DOI 10.31558/2519-2949.2025.3.13
УДК 327:355.45:654.197(477)

ORCID ID: https://orcid.org/0000-0002-8827-3569
Сащук Г. М., Київський національний університет імені Тараса Шевченка

ЕВОЛЮЦІЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ ЯК ІНСТРУМЕНТУ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

Досліджується становлення й еволюцію стратегічних комунікацій (StratCom) сектору безпеки та оборони України з 2014 р. до 2025 р. як інструменту протидії інформаційним загрозам. На основі інституційно-правового, порівняльного та комунікативно-стратегічного аналізу простежено перехід від реактивних інформаційних практик до системної моделі урядових комунікацій з акцентом на довіру, прозорість, координацію та багатоканальність. Виокремлено три хвилі розвитку: 1). 2014–2016 — імпульс від гібридної агресії РФ і перші інституційні рішення; 2). 2017–2021 — закріплення принципів StratCom у доктринальних і секторальних стратегіях, розбудова спроможностей; 3). 2022–2025 — воєнна трансформація: синхронізація міжвідомчих повідомлень, оперативні спростування дезінформації, міжнародна стратегічна аудиторія, публічна дипломатія, залучення цифрових спільнот і платформ. Показано, що ефективність українських StratCom зростала пропорційно до інституційної зрілості (наявність центрів протидії дезінформації та стратегічних комунікацій) і до спроможності уряду працювати з OSINT, фактчекінгом та візуальними наративами. Сформульовано практичні рекомендації щодо подальшої інституційної консолідації, удосконалення правової рамки, етики ризик-комунікації та міжнародної кооперації. Еволюція стратегічних комунікацій України пройшла три етапи — від реактивної відповіді до інституційно оформленої, доказової та багатоканальної системи, здатної працювати в умовах затяжної війни. Інституційні інновації (ЦПД, ЦСКІБ), доктринальні рамки (Доктрина інформаційної безпеки, Стратегія кібербезпеки) і міжнародні партнерства (NATO StratCom COE) створили цілісний «контур комунікаційної безпеки». Подальший поступ залежить від кодифікації термінів, SOP кризової комунікації, кадрового зміцнення та поглиблення платформних альянсів. Український кейс доводить: у гібридній війні стратегічні комунікації — не «додаток» до політики, а серцевина стійкості держави.

***Ключові слова**: стратегічні комунікації, інформаційна безпека, протидія дезінформації, публічна дипломатія, сектор безпеки і оборони, Україна, євроінтеграція, гібридна війна.*

Постановка питання. Повномасштабна агресія РФ радикально підсилила вимоги до урядових комунікацій: від пояснення політики — до проєкції стійкості, мобілізації суспільства, консолідації союзників і швидкого нейтралізування ворожих інформаційних операцій. Україна пройшла шлях від фрагментарних прескомунікацій до інтегрованої моделі стратегічних комунікацій, що поєднує державні інституції, сектор безпеки й оборони, громадянське суспільство та міжнародних партнерів. На нормативному рівні важливими орієнтирами стали Доктрина інформаційної безпеки (2017), Стратегія кібербезпеки (2021) та створення спеціалізованих центрів (Центр протидії дезінформації при РНБО [1]; Центр стратегічних комунікацій та інформаційної безпеки [2] при Міністерстві культури та інформаційної політики України (МКІП) [3].

Мета статті - проаналізувати еволюцію українських StratCom у секторі безпеки та оборони як інструменту протидії інформаційним загрозам, окреслити уроки та запропонувати практичні рекомендації.

Методи дослідження: нормативно-правовий аналіз дозволив з’ясувати повноваження інституцій та координації їх дій; контент-аналіз публічних повідомлень сприяв ілюстративному спростувань шейків; порівняльний аналіз із практиками НАТО/ЄС, а також кейс-стаді воєнного періоду 2022–2025 рр. сприяли ефективності застосування засобів протидії інформаційним загрозам (оперативні брифінги, взаємодія з платформами, публічна дипломатія). Для валідації тверджень використано відкриті звіти NATO StratCom COE і матеріали РНБО/ЦПД та ЦСКІБ [4-6].

Виклад основного матеріалу. Першою всеосяжною рамкою еволюції стратегічних комунікацій

сектору безпеки та оборони України як інструменту протидії інформаційним загрозам стала нормативно-правова еволюція стратегічних комунікацій в Україні, зокрема затвердження Доктрини інформаційної безпеки (Указ Президента №47/2017), що визначила національні інтереси в інформаційній сфері, основні загрози й пріоритети державної політики, включно з розвитком стратегічних комунікацій як відповіді на гібридну агресію [7].

У 2021 р. ухвалено Стратегію кібербезпеки України (Указ №447/2021), яка закріпила довгострокові цілі, міжвідомчу координацію та пріоритети взаємодії з союзниками, що опосередковано посилило спроможності StratCom для кризових комунікацій і кіберінцидентів [8].

Ключовим елементом еволюції стала інституціоналізація: у 2021 р. створено Центр протидії дезінформації як робочий орган РНБО (Указ №106/2021) [9] та Центр стратегічних комунікацій та інформаційної безпеки [2] у системі Міністерстві культури та інформаційної політики України — обидва з мандатом на системну протидію дезінформації, побудову стійких урядових комунікацій і взаємодію з суспільством та міжнародними партнерами.

Водночас у низці наукових оглядів і юридичних аналізів підкреслюється, що понятійно-категоріальний апарат StratCom в Україні поступово зближався з документами НАТО, але потребує подальшої систематизації (термінологічна узгодженість, баланс між свободою вираження та інформаційною безпекою, модернізація законодавчих ініціатив у контексті євроінтеграції) [10].

Інституційна архітектура та ролі акторів. Центр протидії дезінформації при РНБО координує виявлення і спростування дезінформації, оперативно інформує громадськість, розбудовує співпрацю з цифровими платформами (Meta, Google, TikTok), медіа та фактчекерами (VoxCheck тощо), а також працює з лідерами думок та інфлюенсерами [11].

Центр стратегічних комунікацій та інформаційної безпеки при МКІП фокусується на побудові стійких комунікацій держави, протидії зовнішнім інформаційним атакам, стратегічному сторітелінгу для внутрішньої й міжнародної аудиторій; організовує події на кшталт «Kyiv Stratcom Forum», розвиває наративи й практики комунікацій стійкості [2].

Міжнародний компонент посилюють партнерства з НАТО та країнами ЄС (у т. ч. через NATO StratCom COE), що забезпечує обмін методологіями, навчання та дослідницьку підтримку[4-6].

Три хвилі еволюції українських StratCom (2014–2025)

1) 2014–2016: реактивна відповідь і усвідомлення загроз. Російська операція впливу проти України виявила вразливості державних комунікацій і відсутність централізованої координації. У цей період формувався попит на єдині наративи, критичні навички роботи з фактами та нові канали донесення позиції держави до міжнародної аудиторії. Дослідження NATO StratCom COE 2016 р. зафіксували методи російської інформаційної кампанії проти української держави та сил оборони, підкресливши потребу в інституційній відповіді [4].

2) 2017–2021: доктриналізація та нарощення спроможностей. Доктрина інформаційної безпеки (2017) надала спільну рамку ризиків і цілей; далі — секторальні стратегії, міжвідомчі механізми та навчання за підтримки партнерів. До 2021 р. інституційний ландшафт поповнили Центр протидії дезінформації (ЦПД) та Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ) як центри компетенцій і координатори наративів, а також оновлена Стратегія кібербезпеки, що закріпила кризові протоколи комунікації у випадку кібератак на критичну інфраструктуру [1; 11].

3) 2022–2025: воєнна трансформація і глобальна аудиторія. Повномасштабне вторгнення стимулювало оперативну, багатоканальну й доказову комунікацію: щоденні брифінги та спростування фейків, тісна синхронізація повідомлень сил безпеки, дипломатії та уряду, широке використання OSINT і візуальних доказів, а також адресна робота з міжнародними медіа та лідерами думок. ЦПД системно спростовує інформаційні вкиди (напр., «скасування безвізу з Польщею», «умовні домовленості»), знижуючи резонанс маніпуляцій. Паралельно українські інституції вибудовують співпрацю з платформами для зменшення видимості ворожих операцій і посилення фактчекінгу [12].

Аналітика NATO StratCom COE (2024) та пізніші звіти фіксують, що ефективність українських наративів підсилювалась узгодженістю з реальними політичними діями, військовими досягненнями та гуманітарною допомогою, а також спроможністю швидко оновлювати меседжі в умовах динамічних операцій РФ [6-7].

Інструментарій українських StratCom у секторі безпеки та оборони:

- оперативні спростування та ризик-комунікація. ЦПД та інші органи використовують короткі, верифіковані повідомлення з посиланнями на першоджерела; при цьому розробляються

попереджувальні меседжі щодо очікуваних вкидів і «тестових» інформаційних операцій противника. Практика оперативних спростувань знижує амплітуду паніки й запобігає вторинному поширенню фейків у соціальних мережах [12];

- платформні альянси та модерація. Офіційно декларована взаємодія державних органів із платформами (Meta, Google, TikTok) у питаннях видалення координованої недобросовісної поведінки, підвищення видимості верифікованих джерел і запуску спільних проєктів із фактчекерами та інфлюенсерами — один із ключових каталізаторів масштабування протидії дезінформації [13];

- публічна дипломатія та міжнародні наративи. Україна перейшла від реактивного до проактивного сторітелінгу: системна участь у міжнародних форумах і власні платформи (Kyiv Stratcom Forum) допомагають формувати порядок денний і підсилювати підтримку союзників (Міністерство Закордонних Справ України);

- аналітика та дослідження. NATO StratCom COE, академічні та урядові аналітичні центри забезпечують доказову базу для коригування стратегії — від аналізу проксі-акторів до розгортання кремлівської медіаекосистеми, що дозволяє таргетувати контрнаративи та комунікаційні «щеплення» проти дезінформації [6; 13].

Відзначаючи весь позитив інструментарію українських StratCom у секторі безпеки та оборони слід зазначити, що залишаються дискусійні вузли та виклики. Перш за все, це:

- термінологічна узгодженість і правова рамка. Наукові огляди відзначають потребу уніфікації понять («урядові», «державні», «національні» стратегічні комунікації), а також збалансування між інформаційною безпекою і свободою вираження в законодавчих ініціативах (у т.ч. у світлі висновків Ради Європи щодо медіареформ 2024–2025 рр.) [14-15] ;

- стійкість до ескалаційних інформаційно-психологічних операцій, тобто комплексу спланованих заходів, спрямованих на вплив на психологічний стан та поведінку певної цільової аудиторії шляхом маніпулювання інформацією. РФ адаптує проксі-мережі та наративи; для протидії потрібні раннє виявлення, прогнозування «вікон вкидів» і симуляції інформаційних криз [5-6];

- етика ризик-комунікації. Баланс між оперативністю й точністю, неприпустимість «надмірних обіцянок»; потреба у стандартизованих SOP для кризових повідомлень у багатомовних середовищах. (Аналітичні висновки на основі оглядів практик StratCom COE) [13];

- людський капітал і навчання. Потреба в довгострокових програмах підготовки комунікаторів сектору безпеки (OSINT, візуальна верифікація, робота з платформами, психологічна стійкість команд) з урахуванням стандартів НАТО та досвіду балтійських країн [6].

Які Кейс-ілюстрації у 2022–2025 спрацювали найкраще:

- швидкі спростування й «розмінування» фейків (приклади ЦПД про «скасування безвізу з Польщею» та «міфічні домовленості»): короткі повідомлення з первинними джерелами в межах годин після появи вкидів. Це знижує «вікно віральності» та перекриває канали поширення [16];

- коаліційні меседжі: узгоджені заяви між силовим блоком, МЗС та урядом щодо ключових тем (зброя, санкції, безпекові гарантії) — зменшують шум і підвищують довіру міжнародних медіа. Дослідження NATO StratCom COE підкреслюють, що узгодженість меседжів і дій підсилює комунікаційний ефект [17];

- партнерства з платформами та фактчекерами (VoxCheck, Bihus.Info, освітні ініціативи): масштабують охоплення контрнаративів і підвищують «щепленість» аудиторій [18];

- публічна дипломатія через спецподії і тематичні форуми (Kyiv Stratcom Forum): забезпечує перенесення українських наративів у міжнародні дискусії безпекової політики (Міністерство закордонних справ).

Загалом, український досвід підтверджує тезу, що ефективні стратегічні комунікації невіддільні від узгоджених політичних дій та національної стійкості. Аналітики наголошують: комунікація працює тоді, коли наративи «підкріплені реальністю» — оборонною спроможністю, дипломатичними рішеннями, волонтерськими мережами та результатами на полі бою. Це узгоджується із сучасними студіями з медіатизації війни і практиками StratCom COE щодо протидії кремлівській медіа екосистемі [19].

Які можливі практичні рекомендації посилення ефективності стратегічних комунікацій. Насамперед це:

1) Кодифікація понятійної бази StratCom. Прийняти єдині визначення й розмежування повноважень у законодавстві (урядові/державні/секторальні StratCom), синхронізувати з acquis ЄС та доктринальними положеннями НАТО;

2) Створити єдиний міжвідомчий SOP для кризової комунікації. Встановити часові нормативи, джерела верифікації, процедури багатомовних випусків і механізми «комунікаційної тривоги» на рівні уряду та сектору безпеки. (Узагальнення практик, рекомендованих міжнародними партнерами);

3) Стійка співпраця з платформами. Інституціоналізувати обміни сигналами про ворожі впливові операції, розширити співпрацю у сфері прозорості політичної реклами та антиботових практик;

4) Розвиток людського капіталу. Регулярні тренінги з OSINT, верифікації, кризової етики, візуальної комунікації; створення «кадрового резерву комунікаторів» для ротацій у відомствах безпекового сектору;

5) Аналітика і раннє попередження. Постійні дослідження проксі-мереж, «наративних хвиль» та «вікон уразливості»; використання симуляцій для тестування реагування на інформаційні кризи.

Висновки. Еволюція стратегічних комунікацій України пройшла три етапи — від реактивної відповіді до інституційно оформленої, доказової та багатоканальної системи, здатної працювати в умовах затяжної війни. Інституційні інновації (ЦПД, ЦСКІБ), доктринальні рамки (Доктрина інформаційної безпеки, Стратегія кібербезпеки) і міжнародні партнерства (NATO StratCom COE) створили цілісний «контур комунікаційної безпеки». Подальший поступ залежить від кодифікації термінів, SOP кризової комунікації, кадрового зміцнення та поглиблення платформних альянсів. Український кейс доводить: у гібридній війні стратегічні комунікації — не «додаток» до політики, а серцевина стійкості держави.

Бібліографічний список :

1. Центр протидії дезінформації (Center for Countering Disinformation, CCDI). (б.д.). Про Центр протидії дезінформації. https://cpd.gov.ua/en/docs/about-center-for-countering-disinformartion/

2. Центр стратегічних комунікацій та інформаційної безпеки (Spravdi). (б.д.). Про Центр. https://spravdi.gov.ua/en/about-us/

3. Міністерство культури та інформаційної політики України. (б.д.). Центр стратегічних комунікацій та інформаційної безпеки. https://mcsc.gov.ua/en/projects/a-href-https-spravdi-gov-ua-tsentr-stratehichnykh-komunikatsiy-ta-informatsiynoi-bezpeky-a/

4. NATO. (2018). *NATO's support to Ukraine* (Factsheet, 6 Nov 2018). https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181106_1811-factsheet-nato-ukraine-sup.pdf

5. NATO Strategic Communications Centre of Excellence (StratCom COE). (2024). *War on all fronts: How the Kremlin's media ecosystem broadcasts the war in Ukraine*. https://stratcomcoe.org/publications/war-on-all-fronts-how-the-kremlins-media-ecosystem-broadcasts-the-war-in-ukraine/301

6. NATO Strategic Communications Centre of Excellence (StratCom COE). (2024). *The use of Russian proxy actors in the media environment in Ukraine (2017–2023)*. https://stratcomcoe.org/publications/the-use-of-russian-proxy-actors-in-the-media-environment-in-ukraine-a-comparison-between-occupied-and-non-occupied-areas-20172023/312

7. Указ Президента України № 47/2017 «Про доктрину інформаційної безпеки України». https://www.preident.gov.ua

8. Указ Президента України № 44/2021 «Про Стратегію кібербезпеки України». https://www.preident.gov.ua

9. Указ Президента України № 106/2021 «Про створення Центру протидії дезінформації». https://www.preident.gov.ua

10. Pylypchuk, V. (2020). Theoretical and legal basis for the security and defense strategic communications system of Ukraine. *Public Administration and Law, 12*. (English PDF). https://cris.mruni.eu/cris/bitstreams/b2723f5f-638d-444e-bfbe-5db20525d799/download

11. Рада національної безпеки і оборони України (RNBO). (2024, груд.). Подолати брехню ворога: Центр протидії дезінформації… https://www.rnbo.gov.ua/en/Diialnist/7169.html

12. Interfax-Ukraine. (2025, серп.). Head of CCDI: Media 'agreements' on Ukraine are fiction; CCDI denies info about Poland cancelling visa-free travel. https://en.interfax.com.ua/news/general/1094409.html ; https://en.interfax.com.ua/news/general/1093261.html

13. StratCom COE. (2016). *Russian information campaign against Ukrainian state and defence forces; Framing of the Ukraine–Russia conflict in online and social media*. https://stratcomcoe.org/publications

14. Nilsson, P. E. (2024). Be brave like Ukraine: Strategic communication and the mediatization of war. *Medijska istraživanja, 30*(1), 5–26. https://hrcak.srce.hr/file/456562

15. Gnomon Wise (Аналітика). (2023). Стратегічні комунікації України проти російської агресії. https://gnomonwise.org/en/publications/analytics/147

16.Council of Europe. (2017). Doctrine of Information Security of Ukraine (English summary). https://rm.coe.int/doctrine-of-information-security-of-ukraine-developments-in-member-sta/168073e052

17. Antipova, O. (2023). Strategic communications as a component of state information security. *Law Journal of*

the National Academy of Sciences of Ukraine, 13(1). https://lawjournal.com.ua/en/journals/tom-13-1-2023/strategichni-komunikatsiyi-yak-skladova-informatsiynoyi-bezpeki-derzhavi

18. FOI (Swedish Defence Research Agency). (2025). *All eyes on Ukraine*. https://www.foi.se/rest-api/report/FOI-R--5758--SE

19. Ukrainian Cybersecurity Cluster (unofficial translation). (2021). *Decree of the President of Ukraine №447/2021 (Cyber Security Strategy)*. https://cybersecuritycluster.org.ua/wp-content/uploads/2021/12/cybersecurity-strategy-decree-august-2021_en_unofficial-translation.pdf

References:

1. Center for Countering Disinformation (CCDI). (n.d.). About Center for Countering Disinformation. https://cpd.gov.ua/en/docs/about-center-for-countering-disinformartion/

2. Spravdi — Centre for Strategic Communication and Information Security. (n.d.). About the Centre. https://spravdi.gov.ua/en/about-us/

3. Ministry of Culture and Information Policy of Ukraine. (n.d.). Center for Strategic Communications and Information Security. https://mcsc.gov.ua/en/projects/a-href-https-spravdi-gov-ua-tsentr-stratehichnykh-komunikatsiy-ta-informatsiynoi-bezpeky-a/

4. NATO. (2018). NATO's support to Ukraine (Factsheet, 6 Nov 2018). https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181106_1811-factsheet-nato-ukraine-sup.pdf

5. NATO Strategic Communications Centre of Excellence (StratCom COE). (2024). War on All Fronts: How the Kremlin's Media Ecosystem Broadcasts the War in Ukraine. https://stratcomcoe.org/publications/war-on-all-fronts-how-the-kremlins-media-ecosystem-broadcasts-the-war-in-ukraine/301 stratcomcoe.org

6. NATO Strategic Communications Centre of Excellence (StratCom COE). (2024). The use of Russian proxy actors in the media environment in Ukraine (2017–2023). https://stratcomcoe.org/publications/the-use-of-russian-proxy-actors-in-the-media-environment-in-ukraine-a-comparison-between-occupied-and-non-occupied-areas-20172023/312 stratcomcoe.org

7. President of Ukraine. (2017). Decree No. 47/2017 "On the Doctrine of Information Security of Ukraine." https://www.president.gov.ua

8. President of Ukraine. (2021). Decree No. 44/2021 "On the Cybersecurity Strategy of Ukraine." https://www.president.gov.ua

9. President of Ukraine. (2021). Decree No. 106/2021 "On the Establishment of the Center for Countering Disinformation." https://www.president.gov.ua

10. Pylypchuk, V. (2020). Theoretical and legal basis for the security and defense strategic communications system of Ukraine. *Public Administration and Law*, 12. (English PDF). https://cris.mruni.eu/cris/bitstreams/b2723f5f-638d-444e-bfbe-5db20525d799/download

11. National Security and Defense Council of Ukraine (RNBO). (2024, Dec.). To overcome the enemy's lies: Center for Countering Disinformation has… https://www.rnbo.gov.ua/en/Diialnist/7169.html

12. Interfax-Ukraine. (2025, Aug.). Head of CCDI: Media 'agreements' on Ukraine are fiction; CCDI denies info about Poland cancelling visa-free travel. https://en.interfax.com.ua/news/general/1094409.html ; https://en.interfax.com.ua/news/general/1093261.html

13. StratCom COE. (2016). Russian Information Campaign Against Ukrainian State and Defence Forces; Framing of the Ukraine–Russia conflict in online and social media. https://stratcomcoe.org/publications

14. Nilsson, P. E. (2024). Be Brave Like Ukraine: Strategic communication and the mediatization of war. Medijska istraživanja, 30(1), 5–26. https://hrcak.srce.hr/file/456562

15. Gnomon Wise (Analytical). (2023). Ukraine's Strategic Communication Against Russian Aggression. https://gnomonwise.org/en/publications/analytics/147

16. Council of Europe. (2017). Doctrine of Information Security of Ukraine (English summary). https://rm.coe.int/doctrine-of-information-security-of-ukraine-developments-in-member-sta/168073e052

17. Antipova, O. (2023). Strategic communications as a component of state information security. *Law Journal of the National Academy of Sciences of Ukraine*, 13(1). https://lawjournal.com.ua/en/journals/tom-13-1-2023/strategichni-komunikatsiyi-yak-skladova-informatsiynoyi-bezpeki-derzhavi

18. FOI (Swedish Defence Research Agency). (2025). All Eyes on Ukraine. https://www.foi.se/rest-api/report/FOI-R--5758--SE

19. Ukrainian Cybersecurity Cluster (unofficial translation). (2021). Decree of the President of Ukraine №447/2021 (Cyber Security Strategy). https://cybersecuritycluster.org.ua/wp-content/uploads/2021/12/cybersecurity-strategy-decree-august-2021_en_unofficial-translation.pdf

Sashchuk H. Evolution of Strategic Communications in Ukraine's Security and Defense Sector as a Tool for Countering Information Threats

The study examines the development and evolution of strategic communications (StratCom) in Ukraine's security and defense sector from 2014 to 2025 as a tool for countering information threats. Based on

institutional-legal, comparative, and communicative-strategic analysis, it traces the transition from reactive information practices to a systemic model of government communications focused on trust, transparency, coordination, and multichannel engagement. Three waves of development are identified: 1) 2014–2016 — the impetus from the Russian Federation's hybrid aggression and the first institutional decisions; 2) 2017–2021 — consolidation of StratCom principles in doctrinal and sectoral strategies, capacity building; 3) 2022–2025 — wartime transformation: synchronization of interagency messaging, rapid debunking of disinformation, engagement with an international strategic audience, public diplomacy, and the involvement of digital communities and platforms. The study demonstrates that the effectiveness of Ukraine's StratCom has increased proportionally to institutional maturity (establishment of disinformation counteraction and strategic communications centers) and the government's ability to work with OSINT, fact-checking, and visual narratives. Practical recommendations are formulated for further institutional consolidation, improvement of the legal framework, risk communication ethics, and international cooperation. Institutional innovations (CPS, CSCIB), doctrinal frameworks (Information Security Doctrine, Cybersecurity Strategy) and international partnerships (NATO StratCom COE) have created a holistic "communication security contour". Further progress depends on the codification of terms, crisis communication SOPs, personnel strengthening and deepening of platform alliances. The Ukrainian case proves: in hybrid warfare, strategic communications are not an "appendix" to politics, but the core of the state's resilience.

Keywords: *strategic communications, information security, countering disinformation, public diplomacy, security and defense sector, Ukraine, hybrid warfare.*