the "*Symbolic Actions*" 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. 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. The consequences of these leaks range from damaging operational (intelligence-gathering) security to undermining trust in a nation's political system and its leadership. See also *"Macron Leaks".*	MSB (2018) – p.19, 27 Treverton et al. (2018) - p.58
10.	**Відкриття** процес збирання й правильного інтерпретування інформації, пов'язаної з потенційно ворожою дією супротивника, про яку раніше не було відомо. Містить підходи до виявлення неоднозначних або прихованих гібридних загроз шляхом знаходження та фільтрування непередбачених аномалій. Це спроба вирішити проблему "*Невідомих Невідомих*" (на відміну від *Моніторингу*).	**Discovery** a process of capturing and then correctly interpreting information related to a potentially hostile adversarial action that has not been previously conceived. Includes approaches to discovering ambiguous or hidden hybrid threats by finding and filtering unanticipated anomalies. This is an attempt to manage the problem of "*Unknown Unknowns*" (by contrast of *Monitoring*).	MCDC(a) (2019) – p.26, 33

11.	**Відмивання** Відмивання означає поступове спотворення та деконтекстуалізацію інформації в такий спосіб, що стає неможливим визначити, чи є її джерело істинним чи хибним. Ця стратегія може використовувати *Оманливі Ідентичності, Дезінформацію, Технічні Маніпуляції* та *Символічні Дії* у поєднанні із *Соціальним / Когнітивним Зломом*, щоб зіткати павутину неправдивої інформації.	**Laundering** Laundering refers to gradually distorting and de-contextualizing information, so that it becomes impossible to tell if its source is true or false. 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
12.	**Відомі невідомі** належать до режимів гібридної атаки, про які ми знаємо, що можемо їх не знати (на відміну від "*Невідомі Невідомі*")	**Known unknowns** refer to modes of hybrid attack that we know we may be unaware of (by contrast "*Unknown Unknowns*")	MCDC(a) (2019) – p.26
13.	**Внутрішньо переміщені особи (ВПО)** 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).** 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
14.	**Вразливості** персонал, діяльність, ресурси або процеси потенційної цілі, які можуть бути використані або створені потенційним супротивником.	**Vulnerabilities** personnel, activities, resources or processes within a potential target that are susceptible of being exploited or created by a potential adversary.	MCDC(a) (2019) – p.90

15.	**Горизонтальна ескалація** одночасне застосування різних військових, політичних, економічних, цивільних, інформаційних засобів (*MPECI*).	**Horizontal escalation** the applied combination of multiple military, political, economic, civil, informational (*MPECI*) means.	MCDC(a) (2019) – p.89
16.	**Гібридний вплив** цілеспрямований вплив, який здійснює певна сторона, 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. Тоді як *Гібридна Загроза* є втіленням методів впливу, які вважали загрозою.	**Hybrid influencing** conscious influence exerted by a party, utilizing multiple influence 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. While a *Hybrid Threat* is an embodiment of influence methods that has been deemed to be a threat.	Harjanne et al. (2018) - p.5
17.	**Гібридна війна** 1) синхронізоване використання багатьох інструментів влади, підібраних з урахуванням конкретних вразливостей у всьому спектрі соціальних функцій для досягнення синергетичних ефектів. Аналітична модель для розуміння гібридної війни складається з трьох взаємозалежних частин: - критичні функції та вразливості захисника; - синхронізоване використання зловмисником декількох засобів та використання горизонтальної ескалації; і - лінійні та нелінійні ефекти від гібридних атак.	**Hybrid warfare, Hybrid war** 1) the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects. The Analytical Framework for understanding hybrid warfare is composed of three interlocking parts: - defender's critical functions and vulnerabilities; - attacker's synchronized use of multiple means and exploitation of horizontal escalation; and - linear and non-linear effects of an hybrid warfare attack. 2) the non-military aspects of what had previously been presumed to be	MCDC(a) (2019) – p.12 MCDC (2017) – p.7-8, 31 MCDC(b) (2019) – p.1

2) невійськові аспекти того, що раніше передбачалось досягти в результаті військової кампанії.	achieved through a military campaign.	
3) вид змішаних воєнно-політичних, розвідувально-економічних операцій, які Росія розпочала в Україні.	3) the kind of blended military-political-intelligence-economic operations Russia has launched in Ukraine	Galeotti (2015)
4) стратегічне використання (невизначеної) сили для завоювання території або досягнення іншої стратегічної мети. навмисна силова гра, спрямована на передавання повідомлення з використанням неоднозначності дій, достатньої, щоб уникнути помсти чи ескалації. вона є найбільш *туманною* формою війни з огляду на навмисні заплутування, що відбуваються задля приховування особистості держави-злочинця.	4) the strategic application of the use of (ambiguous) force to gain territory or attain another strategic goal deliberate powerplay aimed at communicating a message whilst utilizing enough ambiguity of action to avoid retaliation or escalation. it is representing the *foggiest* form of war given the deliberate obfuscations that occur in hiding the identity of the perpetrator state.	Mumford (2020) – p.3, 4
5) використання багатьох інструментів влади та впливу з акцентом на невійськові інструменти, для реалізації своїх національних інтересів поза власними кордонами.	5) using multiple instruments of power and influence, with an emphasis on nonmilitary tools, to pursue its national interests outside its borders.	Treverton et al. (2018) - p.18 Chivvis (2017)
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*)	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, and diplomatic). By contrast of *Hybrid threat, Hybrid conflict*	Pawlak (2017) – p. 2
7) Російське трактування (**Гібрідная война**): "західний підхід до дестабілізації режимів шляхом	7) Russian interpretation (**Gibridnaya voina**): "the western approach to destabilising regimes	Galeotti (2020) – p.4

	диверсії, яка може призвести до насильницького втручання."	through subversion that may lead to violent intervention".	
18.	**Гібридний Бюлетень** 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** 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)
19.	**Гібридний конфлікт** 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 (на відміну від *Гібридної загрози, Гібридної війни*)	**Hybrid conflict** 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. (by contrast of *Hybrid threat, Hybrid war*)	Pawlak (2017) – p. 2
20.	**Гібридні загрози** 1) скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів, за використанням широкого кола засобів. 2) "Термін гібридна загроза належить до дії […], метою якої є підрив або нанесення шкоди цілі, впливаючи на прийняття рішень [...] Дії можуть мати місце,	**Hybrid Threats** 1) coordinated and synchronised action, that deliberately targets democratic states' and institutions systemic vulnerabilities, through a wide range of means. 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,	Hybrid CoE(a) (2021) NATO (2010) – p.2

наприклад, у політичній, економічній, військовій, цивільній або інформаційній сферах."	military, civil or information domains."	
3) "…загрози, створені супротивниками, з можливістю одночасно адаптивно застосовувати звичайні та нетрадиційні засоби для досягнення своїх цілей."	3) "…posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."	Treverton et al. (2018) - p. 10
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".	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."	
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*)	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*).	Pawlak (2017) – p. 2
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 трансформувались у зброю в різних сферах операцій	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

	(дипломатичних, інформаційних, економічних, фінансових, торгових, соціальних тощо). мають на меті примусити об’єкт агресії до вимог, що суперечать його національним інтересам, незалежно від оголошення війни. 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. 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.	
21.	**Громадянське суспільство** форми соціальних організацій, які пропонують альтернативи тоталітаризму або надмірному державному контролю. Ключовим аспектом є існування проміжної "зони" між приватним життям та 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.	**Civil society** 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 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.	McQuail's, D. (2010) – p. 550
22.	**Даркнет** мережева сфера, яка не дотримується правил, що регулюють Інтернет, особливо сприяє обміну незаконно набутою інформацією.	**Darknet** 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
23.	**Дезінформація** навмисне розповсюдження інформації, яка є повністю або частково неправдивою (на відміну від *Помилкової Інформації*)	**Disinformation** the intentional dissemination of information that is wholly or partly false (as opposed to *Misinformation*)	Vilmer et al. (2018) - p.19

	свідомо неправдива або оманлива інформація, створена, представлена та розповсюджена з метою отримання економічної вигоди або навмисного обману громадськості	verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public	European Commission (2020)
	неправдива, неточна або оманлива інформація, розроблена, представлена та популяризована з метою навмисного заподіяння шкоди суспільству або для отримання прибутку.	false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.	European Commission (a) (2018)
	Один із методів інформаційного впливу (див. *Кампанії Впливу*). 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 аудіо. Дезінформація може бути використана для підтримки неправдивих уявлень, внесення сум'яття та дискредитації законної інформації, осіб та організацій. Сюди входять: *Фабрикація, Маніпулювання, Невірне Призначення, Сатира та Пародія тощо.*	one of the information influence techniques (see *Influence Campaigns*). 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. it includes: *Fabrication, Manipulation, Misappropriation, Satire and Parody* etc.	MSB (2018) – p.19, 25
24.	**Діагностика DIDI** діагностичний тест на інформаційну активність (обман, намір, зрив, втручання). Така діагностика дає можливість як своїм користувачам, так і громадській думці відрізнити	**DIDI diagnostic** a diagnostic test on informational activities (Deception, Intention, Disruption, Interference). Such a diagnostic offer the possibility for both its users as well as public opinion to differentiate information manipulation from	Vilmer et al. (2018) - p.121 Pamment et al. (2018) - – p.9, 10,16

	маніпуляції інформацією від більш відвертих операцій впливу. Щоб кваліфікуватися як дезінформація, інформаційна діяльність має 1) містити оманливі елементи; 2) мати намір заподіяти шкоду; 3) бути руйнівною; та 4) встановити втручання.	more sincere operations of influence. To qualify as disinformation, an informational activity must 1) contain deceptive elements; 2) have the intention to harm; 3) be disruptive; and 4) constitute an interference.	
25.	**Доброчесність** один із інструментів "гібридної оборони" 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** one of the 'hybrid defence' instrument 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 Transparency International (b)
26.	**Допорогові виклики** (або ***виклики сірої зони***) є "спробами досягнення цілей своєї безпеки, не вдаючись до прямого та значного застосування сили".	**Sub-Threshold Challenges** (or **gray zone challenges**) are "attempts to achieve one's security objectives without resort to direct and sizable use of force."	CSIS (2018) Takahashi (2018) – p.787 - 810
27.	**Ефекти (в умовах гібридної війни)** зміна стану об'єкту в результаті дій проти конкретних вразливостей цільової системи	**Effects (In hybrid warfare)** a change of state of an entity as the result of actions against specific vulnerabilities of a target system.	MCDC(a) (2019) – p.89
28.	**Європейський центр з протидії гібридним загрозам (Hybrid CoE)** 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)** 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) (2021)

29.	**Індикатори** вимірювані змінні величини, необхідні для чіткої та достатньої ідентифікації / опису / представлення / моніторингу явища відповідно до визначеного базового рівня.	**Indicators** measurable variables necessary to clearly and sufficiently identify/ describe/represent/monitor a phenomenon in relation to a specific baseline.	MCDC (2017) – p.31
30.	**Інтелектуальна лінь** неспроможність систематично проявляти критичне мислення та наївний вибір розповсюдження інформації без пошуку доказів, що підтверджують цю інформацію.	**Intellectual Laziness** 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
31.	**Інформаційна безпека** 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** 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
32.	**Інформаційна війна** є частиною військових операцій, метою яких є досягнення військових цілей за допомогою різних нетрадиційних засобів, включаючи нові засоби комунікації та розповсюдження інформації. протиборство в інформаційному просторі, яке ініціюється агресором з метою здійснення комплексного впливу на соціальне, економічне, військове	**Information war** 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. the combat in information environment, initiated by the aggressor to comprehensively affect social, economic, military and	Szwed (2016) – p. 19 Horbulin (2017) – p.158

	та політичне життя супротивника задля досягнення своїх стратегічних цілей щодо атакованої держави.	political life of the opponent to achieve its strategic goals regarding the attacked country.	
33.	**Інформаційна маніпуляція** 1) навмисне та масове розповсюдження неправдивих або упереджених новин у ворожих політичних цілях 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** 1) the intentional and massive dissemination of false or biased news for hostile political purposes 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 Guillaume (2019) – p.4
34.	**Інформаційний простір** 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.	**Information environment** 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.	Horbulin (2017) – p.157
35.	**Інформаційний суверенітет** різновид національно-державного суверенітету; невідчужувана юридична якість незалежної держави, яка символізує її політико-правову самостійність, вищу відповідальність та цінність як первинного суб'єкта міжнародного права. Інформаційний суверенітет означає, що всі правила поведінки в інформаційному просторі певної	**Information sovereignty** the kind of national state sovereignty; unalienable legal property of an independent state, which symbolizes its political and 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	Horbulin (2017) – p.157

	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.	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.	
36.	**Інформаційні операції** 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** 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
37.	**Інформаційно-психологічна операція** 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.** 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
38.	**Квазі реальність** 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, в тому числі *Анексії Криму* та підтримки сепаратистів на Донбасі.	**Quasi reality** 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

39.	**Кібервійська** команди, що мають належність до уряду, армії чи політичних партій, місія яких полягає у маніпулюванні громадською думкою за допомогою соціальних мереж.	**Cybertroops** 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 Vilmer et al. (2018) - p.48
40.	**Когнітивний злам** (або *Соціальний Злам*) є одним із методів інформаційного впливу (див. *Кампанії Впливу*) 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. Сюди входять: *Темна реклама, Ефект приєднання до більшості, Спіраль мовчання*, *Луна-Камери*, *Бульбашка фільтрів* тощо.	**Cognitive Hacking** (or *Social Hacking*) is one of the information influence techniques (see *Influence Campaigns*) 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. it includes: *Dark Ads, Bandwagon-Effect, Spiral of Silence, Echo Chambers, Filter Bubbles* etc.	MSB (2018) – p.19
41.	**Компромат (метод)** компрометація цілі, яку таким чином можна контролювати та маніпулювати нею.	**“Kompromat” Method** compromising a target who can thus be controlled and manipulated.	Vilmer et al. (2018) - p.160
42.	**Комп’ютерна пропаганда** використання алгоритмів, автоматизації, аналізу великих даних та кураторства для маніпулювання громадським життям через соціальні мережі.	**Computational propaganda** the use of algorithms, automation, big data analytics and human curation to manipulate public life over social media networks.	Neudert & Marchal (2019) – p.5
43.	**"Комунікація"** двостороннє розуміння та сприйняття, що використовується	**"Communication"**	MCDC(a) (2019) – p.35

	обома сторонами для визначення витрат та вигід. Один із "*трьох С" – компонентів стримування*.	the two-way understanding and perception that informs cost-benefit calculations on both sides. One of the *'three Cs' of deterrence*.	
44.	**Конспірологічна теорія** Див. *Теорія Змови*	**Conspiracy theory of society** See*: conspiracy theory of society*	
45.	**Корисні ідіоти** (вираз, мабуть, помилково приписуваний Леніну) інтелектуали, яких Кремль намагається "захопити" за допомогою таких форумів, як клуб "Валдай". Це можуть бути політичні діячі ультраправих чи вкрай лівих рухів або активісти різних рухів. є постійними коментаторами, які несвідомо надихаються на розповсюдження дезінформації.	**Useful Idiots** (an expression attributed to Lenin, probably falsely) intellectuals whom the Kremlin is trying to "capture" through forums such as the Valdai club. They may be political figures from far right or far left movements or activists from various movements. is regular commenters unconsciously inspired to proliferate disinformation.	Vilmer et al. (2018) - p.71 Szwed (2016) – p.55
46.	**Критичні функції** діяльність або операції, розподілені за політичним, військовим, економічним, соціальним, інформаційним, інфраструктурним (*PMESII*) спектром, припинення роботи яких призведе до порушення служб, від яких залежить функційна система (наприклад, держава, суспільство або його складова). 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** 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. 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 MCDC (2017) – p.11

47.	**Крос-доменне стримування** використання загроз в одному домені (сфері) для протидії діяльності в інших доменах (сферах).	**Cross domain deterrence** involves the use of threats in one domain to counter activities in other domains.	Sweijs & Zilincik (2019) – p. 12
48.	**Маніпуляція** є одним із методів *Дезінформації*. додавання, видалення або зміна змісту тексту, фото, відео чи аудіо для передачі іншого (зміненого) повідомлення.	**Manipulation** is one of the *Disinformation* methods. adding, removing or changing the content of text, photo, video or audio to communicate a different message.	MSB (2018) – p.19, 25
49.	**Медіаграмотність** забезпечення гарантування того, що будь-яка особа, яка стикається з інформацією, може оцінити її достовірність (аргументи, докази) та її джерело (надійність, мотивації). Це здатність до дій, зокрема: - отримати доступ до відповідної та точної інформації за допомогою засобів масової інформації (далі – ЗМІ) у різних формах; - критично аналізувати контент ЗМІ та вплив їх різних форм; - оцінити вичерпність, актуальність, достовірність, авторитет та точність інформації; - приймати освічені (свідомі) рішення на основі інформації, отриманої із ЗМІ та цифрових джерел; - використовувати різні форми технологій та цифрові інструменти; - аналізувати як використання ЗМІ та технологій може вплинути на приватне та суспільне життя.	**Media literacy** 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). The ability to the following actions: - to access relevant and accurate information through media in a variety of forms; - critically analyze media content and the influences of different forms of media; - evaluate the comprehensiveness, relevance, credibility, authority, and accuracy of information; - make educated decisions based on information obtained from media and digital sources; - operate various forms of technology and digital tools; - and reflect on how the use of media and technology may affect private and public life.	Vilmer et al. (2018) - p.178 USA Congress (2019) – sec.3, # 5

50.	**Мікро таргетинг** 1) мікро-націлювання з підвищеною точністю, завдяки якій населення сегментоване на цільові групи. Див. також: *Бульбашки Фільтрів, Інтернет-Кокон* 2) Поєднання кількох технологій (великі дані, IoT, мікроботи тощо) з метою відстеження та усунення (цільових) осіб. Приклади "гібридних" застосувань: використання бойових роботів для усунення конкретних людей або груп.	**Micro-targeting** 1) the increased precision with which the population is segmented and targeted. see also: *Filter Bubbles, Internet-Cocooning* 2) Micro-targeting: The combination of several technologies (Big Data, IoT, Micro-robots etc.) in order to track, trace and eliminate (target) individuals. Examples of hybrid applications: employing slaughter bots and use these to eliminate specific persons or groups.	Vilmer et al. (2018) - p.39 Bekkers et al. (2019) – p.27
51.	**Моніторинг** процес сканування навколишнього середовища на наявність "*Відомих Невідомих*" – зазвичай за допомогою індикаторів – для пошуку упередженої інформації про можливі гібридні атаки. Спосіб управління проблемою "*Відомих Невідомих*" (на відміну від *Виявлення*).	**Monitoring** 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. A way to manage the problem of "*Known Unknowns*" (by contrast of *Discovery*).	MCDC(a) (2019) – p.26
52.	**М'яка сила** здатність впливати на інших для досягнення бажаних результатів через залучення, а не примус чи оплату.	**Soft power** the ability to affect others to obtain the outcomes one wants through attraction rather than coercion or payment.	Simons (2015) – p.2
53.	**Надлишок інформації** явище, відоме як надмірна кількість інформації. сприяє дезінформації, оскільки це призводить до зниження концентрації уваги, що послаблює нашу пильність і здатність обробляти контраргументи.	**Infobesity** a phenomenon known as the overabundance of information 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

54.	**Невідомі невідомі** 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*"). Цей тип інформації не піддається методології *Моніторингу*, який побудованій на "сприйнятті того, що ми очікуємо сприймати" за допомогою шаблонів 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.	**Unknown unknowns** 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*"). 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 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.	MCDC(a) (2019) – p.26
55.	**Невірне інформування** ненавмисне поширення інформації, яка є повністю або частково неправдивою (на відміну від *Дезінформації*).	**Misinformation** the unintentional dissemination of information that is wholly or partly false (as opposed to *Disinformation*).	Vilmer et al. (2018) - p.19
56.	**Невірне призначення** є одним із методів Дезінформації. 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** is one of the *Disinformation* methods. 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

57.	**Нелінійність** належить до непередбачуваних (які не є причинно-лінійними) наслідків атак гібридної війни. Вони 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** refers to unanticipated 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
58.	**Неоднозначність** ворожі дії, які державі важко визначити за певною ознакою або публічно визначити як 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.	**Ambiguity** defined here as hostile actions that are difficult for a state to identify attribute or publicly define as coercive uses of force. Ambiguity is 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.	MCDC (2017) – p.31
59.	**Пакети синхронізованих атак (SAP)** конкретний MPECI-набір, який синхронізований та пристосований до конкретних вразливостей, які використовуються в атаках гібридної війни. Див. також: *Синхронізація Засобів*	**Synchronized attack packages (SAPs)** specific MPECI means that are synchronized and tailored to specific vulnerabilities that are used in a hybrid warfare attack. See also: *Synchronization of Means*	MCDC (2017) – p.32 MCDC(a) (2019) – p.90
60.	**Підробки** метод, який використовується в *Оманливих Ідентичностях*. являє собою фабрикування офіційних документів.	**Forgeries** a method that is used in *Deceptive Identities.* Fabricating official documents is an effective way of making	MSB (2018) – p.19, 20

	Це ефективний спосіб зробити дезінформацію справжньою. Наприклад, підроблені заголовки листів, штампи чи підписи можуть бути використані для виготовлення підробленої документації.	disinformation appear authentic. For example, fake letter heads, stamps or signatures can be used to produce forged documentation.	
61.	**Поляризація** один із способів поєднання методів інформаційного впливу (див. *Кампанії Впливу*). Політичний, соціальний та ідеологічний поділ суспільств на чітко протилежні групи. Поляризація підтримує дві протилежні крайності конкретної проблеми. Це досягається підтримкою вже існуючих перспектив, використанням *Соціального Зламу, Оманливих Ідентичностей* та *Дезінформації*. Часто *Тролів* та *Ботів* використовують для подальшої поляризації дискусії.	**Polarisation** one of the ways to combine of information influence techniques (see *Influence Campaigns*). The political, social and ideological division of societies into distinctly opposed groups 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 Neudert & Marchal (2019) – p.6
62.	**Поріг** визначення величини або інтенсивності 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. Див. також: *Допорогові виклики*	**Threshold** 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. See also: *Sub-Threshold Challenges*	MCDC(a) (2019) – p.90
63.	**Потьомкінські села** метод, який використовується в *Оманливих Ідентичностях*. Гравці, які мають достатньо ресурсів, можуть створювати	**Potemkin Villages** a method that is used in *Deceptive Identities.* Actors with sufficient resources can set up institutions or even networks	MSB (2018) – p.19 – 20

	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.	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.	
64.	**Пропаганда** 1) спроба вплинути на думку та поведінку суспільства з метою прийняття людиною тієї чи іншої думки та поведінки 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** 1) an attempt to influence the opinion and behavior of society in order for people to adopt a particular opinion and behavior 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 Horbulin (2017) – p.159
65.	**Психологічна війна** заходи, пов'язані із впливом на цінності та систему переконань цільової аудиторії, її сприйняття, емоції, мотиви, міркування та, в ідеалі, на їх поведінку. Метою психологічної війни є послаблення морального духу опонента та зміцнення власного морального духу, створюючи атмосферу, в якій цільова аудиторія стає більш схильна до вселянь.	**Psychological Warfare** those activities associated with influencing a target audience's values and belief system, their perceptions, emotions, motives, reasoning, and, ideally, their behaviour. 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.	Szwed (2016) – p. 62 Nissen (2015) – p.67 Fokin (2016) – p.7
66.	**"Руський Мир"** 1) російська **псевдо-ГО** (громадська організація), що фінансується російською державою і тісно співпрацює з нею, створена в 2007 році для	**"Russkiy Mir"** 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	Vilmer et al. (2018) - p.70

просування російської мови та культури за кордоном і яка насправді служить мостом між урядом та важелями впливу за кордоном	reality as a bridge between the government and relays of influence abroad	
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 цивілізація, яка включає людей, які почуваються культурно близькими до Росії. Тому руський мир має гнучку географію для своїх прихильників. Нинішній наратив руського миру охоплює: - мова (*Російськомовні Громади*) - культура (євразійська православна ідентичність), - історія (росіяни та українці були «одним народом», «Велика Вітчизняна війна» тощо), - спільна спадщина (радянський історичний нарратив), - економічні зв'язки (Євразійський економічний союз, ЄАЕС; Євразійський митний союз), - релігія (російська православна церква, «православні олігархи», православний союз молоді, східно-православна цивілізація…), - консервативні цінності (на противагу західним цінностям лібералізму та прав людини).	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 Russia.The Russian World thus has a fluid geography for its advocates. The current narrative of the Russian World encompasses: - language (*Russian-Speaking Communities*) - culture (EurasianOrthodox identity), - history (Russians and Ukrainians were ‘one people’, ‘the Great Patriotic War‘ etc), - shared heritage (the Soviet historical narrative), - economic links (The Eurasian Economic Union, EAEU; the Eurasian Customs Union), - religion (The Russian Orthodox Church, 'Orthodox oligarchs’, the Orthodox Union of Youth, the Eastern Orthodox civilization…), - conservative values (in opposition to Western values of liberalism and individual human rights).	Lutsevych (2016) – p.3, 8 Rotaru (2018) – p.5 Laruelle (2015)
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	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	Domańska (2019) – p.7

	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).	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).	
67.	**Самооцінка гібридної війни** постійний національний процес для виявлення критичних функцій та пошуку вразливостей у спектрі *PMESII*.	**Hybrid warfare self-assessment** a continuous national process to identify critical functions and find vulnerabilities within the *PMESII* spectrum	MCDC(a) (2019) – p.89
68.	**Сигнали** 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** 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 Denning (2015) - p.15
69.	**Сигналізація** 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. Сигналізація може здійснюватися за допомогою широкого спектру засобів та містить як слова, так і дії.	**Signaling** 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. Signaling can be done through a wide spectrum of means and involves both words and actions.	Sweijs & Zilincik (2019) – p. 23
70.	**Символічні дії** є одним із методів інформаційного впливу (див. *Кампанії Впливу*).	**Symbolic Actions** is one of the information influence techniques (see *Influence Campaigns*).	MSB (2018) – p.19, 27

	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, наприклад, в терористичній діяльності. Також це можна зробити вишукано, посилаючись на точні культурні символи, які стосуються лише певної цільової аудиторії. Це включає: *Витоки, Хакінг, Громадські Демонстрації* тощо	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 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. It includes: *Leaking, Hackning, Public Demonstrations* etc	
71.	**Синхронізація засобів** здатність учасника гібридної війни ефективно координувати *Інструменти Влади (MPECI)* для досягнення бажаних ефектів як горизонтальним, так і вертикальним способом. Див. також: *Горизонтальна Ескалація, Вертикальна Ескалація*	**Synchronization of means** the ability of a hybrid warfare actor to effectively coordinate the *Instruments Of Power (MPECI)* to achieve the desired effects in both horizontal and vertical ways. See also: *Horizontal Escalation, Vertical Escalation*	MCDC(a) (2019) – p.90
72.	**"Сіра зона"** неоднозначна нейтральність між миром та війною, що відображає різновиди агресивних, наполегливих, рішучих кампаній, характерних для війни, але без явного використання військової сили. Війна, яка не відповідає або виходить за межі традиційного розуміння "війни".	**'Gray Zone' / 'Grey Zone'** 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. Warfare that falls short of, or outside of, our traditional understanding of 'warfare'	Mazarr (2015) – p.2 MCDC(a) (2019) – p.31 Takahashi (2018) – p.787

73.	**"Смерть від тисячі порізів"** 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'** 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
74.	**Соціальна мережа** - див. *Цифрова Платформа, Нові ЗМІ*	**Social Network** – see *Digital Platform, New Mass Media*	
75.	**Соціальний злам** - див. *Когнітивний Злам*	**Social Hacking** - see *Cognitive Hacking*	
76.	**"Спроможніть до стримування"** спроможність або технічна здатність здійснювати дії, що нав'язують витрати супротивнику. Один із "*трьох С" – компонентів стримування*.	**"Capability of deterrence "** the ability or technical capacity to carry out actions that impose costs on the adversary. One of the *'three Cs' of deterrence*.	MCDC(a) (2019) – p.35
77.	**Стійкість** здатність суспільства та уряду долати порушення та зовнішні потрясіння, протистояти їм та відновлюватись. Заходи щодо підвищення стійкості сприяють *Стримуванню Шляхом Заперечення*.	**Resilience** the ability of society and government to absorb, withstand and recover from disruption and external shocks. Measures to increase resilience contribute to *Deterrence By Denial*.	MCDC(a) (2019) – p.90
78.	**Стратегічні цілі** цілі стратегії протидії гібридній війні. Стратегічні цілі відображають рівень амбіцій захисника.	**Strategic goals** 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
79.	**Стримування шляхом заперечення** Одна із стратегій стримування як інструмент протидії гібридній війні.	**Deterrence by denial** One of the deterrence strategy as a tool for countering hybrid warfare. Aims to undermine the ability of the adversary to achieve their objective	MCDC(a) (2019) – p.35, 89

	Покликане підірвати здатність супротивника досягти своєї мети, в першу чергу шляхом, наприклад, "загартовування" цілі.	in the first instance through, for example, 'hardening' the target.	
80.	**Стримування шляхом покарання** Одна із стратегій стримування як інструмент протидії гібридній війні. Має на меті переконати противника в тому, що витрати на досягнення його мети будуть занадто високими.	**Deterrence by punishment** One of the deterrence strategy as a tool for countering hybrid warfare. 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
81.	**Теорія змови (Конспірологічна теорія)** 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** "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 Vilmer et al. (2018) - p.35
82.	**"Три війни"** військова стратегія Китаю: Як у мирний, так і у воєнний час застосування трьох видів війни (війна громадської думки, 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"** 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 Kania (2016)

83.	**«Три С» стримування** основні принципи стримування, як важливого інструменту протидії гібридній війні: *Авторитет, Потенціал, Комунікація*.	**'Three Cs' of Deterrence** basic principles of deterrence as an important tool for countering hybrid warfare: *Credibility*, *Capability*, *Communication*.	MCDC(a) (2019) – p.35
84.	**"Туман війни"** відсутність інформації у командира на багатьох рівнях - від тактичного до великого стратегічного	**'Fog of war'** the absence of information a commander has across a multitude of levels, from the tactical to the grand strategic	Mumford (2020) – p. 4
85.	**Управління кіберзагрозами** 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)** 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
86.	**Фабрикація** один із методів *Дезінформації*. 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** is one of the *Disinformation* methods. 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
87.	**Фейкові новини** Поняття фейкових (підроблених, фальшивих) новин включає як спотворення об'єктивних істин, так і оманливі історії. Крім того, розповсюдження фальшивих новин забезпечується	**Fake News** Fake news, a concept, includes both distortions of objective truths as well as misleading stories. Furthermore, spreading fake news is enabled by social media, which in general does not require verification	Treverton et al. (2018) - p.57

	соціальними мережами, які загалом не вимагають перевірки опублікованих матеріалів, а також забезпечують зручну платформу для охоплення аудиторії. Див. також *Нові ЗМІ*	of published posts and also provides a handy platform to reach audiences. See also: *New Mass Media*	
88.	**Центр дослідження асиметричних загроз (CATS)** 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)** 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 Swedish Defence University (2021)
89.	**Цифрова грамотність** Компонент *Медіаграмотності*, який описує здатність людей знаходити, орієнтуватися та критично оцінювати інформацію, знайдену в цифрових середовищах.	**Digital literacy** 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
90.	**MPECI** військові, політичні, економічні, цивільні та інформаційні інструменти влади. **Див. також:** *Інструменти Влади*	**MPECI** military, political, economic, civilian and informational instruments. See also*: Instruments of power*	MCDC (2017) – p.4, 9
91.	**PECI** політичні, економічні, цивільні, міжнародні інструменти.	**PECI** political, economic, civil, international tools.	MCDC (2017) – p.4
92.	**PMESII** політичний, військовий, економічний, соціальний, інформаційний та інфраструктурний спектр	**PMESII** the political, military, economic, social, informational and infrastructure spectrum	MCDC (2017) – p.4
93.	**SAPs** - see *Synchronized Attack Packages*	**SAP** - див. *Пакети Синхронізованих Атак*	

3 ГІБРИДНІ ЗАГРОЗИ В НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

3 HYBRID THREATS TO NATIONAL SECURITY

№	UA	EN	Джерело
94.	**Агресія збройна** Застосування іншою державою або групою держав збройної сили проти будь-якої країни.	**Armed aggression** The use of armed force by a state or a group of states against any country.	Horbulin (2017) – p.156
95.	**"Війна нового покоління"** російська військова доктрина див. *Доктрина Герасимова*	**'New generation warfare'** the Russian military doctrine *See: Gerasimov doctrine*	
96.	**Військово-цивільна адміністрація** 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.** 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
97.	**Доктрина Герасимова** (російська "*Війна Нового Покоління*") російська військова доктрина, її автором є генерал Валерій Герасимов, начальник Генерального штабу ЗС РФ "У двадцять першому столітті ми спостерігаємо тенденцію до стирання меж між станом війни та миру. [...] Роль невійськових засобів для досягнення політичних	**Gerasimov doctrine** (The Russian "*New Generation Warfare*") the Russian military doctrine, its autor is Gen. Valery Gerasimov, the chief of the General Staff of the Russian Federation Armed Forces. "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	Vilmer et al. (2018) - p.55 Gerasimov (2016) – p.24

	і стратегічних цілей зросла, здебільшого, вони перевищили силу зброї в її ефективності. Фокус застосовуваних методів конфлікту 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"	strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. The focus of applied 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"	
98.	**Екосистема (Російська екосистема дезінформації та пропаганди)** 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: - офіційні державні комунікації, - фінансовані державою глобальні повідомлення, - вирощування проксі-джерел, - озброєння соціальних медіа, - дезінформація за підтримки кібер-засобів.	**Ecosystem (Russia’s disinformation and propaganda ecosystem)** 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: - official government communications, - state-funded global messaging, - cultivation of proxy sources, - weaponization of social media, - and cyber-enabled disinformation.	GEC (2020) – p.3
99.	**«Зелені чоловічки» / "увічливі люди"** професіональні солдати в уніформі без розпізнавальних знаків.	**"Little Green Men" / “polite people”** professional soldiers in uniforms without markings	Freedman (2014) Treverton et al. (2018) - p. 17

100.	**Імпортозаміщення в оборонно-промисловому комплексі** заміщення імпорту комплектуючих для створення вітчизняної воєнної продукції, шляхом налагодження їх вітчизняного виробництва або імпорту з інших країн.	**Import substitution in defense industry** 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
101.	**Інформаційна присутність** 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** 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
102.	**Кампанії впливу** 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. До методів Кампаній Впливу відносяться: *Соціальні (Когнітивні) Злами, Оманливі Ідентичності, Технічне Використання, Дезінформація, Риторика Викривлення (Наклепу), Символічні Дії.* Немає універсальної реакції на дії інформаційного впливу. Існує чотири категорії відповідей (оцінювати, інформувати, відстоювати і боронити), кожна з яких складається з декількох	**Influence Campaigns** 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. Information influence techniques include: *Social (Cognitive) Hacking, Deceptive Identities, Technical Exploitation, Disinformation, Malign Rhetoric, Symbolic Actions.* 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

	специфічних комунікативних прийомів.		
103.	**Китайський еволюціонуючий підхід до "інтегрованого стратегічного стримування"** 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". Китайці думають про стримування в багатьох сферах, пояснюючи, що воно ґрунтується на поєднанні ядерних, звичайних, інформаційних, космічних та цивільних сил. Див також: *Крос-Доменне Стримування*	**China's Evolving Approach to 'Integrated Strategic Deterrence'** 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." Chinese thinking about deterrence across multiple domains, explaining that it rests upon a combination of nuclear, conventional, information, space, and civilian forces. See also: *Cross Domain Deterrence*	Chase & Chan (2016) – p.3 Sweijs & Zilincik (2019) – p.14
104.	**Міжнародна безпека** 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** 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
105.	**Національні інтереси** життєво важливі потреби людини, суспільства та держави, реалізація яких забезпечує державний суверенітет та добробут України, її прогресивний демократичний розвиток.	**National interests** the vital needs of a person, society and state. Their implementation ensures state sovereignty and welfare of Ukraine, it's progressive democratic development.	Horbulin (2017) – p.158

106.	**Національні цінності** основоположні матеріальні, інтелектуальні та духовні надбання українського народу, визначальні умови існування та розвитку людини, суспільства та держави.	**National values** the basic material, intellectual and cultural heritage of Ukrainian people, key conditions of existence and development of a person, society and state.	Horbulin (2017) – p.158
107.	**Операції зі стабілізації** 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** 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
108.	**"Переконливість стримування"** воля здійснювати дії, які вимагають витрат від супротивника Один із "*трьох С" – компонентів стримування*.	**"Credibility of deterrence"** the will to carry out actions that impose costs on the adversary One of the *'three Cs' of deterrence*	MCDC(a) (2019) – p.35
109.	**Політика паспортизації** неформальна політика Кремля щодо надання російських паспортів, особливо населенню сепаратистських регіонів. Ідеться про надання російського громадянства без здачі паспорта з рідної країни.	**Passportization policy** Kremlin's informal policies to deliver Russian passports especially to the populations of secessionist regions. This involves granting Russian citizenship without the surrendering the passport from the home country.	Rotaru (2018) – p.7
110.	**Постконфліктна (деокупована) територія** частина території, на якій відбувся збройний конфлікт і яка була звільнена. Для такої території характерні дестабілізація економічної ситуації, руйнування виробничої, транспортної,	**Post-conflict (de-occupied) area** 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	Horbulin (2017) – p.158

	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.	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.	
111.	**Проросійські псевдо-ГО** (громадська організація) ГО-подібні структури, які фінансує уряд Росії. спосіб інструменталізації громадянського суспільства Кремлем. багато з цих "ГО" імітують західні підходи, наприклад, звинувачуючи уряди колишніх радянських республік у серйозних порушеннях 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. варіюються від асоціацій, що представляють російські меншини,	**(pro)-Russian pseudo “NGOs”** NGO-like structures financed by the Russian government. way of instrumentalization of civil society by the Kremlin. 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 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. range from associations representing Russian minorities, pro-Russian youth movements, think tanks, analytical centers, election-monitoring organizations, and	Rotaru (2018) – p.8

	проросійські молодіжні рухи, аналітичні центри, організації з моніторингу виборів та проросійські або сепаратистські установи.	proRussian or secessionist institutions.	
112.	**Російське крос-доменне стримування** 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. 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". Кінцевою метою такого виду стримування є "деескалація або відгородження противника від агресії та нав'язування волі Росії, бажано з мінімальним насильством" Див також: *Крос-Доменне Стримування*	**Russian cross-domain deterrence** 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. 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” The ultimate purpose of this kind of deterrence is “to deescalate, or dissuade the adversary from aggression, and impose Russia’s will, preferably with minimal violence.” See also: *Cross Domain Deterrence*	Adamsky (2015) – p. 37 Sweijs & Zilincik (2019) – p.14
113.	**Роскомнадзор** Російське державне агентство, яке здійснює нагляд за ЗМІ; інструмент гібридного впливу	**Roskomnadzor** The Russian state agency that oversees mass media; a hybrid influence tool	GEC (2020) – p.31
114.	**Россотрудничество** Російське державне агентство, завданням якого є посилення	**Rossotrudnichestvo** Russian public agencie, whose mission is to further Russian	Vilmer et al. (2018) - p.70

	впливу Росії за кордоном, особливо в країнах СНД. 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 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".	influence abroad, especially in CIS countries. 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-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'.	Lutsevych (2016) – p.9 Rotaru (2018) – p.3
115.	**Цифрова платформа** (включаючи *Соціальну Мережу*) в контексті французької національної стратегії цифрової безпеки "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".	**Digital Platform** (*including Social Network*)- in the context of the French national digital security strategy "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." See also *Digital Platform* in "Hybrid Threats in Software Engineering"	SGDSN (2015) – p.20

	Див. також *Цифрова Платформа* в розділі "Гібридні загрози в інженерії програмного забезпечення"		
116.	**Цифровий авторитаризм** 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** 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
117.	**"Четверта хвиля" теорії стримування** новий напрямок роботи щодо стримування, який почав з'являтися після закінчення холодної війни і набрав обертів після терактів 11 вересня. 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** 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. 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 Jervis (1979) Knopf (2010)

4 ГІБРИДНІ ЗАГРОЗИ В ПУБЛІЧНОМУ УПРАВЛІННІ ТА АДМІНІСТРУВАННІ

4 HYBRID THREATS IN PUBLIC ADMINISTRATION

№	UA	EN	Джерело
118.	**Адаптація держави до мережевого управління** 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.	**Adaptation of the state to network management** "…Second, states are adapting to networked governance not by asserting direct, hierarchical control over it, but by inserting themselves into the technical and operational networks and attempting to shape standards and practices in a multistakeholder environment"	Milton et al. (2013) - p.100
119.	**“Витік Макрона”** 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. Ці цілеспрямовані дії проти кандидата в президенти Еммануеля Макрона та організована проти нього кампанія (яка розпочалася кількома місяцями раніше, завдяки численним операціям із маніпуляцій інформацією) розглядалися як спроба втручання у вибори президента Франції 2017 року.	**“Macron Leaks”** 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. These targeted actions against presidential candidate Emmanuel Macron and the orchestrated campaign against him (that started several months earlier, through numerous information manipulation operations) seen as the attempted interference in the 2017 French presidential election.	Vilmer et al. (2018) - p.106
120.	**Громадська безпека** функція урядів держав, що забезпечує захист громадян країни, осіб на її території, організацій та інституцій від загроз	**Public safety** the function of governments which ensures the protection of citizens, persons in their territory, organizations, and institutions	DRDC CSS (2013) – p.9

	їх добробуту та процвітанню громад.	against threats to their well-being – and to the prosperity of their communities.	
121.	**Державна інформаційна політика** Сукупність основних напрямів і способів діяльності держави щодо одержання, використання, поширення та зберігання інформації.	**Government information policy** There is the total of core areas and activities of a state to collect, use, disseminate and store information.	Horbulin (2017) – p.157
122.	**Десек'юритизація в політичній сфері** перенесення питань із надзвичайного режиму до нормального переговорного процесу в політичній сфері.	**Desecuritization** the shifting of issues out of emergency mode and into the normal bargaining processes of the political sphere	Buzan et al. (1998) - p.4
123.	**Дипломатичне прикриття** Одна з форм та дій неоголошеної гібридної війни, мета яких прикриття та нівелювання російської участі в діях проти суверенної Української держави.	**Diplomatic cover** The one of the forms and actions of non-declared hybrid warfare, aiming at concealing and minimizing the Russian role in the activities undermining the sovereignty of Ukraine.	Horbulin (2017) – p.157
124.	**Дослідження (міжнародної) безпеки** 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 суспільства, а також конкретна політика, яку держави приймають для підготовки, запобігання або участі у війні.	**Security studies** 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 in order to prepare for, prevent, or engage in war	Walt (1991) – p.212

125.	**Електронний уряд** електронне управління або застосування інформаційних та комунікаційних технологій для надання державних послуг.	**E-governance** electronic governance, or the application of information and communication technologies for delivering government services.	Neudert & Marchal (2019) – p.5
126.	**Євроскептицизм** напрям політичної думки в країнах Європи, що ставить під сумнів доцільність процесу політичної, правової та економічної інтеграції європейських держав у межах ЄС і власне самого існування Європейського Союзу як наднаціонального інституціоналізованого утворення.	**Euroscepticism** the way of political thinking in European countries, which questions the advantages of political, legal and economic integration within the EU member-countries to the extent of principle opposition to the existence of the European Union as a supranational institutionalized unity.	Horbulin (2017) – p.157
127.	**Кібер дипломатія** 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** 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
128.	**Кібер злочинність** злочинні діяння, вчинені в онлайновому режимі з використанням електронних комунікаційних мереж та інформаційних систем	**Cybercrime** consists of criminal acts committed online by using electronic communications networks and information systems	European Commission (2021)

129.	**Контроль за експортом зброї** 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** (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
130.	**Міжнародна криза** соціальна та культурна конструкція, яку створюють державні чиновники в процесі формування та відтворення національної ідентичності (унаслідок чого можуть виникати непередбачувані ситуації, проявлятися нові або приховані раніше конфлікти на міжнародному рівні).	**International crisis** crises more generally, are social, and specifically cultural, constructions. ... crises are social constructions that are forged by state officials in the course of producing and reproducing state identity.	Weldes (1999) – p.37
131.	**Небезпека у міжнародних відносинах** наявність реальних загроз міжнародній безпеці, проти яких немає адекватних контрзаходів.	**dangers in international relations** insecurity (threats against which no adequate countermeasures are available)	Buzan et al. (1998) - p.4
132.	**Нелетальні психологічні операції з використанням соціальних мереж** формування суспільної поведінки за допомогою використання	**Non-lethal psychological operations using social networks** shaping public behavior through the use of “dynamic narratives” to combat the political propaganda	Bradshaw & Howard (2017) – p.4

	"динамічних наративів" для боротьби з політичною пропагандою яка поширюється терористичними організаціями.	disseminated by terrorist organizations	
133.	**Інституційний механізм** процеси, механізми, люди та навички, необхідні національним урядам та транснаціональним установам для реалізації стратегій протидії гібридній війні.	**Institutional machinery** 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
134.	**Інструменти влади** елементи середовища *MPECI*. Коли ці елементи "озброєні", інструменти влади можуть стати знаряддям атаки. Див. також *MPECI*	**Instruments of power** elements of the *MPECI* environment. When these elements are 'weaponized' the instruments of power can become tools of attack. See also: *MPECI*.	MCDC(a) (2019) – p.90
135.	**Стратегічні комунікації** скоординоване та належне використання комунікаційних можливостей держави - публічної дипломатії, зв'язків із громадськістю, військових зв'язків із громадськістю, інформаційно-психологічних операцій, заходів, спрямованих на просування завдань держави.	**Strategic communications** the mean coordinated and proper use of state communication capacities – public diplomacy, public relations, military public relations, information and psychological operations, events designed to facilitate and meet the targets of the country.	Horbulin (2017) – p.159
136.	**Фінансовані урядом аккаунти, веб-сторінки чи програми** 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** own government-sponsored accounts, websites and applications designed to spread political propaganda. These accounts and the content that comes out of them are clearly marked as government operated.	Bradshaw & Howard (2017) – p.10
137.	**Цивільні аспекти кризового менеджменту в Спільній зовнішній політиці і політиці безпеки Європейського Союзу**	**Civilian Aspects of Crisis Management in The Common Foreign and Security Policy (CFSP) of the European Union**	Stevens (2011) – p.37

	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)	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.

5 ГІБРИДНІ ЗАГРОЗИ В МЕНЕДЖМЕНТІ ОРГАНІЗАЦІЙ І АДМІНІСТРУВАННІ

5 HYBRID THREATS IN ORGANISATION MANAGEMENT AND ADMINISTRATION

№	UA	EN	Джерело
138.	**Гібридна адхократія** 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** 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
139.	**Захист критичної інфраструктури** комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури	**Critical infrastructure protection.** 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
140.	**Критична інфраструктура** 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** 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
141.	**Критична інфраструктура ЄС** активи, системи або їх частини, розташовані в державах-членах	**EU Critical Infrastructure** asset, system or part thereof located in Member States which is essential	European Council

	ЄС, що мають важливе значення для 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	for the maintenance of vital societal 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	(2008). - 345/77
142.	**Руйнівні технології** специфічна технологія, яка може принципово змінити не тільки усталені технології, але також правила та бізнес-моделі певного ринку, а часто бізнесу та суспільства загалом.	**Disruptive technologies** 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)
143.	**Сила слабких** навички ведення переговорів та ведення торгів, вміння правильно визначати час (наприклад, провокації та / або заподіяння шкоди репутації) та видимість узгодженості.	**The power of the weak** negotiation and bargaining skills, being able to time action correctly (for example provocations and/or inflict damage on reputation) and appearance of coherence.	Smith (2017) – p. 5
144.	**Стійкість критичної інфраструктури** 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.** 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
145.	**Стратегія “цільового зміцнення”** термін, який використовують поліцейські, працівники охорони та військові; передбачає посилення безпеки будівлі чи	**“Target hardening” strategy** 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	Falk (2020) – p. 3

	споруди з метою її захисту у випадку нападу або зменшення ризику крадіжки. Вважається, що "сильний, видимий захист стримуватиме або затримуватиме атаку".	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”

6 ГІБРИДНІ ЗАГРОЗИ В УПРАВЛІННІ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ

6 HYBRID THREATS IN FINANCIAL AND ECONOMIC SECURITY MANAGEMENT

№	UA	EN	Джерело
146.	**Бізнес-модель на основі залежності та збору даних** платформи соціальних медіа 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** social media platforms 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
147.	**Борг Януковича** 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 2015 року. Була сформована суто на політичних умовах (відмова від євроінтеграційного курсу України).	**Yanukovych Debt** 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 from the European integration of Ukraine).	Horbulin (2017) – p.159
148.	**Гібридна загроза з погляду муніципалітету** шкідливий вплив, спрямований на критичні операції. Критичні	**Hybrid Threat from the perspective of a municipality** is harmful influencing targeted at critical operations. Critical	Harjanne et al. (2018) – p.6

	операції стосуються інфраструктури, процесів та організацій, необхідних для основних операцій міста, а також, можливо, деяких осіб.	operations refer to the infrastructure, processes and organisations necessary for the city's basic operations as well as, possibly, some individuals.	
149.	**Економічний важель** Економічні важелі можуть бути у формі 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** Economic levers can come 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
150.	**Енергетична безпека** 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** 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
151.	**"Корупційний трикутник"** є одним із способів концептуалізації корупції.	**'Corruption Triangle'** is one way of conceptualising corruption.	MCDC(b) (2019) – p.1

	Основна ідея: щоб корупція мала місце, потрібні три ключові фактори: - мотивація, - можливість і - раціоналізація тих, хто здійснює корупцію.	Main idea: for corruption to take place requires three key factors to come together: - motivation, - an opportunity and - a rationalisation by those carrying out the corruption.	
152.	**Корупція** зловживання довіреною владою з метою отримання приватної вигоди. зловживання службовим становищем і неналежне функціонування державних установ, яке шкодить загальному благу. є одним з 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 зриву; 4) як зброя масового відволікання. Це нечесна чи шахрайська поведінка владних структур, як правило, пов'язана з підкупом. Корупція має як фізичну, так і психологічну складову. Фізичний компонент зосереджується на втраті ресурсу для того, для чого 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** the abuse of entrusted power for private gain. the misuse of public institutions and office to the detriment of the common good. 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. Is the dishonest or fraudulent conduct by those in power, typically involving bribery. 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) Lough & Dubrovskiy (2018) – p.4 MCDC(b) (2019) – p.1

153.	**Криза економічної моделі** одно з явищ "кризи преси". 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 цифрових ЗМІ навряд чи забезпечив компенсацію: 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 менше людей і менше часу для їх виявлення, а також завдяки більшій кількості, ніж якості. Тим не менше, постійно з'являються нові економічні моделі, за якими сплачують підписку, та диверсифікація джерел доходів (наприклад, з розширенням планування подій).	**Crisis of the economic model** one of "the crisis of the press" phenomenon. 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. 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. Nevertheless, new economic models are constantly cropping up, and are paid for by subscriptions and the diversification of revenue sources (with expansions in event planning, for example).	Vilmer et al. (2018) - p.38, 187 Tworek (2018) – p.2
154.	**Торгова війна** 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-	**Trade war** 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	Horbulin (2017) – p.159

	супротивноким. Може бути спрямована на захоплення ринків інших країн, а також на захист національного ринку. Є різновидом економічних війн (як-от валютна, енергетична, продовольча тощо).	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.).	
155.	**Фінансування організацій** багато країн 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** 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
156.	«**Чорний рахунок» (чорна каса)** фінансові перекази прихованих грошей, які важко простежити.	**'black account' (chernaya kassa)** financial transfers of hidden money, which are much harder to trace.	Galeotti (2020) – p.7

7 ГІБРИДНІ ЗАГРОЗИ В ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

7 HYBRID THREATS IN SOFTWARE ENGINEERING

№	UA	EN	Джерело
157.	**Агент Ікс** шкідливе програмне забезпечення, яке дозволяє віддалено виконувати команди, передавати файли та реєструвати ключі, функція, яка реєструє кожне натискання клавіші, зроблене на скомпрометованому комп’ютері, що забезпечує легкий доступ до паролів. X-Agent також налаштований на можливість роботи як на комп'ютері, так і на мобільних платформах.	**X-Agent** a malware that allows for remote commands, file transmissions, and keylogging, 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
158.	**Інтернет речей (IoT):** 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. 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):** 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. 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
159.	**Квантові науки** нові технології, які дозволяють підвищити продуктивність	**Quantum sciences** new technologies which enable the performance of electronics to	

	електроніки понад законом Мура, який уже говорить, що ми можемо очікувати збільшення швидкості та можливостей комп'ютерів кожні два роки.	increase beyond Moore's Law, which already states that we can expect the speed and capability of computers to increase every couple of years	Thiele(b) (2020) – p.6 European Commission (b) (2018)
	використовуючи квантові комп'ютери, функціональні можливості наявних звичайних технологій можна значно покращити з погляду чутливості, точності, швидкості або зручності для користувача.	using quantum computers, the functionalities of already existing conventional technologies can be significantly improved in terms of sensitivity, accuracy, speed or user-friendliness	Inglesant et al. (2016)
	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 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
160.	**Квантові обчислення** надшвидкі комп'ютери, які використовують відмінні від класичних алгоритми. Приклади "гібридних" застосувань: злом кодів кібербезпеки з безпрецедентною швидкістю, що ускладнює кібербезпеку**.**	**Quantum computing** super-fast computers that utilise different algorithms to classical computers Examples of hybrid applications: Cracking cyber security codes with unprecedented speed, making cyber security even more difficult.	Bekkers et al. (2019) – p.26
161.	**Квантова технологія** нова галузь фізики та техніки; використовує властивості квантових ефектів - взаємодії молекул, атомів і навіть менших частинок, відомих як квантові об'єкти - для створення	**Quantum technology** an emerging field of physics and engineering; it uses the properties of quantum effects – the interactions of molecules, atoms, and even smaller particles, known as quantum objects – to create practical applications in many different fields.	Thiele(b) (2020) – p.6

	практичних застосувань у багатьох різних сферах.		
162.	**Кібератака** 1) сукупність кількох короткочасно узгоджених за метою і часом заходів інформаційно-технологічного впливу, спрямованих на деструктивні зміни визначеного об'єкта інформаційної інфраструктури. 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 C2. Друга категорія кібератак буде спрямована на здатність та готовність цілі вести війну протягом тривалого періоду часу.	**Cyberattack** 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. 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 C2 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 Schroefl (2020) – p.3,5
163.	**Кібервійна** 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, комп’ютерних програм та основних мереж, а також з точки зору дезінформації та викривлення, і, нарешті, їхні	**Cyberwarfare** 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 networks, as well as in terms of disinformation and defacement, and lastly their political and/or strategic	Schroefl (2020) – p.4

	політичні та / або стратегічні цілі - все це вказує на їхню характеристику як кібервійни.	goals point to their characterization as cyber “warfare”.	
164.	**Кібер шпигунство** 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** 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
165.	**Набір інструментів для кібердипломатії** "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** “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 Sweijs & Zilincik (2019) – p.21
166.	**Стакснет** 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** 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 auto-mated control systems of industrial enterprises, power plants, airports, etc.	Treverton et al. (2018) - p. 54
167.	**Технічне використання** є одним із методів інформаційного впливу (див. *Кампанії Впливу*)	**Technical exploitation**	MSB (2018) – p.19, 23

	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 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. Сюди відносимо: *Боти, Маріонетка, Діпфейки, Фішинг* тощо.	is one of the information influence techniques (see *Influence Campaigns*) 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 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. it includes: *Bots, Sock Puppet, Deep Fakes, Phishing* etc.	
168.	**Фішинг** є одним із інструментів *Технічного Використання* 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. Цільовий фішинг передбачає більш складне націлювання на користувачів для отримання доступу, наприклад, до захищеної комп'ютерної системи роботодавця.	**Phishing** Is one of the *Technical Exploitation* tools. 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. 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

169.	**Хакінг** (дослівно - злам) злам означає отримання несанкціонованого доступу до комп'ютера або мережі та є злочином. є одним із методів *Символічних Дій*. В діяльності з інформаційним впливом хакерство може слугувати символічною дією, повідомляючи, що такі організації можуть бути скомпрометовані, що платформа не захищена або відкрита для шантажу.	**Hackning** hacking means to gain unauthorized access to a computer or a network and is a crime. is one of the *Symbolic Actions* methods. In information influence activities, hacking can serve as a symbolic action, by communicating that an organisation's data can be compromised, that a platform lacks security, or to open for blackmail.	MSB (2018) – p.19, 27
170.	**Цифрова платформа** (включаючи *Соціальну Мережу*) 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, який потім надається спільно та публікується. Див. також *Цифрова Платформа* в розділі "Гібридні загрози в Національній безпеці"	**Digital Platform** (including *Social Network*)- 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. See also *Digital Platform* in "Hybrid Threats in National Security"	Vilmer et al. (2018) - p.80
171.	**Шкідливе програмне забезпечення** програмне забезпечення, яке використовується для зриву роботи комп'ютерних систем, збору конфіденційних даних або отримання доступу до приватних комп'ютерних систем. Приклади "гібридних" застосувань: маніпулювання	**Malware** software that is used to disrupt computer systems, to collect sensitive data or to get access to private computer systems. 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	Bekkers et al. (2019) – p.27

	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.	aircraft, resulting in all kinds of dangerous situations.	
172.	**CozyBear and FancyBear** (дослівно - "Затишний ведмежа" та "Модний ведмежа") 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** the hacker groups, 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

8 ГІБРИДНІ ЗАГРОЗИ В СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ

8 HYBRID THREATS IN ARTIFICIAL INTELLIGENCE SYSTEMS

№	UA	EN	Джерело
173.	**Боти** 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). 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. див. також: *Астротурфінг*.	**Bots** 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). 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. see also: *Astroturfing*.	Bradshaw & Howard (2017) – p.11, 83 MSB (2018) – p.19, 23
174.	**"Бульбашки фільтрів"** алгоритми персоналізації, який використовується пошуковими системами та соціальними мережами. Через це результати пошуку в Google не однакові для всіх користувачів; вони залежать від уподобань користувача, які випливають з його історії пошуку та геолокації. див. також: *Мікро-таргетування, Інтернет-Кокон*	**“Filter Bubbles”** personalization algorithms used search engines and social networks. 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. see also: *Micro-Targeting, Internet-Cocooning*	Vilmer et al. (2018) - p.31 Pariser (2011)

175.	**Великі дані** 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, соціальних, технічних , а також юридичних претензій.	**Big Data** 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
176.	**Діпфейк** ("глибока підробка") такі фейкові новини, які дуже переконливо створюють ефект реальності. Є одним із інструментів *Технічного Використання*. Техніка синтезу зображень на основі штучного інтелекту, яка передбачає створення підробленого, але надзвичайно реалістичного відеовмісту, що спотворює слова чи дії політиків та знаменитостей. Використовує алгоритми навчання для імітації рухів голосу та рота для маніпулювання аудіо та відео матеріалом. 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.	**Deep Fake** such fake news that can very convincingly reproduce the effects of reality. Is one of the *Technical exploitation* tools. An artificial intelligence-based image synthesis technique that involves creating fake but highly realistic video content misrepresenting the words or actions of politicians and celebrities. 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.	Vilmer et al. (2018) - p.149 MSB (2018) – p.19, 23 Neudert & Marchal (2019) – p.5

177.	**Непрозорі алгоритми** *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** *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 Konaev (2019)
178.	**Тактичний рівень штучного інтелекту** 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** 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 Horowitz (2018)
179.	**Темна реклама** є одним із методів *Когнітивного Зламу* це повідомлення, які побудовані на основі психографічного профілю людини. Великі дані	**Dark Ads** is one of the *Cognitive Hacking* methods is messages, which are tailored based upon an individuals' psychographic profile. Big data can	MSB (2018) – p.19-20

	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.	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.	
180.	**Штучний інтелект (ШІ)** Інтелект, продемонстрований машинами та / або (напів-) автономними системами; 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. 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	**Artificial intelligence (AI)** Intelligence demonstrated by machines and/or (semi-) autonomous systems; 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. 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.	Bekkers et al. (2019) – p.26 Thiele (a) (2020) – p.6

адаптуватися до нових ситуацій. Також стає важко визначити, хто за цим стоїть.

9 ГІБРИДНІ ЗАГРОЗИ В ПОЛІТОЛОГІЇ

9 HYBRID THREATS IN POLITICAL SCIENCE

№	UA	EN	Джерело
181.	**Галоп Гіша** є одним із методів *Риторики Викривлення.* Засипання опонента потоком аргументів, фактів та джерел, багато з яких хибні або не пов'язані з проблемою.	**Gish-Gallop** is one of the *Malign Rhetoric* methods. 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
182.	**Гібридність на політичному рівні** можливість для держави або могутнього недержавного утворення, що бажає кинути виклик міжнародному порядку силою.	**Hybridity at the political level** 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
183.	**Громадські демонстрації** є одним із методів "*Символічних дій*". 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** is one of the "*Symbolic Actions*" methods. 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
184.	**Ефект приєднання до більшості** явище, яке використовується для *Когнітивного Злому*. Люди, які відчувають себе частиною більшості, частіше висловлюють свої думки. Наприклад, боти можуть бути	**Bandwagon Effect** a phenomenon that is used in *Cognitive Hacking*. 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	MSB (2018) – p.19-20, 45

	використані для збільшення початкової кількості лайків, коментарів та репостів в соціальних мережах, щоб полегшити подальше залучення "реальних" користувачів. Це створює враження соціального визнання, яке апелює до необхідності соціальної відповідності. (на відміну від ефекту *Спіралі Мовчання*).	likes, comments and shares of a social media entry to facilitate further engagement from “real” users. This gives the impression of social acceptance, which appeals to the need for social conformity. (by contrast of *Spiral of Silence* effect)	
185.	**"Заїжджена платівка"** один з методів введення ідеологічного змісту. 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. див. також *"Побудова платформ"*	**‘Broken Record’** is one of the methods of introducing ideological content. 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. see also *‘Building Platforms’*	Szwed (2016) – p. 81
186.	**Імітатори та самозванці** метод, який використовується в *Оманливих Ідентичностях*. 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** a method that is used in *Deceptive Identities.* 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

187.	**Медіація** концепція про необхідність пристосування політичної діяльності до логіки ЗМІ.	**Mediatisation** the concept about the necessity to adjust political activity to media logic.	Szwed (2016) – p. 16
188.	**Напад** один із методів *Риторики Викривлення*. Втручання в існуючу дискусію шляхом зміни її мети чи теми. Особливо ефективний при застосуванні хештегов, мемів, подій або контркультурних соціальних рухів.	**Hijacking** is one of the *Malign Rhetoric* methods. 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.	MSB (2018) – p.19, 26
189.	**Обмеження рамками** – див. *Фреймінг*	**Framing**	
190.	**Озлоблення** один із способів поєднання методів інформаційного впливу (див. *Кампанії впливу*). 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** one of the ways to combine of information influence techniques (see *Influence Campaigns*). 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
191.	**Перехід на особистості** (лат. - "аргумент, спрямований на людину") - напад, дискредитація та висміювання особи, яка стоїть за аргументом, для примушення особи до мовчання, стримування чи знеохочення. Один з методів *Риторики Викривлення.*	**Ad Hominem** attacking, discrediting and ridiculing the person behind an argument to silence, deter or discourage. Is one of the *Malign Rhetoric* methods.	MSB (2018) – p.19, 26

192.	**Підтверджувальна упередженість** психологічне явище: ми схильні надавати перевагу інформації, яка підтверджує наші пущення, підтримує наші позиції і не ображає наші відчуття.	**Confirmation Bias** 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
193.	**"Плюралістичне невігластво"** 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'** 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 discussion. In this situation we rely on 'their opinions', even though those opinions do not actually exist.	Szwed (2016) – p. 39
194.	**"Побудова платформ"** один із методів привнесення ідеологічного контенту. 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. див. також *"Заїжджена Платівка"*	'**Building Platforms'** is one of the methods of introducing ideological content. 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. see also *'Broken Record'*	Szwed (2016) – p. 81
195.	**Полемічний аргумент**	**Eristic Argument** an argument that aims to successfully dispute another's	Szwed (2016) – p. 44

	аргумент, метою якого є успішне оскарження чужого аргументу, а не пошук істини.	argument, rather than searching for truth.	
196.	**Популізм** показний політичний стиль, який використовує проти істеблішменту риторику, що викликає розкол та протиставляє "людей" та невловиму "еліту".	**Populism** a performative political style that employs a divisive, anti-establishment rhetoric pitting 'the people' against an elusive 'elite'.	Neudert & Marchal (2019) – p.6
197.	**Публічна демократія** 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. 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** 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. 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
198.	**Риторика викривлення (наклепу)** є одним із методів інформаційного впливу (див. *Кампанії Впливу*). 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	**Malign Rhetoric** is one of the information influence techniques (see *Influence Campaigns*). 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-	MSB (2018) – p.19, 26

	фрагментований характер розмов у сучасній публічній сфері, щоб скаламутити воду, обдурити та ввести в оману, а також знеохотити учасників брати участь у публічних дебатах. Поширеним засобом наклепницької риторики в Інтернеті є *Тролі*. Це включає: *Перехід на особистості, Якщодоізм, Галоп Гіша, Солом'яне опудало, Напад* (чорна риторика) тощо.	fragmented nature of conversations in the contemporary public sphere to muddy the waters, deceive and mislead, and discourage actors and voices to participate in the public debate. A common vehicle for online malign rhetoric is *Trolls*. It includes: *Ad Hominem, Whataboutism, Gish-Gallop, Strawman, Hijacking* etc.	
199.	**Солом'яне опудало** Один з методів *Риторики Викривлення.* дискредитувати супротивників, приписуючи позиції або аргументи, яких вони не дотримуються, а потім виступати проти цих позицій.	**Strawman** is one of the *Malign Rhetoric* methods. Discredit an adversary by attributing positions or arguments that they do not hold and then arguing against those positions.	MSB (2018) – p.19, 26
200.	**Фреймінг** (або **Обмеження рамками**) (для медійних зображень об'єктів, подій, особистостей або груп) 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. 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,	**Framing** (for media representations of objects, events, personalities or groups) 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. 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	Szwed (2016) – p.14-15 Goffman (1986) – p.8-10 Benford & Snow (2000) – p.614

	незв’язані елементи або події будують єдине ціле, відповідаючи на питання "Що тут відбувається?"	coherent whole, answering the question “What is going on here?”	
201.	**Якщодоізм** один з методів *Риторики Викривлення (наклепу)*. відхилення аргументу через привернення уваги до подібного явища, якому не приділяється стільки уваги.	**Whataboutism** one of the *Malign Rhetoric* methods. deflecting an argument by drawing attention to a similar phenomenon which does not get as much attention.	MSB (2018) – p.19, 26

10 ГІБРИДНІ ЗАГРОЗИ В СЕРЕДНІЙ ОСВІТІ (ІСТОРІЯ)

10 HYBRID THREATS IN SECONDARY EDUCATION (HISTORY)

№	UA	EN	Джерело
202.	**Аннексія Криму** 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 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.	**Annexation of Crimea** 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 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.	Grigas (2016) – p.127

203.	**Багатовекторність зовнішньої політики України** 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.** 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
204.	**Близьке зарубіжжя (пострадянський простір)** (один із наративів, що окреслює сфери інтересів Кремля) ті колишні радянські республіки, які зараз є незалежними державами. Росія вважає, що ці слабкіші (особливо в економічному сенсі) країни повинні "природним чином" тяжіти і тягнутись до сильнішої російської держави, посилаючись на спільний з Росією історичний досвід, культуру, мову тощо.	**"Near abroad" (post-Soviet space)** (one of the narratives that outline the Kremlin's spheres of interest) those ex-Soviet republics that are now independent states. Russia assumes that these weaker (especially in an economic sense) countries should ‘naturally’ gravitate and be drawn to the stronger Russian state referring to shared historical experience, culture, language and so forth of these countries with Russia	Rotaru (2018) – p.1 Simons (2015) – p.4

205.	**Велика Вітчизняна війна (1941 - 1945)** один із кремлівських наративів, російська інтерпретація історії. 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** one of the Kremlin narratives, the Russian interpretation of history 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 Domańska (2019) – p.1
206.	**"День Перемоги"** один із кремлівських наративів, російська інтерпретація історії День Перемоги відзначається в Росії щороку 9 травня. 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. 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"** one of the Kremlin narratives, the Russian interpretation of history Victory Day is celebrated in Russia annually on May 9 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. 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 Simons (2015) – p.6

207.	**Доктрина "обмеженого суверенітету"** (доктрина Брежнєва) 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. 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) 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 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
208.	**Євромайдан** рух України 2014-го року, який прагнув наблизити країну до Заходу.	**Euro-maidan** the 2014 Ukraine’s movement, which sought to bring the country closer to the West.	Grigas (2016) – p.28, 109
209.	**"Катинська різанина" 1940** один з наративів Кремля, "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	**"Katyń massacre" 1940** one of the Kremlin narratives, "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	Domańska (2019) – p.3

	були інфекційні хвороби, які забрали життя 16 000–20 000 (російська пропаганда наводить завищену цифру 100 000).	Russian propaganda most often cites the inflated number of 100,000).	
210.	**Кольорова революція** ненасильницьке повалення урядів масовими протестами; не військова війна	**Colour revolution** the non-violent nature of the regime change resulting from mass protests; non-military warfare	Bouchet (2016) – p.1
211.	**Пакт Молотова – Ріббентропа про ненапад (Пакт Гітлера-Сталіна)** Один з наративів Кремля 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. 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. Резолюція Європарламенту 2019 позначила Пакт Молотова – Ріббентропа як безпосередню причину початку Другої світової війни	**Molotov–Ribbentrop Non-Aggression Pact (Hitler-Stalin Pact)** one of the Kremlin narratives, 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. 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. 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 European Parliament (2019) – p.3
212.	**Російська політика пам'яті** становить важливий елемент [російської] державної пропаганди: історичні факти та їхні інтерпретації підпорядковують політичним інтересам тих, хто приймає рішення.	**Russia's politics of memory** constitutes an important element of [Russian] state-sponsored propaganda: historical facts and their interpretations are subordinated to the political interests of decision makers.	Domańska (2019) – p.1, 3

	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 легітимізуючих факторів (економічних, політичних, соціальних та міжнародних) зменшується.	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, political, social and international) wanes.	
213.	**"Співвітчизники" (соотєчєствєннікі)** одна з концепцій, що окреслює сфери інтересів Кремля, 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.	**"Russian Compatriots" (sootechestvenniki)** one of the concepts that outline the Kremlin's spheres of interest 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.	Rotaru (2018) – p.7
214.	**Спільне радянське минуле (спільна історія)**	**The shared Soviet past (Common history)**	Rotaru (2018) – p.7

	є не лише джерелом м'якої сили для Кремля, але й важливим елементом для створення спільної ідентичності на пострадянському просторі.	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.	
215.	**Українська "Революція гідності"** (також відома як Євромайдан) Див. *Євромайдан*	**Ukraine's "Revolution of Dignity"** (also known as the Euromaidan) See *Euromaidan*	
216.	**«Ялтинський порядок» 1945** ознаменував апогей статусу великої держави Росії та СРСР. Нинішні геополітичні амбіції Москви базуються на двох основних елементах цього порядку. 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. 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 російської безпеки, а не свої, що було б рівнозначно створенню в цьому регіоні своєрідної буферної зони.	**the "Yalta order" 1945** marked the apogee of Russia-USSR great power status. Moscow's current geopolitical ambitions build upon two main elements of this order. 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. 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 the creation of a sort of security buffer zone in this region.	Domańska (2019) – p.6

11 ГІБРИДНІ ЗАГРОЗИ В МЕНЕДЖМЕНТІ СОЦІОКУЛЬТУРНОЇ ДІЯЛЬНОСТІ

11 HYBRID THREATS IN SOCIO CULTURAL MANAGEMENT

№	UA	EN	Джерело
217.	**Агент культури** 1) людина, яка сприяє змінам, висвітлюючи та досліджуючи безліч способів впливу культурних практик на наші суспільства. 2) це визначення представляє концепцію культури як агентства, що являє собою низку креативних видів діяльності, які сприяють розвитку суспільства, зокрема педагогіку, дослідження, активізм та мистецтво.	**Cultural agent** 1) is an individual who promotes change by highlighting and exploring the many ways in which cultural practices affect our societies. 2) This definition represents us 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) Barbero et al. (2006)
218.	**Акультурація** процес, який втілює людина/агент (це не процес, який трапляється з людиною) після зустрічі та приєднання до культурної спільноти, яка відрізняється від культурної спільноти, де вона була соціалізована.	**Acculturation** a process executed by an agentic individual (it is not a process that happens to an individual) after meeting and entering a cultural community that is different from the cultural community where he or she was originally socialized.	Chirkov, V. (2009) – p.94 Maehler et al. (2019)
219.	**Аномія** соціальна ситуація, коли старі інститути перестають функціонувати стабільно й люди вже не можуть розраховувати на отримання очікуваних винагород за відповідними очікуваними стандартами (концепція Дюргейма). відсутність (знецінення) норм, що проявляється у формі деінституціоналізації правових (законних) засобів суспільства (концепція Мертона). Таким чином, цілі, до яких навчили прагнути людей	**Anomie** 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). normlessness, manifested in such a form as a deinstitutionalization of the legitimate means of society (conception of Merton) 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	Spencer & Lalgee (2008) – p.1970 - 1982 Deflem (2018) – P.147

	(наприклад, досягти процвітання завдяки добре оплачуваній роботі), не відповідають інституціоналізованим наявним засобам та нормам, які влада може запропонувати людям.	institutionalized means that are actually available and the norms by which people are supposed to compete.	
220.	**Єврабія** (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. Є прикладом анти-наративів, які атакують "наші інституції"; інструмент гібридного впливу.	**Eurabia** (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. the example of the anti narratives that attack "our institutions"; a hybrid influence tool.	Vilmer et al. (2018) - p.78 Brown (2019)
221.	**Культурна дипломатія** 1) спосіб "демонстрації культури країни за допомогою концертів чи виставок» та інших креативних практик. 2) це обмін ідеями, інформацією, мистецтвом та іншими аспектами культури між країнами для сприяння та розвитку взаєморозуміння" (Концепція М. С. Каммінгса).	**Cultural diplomacy** 1) a way for "showcasing a country's culture through concerts or exhibitions» and other creative practices". 2) an exchange of ideas, information, art, and other aspects of culture between countries to facilitate mutual understanding" (Conception of M. C. Cummings).	Williams S. (2021) Ryniejska–Kiełdanowicz, M. (2009) – p.8
222.	**Культурна діяльність, товари та послуги** діяльність, товари та послуги, які розглядаються як певний атрибут, використання чи мета, що втілюють або передають форми	**Cultural activities, goods and services** 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	UNESCO (2015) – p.7

	проявів культури, незалежно від їх комерційної цінності. Культурна діяльність може бути самоціллю або сприяти виробництву культурних товарів та послуг	the commercial value they may have. Cultural activities may be an end in themselves, or they may contribute to the production of cultural goods and services	
223.	**Культурна належність** 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** 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)
224.	**Культурна спадщина** це успадкована з минулого сукупність ресурсів, яку люди, незалежно від форм власності, визначають як відображення та вираження своїх цінностей, які постійно еволюціонують, вірувань, знань та традицій. Вона включає в себе всі аспекти навколишнього середовища, що є результатом взаємодії між людьми та місцевостями (місцями) у часі.	**Cultural heritage** 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. It includes all aspects of the environment resulting from the interaction between people and places through time.	COE (2005). – p.2
225.	**Культурна травма -** є культурно інтерпретованою раною самої культурної текстури суспільства. 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	**Cultural trauma** – Is culturally interpreted wound to cultural tissue itself. 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.	Sztompka (2000) – p.458 - 459

	колективу, можуть порушити наявне семантичне поле. 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. Культурна травма включає такі симптоми: аномія, цивілізаційна некомпетентність, колективна вина, колективна ганьба, синдром недовіри, криза ідентичності, криза легітимності, культурне відставання та соціальна напруга.	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. 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.	
226.	**Культурний геноцид** 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** 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
227.	**Культурний контент** символічне значення, художній вимір та культурні цінності, що походять з культурних ідентичностей чи виражають їх.	**Cultural content** the symbolic meaning, artistic dimension and cultural values that originate from or express cultural identities.	UNESCO (2015) – p.7
228.	**Міжкультурність** наявність та рівноправна взаємодія різноманітних культур та можливість генерувати спільні	**Interculturality** the existence and equitable interaction of diverse cultures and the possibility of generating shared	UNESCO (2015) – p.8

	форми прояву культури шляхом діалогу та взаємоповаги	cultural expressions through dialogue and mutual respect	
229.	**Мова ненависті** текст, який погрожує, ображає або нападає на людину чи групу на основі національного походження, етнічної приналежності, раси чи релігії.	**Hate Speech** text that threatens, insults or attacks a person or group on the basis of national origin, ethnicity, race or religion.	Szwed (2016) – p.10
230.	**Російськомовні громади** складова "*Руського Миру*", що є основою російської мережі за кордоном. Основна ідея: "якщо вирощувати проросійське мислення за кордоном, важливо вкладати кошти у посилення російської мови". Але законні зусилля з просування російської мови використовують із підривною метою: - отримання лояльності "російськомовних" (фінансуючи проєкти, що просувають російську мову), - "захист прав" російськомовного населення (в Україні та інших країнах), - розпалювання напруженості та сепаратистських настроїв в Україні (підтримуючи маргинальні сепаратистські крила слов'янофільських та русофільських організацій). "Руський мир всюди, де говорять російською"	**Russian-Speaking Communities** 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 reinforcement of the Russian language". But legitimate efforts to promote the Russian language is used for subversive purposes: - to buy the loyalty of Russian-speakers (by financing projects promoting the Russian language), - to "defend rights" of Russian-speaking population (in Ukraine and other countries), - to foment tensions and separatist sentiments in Ukraine (by supporting the fringe separatist wings of Slavophile and Russophile organizations). " the Russian World is everywhere where the Russian language is spoken"	Lutsevych (2016) – p.14, 16
231.	**Сатира та пародія** є одним із методів *Дезінформації*. Висміювання, викриття та критика людей, розповіді чи думки з використанням гумору та	**Satire And Parody** is one of the *Disinformation* methods. Ridicule, exposure and critique of individuals, narratives or opinions	MSB (2018) – p.19, 25

	перебільшення. Хоча найчастіше нешкідливе, це може бути використано агресивно в рамках більш широких зусиль з дезінформації. Гумор також дуже ефективний для легітимації суперечливих думок.	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.	
232.	**Соціокультурна система** система, до складу якої входять три типи явищ: матеріальні, структурні та ідеаційні. 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** the system, which consist of three types of phenomena: material, structural and ideational. 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
233.	**Транс-культурна (етнічна) дифузія** 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** 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.	World Heritage Encyclopedia (2021)
234.	**Ю-есес-мен** кліше російської інтернет-пропаганди. це гра слів, що зв'язує есесівців (SS, нацистська Німеччина) та американців (USA, США).	**USS-Men** a clichés of Russia's internet propaganda. is a play on words to link SS-men (Nazi Germany) and US-men (United States).	Szwed (2016) – p.47

12 ГІБРИДНІ ЗАГРОЗИ В МЕДІАКОМУНІКАЦІЯХ

12 HYBRID THREATS IN MEDIA COMMUNICATIONS

№	UA	EN	Джерело
235.	**Блог** 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** 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
236.	**Валентність повідомлення** сила привабливості (доброти) або огидності (поганості) повідомлення, події чи речі.	**Valence Of A Message** the power of attractiveness (goodness) or averseness (badness) of a message, event or thing.	Bradshaw & Howard (2017) – p. 9
237.	**Індивідуальне таргетування** стратегія кібервійськ, що передбачає вибір особи чи групи для впливу на соціальні мережі (як у формі співпраці, так і у формі домагань)	**Individual targeting** 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
238.	**Інтернет-кокон** ефект ізоляції користувачів Інтернету в закритих когнітивних просторах, де вони знаходяться під впливом лише того змісту, який підтверджує їхні переконання. Пошуковик стає	**Internet-cocooning** the effect of internet users insulation "in closed cognitive spaces where they were only exposed to content that supported their beliefs. The engine would	Vilmer et al. (2018) - p.31

	інструментом підтвердження, а не інформування. це комфортні когнітивні простори, що підтверджують забобони, а не протистоять забобонам інших. див. також: *Мікро-таргетування*, *Бульбашки Фільтрів*	become a tool of confirmation rather than information. comfortable cognitive spaces that confirm prejudices rather than confront them with the prejudices of others see also: *Micro-Targeting, Filter Bubbles*	
239.	**Каскадна інформація** 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 використовуємо критичне мислення для її оцінки.	**Cascading Information** 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
240.	**Лідери думок** люди, які впливають 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** 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
241.	**Луна-камери** явище, яке використовується для *Когнітивному Зламу*. Органічно створені підгрупи, в яких люди спілкуються лише з людьми подібних думок. Луна-камери існують як в Інтернеті, так і	**Echo Chambers** a phenomenon that is used in *Cognitive Hacking*. Organically created sub-groups in which people only engage with others of similar opinions. Echo chambers exist both online and in	MSB (2018) – p.19-20

	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. Див. також *Бульбашки Фільтрів*	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. See also *Filter Bubbles*	
242.	**Маріонетка** Є одним із інструментів *Технічного Використання*. 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** Is one of the *Technical Exploitation* tools. 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
243.	**Меми** оцифровані одиниці інформації (текст, зображення, фільм, звук), які копіюються, обробляються і в цій обробленій формі повторно публікуються в Інтернеті; інструмент *Гібридного Впливу*.	**Memes** 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
244.	**Моральна паніка** уперше цей термін ужив криміналіст Джон Янґ стосовно	**Moral panic** the term was first applied by the criminologist Jock Young to sudden	McQuail's, D. (2010) – p. 564

	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.	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.	
245.	**Нові ЗМІ** (нові засоби масової інформації, нові мас медіа) соціальні медіа, керовані "аматорами"; в кінцевому підсумку вони можуть виконувати ті самі функції, що й звичайні журналісти (на відміну від *Традиційних Засобів Масової Інформації*).	**New Mass Media** the social media run by ‘amateurs’ who ultimately may fulfil the same functions as regular journalists (by contrast of the *Traditional Mass Media*).	Robbin & Buente (2008) – p.2214 – 2215 (p.5 – 6) Szwed (2016) – p. 12
246.	**Оманливі ідентичності** є одним із методів інформаційного впливу (див. *Кампанії Впливу*) Ми часто оцінюємо достовірність інформації, виходячи з її джерела. Хто зі мною розмовляє і чому? Що вони знають про цю проблему? Вони - саме такі, якими видаються? Імітуючи законні джерела інформації (чи то особи, організації або платформи), учасники діяльності, що займаються інформаційним впливом, експлуатують довіру до	**Deceptive Identities** is one of the information influence techniques (see *Influence Campaigns*) We often evaluate the credibility of information by looking at its source. Who is talking to me and why? What 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	MSB (2018) – p.19, 21

	месенджера, використовуючи оманливі ідентичності. Сюди відносять*: Шиллінг, Імітатори та самозванці, Підробки, Потьомкінські села, Фейкові медіа* тощо.	messenger by utilizing deceptive identities. it includes: *Shilling, Impersonators & Impostors, Forgeries, Potemkin Villages, Fake Media* etc.	
247.	**“Отруєння хештегами”** хештеги, "поведінка" яких схожа на спам, щоб зруйнувати критику або інші небажані дискусії через потік не пов’язаних твітів	**“Hashtag Poisoning”** the spam trending hashtags to disrupt criticism or other unwanted conversations through a flood of unrelated tweets	Bradshaw & Howard (2017) – p.9
248.	**Побудова інформації** 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.	**Information Building** 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.	Szwed (2016) – p.13
249.	**Соціальні медіа** *цифрові платформи*, що сприяють створенню та обміну інформацією в мережевих спільнотах.	**Social media** *digital platforms* that facilitate the creation and sharing of information in networked communities.	Neudert & Marchal (2019) – p.6
250.	**Спін-доктор / політтехнолог** 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** 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
251.	**"Спіраль мовчання"** явище, коли ми мовчимо, боячись думки більшості, не бажаючи їхньої критики. Інтернет-користувачі, як правило, не діляться своїми поглядами,	**‘Spiral of Silence’** a phenomenon when we keep quiet in fear of the majority’s opinion, not wanting to be criticized by them. Internet surfers tend not to share their viewpoints if these viewpoints	Szwed (2016) – p.40 Vilmer et al. (2018) - p.87

	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. Дивіться також *Астротурфінг*	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. See also *Astroturfing*	
	явище, яке використовується в *Когнітивному Зламі.* 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.	a phenomenon that is used in *Cognitive Hacking.* 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.	MSB (2018) – p.19-20
252.	**Спіраль цинізму** 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 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.	**Spiral of cynicism** 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 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.	McQuail's, D. (2010) – p. 571

253.	**Традиційні ЗМІ** засоби масової інформації, що керуються професіоналами (на відміну від *Нових ЗМІ*)	**Traditional Mass Media** the media which operated by professionals (by contrast of the *New Mass Media*)	Robbin & Buente (2008) – p.2214 – 2215 (p.5 – 6) Szwed (2016) – p.12
254.	**Тролі** особи, які поширюють інформацію, насичують певні веб-сайти коментарями та / або переслідують інші. користувач акаунту в соціальних мережах, який навмисно викликає незадоволення в інших користувачів своїми коментарями та поведінкою, що сприяє 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.	**Trolls** individuals who spread information, saturate certain websites with comments, and/or harass others. a user of a social media account who deliberately antagonises other users through their comments and behaviour. This contributes to increased polarization, silences 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	Vilmer et al. (2018) - p.84 MSB (2018) – p.19, 25
255.	**Тролінг** така поведінка, як публікація провокаційних коментарів в Інтернеті з метою викликати конфлікт. Як правило, протікає у три фази: заманювання, захоплення приманки та витягування.	**Trolling** behaviour such as publishing provocative comments on the internet with the intention of causing conflict. Generally proceeds in three phases: luring, taking the bait and hauling in.	Vilmer et al. (2018) - p.86 Szwed (2016) – p.7, 54
256.	**Ухил / Упередженість** Будь-яка тенденція ухилятися в новинах від точного, нейтрального, збалансованого та неупередженого зображення “реальності” подій і соціального світу відповідно до визначених критеріїв. Зазвичай розрізняють	**Bias** 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	McQuail's, D. (2010) – p. 549

	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.	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.	
257.	**Фейковий аккаунт** або обліковий запис (профіль), яким керує хтось, хто видає себе за когось іншого, або облікові записи, якими керують не люди, а автоматизовані (боти). 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** 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). 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 Parliament Of Singapore (2018) - p. 15 (# 71) Nimmo, B. (2018) – p.6 (# 33)
258.	**Фейкові медіа** метод, який використовується в *Оманливих Ідентичностях*. Дезінформація може розповсюджуватися шляхом створення підроблених медіа платформ, які виглядають або мають веб-адресу, як справжні сайти новин.	**Fake Media** a method that is used in *Deceptive Identities*. 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
259.	**Фільтрування** 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,	**Gatekeeping** 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	McQuail's, D. (2010) – p. 558

	наскільки вони “вартують” бути новинами, та на інші критерії. Найважливіші питання стосуються критеріїв добору і систематичного упередження, які виявляються у процесі фільтрування.	systematic bias that has been discerned in the exercise of the role.	
260.	**Флуд** один із способів поєднання методів інформаційного впливу (див. *Кампанії Впливу*). Флуд створює плутанину, перевантажуючи аудиторію будь-якою інформацією: позитивною, негативною чи неактуальною. Це робиться за допомогою спаму та *Тролінгу* в соціальних мережах або шляхом поширення дезінформації до правомірних джерел ЗМІ. Флуд витісняє легітимну інформацію.	**Flooding** one of the ways to combine of information influence techniques (see *Influence Campaigns*). Flooding creates confusion by overloading audiences with information, either positive, negative or irrelevant. This can be done by spamming and *Trolling* on social media, or by disseminating disinformation to legitimate media sources. Flooding crowds out legitimate information.	MSB (2018) – p.29
261.	**Шиллінг** метод, який використовується в *Оманливих Ідентичностях*. 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** a method that is used in *Deceptive Identities*. 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

15 ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

15 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. 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
4. Bekkers, F., Meessen, R., & Lassche, D. (2019). Hybrid conflicts: the new normal?. Den Haag: TNO. – 17 p. https://hcss.nl/sites/default/files/files/reports/Hybrid%20conflicts.%20The%20New%20Normal%20-%20HCSS%20%20TNO%20(1901)_0.pdf
5. 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
6. 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
7. 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
8. 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
9. 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

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

11. 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.

12. 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

13. 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

14. 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

15. 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

16. 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

17. 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

18. 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

19. 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

20. 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

21. 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

22. 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/

23. European Commission (2021). Cybercrime. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

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

25. European Commission (a) (2018). A Multi-Dimensional Approach to Disinformation. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

26. European Commission (b) (2018). Quantum Technologies Flagship. Brussels, October 2018. https://ec.europa.eu/digital-single-market/en/quantum-technologies

27. 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

28. 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

29. 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

30. 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

31. 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

32. 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

33. 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

34. 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/

35. 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/

36. 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

37. 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

38. 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

39. Grigas, A. (2016). Beyond Crimea: the new Russian empire. Yale University Press. – 352 p. ISBN 0300220766 http://maxima-library.org/knigi/genre/b/382587?format=read

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

41. 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/fileadmin/user_upload/downloads/ourwork/IFTF_ODNI_Cognitive_Immunity_Map__2019.pdf

42. 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

43. 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

44. 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

45. 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/

46. Hybrid CoE(a) (2021). Hybrid Threats https://www.hybridcoe.fi/hybrid-threats/

47. Hybrid CoE(b) (2021). What is Hybrid CoE https://www.hybridcoe.fi/who-what-and-how/

48. 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

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

50. 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

51. 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

52. Konaev, M. (2019). With AI, We'll See Faster Fights, but Longer Wars. War on the Rocks, October 29, 2019. https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/

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

54. Laruelle, M. (2015). The "Russian World": Russia's soft power and geopolitical imagination. Center on Global Interests. – 30p. http://globalinterests.org/wp-content/uploads/2015/05/FINAL-CGI_ Russian-World_Marlene-Laruelle.pdf.

55. 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

56. 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

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

58. 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

59. 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

60. 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

61. 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

62. 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

63. 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

64. 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

65. MSB (Swedish Civil Contingencies Agency, 2018) Countering information influence activities: A handbook for communicators. Sweden, Karlstad. 48 p. https://www.msb.se/RibData/Filer/pdf/28698.pdf

66. NATO (2010) Capstone Concept for the Military Contribution to Countering Hybrid Threats. Brussels: NATO Military Committee. – 18 p. https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

67. 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

68. 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

69. Nissen T. E. (2015). Weaponization of Social Media. Characteristics of Contemporary Conflicts. Copenhagen: Royal Danish Defence System. – 148 p. https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media

70. Pamment, J., Nothhaft, H., & Fjällhed, A. (2018). Countering Information Influence Activities: A Handbook for Communicators. MSB & Lund University. 137 p. https://www.msb.se/RibData/Filer/pdf/28697.pdf

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

72. 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.

73. 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

74. 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

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

76. 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

77. 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

78. Ryniejska–Kiełdanowicz, M. (2009). Cultural diplomacy as a form of international communication. Institute for Public Relations. http://www. instituteforpr. org/wp-content/uploads/Ryniejska_Kieldanowicz. pdf

79. 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

80. 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

81. 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

82. 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

83. 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

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

85. 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

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

87. Swedish Defence University (2021). https://www.fhs.se/en/centre-for-societal-security/about-ctss/organization/cats.html

88. Sweijs, T., & Zilincik, S. (2019). Cross Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p. https://hcss.nl/sites/default/files/files/reports/Cross%20Domain%20Deterrence%20-%20Final.pdf

89. 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

90. 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

91. 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

92. 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

93. 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

94. 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

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

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

97. 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

98. UNESCO (United Nations Educational, Scientific and Cultural Organization, 2015). Basic Texts of the 2005 Convention on the Protection and Promotion of the Diversity of Cultural Expressions, 2015 edition. France, Paris. 133 p. https://en.unesco.org/creativity/sites/creativity/files/convention2005_basictext_en.pdf

99. 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

100. 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

101. Vilmer, J.-B. Jeangène, Escorcia, A., Guillaume, M., Herrera, J. (2018) Information Manipulation: A Challenge for Our Democracies, 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

102. 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.

103. 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

104. 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

105. World Heritage Encyclopedia (2021) Trans-cultural diffusion. Article Id: WHEBN0000994299. http://www.self.gutenberg.org/articles/trans-cultural_diffusion