РОЗДІЛ ІІ. СУСПІЛЬНІ КОМУНІКАЦІЇ ТА МОВНІ УНІВЕРСАЛІЇ

УДК 327.019/.5:004.9.056(061.1ЄС:100)

Сергій Федонюк,
кандидат географічних наук, доцент кафедри міжнародних комунікацій та політичного аналізу,
Волинський національний університет імені Лесі Українки,
sergii.fedoniuk@vnu.edu.ua
ORCID ID: 0000-0003-2853-8905

Ігор Карпук,
аспірант,
Волинський національний університет імені Лесі Українки,
Karpuk.Igor@vnu.edu.ua
ORCID ID: 0000-0003-4430-6004
DOI 10.29038/2524-2679-2022-02-44-65

РОЗВИТОК КОНЦЕПЦІЇ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЄС

Ми дослідили основні тенденції розвитку підходів Європейського Союзу у сфері стратегічних комунікацій. Ця діяльність пов'язана з викликами й загрозами безпеці у світлі стратегічних пріоритетів об'єднання. Концепція стратегічної комунікації змінювалась із часом і сьогодні формується під зростаючим впливом гібридних загроз та дезінформації, особливо у зв'язку з початком російської гібридної агресії проти України у 2014 р. Також суттєво впливає на систему стратегічних комунікацій міжнародна ситуація, що відображається на загальних стратегічних пріоритетах того, хто їх здійснює. Рішення в Європейському Союзі та його країнах-членах приймаються з урахуванням діяльності головних міжнародних акторів і партнерів, зокрема стратегічних рішень у США, НАТО, G7. Це може спричиняти пошук нових концептів, таких як стратегічна автономія з відповідними цілями стратегічних комунікацій.

У цьому дослідженні проведено аналіз основних стратегічних документів вторинного права Європейського Союзу у сфері інформаційної безпеки

та безпеки мереж на предмет виявлення відповідності одному з підходів. Детальніше розглянуто «Стратегію кібербезпеки для цифрової декади», прийняту наприкінці 2020 р., і пов'язані з нею документи. Установлено близькість підходів Європейського Союзу до західної моделі інформаційної (кібер) безпеки, його активність щодо її просування у світі. Також ми розглянули ініціативи держав- членів Європейського Союзу щодо активного впливу на перебіг процесів міжнародної співпраці в цій сфері, зокрема з урахуванням подій і тенденцій, пов'язаних із діяльністю провідних акторів на рівні ООН.

У підсумку можемо зробити висновок про все більш чітке оформлення політики ЄС у сфері інформаційної (кібер) безпеки та просування його конструктивної позиції з цього питання на світовій арені.

Ключові слова: кібербезпека, міжнародна політика, Європейський Союз.

Serhii Fedoniuk,
Lesya Ukrainka Volyn National University,
ORCID ID: 0000-0003-2853-8905

Ihor Karpuk,
Lesya Ukrainka Volyn National University,
ORCID ID: 0000-0003-4430-6004

DEVELOPMENT OF THE CONCEPT OF EU STRATEGIC COMMUNICATIONS

We have studied the main trends in the development of the European Union's approaches to strategic communications. These activities address security challenges and threats in the light of the association's strategic priorities. The concept of strategic communication has changed over time and today is formed under the growing influence of hybrid threats and misinformation, especially in connection with the beginning of Russia's hybrid aggression against Ukraine in 2014. The strategic situation is also significantly affected by the international situation. who carries them out. Decisions in the European Union and its member states are made taking into account the activities of major international actors and partners, including strategic decisions in the United States, NATO, G7. This may lead to the search for new concepts, such as strategic autonomy, with the corresponding goals of strategic communications.

This study analyzes the main strategic documents of the secondary law of the European Union in the field of information security and network security to identify compliance with one of the approaches. The «Cyber Security Strategy for the

Digital Decade», adopted in late 2020, and related documents are discussed in more detail. The closeness of the European Union's approaches to the Western model of information (cyber) security and its activity in promoting it in the world has been established. We also considered the initiatives of the member states of the European Union to actively influence the processes of international cooperation in this area, in particular, taking into account the events and trends related to the activities of leading actors at the UN level.
As a result, we can conclude that the EU's policy in the field of information (cyber) security is becoming clearer and that its constructive position on this issue is being promoted on the world stage.
Key words: cybersecurity, international politics, European Union.

1. ВСТУП

Постановка проблеми. Стратегія зовнішньої політики Європейського Союзу розвивається з урахуванням актуальних і потенційних викликів. Серед головних загроз сьогодні – ті, що пов'язані з геополітичними амбіціями РФ, які чинять вплив на країни-члени й загалом на ЄС переважно у сферах зв'язків із громадськістю, публічної дипломатії, а також інформаційно-психологічних впливів. У цьому аспекті адекватною відповіддю є розвиток стратегічних комунікацій у контексті політики безпеки й оборони Європейського Союзу. Але до недавнього часу відповідні документи ЄС та ухвалені концепції Стратегічних комунікацій не покривали повною мірою нових викликів, таких як гібридна війна, інформаційна інтервенція, кібербезпека [1]. Тому в структурах Євросоюзу, країнах-членах, а також у провідних науково-дослідних та експертних центрах розпочалася безпосередня робота над розробкою нової стратегії зовнішньої політики й політики безпеки та оборони з відповідним компонентом стратегічних комунікацій. Ця проблематика відносно нова для європейського контексту, вона динамічно розвивається у зв'язку з міжнародною обстановкою. Актуальність дослідження пов'язана також із новизною європейських підходів щодо розвитку стратегічних комунікацій як в аспекті розвитку політики Європейського Союзу, так і формування відповідних стратегій у країнах-партнерах ЄС, передусім тих, хто обрав курс на приєднання до унії, як-от Україна.

Аналіз останніх досліджень і публікацій. Концепція стратегічних комунікацій в аспекті стратегій міжнародного масштабу стосовно країн Європи почала розвиватися ще у 2000-х рр., коли оформлено відповідну візію НАТО [2;3]. У цей період опубліковано ґрунтовні дослідження в цій сфері, автори яких, проте, не розглядали стратегічні комунікації на

рівні національної стратегії як формалізований та інституціоналізований інструмент, а лише в ролі певного спільного стратегічного мислення чи культури комунікацій на кожному рівні національної політики й стратегії [4], зокрема в контексті публічної дипломатії [5; 6, с. 10]. Подібний підхід помітний і в офіційних документах державного стратегічного планування [7, с. 7]. Водночас стратегічні комунікації розглядалися як засіб протидії загрозам локального й обмеженого характеру, таких як тероризм, радикалізм, кіберзагрози [8, с. 19–20; 9; 10; 11; 12], в офіційних документах [13; 14], а також у рамках військових операцій [15, с 288; 16; 17]. Але у фокусі уваги не перебували масштабні конфлікти й геополітика.

Така концепція стратегічних комунікацій пов'язана з тогочасною візією системи міжнародних відносин, що зафіксовано в документах, які відображають інтегральну позицію акторів. Безпекові підходи країн Європи загалом інтегровано в тогочасній стратегічній концепції НАТО (1999 р.) [18], у якій не йшлося про стратегічну рівновагу, а росія розглядалася не в контексті загроз і викликів, а в розділі про партнерство, співпрацю й діалог. У стратегічній концепції 2010 р. [19] НАТО також жодну державу не розглядає як противника, а спільні зусилля орієнтуються на відбиття наявних і потенційних загроз. У документі як одну з ключових сфер діяльності визначено політику партнерства – безпека у співробітництві.

Ситуація радикально змінилася після початку російської гібридної агресії проти України й переосмислення інформаційних загроз у контексті безпеки. Починаючи з 2014 р., розробляється питання протидії гібридним загрозам і їхнім джерелам, які становлять потенційну небезпеку для країн Європи й НАТО [20]. Європейські видання відображають нову реальність стратегічних комунікацій, говорячи про геостратегічний вимір загроз, їхні природу й особливості, при цьому чітко ідентифікуючи джерело та характер цих загроз [21; 22; 23; 24; 25; 26; 27; 28; 29; 30; 31; 32; 33; 34; 35; 36; 37; 38; 39; 40; 41]. Це відображено в офіційних докусvментах і доктринах, звітах [42; 43; 44; 45; 46], набуло поширення в медіасередовищі [47; 48]. Із позиції глобальної стратегії розглядається також вплив Росії на проблемні теми в країнах ЄС (такі як каталонський сепаратизм [49; 50] і діяльність інших акторів, насамперед Китаю [51; 52]. Із позиції стратегічних цілей аналізується медіасупровід подій і кампаній глобального значення, як-от проблема коронавірусної пандемії, у т. ч. в аспекті інтересів провідних міжнародних акторів [53; 54; 55].

Мета статті. Дослідження охоплює питання підходів ЄС у сфері стратегічних комунікацій відповідно до розвитку міжнародної ситуації, зокрема а аспекті актуалізації гібридних загроз.

Методика дослідження. Використано описовий, аналітичний підхід, який переважно ґрунтується на аналізі джерел, що стосуються діяльності ЄС у сфері стратегічних комунікацій, протидії гібридним загрозам і дезінформації. Застосовано якісний підхід із метою вивчення проблематики в цій сфері, яка потребує дослідження з погляду розвитку міжнародних відносин.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Базис концепції. Концепція стратегічних комунікацій у сфері безпеки, що прийшла на зміну доктрині стратегічного інформаційного протиборства [56; 57] й інформаційних операцій, застосовується в США та на рівні стандартів НАТО [58]. США застосовують системний підхід у плануванні й реалізації стратегічних комунікацій залежно від динаміки міжнародної обстановки, починаючи від завершення Холодної війни. Із 1987 р. періодично приймаються стратегії національної безпеки, у яких сформульовано концептуальні бачення викликів і фокусів національної політики, що відображається на комунікаційній стратегії. Кожне нове видання NSS США зосереджується на різних питаннях, пов'язаних зі стратегічними комунікаціями. Свого часу серед цих викликів були проблеми міжнародного тероризму, а у 2017 р. адміністрація Трампа сформулювала ключову проблему національної безпеки США як стратегічну конкуренцію з іншими державами, зокрема Китаєм і росією [59]. У березні 2021 р. Білий дім опублікував Тимчасові стратегічні вказівки щодо національної безпеки з новим фокусом на різноманітних зовнішніх стратегічних викликах, уключаючи (але не обмежуючись) Китай, росію, пандемію COVID-19, тероризм насильницьких екстремістів і розповсюдження ядерної зброї [60].

Оскільки Європейський Союз у безпекових питаннях загалом координує свою стратегію з НАТО, то це стосується й концептуальних питань у розвитку стратегічних комунікацій. Наприклад, прийнято до використання як стандарт у військових операціях під проводом Європейського Союзу в рамках Європейської політики безпеки та оборони вимоги стандарту НАТО STANAG 2508 Ed. 4 / AJP-3.10.1 Ed. B [61]. У цьому документі (Доктрина психологічних операцій НАТО) психологічні операції розглянуто як один із головних компонентів системи стратегічних комунікацій.

Що стосується формалізації в рамках окремого документа, то Північноатлантичний альянс утілює новий підхід у перспективному порядку денному НАТО 2030 [62], орієнтованому на стримування майбутніх

загроз, у тому числі зростаючої агресивності росії. Відповідно змінюється й бачення стратегічних комунікацій із позиції Альянсу, Європейського Союзу, їхніх членів і партнерів.

На глобальному рівні орієнтиром в аспекті підходів до протидії гібридним загрозам для країн ЄС є політика G7 зі створеним країнами групи у 2018 р. Механізмом швидкого реагування. Країни G7 оприлюднили зобов'язання, прийняте в Шарлевуа (Канада), щодо захисту демократії від зовнішніх загроз, де зобов'язалися «створити механізм швидкого реагування G7 для посилення координації для виявлення та реагування на різноманітні й мінливі загрози нашим демократіям, шляхом обміну інформацією та аналізом, а також виявлення можливості скоординованого реагування» [63].

У результаті розширення застосування «м'якої сили» для виконання політичних і військових завдань під час урегулювання кризових ситуацій у різних регіонах світу продемонстровано високу ефективність цілеспрямованого інформаційно-психологічного впливу на активних та опосередкованих учасників збройних конфліктів. Також події «Арабської весни» (2010–2011 рр.), української «Революції гідності» (2013–2014 рр.) та інших масових протестів і конфліктів другого десятиліття XXI ст., насамперед російської збройної агресії на сході України, показали, що масоване використання інформаційних ресурсів дає змогу управляти громадською думкою й спричиняти революційні зміни в суспільствах. Відтак у цей період у НАТО утверджується сучасна концепція стратегічних комунікацій (Strategic Communications), яка передбачає перехід від відокремленого застосування військових та цивільних інформаційно-пропагандистських структур до координації їхньої діяльності під час підготовки й проведення операцій з урегулювання криз. Власне, стратегічні комунікації розглядаються як поєднання публічної дипломатії, зв'язків із громадськістю (громадських справ, військових справ) та інформаційних операцій і психологічних операцій на підтримку політики суб'єкта, його операцій, діяльності та для досягнення стратегічних цілей [64].

Після стратегічної оцінки ключових змін і викликів у глобальному середовищі виникла потреба переглянути Європейську стратегію безпеки від 2003 р. й у 2016 р. прийнято нову Глобальну стратегію ЄС із зовнішньої політики та політики безпеки [66], мета якої полягала в тому, щоб забезпечити широку стратегічну структуру, за допомогою якої ЄС міг би чітко та узгоджено розуміти й протистояти сучасним міжнародним викликам, використовуючи широкий спектр інструментів та механізмів, які є в його розпорядженні.

Новий підхід стосується загалом стратегії безпеки ЄС, у якій в інформаційно-комунікаційній сфері поряд із кібербезпекою важливі позиції починають займати такі напрями, як протидія гібридним загрозам і дезінформації та стратегічні комунікації. Після надзвичайних подій у плані безпеки, що сталися протягом другого десятиліття ХХ ст. (брекзит, криза мігрантів, євроскептичний популізм у Центральній та Східній Європі, жорстка інформаційна активність Росії на тлі гібридної агресії в Україні), у Європейському Союзі намітився поворот до більш широкого розуміння інформаційної безпеки, не обмежуючись, як було до цього, фактично питаннями безпеки мереж й інформаційних систем.

Концепція стратегічних комунікацій віднедавна впроваджується й у сфері Спільної політики безпеки та оборони Європейського Союзу й охоплює діяльність спеціалізованих підрозділів у сферах зовнішніх справ і спільної політики безпеки й оборони. Останні роки відзначені безпрецедентним прогресом в оборонних ініціативах ЄС.

У звіті, підготовленому Інститутом досліджень безпеки ЄС, стратегічні комунікації визначаються як «комунікаційна діяльність з порядком денним або планом» [65 с. 4]. У дослідженні, спонсорованому міноборони Великобританії, наведено таке визначення [66]: «Систематичні серії постійних і узгоджених заходів, що проводяться на стратегічному, оперативному та тактичному рівнях, які дозволяють зрозуміти цільову аудиторію, визначають ефективні канали, а також розвивають і просувають ідеї та думки через ці канали для просування й підтримки певних типів поведінки».

У спеціальному дослідженні, спонсорованому Європарламентом, узагальнено характеристики стратегічних комунікацій [67]: здійснення за заздалегідь визначеним і систематичним планом, а не лише як реакція на поточні події; дії на стратегічному, оперативному та тактичному рівнях; реалізація в конкурентному й навіть конфліктному середовищі; вимога високого рівня координації та синхронізації між зацікавленими сторонами; необхідність конкретного визначення цільової аудиторії та вибору найбільш адекватних каналів зв’язку; мета інформування, впливу й сприяння змінам у поведінці цільової аудиторії; узгодження із загальними цілями країни або організації-промоутера; зосередження на як коротко-, так і довгостроковій перспективі.

Після прийняття у 2016 р. Глобальної стратегії ЄС запропоновано та запущено низку ініціатив для посилення військового, промислового й цивільного вимірів співробітництва ЄС у сфері безпеки та оборони. Принципово новим й амбітним рішенням у цьому плані стало

започаткування у 2020 р. процесу, відомого як «Стратегічний компас», що передбачає комплексне стратегічне вивчення, аналіз загроз і стратегічний діалог між державами-членами. Проєкт структурований навколо чотирьох взаємопов'язаних тематичних блоків: кризового управління, обороноздатності, стійкості та партнерства. Процес керується державами-членами, а установи ЄС відіграють допоміжну й координуючу роль [68].

У середовищі безпеки, що швидко розвивається, Стратегічний компас передбачає необхідність розробки всеохопної політики, яка могла б допомогти подолати комплексні загрози проти ЄС, дотримуючись чіткої політичної мети, що може мати форму гібридного інструментарію ЄС, котрий охоплює заходи проти кібератак, дезінформації, а також інших форм утручання, таких як використання міграційних потоків як інструментів гібридних атак проти ЄС [69]. Це – доповнення до поточних напрямів роботи в контексті посилення Стратегії кібербезпеки ЄС, уключаючи інструментарій кібердипломатії. У такій ширшій рамці Компас також пропонує розробити подальші заходи для протидії маніпуляції з іноземною інформацією [70]. Перший проєкт Стратегічного компаса представлено в листопаді 2021 р., а прийнято 21 березня 2022 р.

Прийняття нової стратегії тепер здійснювалося з урахуванням викликів, пов'язаних з ескалацією агресивної політики РФ: з'явилася гостра необхідність у посиленні позицій ЄС і його партнерів, зокрема України. Мета Стратегічного компаса – зробити ЄС сильнішим та більш спроможним гарантом безпеки. ЄС має бути в змозі захистити своїх громадян і сприяти міжнародному миру й безпеці. Це особливо важливо в той час, коли війна повернулася до Європи після невиправданої та неспровокованої агресії Росії проти України, а також серйозних геополітичних зрушень. Стратегічний компас посилить стратегічну спроможність ЄС і його здатність працювати з партнерами для захисту своїх цінностей та інтересів. Сильніший і більш спроможний ЄС у сфері безпеки й оборони сприятиме глобальній та трансатлантичній безпеці й доповнює НАТО, яке залишається основою колективної оборони для його членів. Це також посилить підтримку глобального порядку, заснованого на правилах, ядром якого є Організація Об'єднаних Націй [71].

Стратегічний компас охоплює всі аспекти політики безпеки та оборони й структурований навколо чотирьох стовпів: дії (actions), інвестиції (investments), партнерство (partnership) і безпека (security). Стосовно сфери стратегічних комунікацій стратегія передбачає, зокрема, такі заходи [72]: посилення цивільних і військових місій та операцій у рамках Спільної політики безпеки й оборони, сприяючи швидкому та гнучкому процесу

прийняття рішень, діючи більш надійно й забезпечуючи більшу фінансову солідарність; повніше використання Європейського фонду миру для підтримки партнерів; розширення можливостей аналізу даних розвідки; розробка інструментів Hybrid Toolbox і Response Teams для виявлення й реагування на широкий спектр гібридних загроз; подальший розвиток кібердипломатичного інструментарію та створення політики кіберзахисту ЄС для кращої готовності до кібератак і реагування на них; розробка інструментарію щодо маніпулювання іноземною інформацією та втручання (Foreign Information Manipulation and Interference Toolbox) [73].

Стратегічні комунікації. Напрям стратегічних комунікацій у Європейському Союзі – один із найновіших. Сьогодні він охоплює діяльність спеціалізованих підрозділів у сферах зовнішніх справ і спільної політики безпеки й оборони, а його актуальну інституційну базу оформлено у 2021 р. із затвердженням нової організаційної структури Європейської служби зовнішніх справ (ЄСЗС), яка й забезпечує цю діяльність [74].

Інституційне забезпечення стратегічних комунікацій реалізовано в апараті ЄСЗС у постаті секретаріату Стратегічних комунікацій і прогнозування, у структурі якого функціонують відділи комунікаційної політики й публічної дипломатії; стратегічних комунікацій, оперативних груп та інформаційного аналізу; політичного планування й стратегічного прогнозування. Також у цій організаційній структурі діє Інститут досліджень безпеки ЄС (EUISS) – Агентство Європейського Союзу, що займається аналізом питань зовнішньої політики, політики безпеки та оборони.

Відділ комунікаційної політики й публічної дипломатії сприяє діяльності Верховного представника ЄС та повідомляє про зовнішні справи ЄС, політику безпеки й оборони, а також зовнішні дії ЄС, ефективно взаємодіючи з цільовою аудиторією. Він співпрацює з представництвами ЄС, місіями та операціями в усьому світі в їхній діяльності, спрямованій на комунікацію з ЄС.

Відділ стратегічних комунікацій та його оперативні групи сприяють ефективній комунікації, що ґрунтується на фактах, протидії дезінформації, і зміцненню загального медіасередовища й громадянського суспільства у відповідних регіонах [75].

На рівні представництв ЄС у державах роботу у сфері стратегічних комунікацій виконують відповідні посадові особи, які співпрацюють зі спеціалістами з питань преси та інформації й забезпечують такі функції [76]:

– контроль розробки інформаційних продуктів, у тому числі для соціальних медіа;

– сприяння розробці, моніторингу та оновленню комунікаційних цілей і методів ЄС у країнах перебування, а також беруть участь у проактивній комунікації;

– контроль інформаційного середовища в країні перебування;

– аналіз тенденцій та розвитку інформаційного середовища й надання рекомендацій щодо покращення розуміння цінностей, політики та проєктів ЄС на основі інформації, що ґрунтується на фактах;

– розробка, упровадження й координація кампаній, місцевих інформаційних заходів і комунікаційних проєктів із конкретних питань та пріоритетів, у тому числі з метою подолання дезінформації, спрямованої на ЄС і його партнерство з країною перебування;

– оповіщення про тенденції та вразливості в інформаційному середовищі, сприяння передбаченню загроз інтересам та репутації ЄС із метою запровадження превентивних заходів;

– сприяння підвищенню обізнаності про негативний вплив дезінформації, допомага в розробці й реалізації спеціальних роз'яснювальних кампаній;

– підтримка зв'язку з місцевими фактчекерами, дослідниками, організаціями громадянського суспільства та журналістами для сприяння аналізу, підвищенню обізнаності, посиленню стійкості до дезінформації й підтримці представництв ЄС у діяльності з моніторингу та підвищення обізнаності;

– співпраця з робочими групами стратегічних комунікацій ЄСЗС.

Сьогодні здійснюється активна робота щодо забезпечення людськими ресурсами всіх ланок організаційної структури стратегічних комунікацій ЄС, що є ознакою початку системної роботи в цьому напрямі в найближчій перспективі.

Стратегічні комунікації розглядаються в ЄС як ключовий фактор у протидії гібридним загрозам [77]. І цей напрям роботи реалізується в рамках спільної політики безпеки й оборони. Гібридні загрози, які ввійшли до політичного порядку денного у зв'язку з російською агресією на сході України, можуть уключати різні стратегії та тактики впливу на процеси прийняття рішень з метою досягнення стратегічних цілей, таких як масові інформаційні кампанії, вербування радикалів або використання довірених осіб для виконання певних дій. Тому вже у квітні 2016 р. у ЄС прийнято Спільне комюніке про протидію гібридним загрозам із метою реалізації скоординованої відповіді на рівні ЄС. Це комюніке визначає концепцію гібридних загроз як «суміш насильницького впливу та підривної діяльності, звичайних і нетрадиційних методів (тобто дипломатичних,

військових, економічних, технологічних), які можуть скоординовано використовувати державні чи недержавні суб'єкти для досягнення конкретних цілей, залишаючись нижче порога офіційно оголошеної війни» [78]. Повідомлення має на меті забезпечити взаємодію між різними інструментами, доступними на європейському рівні, одночасно сприяючи співпраці між усіма відповідними суб'єктами. Ці інструменти включають Європейський порядок денний із безпеки [79], Глобальну стратегію ЄС щодо зовнішньої політики та політики безпеки [80] і Європейський план оборонних заходів [81], Стратегію ЄС із кібербезпеки [82]; Стратегію енергетичної безпеки [83] та Стратегію безпеки на морі [84]. У комюніке викладено перелік заходів, запланованих на рівні держав-членів і європейських інституцій [85]:

– запуск дослідження гібридних ризиків для визначення ключових вразливих місць державами-членами;

– створення відділу гібридних загроз (Hybrid Fusion Cell) у рамках розвідувального та ситуаційного центру ЄС (EU INTCEN), що функціонує в рамках Європейської служби зовнішніх справ, який працюватиме як платформа для обміну інформацією щодо гібридних загроз;

– оновлення й координація стратегічних комунікацій;

– створення Центру передового досвіду для протидії гібридним загрозам, який би тісно співпрацював із наявними центрами передового досвіду ЄС та НАТО;

– створення загальних інструментів для захисту критичної інфраструктури, уключаючи диверсифікацію енергетичних ресурсів, просування стандартів безпеки й підвищення стійкості ядерної інфраструктури, моніторинг загроз, що виникають у транспортному секторі, та сприяння стійкості космічної інфраструктури (супутникового зв'язку);

– пропонування важливих для ЄС проєктів щодо адаптації обороноздатності й розвитку;

– підвищення рівня обізнаності про гібридні загрози в секторі охорони здоров'я та безпеки харчових продуктів;

– цільове фінансування протидії гібридним загрозам;

– формування стійкості до радикалізації й насильницького екстремізму;

– співробітництво з третіми країнами;

–розбудова процедур антикризового управління й інтегрованого політичного реагування на кризи;

– посилення співпраці з НАТО.

Важливо, що в ЄС розбудовують комплексне рішення щодо захисту від гібридних загроз, реалізації стратегічних комунікацій і

протидії кіберзагрозам. Згаданий вище Hybrid Fusion Cell функціонує в координації з інституціями у сфері стратегічних комунікацій, оскільки джерела гібридних загроз можуть систематично поширювати дезінформацію, у тому числі за допомогою цільових кампаній у соціальних мережах, намагаючись таким чином радикалізувати цільову аудиторію, дестабілізувати суспільство й контролювати політичний наратив. Тому ЄС розвиває потенціал і мехінізми реагування на гібридні загрози, використовуючи розумну стратегічну комунікаційну стратегію, вважаючи, що надання швидкої фактичної відповіді та підвищення обізнаності громадськості про гібридні загрози є основними факторами для формування стійкості суспільства [86].

Рамкою щодо протидії гібридним загрозам визначено, що в стратегічних комунікаціях ЄС мають повною мірою використовуватись інструменти соціальних медіа, а також традиційні візуальні, аудіо та веб-ЗМІ. Відповідальною структурою в цьому контексті є ЄСЗС, яка повинна оптимізувати використання лінгвістів, котрі вільно володіють відповідними мовами, що не входять до ЄС, і спеціалістів із соціальних медіа, які можуть контролювати інформацію за межами ЄС та забезпечувати цілеспрямовану комунікацію для реагування на дезінформацію. Крім того, держави-члени повинні розробити скоординовані механізми стратегічної комунікації для підтримки атрибуції й протидії дезінформації з метою виявлення гібридних загроз [87].

Важливо, що питання інформаційної безпеки, які координуються в рамках спільної політики безпеки й оборони, пов'язані з кібербезпекою. Такі сектори, як енергетика, транспорт, фінанси й охорона здоров'я, а також цифрові послуги, повинні повідомляти національні органи влади про серйозні інциденти, у тому числі з гібридними характеристиками. Комюніке про протидію кіберзагрозам заохочує держави-члени повною мірою скористатися перевагами груп реагування на кома'ютерні інциденти (CSIRT та CERT-EU), створених згідно з Директивою NIS. Важливого значення надано зближенню підходів до управління ризиками, підкреслюючи державно-приватне співробітництво й Платформу мережевої й інформаційної безпеки Європейської комісії, яка є ініціативою на європейському рівні для встановлення найкращих практик в управлінні ризиками, відповідно до директиви NIS. Щодо кібербезпеки в Комюніке визначено пріоритети трьох секторів: енергетики, фінансів та транспорту й окреслено конкретні дії [88].

Спроможності ЄС у протидії гібридним загрозам і потенціал стратегічних комунікацій розвиваються у взаємозв'язку з відповідними

зусиллями НАТО й у співпраці з Альянсом, що відображено в Комюніке, зокрема в питаннях співпраці з ініціативами НАТО у сферах стратегічних комунікацій, кібербезпеки, запобігання кризам та реагування на них, а також ситуаційної обізнаності. В інституційному плані здійснюється обмін інформацією про інциденти між Hybrid Fusion Cell Європейського Союзу та підрозділом з аналогічною назвою в НАТО, а також спільні навчання.

Протидія дезінформації. У зв'язку з масованим стратегічним пропагандистським впливом із боку Росії важливим напрямом роботи у сфері політики безпеки й оборони ЄС стала протидія дезінформації.

Відповідальність за боротьбу з дезінформацією передусім несуть країни-члени ЄС. Роль ЄС полягає в підтримці держав-членів зі спільним баченням і діями для посилення координації, комунікації та поширення передового досвіду.

Боротьба з дезінформацією стосується різних сфер політики, за які відповідають різні Генеральні директорати Комісії, а також інші органи (ЄСЗС, Європейська рада та Європейський парламент).

Розробку цього напряму розпочато в березні 2015 р., коли Європейська рада звернулася до Верховного представника ЄС із закордонних справ і політики безпеки з пропозицією розробити план дій щодо стратегічної комунікації у співпраці з державами-членами та інституціями ЄС, щоб подолати поточні дезінформаційні кампанії Росії. Це призвело до створення робочої групи East Stratcom у рамках ЄСЗС, із мандатом на боротьбу з дезінформацією, що надходить із-за меж ЄС, фактично – для протидії російській дезінформації, а також розробки й реалізації позитивних стратегічних комунікацій у країнах Східного сусідства. У 2017 р. за цим зразком створено ще дві цільові групи для регіонів Південної Європи й Західних Балкан.

Наприкінці 2017 р. Єврокомісія після широких консультацій створила експертну групу високого рівня для надання конкретних порад щодо боротьби з дезінформацією. Група представила свій звіт у березні 2018 р., на основі якого вже за місяць розроблено «Комюніке Комісії щодо боротьби з дезінформацією в інтернеті: європейський підхід», зосереджене довкола чотирьох основних принципів і цілей [89]:

– покращення прозорості походження інформації та способів її створення, фінансування, поширення й цільового призначення (посилення робочих групи стратегічних комунікацій і представництв ЄС, алокація додаткових людських та фінансових ресурсів для виявлення, аналізу й викриття дезінформаційної діяльності, перегляд мандатів Оперативних груп);

– сприяння різноманітності інформації для прийняття обґрунтованих рішень за підтримки високоякісної журналістики та медіаграмотності (створення у 2019 р. й підтримка системи швидкого оповіщення, яка тісно співпрацює з іншими відомими мережами (Європарламенту, НАТО та G7), посилення комунікації перед виборами до ЄП, посилення стратегічних комунікацій у сфері сусідства);

– сприяння довірі й достовірності інформації шляхом роботи з ключовими зацікавленими сторонами (організація з державами-членами цілеспрямованих кампаній для підвищення обізнаності про негативні наслідки дезінформації, підтримка роботи незалежних ЗМІ та якісної журналістики);

– розробка інклюзивних рішень через підвищення обізнаності, покращення медіаграмотності та широке залучення зацікавлених сторін (створення груп незалежних фактчекерів і дослідників для виявлення та розкриття кампаній дезінформації, пропагування медіаграмотності).

За цим повідомленням іде низка конкретних заходів для його імплементації, зокрема:

– виборчий пакет [90] (вересень 2018 р.), призначений для захисту виборів у ЄС і країнах-членах від дезінформації, а також від кібератак. Вибори до Європарламенту в травні 2019 р. прискорили реалізацію заходів у ЄС та країнах-членах для захисту від дезінформації. Пакет зосереджений на захисті даних, прозорості політичної реклами й фінансування, кібербезпеці, а також санкціях проти зловживання правилами захисту даних із боку політичних партій. Він також уключає Рекомендацію Комісії щодо забезпечення вільних і чесних виборів [90];

– кодекс практики [91] (вересень 2018 р.), який є добровільним саморегулювальним набором зобов'язань онлайн-платформ та рекламної індустрії з метою покращення прозорості політичної реклами, закриття фейкових облікових записів і демонетизації стимулів для поширення дезінформації. Зобов'язання засновані на висновках групи експертів високого рівня, хоча деякі з цих змін уже впроваджувалися в Європі й Сполучених Штатах;

– план дій ЄС проти дезінформації [92] (грудень 2018 р.). У висновках Європейської ради від 18 жовтня 2018 р. закликалося вжити додаткових заходів для «захисту демократичних систем Союзу та боротьби з дезінформацією, у тому числі в контексті майбутніх виборів до Європейського Союзу». Отриманий у результаті План дій ЄС проти дезінформації включає десять конкретних заходів на основі чотирьох стовпів (згаданих вище), які відображають підхід усього суспільства. План

консолідує зусилля ЄС щодо боротьби з дезінформацією та створення ефективної й усеосяжної структури.

У грудні 2019 р. Рада підтвердила, що План дій ЄС залишається в центрі зусиль ЄС щодо боротьби з дезінформацією, і закликала регулярно його переглядати й оновлювати. Крім того, Європейський парламент неодноразово наголошував на важливості посилення зусиль у боротьбі з дезінформацією [93].

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Політика ЄС у сфері інформаційної безпеки формувалася з початку 2000-х рр. навколо проблематики забезпечення кібербезпеки інформаційних систем і мереж в аспекті функціонування єдиного внутрішнього ринку Співтовариств. Робота в цьому напрямі продовжується, але з другої половини минулого десятиліття вона узгоджується з новими для унії сферами інтересів, у царині спільної політики безпеки й оборони. Такими викликами стали необхідність протидіяти дезінформації та гібридним загрозам і розгортання системи стратегічних комунікацій. Сьогодні роботу в цих напрямах координує Європейська служба зовнішніх справ, яка формує розвинуту систему інституцій для узгодження між рівнями унії та країн-членів.

Нові підходи у сфері інформаційної безпеки загалом спрямовані на посилення автономності ЄС у стратегічних питаннях безпеки. Водночас Союз посилює координацію із зазначених питань зі стратегічними союзниками, передусім НАТО.

Оскільки розбудова спроможностей захисту від загроз гібридного характеру й дезінформації зосереджена в площині спільної політики безпеки й оборони, а концепція стратегічних комунікацій відповідає прийнятій у доктринах НАТО та США, можна констатувати, що Європейський Союз залишається прихильним західній (демократичній) моделі інформаційної (кібер) безпеки, не заходячи з цією проблематикою в «цивільний» сектор. Порівняно з концепцією стратегічних комунікацій НАТО, у розбудові системи стратегічних комунікацій ЄС більше покладається на чинник «м'якої сили», передусім надаючи вагу такому компоненту, як публічна дипломатія на ефективній аналітичній основі. Із розвитком нових концепцій з'явилася можливість ефективної протидії новим викликам і загрозам.

Посилення співпраці з державами-членами ЄС, розробка та вдосконалення наявних стратегій ведення стратегічних комунікацій

спрямовані передусім на укріплення своїх позицій. Протидія пропаганді, хакерським атакам, дезінформаційній кампанії РФ є пріоритетними в інформаційному протистоянні. Саме завтердження нових концепцій стратегічних комунікацій зможуть запобігти небезпеці гібридних загроз, дезінформації,

Так удалося кинути виклик діям Росії та звернутися до держав-членів ЄС, розробити план дій зі стратегічних комунікацій і сформувати команду для протидії новим загрозам. Підтримка політики й цінностей ЄС щодо покращення регіональних процесів ведення стратегічних комунікацій, підвищення обізнаності щодо виявлення та протидії дезінформації, однозначно покращать спроможність ЄС відповідати на виклики й мобілізуватись у боротьбі з дезінформацією.

Важливу роль у наведених цілях відіграє концпет Стретегічний Компас-2022. У цьому документі викладено основні положення щодо покращення та нарощування ефективності стратегічних комунікацій. Це особливо важливо в той час, коли війна повернулася до Європи після невиправданої та неспровокованої агресії Росії проти України, а також серйозних геополітичних зрушень. Цей Стратегічний компас посилить стратегічну спроможність ЄС і його здатність працювати з партнерами для захисту своїх цінностей та інтересів. Через свою агресивну політику та нехтування засадами міжнародного права, зокрема початок воєнних дій проти України, Росія стала загрозою для всієї світової спільноти, у тому числі й для країн-членів ЄС та НАТО.

Підвищення ефективності стратегічних комунікацій у сфері спроможності ЄС у протидії гібридним загрозам, нарощування потенціалу стратегічних комунікацій у співпраці з Альянсом і ЄС уже визначають подальшу пріоритетність. Пріоритетом у майбутньому розвитку стратегічних комунікацій ЄС є протидія новим викликам союзу, зокрема ведення вкрай агресивної політики росії та визнання її агресором із боку країн-членів ЄС.

REFERENCES

1. Barrihna, Andre (2018). Virtual Neighbors: Russia and the EU in Cyberspace. Insight Turkey, Summer, 20, No. 3. URL: https://www.insightturkey.com/commentaries/virtual-neighbors-russia-and-the-eu-in-cyberspace

2. NATO (2009, April). NATO -Official text: Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl. URL: https://www.nato.int/cps/en/natolive/news_52837

3. NATO (2009, September). NATO Strategic Communications Policy.

4. Cornish, P., Lindley-French, J., & Yorke, C. (2011, September). Strategic communications and national strategy. *Chatham House.* URL: https://www.chathamhouse.org/sites/default/files/r0911es%E2%80%93stratcomms.pdf

5. Bird Conrad (2008). Public Diplomacy in a Globalised World. *Strategic Communication and Behaviour Change: Lessons from Domestic Policy*, p. 106–119.

6. Taylor, Philip (2009). Public Diplomacy and Strategic Communications, in Snow N. and Taylor Philip M. (eds), *Routledge Handbook of Public Diplomacy.* London: Routledge, 2009, p. 10.

7. UK Cabinet Office, The National Security Strategy of the United Kingdom: Security in an Interdependent World, Cm 7291 (London: The Stationery Office, March 2008), p. 7.

8. Cornish, P., Hughes, R. and Livingstone, D. (2009). Cyberspace and the National Security of the United Kingdom: Threats and Responses. London: Chatham House, p. 19–20.

9. Gunaratna, R., Jerard, J. and Rubin, L. (2011), Terrorist Rehabilitation and Counter-Radicalisation: New Approaches to Counter-Terrorism. London. Routledge.

10. Cornish, Paul (2009). The United States and counterinsurgency: «political first, political last, political always». *International Affairs*, vol. 85, No. 1, January.

11. Tatham, Steve (2008). Strategic Communications: *A Primer, ARAG Special Series*, vol. 8, *Defence Academy of the United Kingdom*.

12. Christopher, Paul (2011). Strategic Communication: Origins, Concepts and Current Debates. Santa Barbara. *Praeger.*

13. Cabinet Office, (2011). CONTEST: The United Kingdom's Strategy for Countering Terrorism London: The Stationery Office.

14. *US Department of Defense* (2009). Strategic Communication Science and Technology Plan: Current Activities, Capability Gap and Areas for Further Investment.

15. US Joint Forces Command, 'Commander's Handbook for Strategic Communication and Communication Strategy'(2010), vol. 3: Headquarters, Department of the US Army (2009). Field Manual 3–24.2, 'Tactics in Counterinsurgency', p. 288.

16. Headquarters, Department of the US Army (2009). «Tactics in Counterinsurgency». URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm3_24x2.pdf

17. Goldman, E. (2007). Strategic communication: A tool for asymmetric warfare. *Small Wars Journal.* URL: https://smallwarsjournal.com/blog/strategic-communication-a-tool-for-asymmetric-warfare

18. NATO (1999). The Alliance's Strategic Concept URL: https://www.nato.int/cps/en/natohq/official_texts_27433.htm#:~:text=At%20their%20Summit%20meeting%20in,years%20of%20the%20Cold%20War.

19. NATO (2010). *Strategic Concept 2010.* URL: https://www.nato.int/cps/en/natohq/topics_82705.htm

20. Allison, R. (2014, November). Russian 'deniable' intervention in Ukraine: How and why Russia broke the rules. *International Affairs*, 90(6), p. 1255–1297. URL: https://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12170

21. Baezner, M. (2018). Cyber and Information warfare in the Ukrainian conflict. Center for Security Studies (CSS), ETH. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securitie sstudies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf

22. Bradshaw, S., & Howard, P. (2019). The global disinformation order. 2019 global inventory of organised social media manipulation (Working Paper, 2019.2). *Oxford Internet Institute.* URL: https://comprop.oii.ox.ac.uk/w pcontent/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

23. Cottiero, C., Kucharski, K., Olimpieva, E., & Orttung, R. W. (2015). War of words: The impact of Russian state television on the Russian Internet. *Nationalities Papers*. URL:. https://doi.org/p

24. Driscoll, J., & Steinert-Threlkeld, Z. (2020). Social media and Russian territorial irredentism: Some facts and a conjecture. *Post-Soviet Affairs*, p. 101–121. URL: https://www.tandfonline.com/doi/full/10.1080/1060586X.2019.1701879

25. Gibson, K. H. (2019, September). *Defence News Conference Lessons learned from NATO's hybrid battlefield* [Panel].

26. Hoffman, F. G. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM*, vol. 7 (4), *National Defense University.* URL: https://cco.ndu.edu/News/Article/1680696/examining-complex-formsof-conflict-gray-zone-and-hybrid-challenges/

27. Laity, M. (2018). NATO and Strategic Communications: 'The Story So Far'. *The Three Swords Magazine*, p. 65–73. URL: http://www.jwc.nato.int/images/stories/threeswords/THREESWORDSMARCH2018_Websitereleased.pdf

28. Marsden, C., & Meyer, T. (2019). Regulating disinformation with artificial intelligence. *European Parliamentary Research Service.* URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf

29. Martens, B., Aguiar, L., Gómez-Herrera, E., & Mueller-Langer, F. (2018). The Digital Transformation of News Media and the Rise of Disinformation and Fake News (JRC Digital Economy Working Paper No. 2018–02). *European Commission, Joint Research Centre.* URL: https://www.ssrn.com/abstract=3164170

30. Nemr, C., & Gangware, W. (2019). Weapons of mass distraction: Foreign State-sponsored disinformation in the digital age. *Park Advisors.* URL: https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-MassDistraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf

31. Nimmo, B., Barojan, D., & Aleksejeva, N. (2017). Russian Narratives on NATO's Deployment. *DFRLab.* URL: https://medium.com/dfrlab/russian-narratives-on-natos-deployment-616e19c3d194

32. Norberg, J. (2018). Training for War – Russia's Strategic-level Military Exercises 2009–2017 (FOI-R--4627--SE; p. 110). *Swedish Defence Research Agency–Ministry of Defence.* URL: https://www.foi.se/rest-api/report/FOI-R-- 4627—SE

33. Peter, M., Alexander, S., Cambridge, A., Renee, S., Kang, R., Kiefer, S., Takayama, K., Laci, F., Michael, G., & Katie, M. (2019). Combating targeted disinformation campaigns. A whole-of-society issue. *2019 Public-private analytic exchange program.* URL: https://www.dhs.gov/sites/default/files/publications/ia/ia_combatti ngtargeted-disinformation-campaigns.pdf

34. Rusnáková, S. (2017). Russian New Art of Hybrid Warfare in Ukraine. *Slovak Journal of Political Sciences*, 17 (vol. 3), p. 343–380.

35. Sari, A. (2019). Legal resilience in an era of grey zone conflicts and hybrid threats (Working Paper No. 2019/1). *Exeter Centre for International Law.* URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315682

36. Snegovaya, M. (2015). Putin's information warfare in Ukraine. Soviet origins of Russia's hybrid warfare. *Institute for the Study of War.* URL: http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

37. Vendil, C., & Oxenstierna, S. (2017). Russian Think Tanks and Soft Power (FOI-R-4451-SE). *FOI–Swedish Defence ResearchAgency.* URL: https://www.foi.se/rest-api/report/FOI-R--4451--SE

38. Wilson, A. (2014). Ukraine Crisis: What it means for the West. *Yale University Press.*

39. US Senate (2019). Report of the selected committee on intelligence on Russian active measures campaigns and interference in the 2016 U.S. election. vol.1: *Russian efforts against election infrastructure with additional views*. URL: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

40. UK Ministry of Defence (2019). Defence Strategic Communication: An approach to formulating and executing strategy (Joint Doctrine Note No. 2/19). Development, Concepts and Doctrine Centre. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/8043 19/20190523-dcdc_doctrine_uk_Defence_Strategic_Communication_jdn_2_19.pdf

41. High Level Group on fake news and online disinformation- European Commission (2018). A multidimensional approach to disinformation – Report of the independent High Level Group on fake news and online disinformation DOI:10.2759/739290). URL: https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b4cea-11e8-be1d-01aa75ed71a1

42. Hybrid CoE (2019). Countering disinformation: News media and legal resilience [COI Records]. European Centre of Excellence and the Media Pool, part of the Finnish Emergency Supply Organization in Helsinki. URL: https://www.hybridcoe.fi/wp-content/uploads/2019/11/News-Media-and-Legal-Resilience_2019_rgb.pdf

43. Mueller, R. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. *US Department of Justice.* URL: https://www.justice.gov/storage/report.pdf

44. NATO StratCom CoE (2019). Hybrid Threats: A Strategic Communications Perspective. *NATO.* URL: https://www.stratcomcoe.org/download/file/fid/80212

45. NATO StratCom CoE (2020). About Strategic Communications | StratCom. URL: https://www.stratcomcoe.org/about-strategic-communications

46. Alandete, D. (2017, November 10). European Union fights the Kremlin's propaganda machine. *El País.* URL: https://english.elpais.com/elpais/2017/11/09/inenglish/1510218067_521677.html

47. Coyer, P. (2016). The Patriarch, The Pope, Ukraine And The Disintegration Of 'The Russian World'. *Forbes.* URL: https://www.forbes.com/sites/paulcoyer/2016/03/20/the-patriarch-the-pope-ukraine-and-thedisintegration-of-the-russian-world/#10471ebd2523

48. Global Spain (2019). The truth about Catalonia's bid for independence. URL: https://www.thisistherealspain.com/wp-content/uploads/2019/11/THE-TRUTH-ABOUT-THE-CATALANINDEPENDENCE-BID-28-nov-2019.pdf

49. Segura, C. (2017, September). Assange alienta que la rebelión en Cataluña se extienda a nivel global. *El País.* URL: https://elpais.com/ccaa/2017/09/26/catalunya/1506456387_836185.html

50. Biswas, A., & Tortajada, C. (2018, February 23). China's soft power is on the rise. *China Daily.* URL: http://www.chinadaily.com.cn/a/201802/23/WS5a8f59a-9a3106e7dcc13d7b8.html

51. Chatzky, A., & McBride J. (2020). China's Massive Belt and Road Initiative. *Council on Foreign Relations.* URL: https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

52. European Commission and the High Representative (2019). EU-China – A strategic outlook. URL: https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategicoutlook.pdf

53. European Commission and the High Representative (2020). Tackling Covid-19 disinformation – Getting the facts right. URL: https://ec.europa.eu/info/sites/info/files/communication-tackling-Covid-19-disinformationgetting-facts-right_en.pdf

54. Gil, T. (2020, March 18). Coronavirus: Cómo el virus se volvió parte de la 'guerra' política entre EE.UU. y China. *BBC News Mundo.* URL: https://www.bbc.com/mundo/noticias-internacional-51938799

55. Karnitschnig, M. (2020, March 18). China is winning the coronavirus propaganda war. *POLITICO.* URL: https://www.politico.eu/article/coronavirus-china-winning-propaganda-war/

56. Molander Roger C., Riddile Andrew, Wilson Peter A. (1996) Strategic Information Warfare. A New Face of War. *RAND.* MR-661-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR661.html

57. Nato Standard ajp-3.10.1 Allied Joint Doctrine for Psychological Operations. Edition B version 1. With uk national elements. September 2014. URL: url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

58. Office of the Secretary of Defense. National Security Strategy. URL: https://history.defense.gov/Historical-Sources/National-Security-Strategy/

59. NATO Deterrence and defence. URL: https://www.nato.int/cps/en/natohq/topics_133127.htm

59. The Interim National Security Strategic Guidance. *Congressional Research Service*, March 29, 2021. URL: https://sgp.fas.org/crs/natsec/IF11798.pdf

60. ALLIED JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATIONS—AJP-3.10.1 EDITION B. URL: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8458/EN?tab=ratifications

61. NATO 2030: MAKING A STRONG ALLIANCE EVEN STRONGER. URL: https://www.nato.int/nato2030/

62. G7 (2018). Charlevoix Commitment on Defending Democracy from Foreign Threats. URL: https://www.mofa.go.jp/files/000373846.pdf

63. Nato Standard ajp-3.10.1 Allied Joint Doctrine for Psychological Operations. Edition B version 1. With uk national elements. September 2014. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

64. Shared vision, common action. A stronger Europe: a global strategy for the European Union's foreign and security policy. URL: https://op.europa.eu/en/publication-detail/-/publication/3eaae2cf-9ac5-11e6-868c-01aa75ed71a1

65. European Union Institute for Security Studies (2016). EU strategic communications with a view to counteracting propaganda. European Parliament. URL: http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf

66. Strategic communications as a key factor in countering hybrid threats (2021). By VillarGarcía JuanPablo, Carlota Tarín Quirós, Blázquez Julio Soria, Galán Carlos Pascual, Galán Carlos Cordero. STOA. *European Union.* URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323

67. Where will the EU's Strategic Compass point? *European Parliamentary Research Service* (2021). URL: https://epthinktank.eu/2021/10/07/where-will-the-eus-strategic-compass-point/

68. Borrell Josep (2021). A Strategic Compass for Europe. URL: https://www.project-syndicate.org/commentary/eu-strategic-compass-by-josep-borrell-2021-11?barrier=accesspaylog

69. Questions and answers: a background for the Strategic Compass. *EEAS* (2021). URL: https://eeas.europa.eu/headquarters/headquarters-homepage/97895/questions-and-answers-background-strategic-compass_en

70. A Strategic Compass for a stronger EU security and defence in the next decade. *Council of the EU. Press release* (2022). URL: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

71. A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

72. EU Rapid Deployment Capacity. *EEAS factsheet.* URL: https://www.eeas.europa.eu/eeas/eu-rapid-deployment-capacity_en

73. A Strategic Compass for the EU. *EEAS factsheet.* URL: https://www.eeas.europa.eu/eeas/strategic-compass-eu-0_en

74. Organisation chart of the EEAS. *EEAS* (2021). URL: https://eeas.europa.eu/headquarters/headquarters-homepage/3602/organisation-chart-eeas_en

75. Strategic communication. *EEAS.* URL: https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en

76. Strategic Communication Press and Information Officer. *EEAC.* URL: https://eeas.europa.eu/headquarters/headquarters-homepage/83986/strategic-communication-press-and-information-officer_en

77. Strategic communications as a key factor in countering hybrid threats. By VillarGarcía JuanPablo, Tarín Quirós Carlota, Soria Julio Blázquez, Pascual Carlos Galán, Cordero Carlos Galán. *STOA* (2021). URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323

78. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. Brussels (2016). 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

79. European Agenda on Security – Legislative documents. *European Commission.* URL: https://ec.europa.eu/home-affairs/what-we-do/policies/internal-security/european-agenda-security-legislative-documents_en

80. EU Global Strategy. *EEAS.* URL: https://eeas.europa.eu/topics/eu-global-strategy_en

81. European Defence Action Plan. *Roadmap.* URL: https://ec.europa.eu/smart-regulation/roadmaps/docs/2016_grow_006_cwp_european_defence_action_plan_en.pdf

82. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013). 1 final. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

83. Communication from the Commission to the European Parliament and the Council. European Energy Security Strategy /* COM/2014/0330 final */. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52014DC0330

84. European Union Maritime Security Strategy as adopted by the Council (General Affairs) (June 2014). URL: https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf

85. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. Brussels, 6.4.2016 JOIN (2016) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

86. Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. Tackling online disinformation: a European Approach. COM/2018/236 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

87. Questions & Answers: Reinforcing democracy and integrity of elections. *European Commission.* URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6212

88. European Democracy: Commission sets out new laws on political advertising, electoral rights and party funding. *European Commission.* URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6118

89. Code of Practice on Disinformation. *European Commission.* URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

90. Joint Communication to the European Parliament, the European Council, the Council, the European Cconomic and Social Committee and the Committee of the Regions. Action Plan against Disinformation. Brussels, 5.12.2018 JOIN (2018) 36 final. URL: https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

91. Audit preview Information on an upcoming audit. EU action plan against disinformation. *European Court of Auditors.* (2020). URL: https://www.eca.europa.eu/lists/ecadocuments/ap20_04/ap_disinformation_en.pdf

92. Kushnir, V. (2020). Proposals for improving the legal mechanism on strategic communications in the armed forces of Ukraine, *Derzhavne upravlinnya: udoskonalennya ta rozvytok*. Vol. 10, URL: http://www.dy.nayka.com.ua/?op=1&z=1796

Матеріал надійшов до редакції 10.05.2022 р.