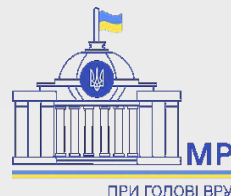


Випуск №9.
Вересень 2026

UDO
NATION



EEYES
EASTERN EUROPE YOUTH
EMPOWERMENT SPACE



Think Tanks Essentials



Think Tanks Essentials

Випуск №9

Київ, 2026

У світі, що швидко змінюється, аналітичні центри стали ключовими гравцями у формуванні міжнародних дискусій та стратегій. Вони не лише генерують ідеї, а й визначають напрями політичних рішень та впливають на суспільні настрої.

Журнал “ThinkTank Essentials” створений з метою узагальнювати та аналізувати найважливіші експертні дослідження, щоб показати, як вони формують наше розуміння світового порядку.

Цей журнал є корисним для всіх, хто прагне орієнтуватися в дедалі складнішій міжнародній політиці. Він дозволяє відстежувати ключові тенденції, аргументацію провідних експертів, які впливають на рішення урядів та міжнародних організацій. Для дослідників та студентів це зручне джерело аналітики й актуальних кейсів, для дипломатів та експертів – інструмент розуміння глобальних процесів і прогнозування можливих сценаріїв, для широкої аудиторії – можливість побачити за заголовками новин глибший контекст.

ЗМІСТ

Передмова.....	8
Розділ 1. Огляд на дослідження think tanks.....	12
НАТО та нова архітектура європейської безпеки.....	13
Можливий вихід США з НАТО з погляду американського права.....	14
Саміт в Анкарі: НАТО належить Трампу, а Європі лишається пристосовуватися.....	15
Східний фланг НАТО	16
Право і реальність: східний фланг та Оттавська конвенція.....	17
Коли старі орієнтири втрачають силу: як країни Північної Європи та Балтії адаптують зовнішню політику.....	18
Європейська оборона та стратегічна автономія.....	21
Стратегічна автономія і нова логіка втручання Європи.....	22
Стійкість як ключова опора оборони Європи, а не просто додаток.....	23
Крах FCAS і давня проблема координації в Європі.....	24
Цифровий арсенал НАТО: як Європі не потрапити в нову залежність від США.....	25
Оборона ЄС: технологічний виклик для Європи.....	26
Кінець дзиччання: як Європі захиститися від дронів.....	27
Російсько-українська війна.....	29
Пастка замикається: як Росія придушує спротив в окупованій Україні та що ще можна зробити.....	30
Як посилити Україну: витратити ефективніше, підтримувати рішучіше.....	31
Спеціальний трибунал для України: як запустити механізм міжнародного правосуддя.....	32
Перед обличчям альянсу Північної Кореї та Росії: стратегії ЄС і Республіки Корея для стримування та співпраці.....	33
Держава в занепаді, але дедалі небезпечніша: як Росія втрачає вплив у сусідніх регіонах.....	34
Розширення ЄС та Україна в Європі.....	37
Майбутнє політики розширення ЄС: чотири сценарії розширення у війсьній Європі...38	
Чарівна десятка: коаліція охочих для просування наступного розширення ЄС.....	39
Україна та наступний бюджетний цикл ЄС: як забезпечити передбачуваність фінансування.....	40
Загострення польсько-української суперечки як оперативна мета Росії в Польщі.....	41
Економічна безпека, санкції та стратегічні залежності.....	43
Енергетична безпека Європи у 2026 році: стійкіша, але системно вразлива.....	44
Європейський Союз перед викликом «китайського шоку 2.0».....	45
Протидія використанню криптоактивів для обходу санкцій проти Росії.....	46
Стратегічна корупція: як російські незаконні фінансові потоки пов'язані з офшорними фінансами.....	47
Що дали дії європейських держав проти російського тіньового флоту — і де їхні межі...48	

Трансформація Заходу та європейська політична суб'єктність.....	51
Франція та Німеччина: подолати розбіжності для зміцнення європейського суверенітету.....	52
Трагедія ностальгії за старим Заходом.....	53
Європа в епоху економіки «America First».....	54
Якщо Марін Ле Пен переможе: що Європі варто знати про крайньо праву Францію.....	55
Розділ 2. Аналітичні матеріали Insight Lab.....	57
Попович Олександра. Російський дрон на території країн НАТО: що це означає?.....	59
Василик Ярина. Від «Шахеда» до спільного виробництва: чого Росія та Іран навчилися один в одного.....	63
Кот Катерина. Диверсії як інструмент зовнішньої політики: як Росія тестує межі реакції Заходу?.....	66
Лончина Юлія. Коли диверсія стає нападом: чи застосовна стаття 5 НАТО до російських гібридних операцій?.....	70
Мелконова Олена. Чи може оборонна промисловість стати новою спеціалізацією України в економіці ЄС?.....	74
Троян Андрій. Оборонна промисловість України після війни: драйвер економічного розвитку чи тимчасова перевага?.....	78
Помогайбо Назарій. Стримування без війни: чи готові країни Балтії до російських гібридних загроз?.....	83
Ткачов Іван. Від прикордонного паркану до поля бою: як Росія може перевіряти Балтійський щит без відкритого вторгнення?.....	87
Команда.....	90
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	92
Фото та зображення.....	103

РОЗБУДОВА ВСЕОСЯЖНОГО СТРИМУВАННЯ НА СХІДНОМУ ФЛАНЗІ НАТО: УКРАЇНСЬКИЙ ДОСВІД ТА АЛЬТЕРНАТИВНА РОСІЙСЬКА ІДЕНТИЧНІСТЬ

Східний фланг і російська загроза

Східний фланг охоплює прикордонний регіон НАТО від Балтійського моря та Естонії до Чорного моря в Болгарії. Фінляндія та Норвегія, які також межують з Російською Федерацією, входять до складу Північного флангу і становлять окрему операційну зону. Кордони Східного флангу було встановлено у 2004 році, коли загроза з боку Російської Федерації ще не була повністю усвідомлена. Сьогодні цей регіон є операційною зоною, головна мета якої — стримування можливої російської агресії.

Після вторгнення Російської Федерації в Україну у 2014 році Східний фланг НАТО перетворився на стратегічний пріоритет. У міру того як Путін продовжував використовувати антизахідну риторику як зброю, загроза для НАТО ставала дедалі відчутнішою. Після гібридних і кібератак проти держав-членів НАТО зміцнення Східного флангу стало питанням колективної безпеки. Після Варшавського саміту 2016 року для стримування можливої агресії з боку Російської Федерації було створено Посилену передову присутність (EFP), що складається з багатонаціональних сил. Присутність багатонаціональних бригад на Східному фланзі означала, що для просування російським силам довелося б атакувати війська кількох держав-членів НАТО, що підвищувало ймовірність застосування статті 5 Північноатлантичного договору.

Спочатку EFP була зосереджена на забезпеченні оборони держав-членів НАТО, що межують з Російською Федерацією: Польщі, Литви, Латвії та Естонії. Однак після 2022 року, коли Російська Федерація розпочала повномасштабне вторгнення в Україну, задіявши армію чисельністю в сотні тисяч військових, дію EFP було розширено на Словаччину, Угорщину, Румунію та Болгарію, охопивши таким чином увесь Східний фланг.

Втім, сама лише присутність сил EFP не гарантує захисту Східного флангу від можливого російського нападу. Початкова концепція розгортання EFP полягала не в тому, що ці сили будуть здатні самотійно відбити масштабний напад, а радше в тому, що напад на бригади EFP втягне у війну більшість держав-членів НАТО. Основну частину цих сил становить піхота, якої може бути недостатньо, щоб протистояти силам Російської Федерації, з огляду на переваги Росії над НАТО у веденні дрової війни, зумовлені її бойовим досвідом, логістикою та налагодженими виробничими потужностями. Ще однією проблемою є логістика: Сувалківський коридор між Польщею та Литвою потенційно може бути перекритий Російською Федерацією, що залишить частини Східного флангу вразливими.

У 2024 році Польща ухвалила рішення побудувати «Східний щит» — оборонну лінію вздовж свого кордону з Російською Федерацією. За наявною інформацією, проект спирається на уроки, здобуті у Російсько-українській війні. Згідно з оприлюдненими планами, оборонна система простягатиметься на кілька сотень метрів углиб території, при цьому значна увага приділяється будівництву та обслуговуванню інфраструктури поблизу кордону.

Підсумовуючи, початкова логіка структурної оборони Східного флангу застаріла. Вона не враховує сучасних змін у веденні війни та геополітичній ситуації.

Дронова революція

Наразі Російська Федерація обмежена війною в Україні. Будь-яка мирна угода чи перемир'я з Україною вивільнили б значні сили, частина з яких, ймовірно, була б розміщена вздовж західного кордону Росії.

Армія, розміщена там, не нагадувала б сьогоднішню російську армію. Це були б досвідчені підрозділи, які вправно володіють FPV-дронами, зокрема дронами на оптоволоконні, а також засобами ураження середньої дальності та глибокими ударами. Оборонна лінія, що складається з позицій завглибшки менш ніж один кілометр, не витримала б штурму. Правильне поєднання типів дронів разом із неминучим перенапруженням систем протидії дронам може призвести до знищення передових оборонних позицій протягом кількох хвилин — за умови попередньої розвідки та завчасного послаблення логістики ударами середньої дальності.

Крім того, жодна оборона не встоїть без належно підготовлених і оснащених військовослужбовців. Країни ЄС просто не мають відповідного бойового досвіду, порівнянного з тривалою війною в Україні. Спеціалізована підготовка піхотинців з протидії дронам і створення власних дронів підрозділів є абсолютно необхідними для бойової готовності цієї оборони, проте чинні військові доктрини недостатньо враховують ці потреби. Наявні засоби протидії дронам або занадто рідкісні й дорогі для широкого впровадження, або надто швидко застарівають, аби встигати за розвитком дронів технологій.

Польщі та балтійським державам варто уважно вивчити досвід України у веденні дровоної війни. Українські інструктори мають реальний бойовий досвід, незрівнянний із жодною теоретичною підготовкою, яку можуть запропонувати інструктори НАТО. Водночас Україна створила так звану «зону ураження» вздовж лінії фронту, яка довела свою ефективність проти чисельніших і безперервно наступаючих російських сил. Ця система складається не з однієї оборонної лінії. «Зона ураження» включає численні позиції, що можуть тягнутися на десятки кілометрів углиб і які належним чином замасковані, з'єднані та скоординовані. Логістика на основі дронів підтримує лінію фронту, де ротація особового складу ускладнена. Уроки війни в Україні не використовуються для побудови належної оборони «Східного щита», і це фатальний недолік, який може призвести до успішного російського наступу на початковому етапі вторгнення.

Підпорогова війна

Водночас Російська Федерація продовжує вести підривну, підпорогову діяльність. Використання проксі-сил, залякування (зокрема дипломатичного тиску), інформаційних операцій, диверсій, кібератак, лоуфару (використання права як зброї), економічного примусу та політичної дестабілізації належить до методів, які зазвичай застосовуються нижче порогу традиційної війни для досягнення політичних цілей. Частота цих підривних дій різко зросла по всій Європі з 2022 року порівняно з періодом до повномасштабного вторгнення. Хоча оборона та стійкість посилюються, встановлення авторства підривних дій і своєчасне реагування залишаються вкрай складними завданнями. Ця статистика не враховує аспектів когнітивної війни та політичної дестабілізації, які ще важче виявити та їм протидіяти. Однак ми можемо достовірно стверджувати, що щонайменше третина всіх операцій були присвячені виборчим та інформаційним кампаніям.

Як зазначають деякі дослідження, Російська Федерація досягла успіху принаймні в частині своїх намірів, коли підливні дії у поєднанні з іншими чинниками призвели до бажаних поведінкових змін у Бельгії та Польщі. Хоча кінцеві цілі російського гібридного впливу залишаються недосягнутими, Російській Федерації вдалося послабити підтримку України та здійснити диверсії проти інфраструктури. Крім того, успіх цих підливних дій виявив затримки у прийнятті рішень, нездатність виробити скоординовану відповідь та поляризацію всередині альянсу.

Наразі Польща та балтійські держави визнали гібридний характер загроз з боку Росії. Проте цілісні операційні механізми протидії російській підпороговій війні досі не створено, хоча ця загроза широко обговорюється і визнається на папері.

Російська ідентичність у рамках стратегічного стримування

Будь-яка концепція стратегічного стримування та гібридної війни неминуче включає когнітивний і соціальний виміри. Усвідомлення гібридних загроз вимагає одночасного зміцнення власної стійкості та проведення політичної, соціальної й когнітивної дестабілізації суперника. Оборонна лінія не зможе довго стримувати ворога, якщо власне населення виступає за капітуляцію, а система врядування суперника залишається недоторканою. Рішення побудувати «Східний щит» — це зобов'язання щодо стримування у сфері жорсткої сили. Але як щодо м'якої сили?

Російську Федерацію слід не лише стримувати — її також необхідно критично й ґрунтовно вивчати. Європа має підвищити свою готовність не тільки у сфері жорсткої сили, а й у сфері когнітивної війни. По-перше, Російську Федерацію слід визнати суперником. Війна проти України показала, що Російська Федерація перетворилася на державу-ізгоя, і будь-яка нормалізація відносин після мирної угоди чи перемир'я створила б більше можливостей для російської підпорогової війни. По-друге, необхідні нові зусилля для зміцнення альтернативних центрів влади, знань і науки, пов'язаних з Росією. Російський режим слід делегітимізувати спільними міжнародними зусиллями. Водночас російську збройну опозицію слід зміцнювати як головний альтернативний центр опору путінській Росії.

Брак проукраїнських російськомовних медіа перешкоджає розвитку наративів, які могли б стати альтернативою тим, що просуває російська влада. Послаблення російського режиму вимагає постійних зусиль щодо делегітимізації як його інституцій, так і наративів, на які він спирається.

Зміна режиму в Російській Федерації неможлива без самих росіян. Польща, і особливо балтійські держави, досі мають значні російськомовні меншини, які залишаються вразливими до російської пропаганди. Підтримка альтернативної російської ідентичності — мирної, дружньої до України та проєвропейської — віддалила б ці спільноти від інституцій і наративів Російської Федерації та сприяла б їхньому залученню до ширшого антипутінського руху. Ядро цього опору становлять російські добровольці, які зі зброєю в руках захищають Україну.

На шляху до нової всеосяжної стратегії стримування

Дронова революція в російсько-українській війні та гібридний характер сучасних загроз змінили правила ведення війни, проте ці зміни інтегруються в національні оборонні доктрини та військову стратегію лише повільно. Нова стратегія стримування для східного флангу НАТО

має включати більше, ніж проект «Східний щит». Будь-яке будівництво оборонних ліній на випадок можливого російського вторгнення повинно враховувати найновіші тенденції у російсько-українській війні. Іншими словами, актуальний військовий досвід України є незамінним.

Крім того, надійне стримування та розвиток жорсткої сили мають йти пліч-о-пліч зі спеціальними заходами у сфері м'якої сили. Ці заходи повинні включати особливу увагу до русистики (досліджень Росії), незмінну прихильність до неможливості співпраці з Російською Федерацією, доки не буде компенсовано всі наслідки російського вторгнення в Україну, а також зміцнення альтернативних полюсів російської ідентичності в Європі з акцентом на російську збройну опозицію, яка залишається єдиною легітимною російською опозицією, визнаною Україною. Лише поєднуючи заходи жорсткої та м'якої сили, адаптовані до сучасних викликів, можна нормалізувати європейську архітектуру безпеки та надати їй потенціал для вдосконалення.



ІВАН ЮРОВ,
директор Дослідницької ініціативи з питань російської ідентичності та врядування



ПЕТРО БАКУМОВ,
старший викладач Києво-Могилянської академії

РОЗДІЛ 1. ОГЛЯД НА ДОСЛІДЖЕННЯ THINK TANKS

НАТО ТА НОВА АРХІТЕКТУРА ЄВРОПЕЙСЬКОЇ БЕЗПЕКИ

Можливий вихід США з НАТО з погляду американського права

(англ. The potential US withdrawal from NATO under American law)

Міхал Долінський, Polish Institute of International Affairs (PISM), Польща
10.07.2026

Автор дослідження аналізує, наскільки реалістичним був би вихід США з НАТО з погляду американського права. Загалом, вихід США з НАТО юридично можливий за статтею 13 Північноатлантичного договору, але на практиці його реалізація була б ускладненою. У випадку США це одразу створює процедурний і конституційний парадокс, адже Вашингтон є стороною, яка зберігає оригінал договору, й фактично мав би надіслати повідомлення про вихід самому собі.

Головна проблема полягає в тому, що Конституція США чітко визначає процедуру укладення договорів, але не встановлює правил їх припинення. Саме тому односторонній вихід президента з НАТО спричинив би суперечку між Білим домом, Конгресом і судами. Особливе значення має Section 1250A – положення, включене до оборонного бюджету США на 2024 рік. Воно забороняє президенту одноосібно припиняти дію Північноатлантичного договору або виходити з нього без згоди двох третин Сенату чи окремого акту Конгресу.

Поштовхом до таких дискусій стали повторні заяви Дональда Трампа про сумнівну цінність членства США в НАТО та його ідеї глибокого реформування Альянсу.



Проте, загалом, короткостроковий ризик виходу США з НАТО залишається низьким, але через непередбачуваність Дональда Трампа його не можна повністю відкидати. Якщо президент спробує діяти одноосібно, Конгрес, імовірно, звернеться до суду. У такому разі суди могли б застосувати підхід, сформульований Верховним судом США у справі *Youngstown Sheet & Tube Co. v. Sawyer* у 1952 році. У цій справі суд визнав незаконним рішення президента Гаррі Трумена взяти під федеральний контроль сталеливарні підприємства без чітких повноважень від Конгресу. Тоді суддя Роберт Джексон запропонував поділяти президентські повноваження на три категорії: найсильніша – коли президент діє за прямим дозволом Конгресу; проміжна – коли Конгрес не висловив чіткої позиції; і найслабша – коли президент діє всупереч прямо вираженій волі Конгресу. У випадку одностороннього виходу з НАТО ситуація, ймовірно, належала б до третьої категорії, оскільки згадана Section 1250A забороняє президенту припиняти дію договору без згоди двох третин Сенату або окремого акту Конгресу. Тому суд міг би визнати такі дії президента незаконними. Тому навіть формально однорічна процедура може перетворитися на тривалу конституційну кризу.

Саміт в Анкарі: НАТО належить Трампу, а Європі лишається пристосовуватися

(англ. The Ankara Summit: It's Trump's NATO – Europe just lives in it)

Фелікс Кестерке, Egmont Institute, Бельгія

15.07.2026

Саміт НАТО в Анкарі формально дав Європі підстави для полегшення, адже декларація підтвердила непохитність статті 5, визначила Росію як довгострокову загрозу євроатлантичній безпеці та зафіксувала підтримку України, зокрема фінансову допомогу з боку європейських союзників і Канади. Це посилило стримування, адже продемонструвало Москві, що Альянс не перебуває у відкритому розпаді.

Водночас автор наголошує, що цей саміт водночас не усунув головної проблеми – НАТО дедалі більше залежить від політичної волі Дональда Трампа. Уся зустріч була фактично побудована так, щоб уникнути конфлікту з американським президентом, тоді як його заяви щодо Ірану, Гренландії та Іспанії підтвердили збереження глибокої непередбачуваності Вашингтона. Тому Європа не може дозволити собі стратегічне самозаспокоєння.

Ключовий висновок полягає в тому, що майбутня європейська стратегія безпеки має не лише підтвердити важливість НАТО, а й визначити, як саме Європа розвиватиме власну спроможність діяти у сфері безпеки. Для цього стратегія повинна окреслити європейські пріоритети, доступні інструменти та роль оборонної промисловості. Водночас Європі потрібно знайти баланс між підходом “Made in NATO”, який дає змогу швидко закуповувати необхідне в межах Альянсу, і принципом “Buy European”, що передбачає довгострокове зміцнення власного оборонно-промислового потенціалу. У ширшому сенсі йдеться про здатність Європи діяти разом зі США, самостійно за відсутності американської підтримки, а за потреби – навіть незалежно від позиції Вашингтона.



Східний фланг НАТО

(англ. NATO's Eastern Flank Frontier)

Center for the study of democracy, Болгарія

30.06.2026



У дослідженні аналізується східний фланг НАТО як активний простір гібридного протистояння, де Росія та ширша ревізіоністська коаліція – Китай, Іран і Північна Корея – постійно випробовують стійкість євроатлантичного порядку. Вразливим також залишається південний сегмент флангу – Чорноморський регіон, де Болгарія та Румунія зіштовхуються з ризиками збройної ескалації, енергетичного примусу, кібератак, дезінформації та обходу санкцій через російський “тіньовий флот”.

Оборона східного флангу не може зводитися лише до військової присутності. Румунія активно посилює роль опорного пункту НАТО через модернізацію баз, закупівлі ППО та участь у європейському інструменті спільного фінансування оборонних закупівель SAFE, тоді як Болгарія нарощує оборонні витрати, але стримується політичною нестабільністю. Формат В9 і співпраця Болгарії, Румунії та Туреччини мають стати основою для кращої координації у морській безпеці, енергетичній стійкості та протидії гібридним загрозам.

Окремий акцент зроблено на технологічному суверенітеті. Європа відстає у ШІ, напівпровідниках і повному технологічному ланцюгу, тому має поєднати розвиток власної технологічної бази, адаптивне регулювання та розвиток власних обчислювальних спроможностей. Водночас тут звертається увага на нову загрозу – LLM grooming, тобто навмисне наповнення відкритого інтернету викривленим або маніпулятивним контентом, який згодом може впливати на відповіді систем штучного інтелекту. Загалом, це ще раз підтверджує, що Європі потрібен комплексний підхід до безпеки, який поєднує розвиток оборонної промисловості й технологій, зміцнення суспільної стійкості, медіаграмотність та використання реального бойового досвіду України.

Право і реальність: східний фланг та Оттавська конвенція

(англ. Legality and Reality: The Eastern Flank and the Ottawa Convention)

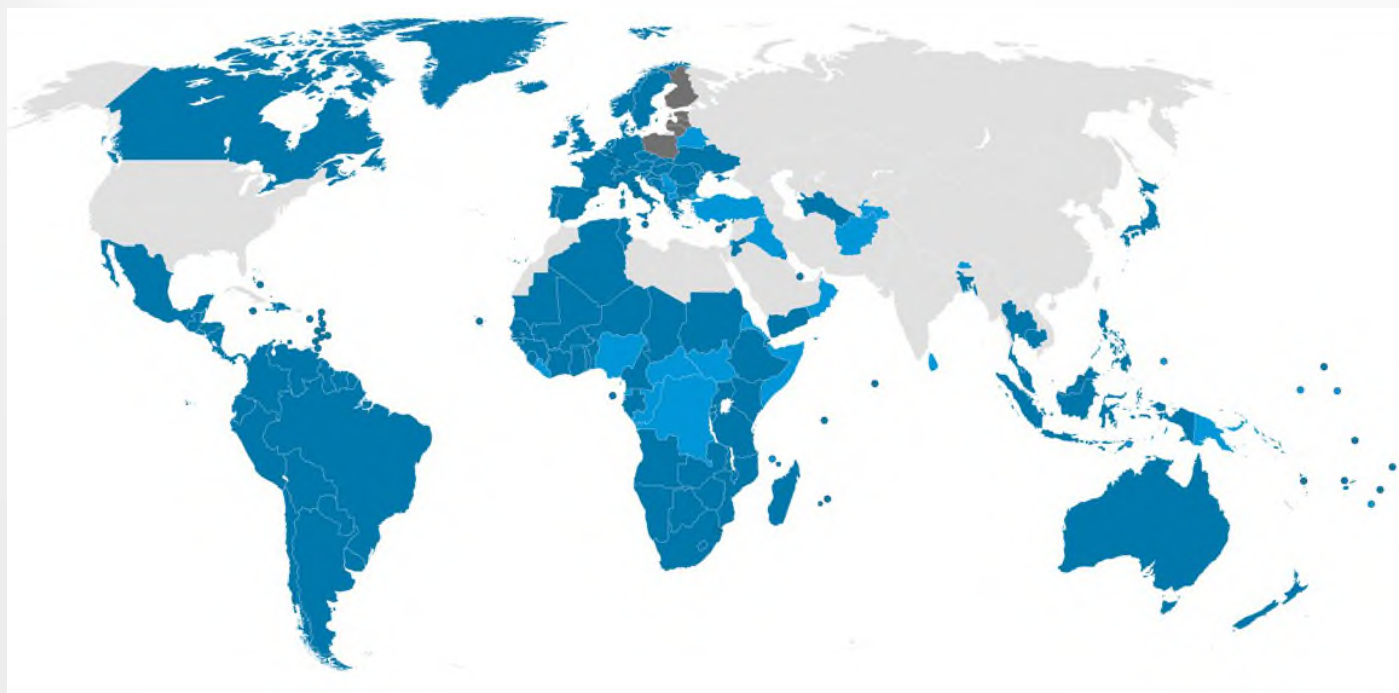
Tea Дельваль, Лука Роджерс, International Centre for Defence and Security (ICDS), Естонія

15.06.2026

Автори аналізують, як війна Росії проти України відновила в Європі дискусію про протипіхотні міни як інструмент стримування й оборони. Проте є дилема: міни залишаються військово ефективними, особливо для сторони, що обороняється, але їхнє застосування створює серйозні гуманітарні ризики та юридичні обмеження для держав, пов'язаних Оттавською конвенцією.

Російсько-українська війна є центральним випадком для дослідження. Росія, спираючись на радянську оперативну традицію, широко використовує мінні поля як частину війни на виснаження. Україна була змушена адаптуватися й також застосовувати міни, хоча вибірковіше й у меншому масштабі. Це поставило Київ у складну правову ситуацію: Україна залишається стороною Оттавської конвенції, але через триваючий збройний конфлікт не може формально вийти з неї. Її спроба призупинити застосування Конвенції через “докорінну зміну обставин” виглядає юридично вразливою.

Саме цей український прецедент пояснює рішення Балтійських держав, Фінляндії та Польщі вийти з Конвенції до того, як вони самі могли б опинитися у війні з Росією. Для них протипіхотні міни розглядаються не як зброя мирного часу, а як елемент потенційної оборони, зокрема в межах Балтійської оборонної лінії, Східного щита і захисту Сувальського коридору. Міни дійсно можуть посилити стримування й ускладнити російське планування, але навіть після виходу з Конвенції держави залишаються зобов'язаними дотримуватися міжнародного гуманітарного права.



*Статус держав у рамках Конвенції про заборону протипіхотних мін
синій – підписали та ратифікували, блакитний – приєдналися,
темно-сірий – вийшли з Конвенції*

Коли старі орієнтири втрачають силу: як країни Північної Європи та Балтії адаптують зовнішню політику

(англ. When Old Certainties No Longer Hold: Nordic-Baltic Foreign Policy Adaptation)

Крісті Райк, International Centre for Defence and Security (ICDS), Естонія
25.08.2026

Авторка аналізує стратегічну дилему держав Північної Європи та Балтії в умовах одночасного послаблення двох ключових опор їхньої безпеки: трансатлантичного альянсу та міжнародного порядку, заснованого на правилах. Росія залишається для регіону екзистенційною загрозою, а США – найсильнішим союзником. Водночас друга адміністрація Дональда Трампа поставила під сумнів традиційну роль Вашингтона як гаранта міжнародного права, союзницької солідарності й стабільності післявоєнного порядку. Авторка наголошує, що наразі ідеться не про відмову від США чи НАТО, а про необхідність адаптувати зовнішню політику до ситуації, у якій Вашингтон залишається найважливішим союзником, але вже не може сприйматися як безумовний захисник міжнародного права й післявоєнного порядку.



Малі держави регіону змушені балансувати між безпековою залежністю та власними принципами. Вони прагнуть підтримувати міжнародне право, але уникають прямої конфронтації зі США, коли американська політика суперечить цим нормам. Приклади Ормузької протоки та Гренландії показові саме тому, що в обох випадках Естонія публічно демонструє готовність підтримувати союзника, але уникає прямої оцінки або критики американських дій. І саме так проявляється структурна дилема малих держав: вони можуть підтверджувати загальні принципи такі, як безпека морських шляхів, суверенітет і територіальна цілісність Данії, однак не мають достатнього політичного простору, щоб відкрито поставити під сумнів політику США.

Війна Росії проти України показала, що міжнародне право залишається необхідною основою для підтримки Києва й тиску на Москву, але саме по собі не захищає від агресії. Тому Північно-Балтійський регіон має посилювати національну, європейську та регіональну оборону, зміцнювати НАТО, поглиблювати співпрацю з Великою Британією, Німеччиною й Польщею та підтримувати інтеграцію України до Європи як частину власної стратегії виживання поруч із Росією.

ЄВРОПЕЙСЬКА ОБОРОНА ТА СТРАТЕГІЧНА АВТОНОМІЯ

Стратегічна автономія і нова логіка втручання Європи

(англ. Strategic autonomy and Europe's new logic of intervention)

Марія-Луїза Клаусен, Петер Альбрехт, *Danish Institute for international studies (DIIS)*, Данія

09.06.2026

Повномасштабна війна Росії проти України змінила не лише масштаби, а й механізми європейського втручання. Раніше ЄС переважно діяв через цивільні інструменти: підтримував реформи, розбудову державних інституцій, верховенство права та кризове управління. Після 2022 року ці підходи доповнилися прямою підтримкою воєнної спроможності України, адже ЄС фінансує постачання озброєння, тренування українських військових, спільні закупівлі та виробництво зброї.



Автори пов'язують цю зміну з двома чинниками. Перший – сама війна, яка змусила європейські держави реагувати на масштабний міждержавний конфлікт, а не на локальну кризу. Другим є невизначеність щодо майбутньої ролі США в європейській безпеці. Через це стратегічна автономія ЄС стає все більш актуальною, адже йдеться вже не лише про здатність самостійно ухвалювати рішення, а про спроможність виробляти, закуповувати й постачати зброю без критичної залежності від зовнішніх партнерів.

Військовий досвід України стає ресурсом для європейської оборонної політики. Українські виробники можуть швидше адаптувати озброєння до потреб фронту, а українські військові мають практичні знання про застосування дронів, розвідки, засобів радіоелектронної боротьби та інших технологій у реальних бойових умовах. Тому співпраця з Україною дає ЄС також і доступ до знань, яких неможливо отримати через звичайні мирні закупівлі чи навчання.

Хорошим прикладом є Данська модель. Україна визначає озброєння, яке її власна промисловість може виробити, але не може повністю профінансувати; Данія та партнери спрямовують зовнішні кошти напряму в контракти з українськими виробниками. Один із перших прикладів такої співпраці – 18 гаубиць “Богдана”, замовлених у липні 2024 року й поставлених на фронт уже через два місяці. У 2025 році ця модель дала близько \$1,8 млрд для українського виробництва зброї.

Отже, Європейський Союз дедалі глибше залучається до воєнної економіки та оборонного планування, але ще не має повністю узгодженої системи спільного виробництва, закупівель і стратегічного ухвалення рішень. Україна стала практичним тестом європейської стратегічної автономії. Вона демонструє, що ЄС здатен швидко створювати нові формати підтримки, але водночас виявляє залежність від національних урядів, зовнішнього фінансування та американських безпекових гарантій.

Стійкість як ключова опора оборони Європи, а не просто додаток

(англ. Not just an addendum: Making resilience a key pillar of Europe's defence)

Надя Ковальчикова, Джузенне Спатафора, European Union Institute for Security Studies (EUISS), аналітичний центр на рівні ЄС

06.07.2026

У дослідженні автори аналізують, чому цивільна готовність і суспільна стійкість мають стати повноцінним стовпом європейської оборони. Сучасні загрози все більше стирають межу між військовим і цивільним. Саботаж, кібератаки, інформаційні операції, економічний примус, дроніві інциденти та атаки на критичну інфраструктуру напряду впливають на здатність Європи стримувати противника й реагувати на кризу.

Відправною точкою для подібних дискусій є реальний досвід України, який довів, що підготовлені громадяни, місцева влада, бізнес, цифрові сервіси, енергетична адаптація та кризова комунікація є не тилковими елементами, а частиною оборонної спроможності. Європа вже рухається в цьому напрямі через Європейську стратегію готовності (Preparedness Union Strategy), механізми цивільного захисту, кібер- і інфраструктурне законодавство, а НАТО дедалі чіткіше розглядає стійкість суспільства як умову ефективного стримування. Вважається, що якщо держава може швидко відновлювати роботу критичних систем, підтримувати населення, протидіяти дезінформації та продовжувати функціонувати під час атак, противнику складніше паралізувати її й досягти своїх цілей.

Однак нинішня система все ще залишається фрагментованою. Бракує спільних стандартів планування, зрозумілих критеріїв вимірювання стійкості, узгодженого обміну інформацією та глибшої цивільно-військової інтеграції. Шведська модель “total defence” і фінська “comprehensive security” дають орієнтир, але не можуть бути механічно перенесені на весь ЄС.

Головною рекомендацією авторів є створення європейського механізму, який визначатиме життєво важливі функції суспільства, оцінюватиме загрози, координуватиме розвиток спроможностей і залучатиме держави-члени, інституції ЄС, місцеву владу, приватний сектор та зовнішніх партнерів, зокрема Україну.



Крах FCAS і давня проблема координації в Європі

(англ. The FCAS Collapse and Europe's Enduring Coordination Problem)

*Тевіан Томсон, International Centre for Defence and Security (ICDS),
Естонія*

22.06.2026

Автор аналізує провал програми Future Combat Air System як симптом глибшої проблеми європейської оборони: нестачі не лише ресурсів, а здатності підпорядковувати національні інтереси спільній стратегічній меті.

FCAS мав стати флагманом європейської оборонної інтеграції – спільним проектом Франції, Німеччини та Іспанії зі створення винищувача шостого покоління за участі Dassault Aviation, Airbus і Indra. Його значення полягало в самому літаку та в демонстрації того, що фрагментована європейська оборонно-промислова база здатна спільно виробляти високотехнологічні системи майбутньої війни.



Конкретний провал FCAS полягав у тому, що партнери не змогли узгодити базові умови розподілу відповідальності між компаніями. Найгострішою стала суперечка між французькою Dassault Aviation і німецьким підрозділом Airbus щодо провідної ролі в розробці винищувача. Dassault наполягала на статусі головного підрядника та прагнула зберегти контроль над ключовими технологіями, тоді як Airbus вимагала більш рівноправного розподілу робіт і доступу до інтелектуальної власності. Через це сторони тривалий час не могли погодити робочу структуру проекту, розподіл технологічних напрямів і правила ухвалення рішень.

Проблеми виникли також навколо розподілу промислових замовлень між Францією, Німеччиною та Іспанією. Кожна держава прагнула гарантувати своїм компаніям значну частку робіт, навіть якщо це не завжди відповідало логіці ефективності чи компетентності. У результаті переговори перетворилися на боротьбу за національні промислові вигоди. Додатковим джерелом напруження стали різні вимоги до майбутньої системи: Франція більше орієнтувалася на стратегічну автономію та можливість самостійного застосування сили, тоді як Німеччина сильніше враховувала рамки НАТО, спільні стандарти й політичні обмеження.

Для держав східного флангу НАТО це важливо не тому, що вони очікували отримати такий літак, а тому, що їхня безпека дедалі більше залежить від спроможності Європи організовувати складні багатонаціональні оборонні проекти. У підсумку автор зазначає, що FCAS не доводить приреченість європейської оборонної інтеграції, але показує, що гроші самі по собі не створюють військової сили. Потрібні довіра, чітке управління, політичне лідерство й готовність долати промисловий націоналізм.

Цифровий арсенал НАТО: як Європі не потрапити в нову залежність від США

(англ. NATO's digital arsenal: How Europe can avoid a new dependence on America)

Густав Грессель, *European Council on Foreign Relations (ECFR)*,
аналітичний центр на рівні ЄС

29.07.2026

Сучасні армії дедалі більше залежать від цифрових систем управління, частина яких уже створена або контролюється США. Ці системи допомагають швидко збирати, обробляти й передавати інформацію між військовими підрозділами. Це може зробити спільні дії союзників ефективнішими, але водночас створює для Європи нову залежність від США. Після саміту НАТО в Анкарі союзники домовилися розвивати безпілотики, спільні системи обміну військовою інформацією, програми штучного інтелекту та єдині технічні правила. Проте автор наголошує, що той, хто створює й контролює основу цих систем, фактично визначає, як армії обмінюватимуться даними, оновлюватимуть програмне забезпечення та використовуватимуть зброю.

Україна вже має практичний досвід, який показує, як це може працювати. Її система Delta об'єднує дані від різних сенсорів, підрозділів і видів озброєння в одному цифровому середовищі. Завдяки цьому військові можуть швидше координувати артилерію, дрони, ППО, евакуацію та інші операції. Водночас армії європейських країн досі використовують багато несумісних між собою систем. Навіть стандарт Link 16, який має забезпечувати обмін даними між союзниками, уже не повністю відповідає сучасним потребам: він передає переважно оброблену інформацію про цілі, а не необроблені дані із сенсорів.

Окрему проблему може створити американська Government Reference Architecture для дронів. Хоча її позиціонують як відкриту й таку, що може працювати з різним обладнанням, ключові рішення щодо її оновлення, сертифікації та частини програмного коду залишаються під контролем ВПС США. Крім того, американські правила ITAR можуть обмежувати експорт і використання європейських систем. Подібна ситуація вже виникала з ракетами Storm Shadow/SCALP, коли їхнє застосування Україною залежало від політичних рішень партнерів.



Тому, на думку автора, НАТО потрібна не просто спільна система, а справді відкрита цифрова архітектура з доступним кодом і незалежним міжнародним управлінням. Якщо США не погодяться на такий підхід, Європі разом із Канадою, Норвегією, Великою Британією та Україною доведеться розробляти власну систему.

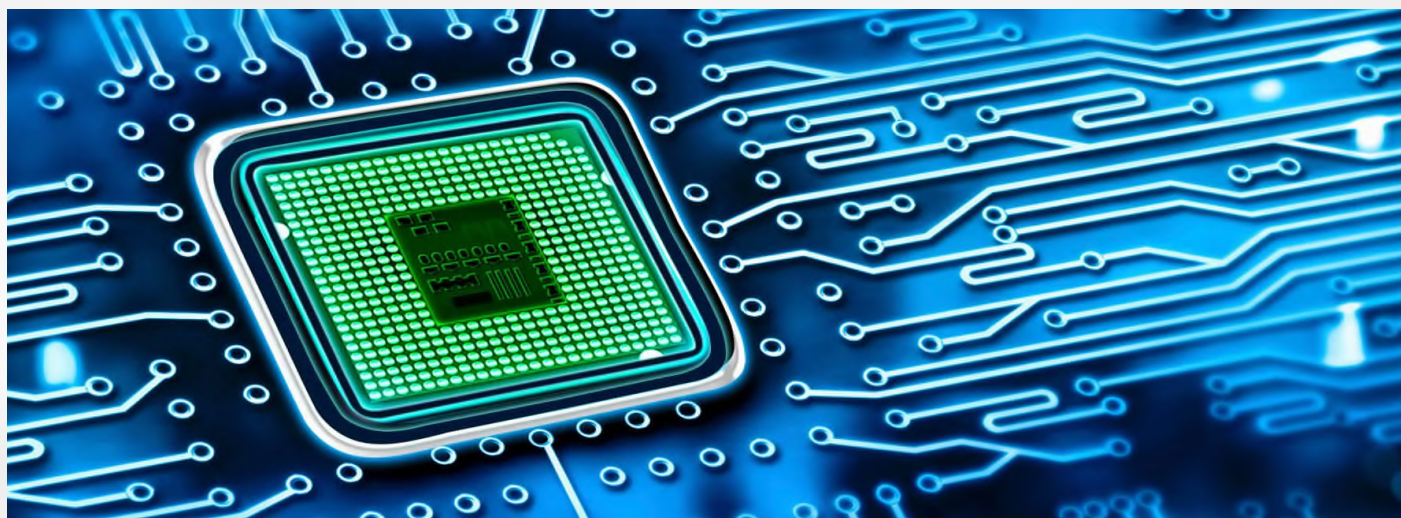
Оборона ЄС: технологічний виклик для Європи

(англ. EU Defence Series: Europe's Tech Challenge)

*Полін Ле Гран, International Centre for Defence and Security (ICDS),
Естонія*

30.07.2026

Авторка аналізує, чому Європі складно швидко розвивати власні оборонні технології. Війни в Україні та на Близькому Сході показали, наскільки важливими стали дрони, системи зі штучним інтелектом і супутникові технології. Водночас Європа не встигає адаптуватися до цих змін. Проблема полягає не лише в нестачі фінансування. Протягом багатьох років європейські країни недостатньо інвестували в оборону, скорочували запаси озброєння, діяли розрізнено під час закупівель і не створили достатніх виробничих потужностей, щоб швидко нарощувати випуск необхідної техніки.



Також звертається увага на дві ключові залежності Європи. Перша стосується Китаю, який контролює значну частину ринку критично важливої сировини: він виробляє близько 90% світових рідкісноземельних мінералів і забезпечує 98% їхнього імпорту до ЄС. Друга залежність пов'язана зі США, від яких Європа значною мірою залежить у таких сферах, як протиракетна оборона, високоточні удари, розвідка та інші передові військові технології. Це створює ризики, особливо якщо змінюються американські політичні пріоритети або виникають обмеження щодо постачання систем, їхнього використання чи доступу до програмного забезпечення. Прикладом таких дискусій є програма F-35.

Європейський Союз намагається реагувати на ці проблеми через низку ініціатив, зокрема Strategic Compass, White Paper for European Defence – Readiness 2030, EDF, EUDIS, PESCO та EDIP. Окрему увагу приділяють технологіям подвійного призначення, які можна використовувати і в цивільній, і в оборонній сферах. Серед конкретних заходів авторка згадує проєкт JEWEL для раннього попередження, €325 млн на European Defence Projects of Common Interest і €260 млн на Ukraine Support Instrument / BraveTechEU.

Тож, Європі потрібно діяти швидше й вкладати більше коштів не лише в закупівлю готового озброєння. Вона має розвивати власні дослідження, підтримувати стартапи, масштабувати виробництво, запускати спільні оборонні проєкти та зміцнювати ланцюги постачання. Інакше Європа й надалі залишатиметься залежною від США та Китаю у критично важливих технологіях і ресурсах.

Кінець дзижчання: як Європі захиститися від дронів

(англ. Buzzkill: How to defend Europe against drones)

Ульріке Франке, *European Council on Foreign Relations (ECFR)*,
аналітичний центр на рівні ЄС

17.08.2026

Авторка описує дві основні дроніві загрози для Європи. Перша стосується малих дронів, які можуть використовувати для спостереження або атак на критично важливі об'єкти – аеропорти, LNG-термінали, військові бази, атомні електростанції та бази підводних човнів. Показовим є інцидент 5 серпня 2026 року в аеропорту Лейпцига, де виявили невеликий дрон із вибухівкою.

Друга загроза має військовий характер. Йдеться про дрони, які перетинають повітряний простір країн на східному фланзі ЄС і НАТО, зокрема з боку Росії та Білорусі. Найсерйозніший випадок стався у вересні 2025 року, коли близько 20 російських дронів увійшли в повітряний простір Польщі. У відповідь НАТО активувало статтю 4 та розпочало операцію Eastern Sentry.

Нинішня система реагування в Європі залишається розрізненою та надто дорогою. Дрони можуть коштувати близько 10 тисяч євро, тоді як для їхнього перехоплення часто використовують винищувачі або ракети вартістю мільйони. Тому Європі потрібна не одна масштабна “стіна дронів”, а багаторівнева система захисту. Вона має поєднувати радары, пасивні сенсори, оптичні та акустичні системи, засоби радіоелектронної боротьби, кіберперехоплення, кінетичні засоби та дрони-перехоплювачі.

Окремо авторка закликає створити спільну систему моніторингу й реагування вздовж усього східного флангу. ЄС має підтримати ініціативи Польщі та країн Балтії, допомогти державам, які поки що не мають достатніх спроможностей, а також узгодити правові правила щодо виявлення та перехоплення дронів. Важливим джерелом практичного досвіду для Європи може стати Україна, яка вже тривалий час протистоїть масованим атакам, активно використовує РЕБ і постійно адаптує свої дроніві технології.



РОСІЙСЬКО-УКРАЇНСЬКА ВІЙНА

Пастка замикається: як Росія придушує спротив в окупованій Україні та що ще можна зробити

(англ. The Trap Closes: How Russia Suppresses Resistance in Occupied Ukraine and How We Can Still Help)

Джейд Макглінн, *International Centre for Defence and Security (ICDS)*,
Естонія
19.06.2026

Автор аналізує, як Росія утримує контроль над окупованими українськими територіями та чому західна підтримка має зосереджуватися не на публічних акціях, а на безпеці людей, збереженні української ідентичності й підтримці тих, хто живе в окупації.



Російська система поєднує репресії, стеження, інформаційний контроль і русифікацію. Заздалегідь підготовлені списки активістів, журналістів, учителів, ветеранів і волонтерів використовують для обшуків, викрадень і допитів. Задokumentовано понад 100 місць незаконного утримання цивільних, а кількість затриманих може сягати щонайменше 15 250 осіб. 92% опитаних колишніх ув'язнених повідомляли про катування або жорстоке поводження.

Контроль поширюється і на повсякденне життя: перевіряють телефони, відстежують інтернет-активність, прив'язують SIM-картки до біометричних даних і змушують людей отримувати російські паспорти. Без них мешканці можуть втрачати доступ до медицини, освіти, виплат, роботи та майна.

Окремим напрямом є діти. Майже 20 000 українських дітей були примусово переміщені до Росії або на підконтрольні їй території. Їх русифікують, обмежують контакти з родичами й нав'язують російську історію. На окупованих територіях дітей також залучають до мілітаризованих програм: наприклад, Voin навчає підлітків зброї, тактики та використання дронів. У Маріуполі близько 63,8% освітнього бюджету, за оцінкою дослідження, спрямовується на ідеологічні активності.

В умовах тотального нагляду масові протести та публічна символіка можуть призводити до арештів, катувань і викрадень. Стійкішими формами спротиву, на думку автора, є збереження мови й культури, передача інформації, допомога іншим, документування злочинів і підтримання зв'язку з Україною. Важливими є невеликі ізольовані групи, мінімізація контактів і безпечна зовнішня координація.

Тому західна підтримка має бути практичною: допомога ВПО, цифрова безпека, захищений зв'язок, підтримка незалежних адвокатів, пошук зниклих, гуманітарна допомога та безпечне документування злочинів. Найважливіше – допомогти людям вижити, зберегти українську ідентичність і продовжити опір без зайвого ризику.

Як посилити Україну: витратити ефективніше, підтримувати рішучіше

(англ. Empowering Ukraine: Spend smarter, support harder)

Ондржей Дітріх, Каспар Гобгаус, Надя Ковальчикова, Росселла Маранджо, Тім Рюліг, Луїджі Скаццієрі, Джузеппе Спатафора, Бояна Зорич, *European Union Institute for Security Studies (EUISS)*, аналітичний центр на рівні ЄС
20.07.2026

Для посилення України недостатньо просто збільшити підтримку, варто зробити її більш продуманою, довгостроковою та узгодженою між партнерами. На початку 2026 року Україна перебуває у сильнішій позиції, ніж раніше: її оборона стала стабільнішою, українські дрони вже можуть уражати цілі на відстані до 3 000 км, а виробництво далекобійних дронів у період із січня до квітня 2026 року зросло на 53%. Водночас Росія все ще здатна атакувати цивільну інфраструктуру, затягувати війну та намагатися послабити єдність між Україною і Європою.



Автори пропонують кілька практичних кроків. По-перше, вони радять тісніше інтегрувати українську оборонну промисловість у європейську систему через спільні підприємства з компаніями з ЄС. Це має допомогти українським виробникам отримати більше інвестицій, технологій, виробничих можливостей і доступу до європейських та натівських закупівель. По-друге, окрему увагу пропонують приділити приблизно п'яти мільйонам українців, які зараз живуть у ЄС, і розглядати їх як важливу демократичну спільноту, особливо напередодні перших повоєнних виборів. По-третє, йдеться про те, щоб ще до повного вступу України до ЄС поступово долучати її до європейських систем у таких сферах, як енергетика, цифрова політика, транспорт, стандарти, оборона та мобільний зв'язок у межах ініціативи “Roam Like at Home”.

Окремий блок пропозицій стосується відбудови України. Серед них – створення платформи для залучення інвесторів на основі DREAM, ініціатива Big on Board для активнішої участі приватного бізнесу, відновлення енергетики з акцентом на розподілену чисту генерацію, а також пропонується обережне залучення Китаю до відбудови через спеціальні запобіжники. Крім того, автори пропонують створити Peace and Prosperity Compact для кращої координації між ЄС, США та країнами G7, розбудувати мережу протидії російським шахрайським схемам і вербуванню в Африці, а також скористатися нинішнім “проукраїнським” моментом у політиці Трампа, щоб розмістити виробництво критично важливих американських систем у Європі або Україні.

Спеціальний трибунал для України: як запустити механізм міжнародного правосуддя

(англ. The Special Tribunal for Ukraine: Turning the Wheels of International Justice)

Tea Дельваль, *International Centre for Defence and Security (ICDS)*,
Естонія

18.06.2026



Створення Спеціального трибуналу щодо злочину агресії проти України має закрити прогалину в міжнародному правосудді, адже Міжнародний кримінальний суд наразі не може притягнути російське керівництво до відповідальності саме за агресію проти України.

15 травня 2026 року в Кишиневі 34 держави Ради Європи, а також Австралія, Коста-Рика та Європейський Союз ухвалили резолюцію про створення Enlarged Partial Agreement. Ця угода має забезпечити адміністративну та фінансову основу для роботи майбутнього трибуналу.

Проблема полягає в тому, що Україна визнала юрисдикцію МКС щодо геноциду, злочинів проти людяності та воєнних злочинів із 20 лютого 2014 року, але це не поширюється на злочин агресії. Щоб МКС міг розглядати такі справи, потрібна або ратифікація Кампальської поправки, або передавання ситуації Радою Безпеки ООН. Однак другий варіант фактично заблокований через право вето Росії.

Тому окремий трибунал має стати спеціальним механізмом для переслідування найвищого політичного та військового керівництва, відповідального за початок агресії. Його робота ґрунтуватиметься на праві України переслідувати цей злочин, а також на положеннях Римського статуту, резолюції Генеральної Асамблеї ООН 3314, практиці Нюрнберзького і Токійського трибуналів та стандартах Європейського суду з прав людини.

Водночас авторка звертає увагу на важливі обмеження. Заочні процеси мають проводитися лише з дотриманням права обвинуваченого на повторний розгляд справи. Крім того, чинні глави держав і урядів та міністри закордонних справ користуються персональним імунітетом, тому притягнути їх до відповідальності під час перебування на посаді буде складно.

Отже, створення трибуналу є важливим кроком, але його успіх залежатиме не лише від самого факту заснування. Щоб стати справді історичним прецедентом, він має працювати професійно, неупереджено та з повагою до права на справедливий суд.

Перед обличчям альянсу Північної Кореї та Росії: стратегії ЄС і Республіки Корея для стримування та співпраці

(англ. Facing the North Korea–Russia alliance: EU–ROK strategies for deterrence and cooperation)

Йонджун Кім, Elcano Royal Institute, Іспанія

24.07.2026

Автор показує, як військова підтримка Росії з боку Північної Кореї вплинула на перебіг і масштаб війни проти України. Пхеньян постачає Росії великі обсяги боеприпасів і направив тисячі військових. Для КНДР це перша масштабна військова операція за кордоном після Корейської війни. Такий крок свідчить про відхід від традиційної політики *Juche*, яка передбачала максимальну самостійність і обережне ставлення до залежності від Китаю чи Росії.

Автор також наголошує, що війна в Україні стала випробувальним майданчиком для нової військової співпраці між авторитарними державами. Китай, Росія та Північна Корея не є повноцінним ідеологічним союзом, однак їх об'єднує спільний прагматичний інтерес – послабити міжнародний порядок, у якому провідну роль відіграють США.

Якщо ця співпраця розвиватиметься, вона може вийти за межі нинішньої підтримки Росії. Серед можливих подальших сценаріїв – спільні військові навчання Китаю, Росії та КНДР, доступ російських і китайських кораблів до північнокорейських портів, зокрема Вонсана, а також координація у сфері ядерного стримування, кібероперацій, космічних технологій та інформаційної війни. Не виключені й командно-штабні навчання, присвячені можливим ударам по таких об'єктах, як Пхьонгхек, Окінава та Гуам.

На думку автора, Європа та Південна Корея мають реагувати одночасно через стримування і дипломатію. Це передбачає регулярні багатонаціональні військові навчання, підвищення сумісності армій, обмін військовим персоналом, спільну роботу у сфері кібербезпеки та космічних технологій, захист критичної інфраструктури, а також поглиблення оборонно-промислової співпраці між європейськими країнами та Південною Кореєю.



Держава в занепаді, але дедалі небезпечніша: як Росія втрачає вплив у сусідніх регіонах

(англ. A Declining, but More Dangerous Power: Russia's Receding Reach in the Neighbourhood)

Штефан Майстер, *International Centre for Defence and Security (ICDS)*,
Естонія

29.06.2026

Дослідження аналізує, як війна Росії проти України прискорила структурний занепад Москви як регіональної сили. Повномасштабне вторгнення мало відновити російську сферу впливу, але дало протилежний результат: Казахстан, Грузія, Молдова, Вірменія та держави Центральної Азії дедалі більше сприймають Росію не як гаранта безпеки, а як ризик, від якого потрібно дистанціюватися.

Ключовим механізмом цього занепаду є концентрація російських ресурсів на українському фронті. Через втрати й санкції Москва перекидала війська та озброєння з Таджикистану, Вірменії, Абхазії й Південної Осетії, що послабило її вплив у сусідніх регіонах. Найпоказовіший приклад – Нагірний Карабах: Росія мала “миротворців” після 2020 року, але не завадила Азербайджану встановити контроль над територією у 2023-му.

Паралельно санкції погіршили переговорні позиції Кремля. Росії потрібні нові енергетичні ринки, санкційні обхідні маршрути й транзит через Азербайджан, Грузію та Центральну Азію. Це посилює суб'єктність регіональних держав: вони розвивають Середній коридор, координують політику між собою, залучають Китай, Туреччину, ЄС, США, Індію, Іран і арабські держави. Найбільше виграє Китай, який перебирає частину російського впливу в торгівлі, інфраструктурі, цифровому нагляді та безпеці.



РОЗШИРЕННЯ ЄС ТА УКРАЇНА В ЄВРОПІ

Майбутнє політики розширення ЄС: чотири сценарії розширення у війнній Європі

(англ. The Future of EU Enlargement Policy: Four Scenarios for Enlargement in Wartime Europe)

Катерина Лозка, Йонас Альтгофф, Лавінія Кларгефер, Марія Гаргано, Марина Ярошевич, Egmont Institute, Бельгія
02.07.2026

Автори розглядають чотири можливі сценарії розвитку політики розширення ЄС до 2029 року. Після повномасштабного вторгнення Росії розширення перестало бути лише способом підтримати демократичні зміни в сусідніх країнах. Тепер це також питання безпеки всієї Європи. Водночас ЄС має знайти баланс між потребою швидше наблизити Україну, Молдову та країни Західних Балкан до європейського простору і необхідністю дотримуватися власних правил: виконання законодавства ЄС, проведення реформ, одностайного ухвалення рішень, бюджетних обмежень і збереження ефективності Союзу.

За сценарієм швидкого розширення Чорногорія та, можливо, Албанія можуть стати повноправними членами ЄС. Україна й Молдова водночас можуть отримати поступовий доступ до окремих частин спільного ринку та європейських безпекових механізмів, але без повного права брати участь у політичних рішеннях Союзу.

За обережнішого сценарію ЄС і надалі вимагатиме від кандидатів послідовного виконання всіх умов. Україна зможе відкривати нові переговорні розділи, долучатися до цифрового простору, європейських енергетичних мереж і програм підтримки оборонної промисловості, однак саме членство буде відкладене.

Ще один варіант передбачає різні рівні участі в ЄС. У такому разі на першому місці буде безпека: Україна та інші кандидати зможуть поступово долучатися до європейської оборонної співпраці, спільного ринку, освітніх програм, енергетичних проєктів і видобутку важливих для промисловості ресурсів. Це дасть змогу тісніше пов'язати їх із ЄС ще до набуття повного членства.

Найгірший сценарій – фактичне замороження розширення. Популізм, блокування рішень окремими державами, економічні труднощі та повільні реформи можуть зупинити процес. У такому разі ЄС втратить частину свого впливу, а Росія та Китай отримають більше можливостей для посилення своїх позицій у регіоні.



Чарівна десятка: коаліція охочих для просування наступного розширення ЄС

(англ. The magnificent ten: A coalition of the willing to drive the EU's next enlargement)

Енг'єллуше Моріна, Габріеле Валодскайте, European Council on Foreign Relations (ECFR), аналітичний центр на рівні ЄС

23.07.2026

Майбутнє членство України, найімовірніше, стане частиною будь-якого мирного врегулювання, прийнятного для Києва. Проте водночас ЄС досі не має готового плану, який дозволив би швидко й безпечно інтегрувати Україну, Молдову та країни Західних Балкан.

Головна пропозиція – створити коаліцію з десяти держав ЄС під керівництвом Німеччини. До неї мають увійти Данія, Німеччина та Швеція, які послідовно підтримують розширення за умови виконання необхідних вимог; Австрія, Франція, Італія та Нідерланди, які ставляться до цього обережніше; а також Литва й Польща, які розглядають розширення передусім як питання безпеки. Угорщину пропонують розглядати окремо – як державу, що потенційно вже не зможе блокувати цей процес.

Спільною основою для такої коаліції має стати принцип: кожна країна-кандидат рухається до членства відповідно до власного прогресу у виконанні вимог. Водночас ЄС має передбачити запобіжники, можливість призупиняти окремі етапи процесу, контроль за міграційними ризиками та обмежений доступ до європейських фондів до набуття повного членства.

Найперспективнішою авторки вважають пропозицію Фрідріха Мерца щодо особливого проміжного статусу для України. Він передбачав би участь України в роботі Європейської ради, Європейської комісії та Європейського парламенту без права голосу. Водночас кінцевою метою залишалося б повноправне членство в ЄС.

Протягом наступних 18 місяців запропонована коаліція могла б розробити цю модель, пояснити її переваги європейським виборцям і заручитися підтримкою лідерів держав ЄС. У 2027 році її можна було б випробувати на Албанії, Молдові, Чорногорії та Україні.



Україна та наступний бюджетний цикл ЄС: як забезпечити передбачуваність фінансування

(англ. Ukraine and the Next MFF: The Strive for Predictability)

Лука Барана, Лука Чинчиріні, *Instituto Affari Internazionali (IAI)*,
Італія

22.07.2026



Автори розглядають, як у наступному довгостроковому бюджеті ЄС на 2028-2034 роки має змінитися підхід до фінансування України. Основним інструментом має стати резерв для України, через який у межах програми “Глобальна Європа” та за умови виконання вимог для вступу можна буде залучити до 100 млрд євро. Автори зазначають, що цієї суми недостатньо, адже потреби України на відновлення оцінюють більш ніж у 520 млрд євро. Водночас резерв може стати основою ширшої системи фінансування.

Ключова думка полягає в тому, що відбудову України та її вступ до ЄС не можна розглядати як два окремі процеси. Кошти мають одночасно спрямовуватися на відновлення зруйнованої інфраструктури, проведення реформ, необхідних для вступу, і поступове наближення України до європейських правил у таких сферах, як енергетика, цифрові технології, транспорт та оборонна промисловість. Важливо також покращувати умови для ведення бізнесу, щоб залучати приватні інвестиції.

Автори наголошують і на необхідності поєднати стабільність із гнучкістю. Україні та інвесторам потрібні зрозумілі й довгострокові гарантії, однак перебіг війни та масштаби руйнувань залишаються непередбачуваними. Тому ЄС має узгодити між собою безповоротну допомогу, кредити, гарантії, підтримку міжнародних фінансових організацій і приватні інвестиції.

У підсумку, Україну слід відбудовувати не просто з перспективою майбутнього вступу до ЄС, а вже за правилами й стандартами майбутньої держави-члена.

Загострення польсько-української суперечки як оперативна мета Росії в Польщі

(англ. Escalating the Polish-Ukrainian dispute: Russia's operational objective in Poland)

Філін Брийка, Александра Вуйтович, *Polish Institute of International Affairs (PISM)*, Польща

24.08.2026

Росія активно використовує польсько-українські суперечності, щоб послабити підтримку України. Автори наголошують, що нинішню кризу створила не Москва, однак саме Росія найбільше виграє від її загострення. Її головна мета – послабити або зруйнувати співпрацю між Польщею та Україною, ускладнити перевезення західної військової допомоги через польську територію, зменшити підтримку України в польському суспільстві та використати історичні суперечки, щоб перешкодити європейській інтеграції України.

Росія застосовує цю тактику щонайменше з 2014 року. Йдеться про антиукраїнські демонстрації, пошкодження пам'ятників УПА, постановочні акції, покликані створити враження переслідування польської меншини в Україні, а також напади на польські дипломатичні установи. Після 2022 року до цього додалися твердження про нібито надмірний вплив українців на польську економіку та соціальну сферу. Із 2023 року Росія також почала активніше вдаватися до саботажу й диверсій.



Одним із головних пропагандистських образів стала так звана “бандерівська Україна” – нібито держава, якою керують націоналісти, налаштовані проти Польщі. Для поширення цього образу використовують підроблені документи, вибірково оприлюднені архівні матеріали російських спецслужб і відео, створені за допомогою штучного інтелекту. Такі матеріали поширювалися, зокрема, під час інформаційної кампанії Overload.

Масштаб цієї кампанії вже можна виміряти. У період із 26 травня до 13 липня 2026 року кількість польськомовних дописів із відвертою антиукраїнською мовою ворожнечі зросла на 171% – до 364 тисяч. Кількість реакцій на такі дописи збільшилася на 345% і сягнула 1,2 мільйона.

Автори попереджають, що інформаційна кампанія може перейти у фізичні провокації: пошкодження майна, напади на українські об'єкти, неправдиві повідомлення про замінування або провокації з використанням безпілотників, які Росія спробує видати за дії України.

ЕКОНОМІЧНА БЕЗПЕКА, САНКЦІЇ ТА СТРАТЕГІЧНІ ЗАЛЕЖНОСТІ

Енергетична безпека Європи у 2026 році: стійкіша, але системно вразлива

(англ. Europe's energy security in 2026: More resilient, but systemically exposed)

Ізабела Сурвілло, Юлія Шваб, *Danish Institute for international studies (DIIS)*, Данія

19.08.2026

Станом на 2026 рік Європа краще підготовлена до енергетичних потрясінь, ніж у 2022-му. Водночас говорити про повну енергетичну безпеку ще зарано. Залежність від російських викопних ресурсів істотно зменшилася, але натомість виникли нові ризики: Європа значною мірою покладається на Норвегію у постачанні газу трубопроводами, близько 45% газу імпортує у зрізженому вигляді, а Сполучені Штати стали її головним постачальником зрізженого газу. Крім того, вразливими залишаються морські шляхи, газові термінали та світові енергетичні ринки.



Авторки наголошують, що урізноманітнення постачальників не означає повної незалежності. У 2024 році Європейський Союз усе ще покривав 57% своїх енергетичних потреб за рахунок імпорту. Перехід на чисту енергію може посилити безпеку, але водночас збільшує значення електромереж. Частка відновлюваних джерел у виробництві електроенергії зросла з 38% у 2021 році до 48% у 2024-му. Однак через обмежені можливості мереж щонайменше 120 ГВт запланованих потужностей можуть бути підключені із затримкою. До 2030 року на розвиток електромереж знадобиться близько 584 млрд євро.

Ще одна проблема – залежність європейської промисловості від Китаю у виробництві технологій для чистої енергетики. Наприклад, близько 98% рідкісноземельних магнітів ЄС отримує з Китаю. Україна тут постає як важливий приклад для перевірки стійкості енергетичної системи. Російські удари показали, що захист енергетики – це не лише протиповітряна оборона та кібербезпека. Не менш важливі запаси трансформаторів і іншого обладнання, підготовлені ремонтні бригади, швидкі державні закупівлі, надійна логістика та здатність оперативно відновлювати критично важливі послуги.

Європейський Союз перед викликом «китайського шоку 2.0»

(англ. The European Union faces “China Shock 2.0”)

Юстина Щудлік, *Polish Institute of International Affairs (PISM)*, Польща
20.07.2026

Авторка аналізує “китайський шок 2.0” – нову хвилю тиску китайського імпорту на Європейський Союз. На відміну від початку 2000-х років, коли Китай переважно експортував дешеві товари невисокої технологічності, тепер він активніше продає продукцію з високою доданою вартістю: автомобілі, електробуси, сонячні панелі, обладнання для вітроенергетики, сталь, феросплави та хімічні товари. Авторка пов’язує це зі зміною китайської економічної моделі після пандемії та кризи на ринку нерухомості у 2023 році. У відповідь Пекін посилив державну підтримку промисловості в межах стратегії “Зроблено в Китаї – 2025”.



Масштаб проблеми вже можна оцінити за конкретними показниками. У 2025 році дефіцит торгівлі ЄС із Китаєм сягнув 360 млрд євро. Від 2015 року імпорт із Китаю зріс на 89%, тоді як експорт ЄС до Китаю – лише на 37%. Того самого року Європейський Союз імпортував понад 1,1 млн нових автомобілів китайського виробництва на суму 15,1 млрд євро. Крім того, Китай постачав 98% сонячних панелей і 61% інверторів, що використовувалися в ЄС. Додатковий тиск створюють онлайн-платформи Shein, Temu та AliExpress: у 2024 році до ЄС надійшло 4,6 млрд посилок, переважно з дешевими товарами вартістю до 150 євро.

На думку авторки, ЄС має активніше захищати свій ринок від недобросовісної конкуренції, зокрема від товарів, виробництво яких підтримується китайськими державними субсидіями. Водночас потрібні сильніша промислова політика, розвиток власного виробництва, пошук надійніших постачальників і зменшення залежності від Китаю. Європейський Союз також має бути готовим до можливих обмежень з боку Пекіна у відповідь на такі заходи.

Головний висновок полягає в тому, що без послідовної промислової політики та диверсифікації постачань ЄС ризикує втратити значну частину своєї промислової бази.

Протидія використанню криптоактивів для обходу санкцій проти Росії

(англ. Countering the use of crypto-assets to circumvent sanctions against Russia)

Ельжбета Каца, Polish Institute of International Affairs (PISM), Польща
17.07.2026

Дослідження демонструє, як Росія використовує криптовалюту для обходу санкцій і створює за їхньою допомогою паралельну фінансову систему. Криптовалюти не замінили традиційні схеми з банками, посередниками, підставними компаніями та готівкою, а доповнили їх. Вони дають змогу швидше проводити міжнародні платежі, зокрема під час закупівлі товарів подвійного призначення – деталей для дронів, електроніки та інших чутливих технологій.

За оцінкою компанії TRM, у 2025 році на Росію припадала більшість із приблизно 158 мільярдів доларів криптовалютних операцій, пов'язаних із обходом санкцій. Важливу роль у цій системі відіграють мережа A7, прив'язана до рубля криптовалюта A7A5, а також біржі Garantex і Grinex. Мережа A7, яку пов'язують з Іланом Шором і російським оборонним банком "Промсвязьбанк", заявляла про понад 90 мільярдів доларів обороту у 2025 році. Також до цих схем залучені біржі та посередники в Киргизстані, Грузії й Об'єднаних Арабських Еміратах. Вони допомагають обмінювати криптовалюту на місцеві гроші.

Західні країни поступово змінюють підхід до санкцій: замість обмежень проти окремих бірж вони дедалі частіше намагаються перекривати роботу цілих мереж, до яких входять емітенти криптовалют, брокери, банки, платіжні сервіси та інші посередники. Водночас Росія швидко пристосовується. Для приховування походження коштів використовують анонімні криптовалюту, особисті цифрові гаманці, прямі обміни між користувачами, сервіси змішування транзакцій, перекази між різними блокчейнами, децентралізовані фінансові платформи та сервіси, які дають змогу обмінювати готівку на криптовалюту, зокрема Aifory Pro.

Для України це має безпосереднє значення, оскільки такі фінансові канали допомагають Росії купувати компоненти для військово-промислового комплексу й підтримувати її здатність продовжувати війну.



Стратегічна корупція: як російські незаконні фінансові потоки пов'язані з офшорними фінансами

(англ. Strategic Corruption: The Nexus Between Russian Illicit Financial Flows and Offshore Finance)

*Мартін Владимиров, Тіхоміра Костова, Маріус Кеппен, Ваня Петрова,
Center for the study of democracy, Болгарія*

28.07.2026

У дослідження розглядаються незаконні фінансові потоки з Росії як частина так званої стратегічної корупції. Йдеться про систему, у якій держава, великий бізнес, офшорні компанії та непрозорі фінансові посередники спільно працюють на збереження впливу Кремля. Автори демонструють, що після початку повномасштабного вторгнення в Україну санкції не зруйнували цю систему, а змусили її стати більш розгалуженою, прихованою та гнучкою.

Один із головних висновків дослідження полягає в тому, що мережа зі 100 найбільших російських компаній не скоротилася, а навпаки – розрослася. У 2015-2025 роках кількість пов'язаних із нею компаній зростає з 8 155 до 10 935, а кількість зв'язків між власниками та компаніями – з 9 895 до 14 459. Водночас пряма російська власність у Європі зменшилася. Натомість зростає частка компаній, контрольованих через Кіпр, Люксембург, Нідерланди, Велику Британію та Британські Віргінські острови: з 15,30% до 31,61%. Це означає, що російський капітал дедалі частіше приховується через складні ланцюги офшорних компаній.

Важливу роль у цій системі відіграють нові способи переказу грошей – криптовалюти, розрахунки, забезпечені золотом, а також стейблкоїн A7A5. Пов'язана з ним мережа A7 заявляла про проведення операцій на понад 90 мільярдів доларів поза міжнародною системою SWIFT. Для України це має безпосереднє значення, оскільки такі канали дають Росії змогу продавати свої ресурси, оплачувати імпорту, купувати товари подвійного призначення та підтримувати військово-промисловий комплекс.

Таким чином, санкції мають бути спрямовані не лише проти окремих компаній. Потрібно відстежувати всю мережу: кінцевих власників, підставні компанії, банки, юристів, криптовалютні біржі, платіжні сервіси та посередників у третіх країнах.



Що дали дії європейських держав проти російського тіньового флоту — і де їхні межі

(англ. The results and limits of European states' interventions against the Russian shadow fleet)

Ельжбета Каца, Polish Institute of International Affairs (PISM), Польща
25.08.2026



Авторка аналізує, наскільки ефективними є дії європейських країн проти російського тіньового флоту та які вони мають обмеження.

Тіньовий флот залишається одним із головних способів обходу санкцій. Водночас він становить загрозу для довкілля, безпеки судноплавства та важливої морської інфраструктури. Із 2025 року країни Північної Європи та Балтії посилили боротьбу із суднами, які не мають справжньої державної реєстрації або ходять під неправдивим прапором. Європейський Союз також розширив повноваження своїх морських місій, щоб вони могли перевіряти підозрілі судна.

Перші результати вже помітні. Під тиском країн G7 Панама, Барбадос і Камерун почали вилучати підсанкційні танкери зі своїх реєстрів. Унаслідок цього кількість суден без підтвердженої державної належності зростає з 15 у грудні 2024 року до 138 у липні 2025-го. У період із грудня 2024-го до серпня 2026 року європейські країни та морська операція ЄС "Irinì" 18 разів перевіряли або намагалися перевірити підозрілі судна. Найчастіше причиною були сумніви щодо справжності їхніх прапорів.

Росія, однак, пристосовується до нових умов. Її танкери намагаються обходити британську економічну зону, частіше використовують арктичний маршрут або плывуть навколо Африки. Деякі судна змінюють неправдиві прапори на формально чинні, а частину танкерів дедалі частіше супроводжують російські військові кораблі або літаки.

На думку авторки, повна військова блокада такого флоту є нереалістичною та надто ризикованою. Натомість спільні перевірки, затримання підозрілих суден, постійне спостереження і створення окремої морської операції ЄС могли б істотно ускладнити обхід санкцій і зробити його значно дорожчим для Росії.

ТРАНСФОРМАЦІЯ ЗАХОДУ ТА ЄВРОПЕЙСЬКА ПОЛІТИЧНА СУБ'ЄКТНІСТЬ

Франція та Німеччина: подолати розбіжності для зміцнення європейського суверенітету

(фр. France-Allemagne : dépasser les différends pour renforcer la souveraineté européenne)

Поль Моріс, *Institut français des relations internationales (IFRI)*, Франція
15.07.2026

Автор пояснює, чому франко-німецьке партнерство залишається важливим для ЄС, але не може триматися лише на символічних заявах і традиційній ролі “двигуна Європи”. Після приходу Фрідріха Мерца до влади у 2025 році спроба перезапустити співпрацю дала лише часткові результати. Париж і Берлін досі мають різні погляди на оборону, промислову політику, енергетику, відносини зі США, угоду з Меркосур і використання заморожених російських активів.

Основна суперечність стосується того, якою має бути європейська самостійність. Після початку повномасштабної війни Росії проти України Німеччина значно збільшує витрати на оборону, переглядає бюджетні обмеження і прагне створити найсильнішу звичайну армію в Європі. Водночас Берлін і надалі розглядає НАТО як основу європейської безпеки. Франція ж наполягає на тому, що Європа повинна мати більше свободи у прийнятті політичних і військових рішень та менше залежати від США.



Провал спільної розробки винищувача в межах програми FCAS/SCAF у червні 2026 року показав, що масштабні оборонні проекти не можуть бути успішними без попередньої домовленості про стратегічні цілі, розподіл відповідальності та промислові інтереси. Наступним випробуванням для двох країн стане програма створення нового основного бойового танка MGCS, яку реалізують компанії KNDS.

Попри суперечності, можливості для співпраці залишаються. Йдеться про консультації щодо ядерного стримування після промови Еммануеля Макрона 2 березня 2026 року, спільний розвиток протиповітряної оборони, систем раннього попередження і далекобійної зброї, а також про співпрацю в космосі, сфері штучного інтелекту, кібербезпеці, високопродуктивних обчисленнях, виробництві напівпровідників і технологіях подвійного призначення.

Автор пропонує перетворити Раду міністрів закордонних справ і оборони Франції та Німеччини на практичний інструмент координації конкретних проектів. На його думку, Парижу й Берліну варто менше зосереджуватися на деклараціях і більше на спільних ініціативах із чіткими цілями, відповідальними та строками виконання. Такі ініціативи мають стосуватися розширення ЄС, ухвалення рішень більшістю голосів, формування бюджету Союзу на 2028-2034 роки, а також підтримки України, Молдови та країн Західних Балкан.

Трагедія ностальгії за старим Заходом

(англ. The tragedy of “Westalgia”)

Марк Леонард, *European Council on Foreign Relations (ECFR)*, Франція
15.07.2026

Автор критикує ностальгію європейських еліт за старою моделлю відносин між Європою та США, за якої Вашингтон автоматично гарантував безпеку європейських країн.

Автор аналізує саміт НАТО в Анкарі. Європейські лідери з полегшенням сприйняли те, що Дональд Трамп не оголосив про вихід США з Альянсу чи виведення американських військ, позитивно висловився про Володимира Зеленського та пообіцяв надати Україні дозвіл на виробництво ракет Patriot. Однак, на думку автора, сам факт, що саміт значною мірою зводився до спроб не роздратувати Трампа, свідчить про стратегічну слабкість Європи.

Мета НАТО спрямовувати 5% ВВП на оборону та пов'язані з нею потреби є радше політичним жестом для заспокоєння Вашингтона, ніж результатом серйозної оцінки реальних потреб. Ця ностальгія за старим Заходом проявляється у трьох речах: небажанні визнати, що США докорінно змінилися і навіть після 2029 року можуть продовжити скорочувати свою присутність у Європі; звичці покладатися на американську допомогу, не беручи на себе достатньої відповідальності; а також у втраті Європою здатності самостійно визначати власну політику перед обличчям Трампа, Путіна та Сі Цзіньпіна.

Головний висновок автора полягає в тому, що Європі потрібна не показова лояльність до США, а чесна оцінка власних можливостей. Європейські країни мають зрозуміти, чи здатні вони самостійно вести масштабну війну, і спрямовувати оборонні витрати на подолання конкретних слабких місць, а не просто виконувати політичні орієнтири.



Європа в епоху економіки «America First»

(англ. Europe in an Age of America First Economics)

Г'юстон Білсон, *Instituto Affari Internazionali (IAI)*, Італія
03.08.2026

У дослідженні аналізується, як економічний націоналізм Республіканської партії США та політика Дональда Трампа «America first» створюють серйозний виклик для Європейського Союзу. Йдеться не лише про окремі торговельні суперечки, а про загальну зміну промислової політики США. Вашингтон дедалі активніше використовує мита, державні субсидії, вимоги купувати американські товари та заходи для повернення виробництва до країни, щоб захистити стратегічні галузі й залучити нові інвестиції.

Найшвидше на ЄС впливають саме мита. Із 2025 року більшість європейських товарів на американському ринку обкладаються загальним митом у 15%. Для сталі, алюмінію та більшості мідної продукції ставка сягає 50%. Уже в першому кварталі 2026 року експорт ЄС до США був на 30% нижчим, ніж за аналогічний період попереднього року. Водночас торговельний профіцит Євросоюзу у відносинах зі США скоротився з 80 до 34 мільярдів євро.

У довгостроковій перспективі ще більшою проблемою можуть стати американські субсидії та вимоги виробляти товари всередині країни. Після ухвалення адміністрацією Джо Байдена закону про зниження інфляції частину стимулів для чистої енергетики було переглянуто, однак адміністрація Трампа зберегла курс на підтримку американського виробництва у таких сферах, як напівпровідники та сучасні технології. У результаті інвестиції та робочі місця можуть переміщуватися з Європи до США.

Водночас автор звертає увагу на певну суперечність. США та ЄС мають спільні побоювання щодо Китаю, напівпровідників, критично важливих корисних копалин, енергетики та надійності ланцюгів постачання. Проте водночас їхня промислова політика дедалі більше перетворюється на конкуренцію. На думку автора, Європа має захищати власну промисловість, урізноманітнювати джерела постачання та зміцнювати спільний європейський ринок. Водночас важливо не допустити, щоб конкуренція між ЄС і США переросла у масштабну торговельну війну.



Якщо Марін Ле Пен переможе: що Європі варто знати про крайньо праву Францію

(англ. If Marine Le Pen wins: A European guide to a far-right France)

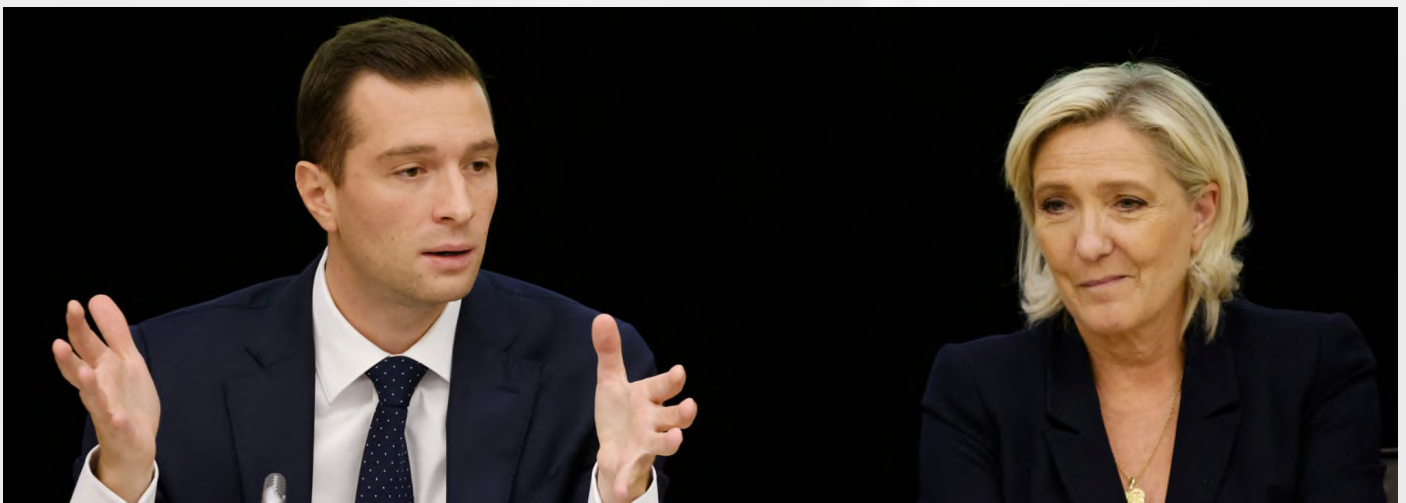
Селія Белен, Джеремі Кліфф, Каміль Лонс, Констанс Віктор, European Council on Foreign Relations (ECFR), аналітичний центр на рівні ЄС
04.08.2026

Автори цього дослідження розглядають, що могла б означати перемога Марін Ле Пен на президентських виборах у Франції 2027 року для Європейського Союзу та європейської зовнішньої політики. Поки що не йдеться про те, що її перемога неминуча, але наголошується, що прихід до влади партії “Національне об’єднання” став би для Європи значно серйознішим викликом, ніж перемога правопопулістів у менших країнах. Франція має ядерну зброю, є постійним членом Ради Безпеки ООН і відіграє ключову роль у франко-німецькому партнерстві, яке традиційно вважають рушієм ЄС.

Головний висновок авторів полягає в тому, що “Національне об’єднання” залишається передусім проектом Марін Ле Пен, навіть попри популярність Джордана Барделли. Барделла висловлюється поміркованіше щодо України та співпраці в Європі, однак у разі перемоги партії саме Ле Пен визначала б її політичний курс. Її партія прагне послабити вплив Європейської комісії, не допустити розширення практики ухвалення рішень більшістю голосів, зменшити внесок Франції до бюджету ЄС і відмовляється від ідеї спільних запозичень. Також вона виступає проти європейської зеленої політики та скептично ставиться до НАТО.

Для України найбільша небезпека полягала б не обов’язково в негайному розриві відносин із Францією, а в непередбачуваності її політики. Париж міг би блокувати нові європейські рішення, критикувати санкції проти Росії та військову допомогу Україні, а також чинити опір подальшому розширенню ЄС. Автори зазначають, що вступ України особливо непокоїть “Національне об’єднання” через можливі наслідки для французького сільського господарства, додаткові витрати з бюджету ЄС і побоювання щодо подальшого посилення централізації Євросоюзу.

Тому автори радять Європі не панікувати, але заздалегідь готуватися до такого сценарію: краще вивчити позиції та можливості “Національного об’єднання”, зберігати обмежені канали діалогу з партією і, якщо Франція блокуватиме спільні рішення, створювати окремі коаліції держав, готових діяти разом. До них могли б увійти Німеччина, Польща, Італія, Іспанія, Велика Британія та європейські інституції.



РОЗДІЛ 2. АНАЛІТИЧНІ МАТЕРІАЛИ INSIGHT LAB

EEYES Insight Lab – аналітичний центр молодіжного напрямку міжнародного благодійного фонду «Ти створюєш націю» (UDoNation) / Eastern European Youth Empowerment Space (EEYES). Центр здійснює дослідження у сферах міжнародної та внутрішньої політики, економіки й безпеки, а також за потреби залучає експертизу у галузі фінансів. Пріоритетом діяльності Insight Lab є забезпечення високих стандартів якості аналітичних продуктів.

Дослідження в межах Insight Lab реалізуються як з ініціативи команди, так і на запит партнерів; вони можуть мати як публічний, так і обмежений характер поширення. Географічний фокус діяльності наразі охоплює Німеччину, Польщу та Францію з перспективою подальшого розширення на європейський регіон загалом. Водночас Insight Lab функціонує як платформа для професійного діалогу, обміну експертизою та розвитку сучасних дослідницьких підходів.

Важливим напрямом роботи центру є програма стажування для молодих дослідників. Insight Lab системно інвестує у розвиток нового покоління аналітиків, створюючи умови для набуття практичних навичок, професійного зростання та публічної презентації результатів їхньої роботи.

Матеріали, представлені у цьому журналі, підготовлені стажерами Insight Lab у межах стажувальної програми під супроводом команди центру.

Російський дрон на території країн НАТО: що це означає?

Олександра Попович

Застосування російськими військами безпілотних літальних апаратів із подальшим їх входженням у повітряний простір країн-членів НАТО стало одним із проявів посилення агресії у відносинах між Росією та Альянсом. Варто, однак, зауважити, що якщо на початку повномасштабного вторгнення більшість таких випадків розглядалися як поодинокі інциденти, то станом на 2026 рік простежується зміна їхнього характеру: вони дедалі частіше супроводжуються матеріальними збитками та створюють безпосередню загрозу цивільному населенню й критичній інфраструктурі.

Практика застосування Росією інструментів демонстрації сили та гібридного впливу не є новим фактором у багаторічних відносинах із безпековим блоком. Попри це, на відміну від традиційних методів: масштабних військових навчань поблизу кордонів Альянсу (зокрема серії навчань «Запад»), небезпечних польотів військової авіації, демонстрації військово-морської присутності в Балтійському та Чорному морях, а також кібератак — інциденти з безпілотними літальними апаратами характеризуються безпосереднім порушенням повітряного простору держав-членів НАТО.

Усі зазначені вище традиційні інструменти російського тиску на Альянс здебільшого можна віднести до діяльності у так званій «сірій зоні», оскільки вони залишалися нижче порогу відкритого військового зіткнення між Росією та НАТО. Саме тому у зв'язку зі зростанням кількості інцидентів за участю безпілотних літальних апаратів постає питання, чи є вони випадковим наслідком бойових дій на території України, чи свідчать про еволюцію російської моделі взаємодії з НАТО, спрямованої на перевірку меж реагування Альянсу. Від відповіді на це питання залежить оцінка ризиків для європейської безпеки, вироблення ефективних механізмів стримування та прогнозування подальшої динаміки відносин між сторонами.

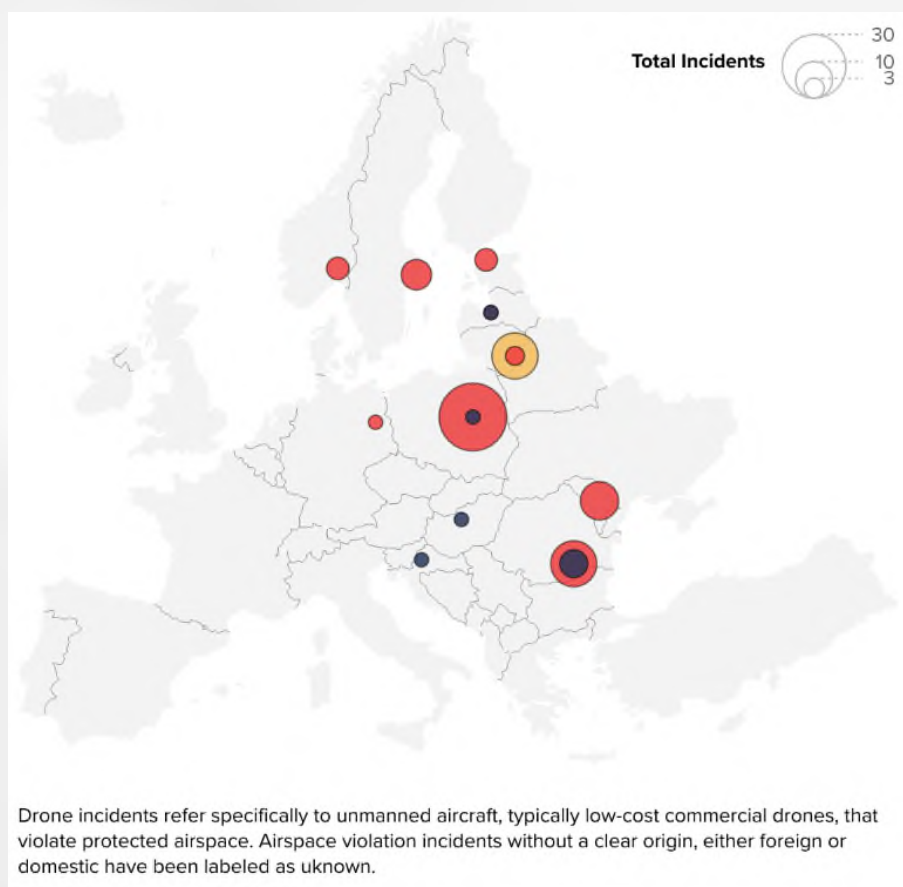
Що ж це таке: випадковість, провокація чи перевірка реакції?

Підходячи до аналізу та конкретної відповіді на питання дослідження, варто розуміти, що достовірно визначити характер кожного окремого інциденту досить складно через обмеженість доступної інформації та складність аналізу намірів російської сторони. Однак для суб'єктивного визначення можливої тактики використання дронів доцільно застосувати однакові критерії для порівняння та оцінювання кожного випадку. Таким чином, варто розпочати з визначення можливих характеристик для здійснення цього дослідження.

На мою думку, доцільними критеріями є близькість до кордону з Україною, адже це дозволяє зрозуміти, чи міг літальний об'єкт потрапити на територію країн НАТО внаслідок відхилення від курсу під час атаки на Україну. Наступним критерієм є повторюваність і частота подібних інцидентів. Разовість і відсутність сталого патерну атак можуть свідчити про їх спорадичний та випадковий характер, тоді як систематичне повторення подібних випадків потребує іншого пояснення. Не менш важливу роль відіграє показник завдання шкоди матеріальним об'єктам, спорудам та особам, адже він дозволяє відстежити та приблизно визначити можливу мету польоту дрона. Однак одним із найважливіших факторів є розуміння контексту здійснення атак та послідовної реакції обох сторін на подібні інциденти, саме це дає змогу більш обґрунтовано оцінити можливу цілеспрямованість дій.

Чи можливо розглядати інциденти потрапляння російських дронів на територію НАТО як випадкові? Насправді це досить складне питання, яке може мати різні відповіді залежно від періоду, в якому воно розглядається. Однак у контексті подій, що відбулися станом на серпень 2026 року, досить складно називати всі подібні інциденти випадковими.

Перш за все, розглядаючи критерій відстані, у багатьох випадках логічним є висновок про відносну близькість інцидентів до території України. Зокрема, найбільше таких інцидентів серед союзників фіксувала Румунія, яка через безпосередню близькість до Одеської області неодноразово зазнавала потрапляння російських безпілотників на свою територію з акваторії Чорного моря. Подібна закономірність певною мірою спостерігається і щодо Польщі та країн Балтії. Така географічна близькість є аргументом на користь гіпотези випадковості, оскільки дрони, які використовуються для атак на українські об'єкти поблизу кордону, потенційно можуть відхилитися від запланованого маршруту або перетинати кордон унаслідок роботи засобів проти-повітряної оборони та радіоелектронної боротьби.



Водночас географічний критерій не може повністю пояснити всю сукупність інцидентів. Розширення географії випадків за межі безпосереднього прикордонного простору України послаблює аргумент про те, що всі порушення повітряного простору НАТО є лише наслідком випадкового відхилення дронів від початкової цілі. Особливо важливим у цьому контексті є поява випадків у державах, які знаходяться на значній відстані від українського кордону. Сам по собі цей фактор не є прямим доказом цілеспрямованості, однак він ускладнює пояснення всіх інцидентів виключно випадковістю та потребує врахування інших критеріїв.

Проте беручи до уваги появу російських літальних апаратів поблизу військових об'єктів на території країн НАТО, зокрема на території Бельгії та Нідерландів, і їхню віддаленість від кордону з Україною теза про випадкове потрапляння потребує додаткового обґрунтування. Поява «невідомого» безпілотного апарата поблизу військових чи критичних об'єктів сама по собі не доводить розвідувального призначення, однак може свідчити про потенційний інтерес до конкретних об'єктів та посилює аргумент на користь навмисного характеру таких дій. Таким чином, теорія випадковості не є доцільною для використання, при застосуванні цього критерія.

Наступним критерієм оцінювання гіпотези випадковості є частота атак. Тут можна помітити суттєве збільшення кількості інцидентів порівняно з 2022 роком, коли подібні випадки були переважно одиничними. Натомість у подальші роки можна простежити тенденцію до збільшення кількості випадків перебування російських безпілотників на території або в повітряному

просторі країн-членів НАТО. За результатами приблизних розрахунків авторки статті на основі відкритих даних, можна стверджувати, що більше 55% випадків за весь період припадає саме на 2025 рік. Така концентрація інцидентів у межах одного року свідчить не лише про збільшення їхньої частоти, але й про зміну масштабу проблеми. Відповідно, повторюваність подібних випадків дедалі складніше пояснювати виключно як сукупність окремих випадкових відхилень. При розгляді цього критерію варто також звернути увагу на кількість дронів, які застосовуються під час одного інциденту. Поява близько 20 безпілотників у повітряному просторі Польщі 9–10 вересня 2025 року суттєво послаблює гіпотезу випадковості, оскільки йдеться вже не про одиначне відхилення окремого літального апарата, а про масштабне проникнення значної кількості БПЛА. За оцінками Інституту вивчення війни (ISW), ця операція могла бути підготовлена Росією заздалегідь протягом кількох місяців, що додатково ставить під сумнів її випадковий характер. Окремо варто звернути увагу на використання дронів-імітаторів, зокрема «Гербер», які могли застосовуватися для збільшення кількості повітряних цілей та ускладнення роботи систем протиповітряної оборони. Таким чином, масштаб, підготовленість та різноманітність використаних БПЛА можуть свідчити не лише про провокативний характер інциденту, але й про можливість перевірки спроможності та реакції НАТО на масоване проникнення безпілотників.

Розгляд наступного показника (рівня завданої шкоди) є досить суб'єктивним, однак разом із тим доцільним для використання. Варто простежити тенденцію до зростання потенційної небезпеки таких інцидентів. Якщо розглядати випадки у 2022 та 2023 роках, то значна частина з них мала транзитний характер або завершувалася падінням уламків без безпосереднього ураження цивільних об'єктів. Натомість надалі фіксуються випадки падіння дронів, утворення вибухів, пошкодження споруд і безпосереднього ураження цивільної інфраструктури, а також непрямой шкоди, зокрема внаслідок перебування ударних або розвідувальних БПЛА поблизу критичної та військової інфраструктури держав-членів НАТО. Так, наявність випадків прямого влучання в цивільну інфраструктуру та завдання шкоди цивільному населенню, як це сталося в Румунії 29 травня 2026 року, є важливим аргументом для оцінювання характеру таких інцидентів. У цьому випадку російський дрон увійшов у повітряний простір Румунії та влучив у житловий будинок, унаслідок чого цивільні отримали поранення. Таким чином, тенденція до збільшення рівня шкоди майну та населенню держав-членів НАТО послаблює пояснення таких інцидентів виключно як випадкових наслідків бойових дій та разом з іншими критеріями може свідчити про зростання навмисного характеру таких дій.

Безсумнівно, розгляд усіх критеріїв комплексно є важливим для підтвердження чи спростування гіпотези, однак розгляд цього питання у вакуумі є неможливим. Аналізуючи випадковість інцидентів, варто звернути увагу на один із ключових критеріїв — реакцію сторін та контекст подій в Україні й у світі. Саме послідовність подій дозволяє зрозуміти, чи залишаються інциденти окремими випадками, чи поступово впливають на поведінку та політику обох сторін.

Так можна виділити щонайменше три показові періоди реакції. Першим є друге півріччя 2023 року, коли після серії падінь російських БПЛА на території прикордонних румунських сіл Альянс посилив свою присутність у регіоні, зокрема розгорнув додаткові засоби повітряного спостереження та винищувальну авіацію. Ці події відбувалися на тлі загострення ситуації в Чорноморському регіоні після припинення Росією участі в Чорноморській зерновій ініціативі та активізації російських атак на українські порти. Таким чином, уже на цьому етапі інциденти з БПЛА почали розглядатися не лише як локальна проблема, а й у ширшому контексті безпеки східного флангу НАТО.

Наступним показовим етапом є 2025 рік. 10 вересня численні російські дрони порушили повітряний простір Польщі, після чого Польща звернулася до НАТО на основі статті 4 Вашингтонського договору щодо проведення консультацій. У відповідь НАТО активувало додаткові засоби протиповітряної оборони та спостереження, а 12 вересня оголосило про запуск програми “Eastern Sentry”, спрямованої на посилення оборони східного флангу. Сам НАТО наголосив, що інцидент 10 вересня не був ізольованим випадком, а частота небезпечних дій Росії в повітрі на східному фланзі зростає.

Ще одним показовим періодом є кінець весни — початок літа 2026 року. Він є особливо важливим не лише для спростування гіпотези про випадковість, а й для оцінки еволюції реакції держав-членів НАТО, зокрема на національному рівні. Саме 29 травня 2026 року російський дрон влучив у житловий будинок у Румунії, завдавши шкоди цивільній інфраструктурі та поранивши цивільних. Цей випадок уже суттєво відрізняється за характером наслідків від ранніх інцидентів, оскільки порушення повітряного простору супроводжувалося безпосереднім ураженням цивільного об'єкта, що продемонструвало практичну необхідність застосування законодавчих змін, ухвалених у лютому 2025 року, які розширили повноваження Румунії щодо реагування на БПЛА, зокрема дозволивши їхнє безпосереднє знищення за визначених законом умов.

Однак неможливо сприймати ситуацію лише через реакцію однієї сторони, тому варто також звернути увагу на російську сторону. Якщо на початкових етапах можна було помітити заперечення або спростування фактів інцидентів із дронами, то в подальшому російська сторона дедалі частіше реагувала на посилення НАТО через звинувачення Альянсу в ескалації та втягуванні у війну. Така зміна риторики також має значення, оскільки демонструє, що Росія сприймає реакцію НАТО не лише як технічну відповідь на окремі інциденти, а як частину ширшого протистояння.

Що ж далі у відносинах РФ та НАТО?

Таким чином, цілком логічним є припустити, що гіпотеза про випадковість інцидентів як універсальне пояснення є недостатньою. Окремі випадки дійсно можуть бути результатом відхилення дронів від курсу, роботи засобів радіоелектронної боротьби або інших непередбачуваних факторів. Однак, звернувши увагу на еволюцію реакції як Альянсу, так і РФ та простеживши їхню взаємодію, можна помітити тенденцію до зміни патернів поведінки. Водночас спростування однієї гіпотези не означає автоматичного підтвердження іншої. Тому, відкидаючи теорію про випадковість як універсальне пояснення через недостатність доказів на її користь, варто розглянути, чому гіпотеза про провокацію або перевірку реакції є більш доречною. Сукупний аналіз усіх критеріїв дозволяє говорити не лише про провокативний характер окремих дій, а й припускати наявність певної стратегічної мети за ними. Зокрема, врахування контексту інцидентів, реакції Альянсу та подальшої зміни характеру дій РФ дає підстави припускати, що такі випадки можуть використовуватися для перевірки меж допустимого та оцінювання можливих відповідей НАТО.

Таким чином, найбільш імовірним сценарієм подальшої поведінки РФ може бути продовження провокативних дій із поступовою перевіркою різних варіантів реакції Альянсу, що потенційно може супроводжуватися подальшим підвищенням рівня ескалації.

*Цю статтю було написано для журналу “Think Tanks Essentials”.
Погляди, висловлені у статті, належать її автору.*

Від «Шахеда» до спільного виробництва: чого Росія та Іран навчилися один в одного

Ярина Василик

Вступ

З 2022 року російсько-іранська співпраця у сфері безпілотних систем пройшла шлях від постачання готових Shahed до локалізованого виробництва та взаємного обміну технологіями й бойовим досвідом. Отримавши іранську платформу, Росія масштабувала її виробництво, модифікувала відповідно до досвіду війни проти України та до 2026 року почала передавати частину вдосконалених рішень назад Ірану. Це перетворило початкову модель «постачальник - отримувач» на двосторонній цикл військово-технологічного навчання.

Початкова модель співпраці

Shahed-136 - розроблений Іраном далекобійний ударний безпілотний літальний апарат (БПЛА) односторонньої дії, призначений для ураження наземних цілей. Його відносно проста конструкція, велика дальність і низька вартість дають змогу застосовувати такі системи у значній кількості.

Російські Shahed базуються на іранській конструкції, а їхнє використання Росією почалося з прямих закупівель безпілотників в Ірану восени 2022 року. На початку 2023 року Іран доставив близько 600 дронів у розібраному вигляді для складання в Росії, після чого їхнє виробництво було локалізоване.

Росія швидко інтегрувала іранські БПЛА у війну проти України, використовуючи відносно дешеві ударні дрони для атак на міста та інфраструктуру. Масовані запуски створювали асиметричне навантаження на українську протиповітряну оборону (ППО), змушуючи її витратити обмежені ресурси на перехоплення.

Однак співпраця швидко вийшла за межі експорту готового озброєння. Іран передавав Росії компоненти та пов'язані з ними технології. За даними Міністерства фінансів США, Міністерство оборони та логістики Збройних сил Ірану співпрацювало з Росією щодо фінансування та виробництва ударних БПЛА іранської конструкції в «Алабузі» (особлива економічна зона, де розташовані потужності з виробництва ударних БПЛА Shahed/Geran) у межах контракту вартістю 1,75 млрд доларів. Наприкінці 2022 року російські посадовці також вели переговори із Sahara Thunder — підпорядкованою Міністерству оборони та логістики Збройних сил Ірану компанією, що відповідає за комерційну діяльність. Переговори стосувалися постачання та виробництва в «Алабузі» тисяч БПЛА на рік.

Наступним етапом стала локалізація. Росія розгорнула в «Алабузі» виробництво власної версії Shahed-136 -Geran-2 з планом поступово локалізувати більшу частину виробництва Geran-2 у Росії.

Російський етап адаптації

Локалізація фабрик не означала простого копіювання Shahed-136. У ході війни Росія поступово змінювала як конструкцію безпілотників, так і тактику їх застосування у відповідь на

українські засоби протидії. Одним із напрямів модернізації стала система навігації. Російські Geran-2 отримали модулі «Комета», які вже використовувалися в інших російських БПЛА та дали змогу спростити внутрішню електроніку системи навігації. Зміни торкнулися і конструкції: замість характерного для іранських Shahed легкого стільникового матеріалу в досліджених російських зразках використовували скловолокно та шари вуглецевого волокна.

Еволюціонувала і тактика застосування. Росія почала комбінувати ударні Geran із дешевшими безпілотниками-приманками та іншими засобами повітряного нападу, формуючи змішані ударні хвилі, покликані ускладнити і зробити більш дорогавартісною роботу української ППО. Водночас Москва масштабувала виробничі та пускові можливості: з вересня 2024 року до березня 2025 року кількість запусків Shahed зросла приблизно з 200 до понад 1 000 на тиждень. Зміна напрямку трансферу

До 2026 року частина напрацювань, отриманих Росією в процесі адаптації Shahed, почала рухатися у зворотному напрямку. Одним із найбільш показових прикладів стала передача Ірану системи супутникової навігації Kometa-M, яка підвищує точність Shahed-136 та їхню стійкість до глушіння.

Обмін не обмежується технічними компонентами. У свідченнях перед Комісією з безпеки та співробітництва в Європі у квітні 2026 року старший науковий співробітник Вашингтонського інституту Аарон Зелін зазначав, що Москва передавала Тегерану компоненти для модифікації Shahed та ділилася досвідом використання безпілотників проти України. Зокрема, йшлося про рекомендації щодо проведення координованих атак кількома дронами одночасно. Отже, зворотний трансфер охоплює не лише технології, а й тактичні практики, перевірені Росією у війні проти України.

Ще одним рівнем співпраці став обмін розвідувальними даними для наведення ударів. За даними The Washington Post, Росія передавала Ірану інформацію про розташування американських військових об'єктів на Близькому Сході, зокрема кораблів та авіації. Це розширює співпрацю від технологічного й тактичного трансферу до розвідувальної підтримки бойових операцій.

Межі взаємного навчання

Російський досвід застосування Shahed не може бути повністю перенесений в інше оперативне середовище. Аналіз російської кампанії проти України показує, що характер застосування ракет і безпілотників залежить, зокрема, від розташування та цінності цілі й дальності удару. Відносно дешеві Shahed дають Росії змогу збільшувати масштаб, частоту та географічне охоплення ударної кампанії.

Варіативність у виборі засобів ураження простежується і в іранській кампанії в Перській затоці. За оцінкою CSIS (Center for Strategic and International Studies), проти ОАЕ та Саудівської Аравії переважали дроніві атаки, тоді як для інших цілей співвідношення дронів і ракет відрізнялося. Такий розподіл вказує на адаптацію складу ударів до конкретних цілей: дрони використовувалися для тривалого й відносно дешевого тиску, тоді як ракети - там, де пріоритетними були швидкість, надійність ураження або сигналізування щодо військових об'єктів.

Отже, Росія та Іран можуть переймати технології й тактичний досвід одне одного, але конкретні способи їх застосування залежать від цілей і оперативного середовища. Спільним є не конкретний шаблон ударів, а принцип адаптації наявних засобів до умов конкретної кампанії.

Висновки

Росія та Іран не просто розвивають виробництво Shahed, а й адаптують технологію та способи її застосування до власних потреб. Росія перетворила отриману від Ірану платформу на масштабовану систему виробництва та адаптувала її конструкцію і тактику до війни проти України. Іран, своєю чергою, отримує російські технологічні модифікації та досвід їх бойового застосування. Водночас конкретні російські тактики не можуть автоматично переноситися на Близький Схід: їх використання залежить від цілей і оперативного середовища. Для України це означає необхідність системно обмінюватися з партнерами даними про модифікації Shahed/Geran і тактику їх застосування та координувати санкційний і експортний контроль щодо спільних ланцюгів постачання компонентів.

Якщо нинішня модель співпраці збережеться, російсько-іранський обмін, імовірно, дедалі більше нагадуватиме цикл взаємної адаптації: рішення, випробувані однією стороною в бойових умовах, доопрацьовуватимуться та інтегруватимуться іншою. Для України це створює ризик повторного потрапляння на поле бою модифікацій Shahed, удосконалених уже з урахуванням досвіду їх застосування на Близькому Сході.

*Цю статтю було написано для журналу "Think Tanks Essentials".
Погляди, висловлені у статті, належать її автору.*

Диверсії як інструмент зовнішньої політики: як Росія тестує межі реакції Заходу?

Катерина Кот

Росію та її союзників не раз звинувачували в організації нападів та інших інцидентів по всій Європі з моменту вторгнення в Україну. Метою Москви у таких випадках визначають підірвання підтримки України та спроби посіяти страх, розколоти європейські суспільства та виявити слабкі місця в системі безпеки континенту.

Вплив диверсій полягає насамперед у створенні передумов для застосування сили: таке зниження ефективності дає час, простір та більш сприятливі умови для результативної дії інших засобів. Ця роль особливо підкреслює, чому технологічні зміни навряд чи змінять ключові характеристики диверсій та їхню подальшу роль у світовій політиці. Після початку повномасштабного вторгнення в Україну у 2022 році РФ розгорнула проти країн Заходу цілий спектр підтверджених видів диверсій: регулярні порушення повітряного простору Румунії, Польщі та Естонії російськими дронами й ракетами, масштабні кібератаки на критичну та державну інфраструктуру, підпали військових і логістичних об'єктів, пошкодження підводних комунікацій у Балтійському морі, а також штучне створення міграційних криз на східних кордонах ЄС. У період після холодної війни, безумовно, відбулося надзвичайно багато змін в інформаційних технологіях, проте останні події свідчать про те, що саботаж цих технологій через кіберпростір часто має меншу силу впливу, ніж старомодні кінетичні дії. Той факт, що нещодавня серія диверсій проти членів НАТО в Європі переважно здійснювалася традиційними, а не кіберзасобами, підкреслює цей розподіл, визначають Джошуа Ровнер, Рорі Кормак та Леннарт Машмейер у своєму дослідженні «Пісок у шестернях: саботаж у світовій політиці».

Так, 16 листопада 2025 року у Польщі машиніст поїзда на лінії між Варшавою та Любліном повідомив про проблеми з колією. Під час візиту на місце події прем'єр-міністр зазначив, що інцидент стався на залізничній лінії, яка має вирішальне значення для доставки гуманітарної допомоги в Україну, а польські чиновники заявили, що впевнені: на ділянці колії було підірвано вибуховий пристрій, а згодом на тій самій лінії було виявлено пошкодження контактної мережі, та обидва випадки, ймовірно, є актами саботажу.

Чоловіком, який, за словами офіційних осіб, стояв за нападом на польську залізницю, що доставляє вантажі до України, є Євген Іванов — українець, засуджений за співпрацю з російською військовою розвідкою з метою організації підпалів у магазинах будівельних матеріалів, кафе та на заводі з виробництва дронів в Україні, як свідчать судові документи. Іванов, який покинув Польщу після нападу там, працював на Юрія Сізова, офіцера російської військової розвідки ГРУ. Доручення роботи таким особам із кримінальним минулим, як Іванов, означає, що Росії не доводиться ризикувати висококваліфікованими співробітниками.

Тактика гібридної війни Росії регулярно ґрунтується на використанні «одноразових» агентів — осіб, яких залучають для виконання окремих завдань. Цих агентів вербують та надають їм інструкції переважно через соціальні мережі. Потім їх використовують для здійснення низки диверсійних операцій та операцій впливу в Європі в інтересах Росії. Подальша доля цих агентів мало цікавить Москву, оскільки їхні одноразові місії не дають їм можливості дізнатися про конкретний масштаб і глибину діяльності російської розвідки. Використання таких «посередників» робить операції значно дешевшими для РФ, при цьому продовжуючи створювати

значне навантаження на європейські служби безпеки, адже транскордонні операції вимагають від країн широкої співпраці в рамках розслідувань. Саме тому у листопаді 2025 року Центр аналізу європейської політики (СЕРА) започаткував новий масштабний проєкт — «Захищати, відбивати, стримувати: протидія тіньовій війні Росії» — з метою сприяння створенню основи для нового трансатлантичного підходу до стримування.

На прес-конференції в Брюсселі президент Фінляндії Олександр Стабб зазначив, що європейські країни повинні зберігати «холодну голову». А ще застеріг від надмірної реакції на випадки ймовірних провокацій з боку Росії, наголосивши: «На жаль, це — нова норма. Росія намагається дестабілізувати наші суспільства за допомогою інформаційних та інших кампаній».

У своїй статті «За словами офіційних осіб, Росія прагне виснажити слідчі ресурси Європи за допомогою своєї диверсійної кампанії» авторка Емма Бурроуз пише, що цей випадок саботажу в Польщі є одним із 145 (станом на грудень 2025 року) інцидентів у базі даних агентства «Асошіейтед Прес», які, за словами західних чиновників, є частиною кампанії з дестабілізації по всій Європі, організованої Росією. Інциденти варіюються від забивання вихлопних труб автомобілів пінопластом, що розширюється, у Німеччині, до змови з метою встановлення вибухових пристроїв на вантажних літаках. Серед них — підпали магазинів та музею, хакерські атаки, спрямовані проти політиків та об'єктів критичної інфраструктури, шпигунська діяльність угруповання, засудженого у Великій Британії, та інші.

Деякі з них могли мати катастрофічні наслідки, зокрема масові жертви, як, наприклад, під час вибухів посилок на логістичних об'єктах у Німеччині та Великій Британії. Західні чиновники заявили, що підозрюють: ці посилки були частиною ширшого задуму російської розвідки з метою підкласти бомби на вантажні літаки, що прямували до США та Канади.

В іншому випадку західні розвідувальні служби викрили, за їхніми словами, російський замах на вбивство керівника великого німецького виробника зброї, який постачає озброєння в Україну.

Європейські органи влади розслідують кілька прецедентів пошкодження інфраструктури на дні Балтійського моря, зокрема електрокабелю, що з'єднує Естонію та Фінляндію. Фінські органи влади затримали судно, яке підозрюють у приналежності до російського «тіньового флоту», що використовується для обходу санкцій, після того, як цей та інші кабелі були пошкоджені.

Коли на фейковому веб-сайті Міністерства оборони Франції з'явилася інформація про те, що громадян призивають воювати в Україні, французький міністр засудив це як російську дезінформацію. Німецькі власті підозрюють, що за кампанією з блокування десятків вихлопних труб автомобілів напередодні національних виборів стояла Росія, за словами представника європейської розвідки, який висловився на умовах анонімності, щоб обговорити делікатні питання.

У жовтні 2025 року британський суд засудив п'ятьох чоловіків до багаторічного тюремного ув'язнення за участь у підпалі лондонського складу, на якому зберігалися пристрої супутникового зв'язку, призначені для України. Під час винесення вироку суддя зазначив, що цей замах було організовано в інтересах російського воєнізованого угруповання «Вагнер» і що він був частиною широкомасштабної диверсійної кампанії.

Барт Шуурман, професор з питань тероризму та політичного насильства, вважає, що окрім очевидної мотивації цих атак у спробі підірвати громадську підтримку України, є й елемент демонстрації сили: таким чином Москва нагадує лідерам Європейських країн про свій вплив і можливості.

Російський підхід до ведення війни «призводить до ескалації не випадково, а навмисно» визначають у роботі «Війна без кінця: “тіньова” війна Росії» Андрій Солдатов та Ірина Бороган. Вступ Швеції до НАТО спричинив вирішальну зміну балансу сил у Балтійському регіоні. Країна відмовилася від своєї 212-річної політики нейтралітету, що діяла з часів, коли Наполеонівські війни сколихнули Європу, фактично перетворивши Балтійське море на «озеро НАТО», що призвело до активізації діяльності російських спецслужб: Росія посилила поширення дезінформації, кібератаки та таємні операції. Служба безпеки Швеції (Säkerhetspolisen, SÄPO) повідомила в березні, що Росія застосовує нову тактику шпигунства. Російська розвідка шукає потенційних рекрутів, які страждають від наркотичної залежності, для здійснення диверсійних атак у Швеції, у зв'язку з чим поліції рекомендується посилити спостереження. Як повідомляється, наркозалежних обирають через їхній низький соціальний статус і, як наслідок, фактичну непомітність — цінні якості для шпигунів.

Російські розвідники у Швеції працюють у багатьох російських установах. За оцінками SÄPO, приблизно 30 відсотків співробітників російського посольства за адресою Gjörwellsgatan 31 у Стокгольмі — це розвідники, до обов'язків яких входить вербування та управління агентами. Крім цього, SÄPO встановило, що Російська православна церква у Швеції є другим «легітимним» ресурсом, який Москва використовує для збору розвідданих, здійснення впливу або інших дій, що становлять загрозу безпеці.

Реакцією ЄС стало запровадження нової системи санкцій 8 жовтня 2024 року, спрямованої проти фізичних та юридичних осіб, пов'язаних із дестабілізуючими гібридними загрозами з боку Російської Федерації щодо ЄС та його союзників, що охоплюють втручання у виборчий процес, саботаж інфраструктури, дезінформацію, кібератаки та використання мігрантів у своїх цілях. Згодом, 20 травня 2025 року, цей режим санкцій було розширено, поширивши його сферу застосування на матеріальні активи, пов'язані з цими зловмисними діями, такі як судна, літаки, нерухомість та фізичні елементи мереж, а також на операції за участю фінансових установ та сервісів криптоактивів.

Відтак, сучасна російська гібридна кампанія в Європі перетворилася на масштабну та багатовимірну загрозу, що переслідує низку чітких стратегічних цілей. Головним вектором атак є підірив логістики та підтримки України. Удари цілеспрямовано наносяться по критичних вузлах постачання, таких як залізниці в Польщі, склади з технікою у Великій Британії та навіть керівництво оборонних підприємств у Німеччині.

Водночас Москва прагне виснажити ресурси європейських безпекових відомств. Через масштаби та різноманітність дрібних інцидентів, яких у базі Associated Press зафіксовано вже понад 180 (станом на серпень 2026 року), спецслужби змушені розпорошувати фінанси та зусилля на розслідування локальних подій. Усе це супроводжується психологічним тиском та демонстрацією сили. Створюючи загрозу масових жертв, Росія нагадує західним лідерам про свою здатність діяти глибоко в їхньому тилу та намагається посіяти паніку в суспільстві.

Задля досягнення цих цілей російська розвідка суттєво адаптувала свою тактику. Всупереч очікуванням епохи цифровізації, пріоритет віддається традиційним кінетичним методам — фізичний саботаж, підриви та підпали часто виявляються більш руйнівними, ніж кібератаки.

При цьому спецслужби РФ (зокрема ГРУ) змінили підхід до виконавців, зробивши ставку на «одноразових» агентів. Вербуючи через соцмережі осіб із кримінальним минулим або маргіналізовані групи, як-от наркозалежних у Швеції, Росія здешевлює свої операції та уникає прямої відповідальності. Координація цієї агентурної мережі здійснюється під надійним легальним прикриттям: використовуються дипломатичні установи та релігійні організації, такі як Російська православна церква.

Ця кампанія вирізняється високою комплексністю гібридних загроз. Росія органічно поєднує прямий фізичний саботаж з інформаційними диверсіями та штучно індукованими міграційними кризами на кордонах Фінляндії, Польщі та країн Балтії.

Відповідно, перед Заходом постають безпрецедентні виклики. Європа змушена прийняти цю реальність як «нову норму», усвідомлюючи, що диверсії є навмисною ескалацією. Як наголошує президент Фінляндії, західним суспільствам критично важливо зберігати «холодну голову», не піддаватися на провокації та не підігрувати Кремлю в поширенні страху. Транскордонний характер атак диктує гостру потребу в інституційній консолідації. Запуск ініціатив на кшталт проекту СЕРА свідчить про те, що Європа готова перейти від реактивного розслідування поодиноких фактів до створення єдиної, системної стратегії стримування російської тіньової війни.

*Цю статтю було написано для журналу "Think Tanks Essentials".
Погляди, висловлені у статті, належать її автору.*

Коли диверсія стає нападом: чи застосовна стаття 5 НАТО до російських гібридних операцій?

Юлія Лончина

Вступ

Гібридні операції стали одним із провідних інструментів сучасної агресії. Комбінація новітніх технологій із важелями прихованого тиску дає агресору змогу втручатися у внутрішні справи іншої держави зсередини, не перетинаючи водночас поріг прямого збройного зіткнення. Це руйнує традиційне уявлення про безпеку й остаточно розмиває межу між миром і війною.

За офіційною термінологією НАТО, гібридні методи охоплюють військові та невійськові засоби, що поділяються на приховані та відкриті, як-от: дезінформація, кібератаки, економічний та політичний тиск, саботаж, диверсії та втручання у виборчий процес. Гібридні методи використовуються для того, щоб посіяти сумніви у свідомості населення та дестабілізувати суспільство.

Гібридні операції — широке поняття, що охоплює різноманітні загрози. Ця робота зосереджується на одному з їхніх видів — диверсіях, тобто фізичних діях, спрямованих на безпосереднє підірвання матеріально-технічного та безпекового потенціалу держави, а також завдання шкоди її інфраструктурі та населенню. На відміну від менш помітних політичних та економічних важелів впливу, диверсії напряду загрожують національній безпеці й порушують надзвичайно важливе питання: коли саме гібридна операція досягає рівня збройного нападу?

Аналіз статті 5 Північноатлантичного договору

Стаття 5 Північноатлантичного договору передбачає, що збройний напад на одного з членів НАТО вважається нападом на Альянс загалом та зобов'язує кожного союзника надати допомогу. Ця допомога може включати будь-які дії, які держави-члени вважатимуть потрібними для відновлення та підтримання безпеки в Північноатлантичному регіоні.

Формально 5-та стаття встановлює обов'язок колективної оборони, проте дає державам-членам простір для розсуду щодо форми допомоги, не накладаючи на них універсальних зобов'язань. Вона може передбачати військові, консультаційні, логістичні, контррозвідувальні та інші заходи.

Складнішим питанням є брак конкретики у визначенні самого поняття «збройний напад». Північноатлантичний договір не містить спеціальної процедури активації. Рішення завжди ухвалюються в межах конкретної ситуації залежно від обставин, а після нападу Північноатлантична рада зобов'язана зустрітися, проконсультуватися та дійти консенсусу.

У НАТО є власне пояснення невизначеності щодо застосування статті 5. Вважається, що чіткий поріг відсутній не випадково. Колишній генеральний секретар НАТО Єнс Столтенберг заявляв, що Альянс не хоче давати противнику можливість заздалегідь знати, де саме проходить межа статті 5. Отож, відсутність чітко окреслених меж дає політичну перевагу та простір для маневру.

Така гнучкість залишає простір для інтерпретації збройного нападу. На перший погляд, терористичний акт 11 вересня 2001 року (перший і донині єдиний випадок використання статті 5) не відповідав класичній формі збройного нападу у вигляді протистояння двох держав. Тож саме гнучкість статті 5 дозволила союзникам визнати цю ситуацію підставою для застосування принципу колективної оборони.

Проте зворотний бік такої абстрактності – повна неокресленість меж загрози, адже немає критеріїв, за якими можна чітко визначити, коли саме гібридна атака перестає бути окремим інцидентом і набуває характеру збройного нападу.

Саме ця невизначеність створює сприятливе для агресора середовище - сіру зону. По-перше, розхитування ситуації в країні гібридними методами потребує менше ресурсів, ніж прямий збройний конфлікт. Крім того, завдяки такій стратегії агресор уникає спротиву з боку цивільного населення, масштабних військових втрат, а також частини політичних і міжнародно-правових наслідків, пов'язаних із відкритою агресією.

Російські гібридні операції

Ця проблема особливо проявляється у характері сучасних російських операцій проти держав-членів НАТО. Диверсії на території країн-членів відбувалися і раніше, але початок повномасштабного вторгнення Росії в Україну призвів до збільшення їхньої кількості та масштабу. Останні роки демонструють численні випадки диверсій, порушень повітряного простору, підпалів, актів саботажу та інших фізичних атак, за якими західні спецслужби простежують російський вплив.

2024 рік став викликом для низки європейських країн у зв'язку з різким збільшенням кількості гібридних атак. Основною метою Москви було перешкоджання постачанню допомоги Україні та підрив безпеки в Польщі, Німеччині та інших країнах за допомогою завербованих через інтернет «одноразових» виконавців.

У травні у Варшаві відбувся підпал торгового центру, який польська влада визнала терористичним актом. Також фіксувалися й інші спроби підпалів інфраструктури. Злочини були скоєні руками третіх осіб, завербованих російською військовою розвідкою - ГРУ. За офіційною версією, головною метою злочинів було залякування суспільства.

Водночас Німеччина зіткнулася з безпрецедентною хвилею підпалів та диверсій, спрямованих проти її оборонного сектору, критичної інфраструктури та логістики. Німецькі спецслужби та уряд пов'язують більшість цих інцидентів із гібридною війною Росії, спрямованою на зрив постачання військової допомоги Україні.

Зокрема, російські диверсійні групи підозрюються у підпалі металургійного заводу компанії Diehl у Берліні, яка допомагає Україні з ППО. Окремо розслідувався випадок із загорянням авіавантажу DHL у липні 2024 року, у якому західні спецслужби простежили російський слід.

Неодноразово від диверсій страждає регіон Балтійського моря, переповнений кораблями так званого "тіньового флоту". Російські нафтові танкери стали новим плацдармом для гібридних операцій. У зв'язку з цим почастишали диверсії, спрямовані проти інфраструктури на морському дні, а також акти саботажу та шпигунства в прибережній зоні. Найбільша шкода від тіньового флоту завдається кабелям передавання даних та газогонам, прокладеним на дні моря.

Європейські уряди вважають це гібридною відповіддю на підтримку України, а щоб чинити опір, НАТО змушене посилювати контррозвідку, стеження та перевірки підозрілих кораблів. Аналітики зазначають: диверсії на дні моря є нічим іншим, як частиною однієї кампанії, і не мають розглядатися як поодинокі випадковості.

Безпрецедентними є численні випадки порушення повітряного простору країн НАТО ракетами та безпілотниками, зокрема на території Польщі й Румунії. Це є прямою загрозою інфраструктурі, а також життю та безпеці громадян.

Прикладом є події в Польщі у вересні 2025 року, коли 19 російських безпілотників увійшли в польський повітряний простір. У відповідь польські та союзницькі сили були приведені в готовність. Варшава ініціювала консультації за статтею 4 Північноатлантичного договору.

Кумулятивний ефект гібридних операцій

Водночас виникає питання, яким чином розглядати гібридні атаки, окремо чи сукупно, адже комбінація диверсій, кібератак та порушень повітряного простору несе значно більшу загрозу, ніж поодинокі випадки.

Отже, виникає дилема кумулятивного ефекту.

Загалом у НАТО немає офіційно прийнятого поняття кумулятивного ефекту для всіх гібридних операцій. Проте Альянс уже визнав необхідність врахування сукупного ефекту в окремих випадках. Наприклад, за результатами Брюссельського саміту 2021 року НАТО прямо визнає можливість кумулятивного ефекту у кіберсфері, коли сукупність окремих шкідливих дій за певних обставин може досягти рівня збройного нападу. Таким чином, Альянс визнає, що оцінка окремих дій не завжди повинна здійснюватися ізольовано, а їхній сукупний ефект може мати значення для правильної оцінки того чи іншого випадку.

Сьогодні цей підхід спрямований лише на протидію кібератакам, тому зарано стверджувати про існування єдиної схеми для всіх гібридних операцій. Водночас цілком логічно припустити, що така схема могла б бути використана у ширшому контексті. Якщо поодинокі інциденти не досягають рівня збройного нападу, то саме їхня взаємопов'язаність, спільне джерело загрози, інтенсивність та масштаб цілком змінюють оцінку ситуації. Отже, ключовим питанням є не просто те, чи досягає одна диверсія межі збройного нападу, а й те, чи створюється сукупність дій, кумулятивна загроза яких становить небезпеку для Альянсу.

Саме в цьому і полягає одна з найбільших переваг структури колективної оборони НАТО – розгляд кожної ситуації у її контексті разом із сукупністю обставин. Така стратегія дозволяє не прирівнювати кожну диверсію до нападу, тим самим уникаючи надмірної реакції та ескалації. Водночас вона дозволяє уникнути іншої крайності, за якої сукупність дій ворога розглядається лише як набір поодиноких і самостійних випадків.

Окрім того, варто пам'ятати, що використання статті 5 це лише один із можливих інструментів протидії російському тиску. Альянс має відпрацьований спектр заходів протидії та захисту. Посилення контррозвідувальних операцій, розвиток ППО, спільне озброєння, захист критичної інфраструктури, консультації, передбачені статтею 4 та економічна протидія тіньовому флоту — усе це означає, що відсутність застосування статті 5 не є сигналом бездіяльності.

Висновок

У підсумку не існує чіткої межі, після перетину якої гібридна операція переростає у збройний напад. Це дозволяє НАТО приймати рішення з урахуванням конкретної ситуації, не будучи надмірно юридично обмеженим.

При цьому окремий інцидент, який сам по собі не досягає порогу збройного нападу, не обов'язково має розглядатися у відриві від ширшої кампанії. Сукупний ефект взаємопов'язаних операцій може створювати якісно інший рівень загрози та має враховуватися під час її оцінки.

Найбільшою проблемою є не бездіяльність чи слабкість Альянсу, а прагнення агресора залишатися в сірій зоні та уникати відповідальності. Саме тому оцінка операцій має бути всебічною, щоб своєчасно виявляти сукупні стратегічні ризики, не зациклюючись на окремих провокаціях.

*Цю статтю було написано для журналу “Think Tanks Essentials”.
Погляди, висловлені у статті, належать її автору.*

Чи може оборонна промисловість стати новою спеціалізацією України в економіці ЄС?

Олена Мелконова

Сьогодні в новинах одночасно розгортаються дві історії, які на перший погляд не пов'язані, але насправді описують одне й те саме явище – прискорену мілітаризацію технологій навколо війни в Україні.

Перша історія про вісь Москва–Тегеран. У березні СБУ та Нацполіція викрили іранського генерала, який організував передачу Росії технологій виробництва дронів Shahed: за даними слідства, понад 13 тисяч ударних БПЛА, якими Росія атакувала українські міста, було випущено на заводі в Алабузі саме за іранською документацією, переданою в межах секретної домовленості між оборонними відомствами двох країн. А вже у липні Reuters повідомив, що американська розвідка перевіряє зворотний зв'язок: чи не Росія допомогла Ірану вдосконалити наведення дронів Shahed після ударів по об'єктах ЦРУ в Ер-Ряді та Іраку. Тобто технологічний обмін між Росією та Іраном давно перестав бути одностороннім, це вже повноцінна кооперація в реальному часі, де бойовий досвід, здобутий на українських містах, повертається назад у вигляді вдосконалених ракетних двигунів, антиглушильних систем та навігації.

Друга історія про Україну. 23 червня на європейському саміті з оборони й безпеки в Брюсселі єврокомісар з питань оборони й космосу Андрюс Кубілюс назвав українську оборонну промисловість найінноваційнішою у світі та закликав інтегрувати її в оборонну систему ЄС, а не просто фінансувати як реципієнта допомоги. За його оцінкою, виробництво зброї в Україні зросло у понад 50 разів порівняно з початком повномасштабного вторгнення. За розрахунками РНБО, виробничі спроможності українського ОПК у 2026 році оцінюються приблизно у 55 млрд доларів, і це вже не разовий сплеск, а стійка галузева траєкторія: понад 160 компаній випускають FPV-дрони сукупною потужністю понад 8 млн одиниць на рік, а перехоплювачі повітряних цілей нарощують виробництво у геометричній прогресії.

Спокуслива й поширена інтерпретація полягає в тому, що ці дві історії пов'язані причинно: мовляв, Україна опинилась у центрі найінтенсивнішої у світі гонки безпілотних технологій саме тому, що є полем випробування для авторитарної осі Росія–Іран. Ця теза приваблива, але вона плутає канал із причиною. Навіть якби Іран узагалі не передав Росії жодної технології Shahed, Росія все одно обстрілювала б українські міста цілодобово: крилатими ракетами Kalibr і X-101, балістичними «Іскандерами», власними дронами-камікадзе «Герань». Іранська кооперація здешевила й масштабувала терор, зробила його численнішим, але не вона є першопричиною того, що Україна перетворилася на світового лідера швидкості воєнних інновацій. Справжня причина фундаментальніша: Україна – єдина країна у світі, яка вже чотири роки веде повномасштабну оборонну війну на власній території проти супротивника, що постійно змінює тактику й арсенал, а отже змушена ітерувати конструкції зброї тижнями, а не роками, як класичні оборонні концерни. Саме цей досвід сьогодні перетворюється на актив, який Брюссель усе відвертіше називає стратегічним ресурсом для всього Євросоюзу.

Питання цієї статті: чи достатньо цього, щоб оборонна промисловість стала повноцінною економічною спеціалізацією України в межах ЄС, подібно до того, як автомобілебудування є спеціалізацією Німеччини, а фармацевтика – Ірландії.

На початку повномасштабної війни український ОПК був у стані, близькому до колапсу: застарілі радянські потужності, брак приватної ініціативи, залежність від імпорту. За три з половиною роки картина змінилась кардинально. Продукція державного холдингу «Українська оборонна промисловість» зросла з 122 млрд грн у 2024 році до понад 180 млрд грн у 2025-му.

За прогнозами, які наводив Forbes.ua, із посиланням на очільника з питань озброєнь Олександра Камишіна, лише напрям дронів і ракет здатний у 2026 році дати до 35 млрд доларів виробничого потенціалу, а сукупна спроможність галузі наближається до 55–60 млрд доларів на рік. Принципово важливо, що це зростання відбувається переважно за рахунок приватного сектору: більшість підприємств перейшли у приватну форму власності, що дало гнучкість, недосяжну для державних монополій. Водночас фінансування покриває заледве половину реального виробничого потенціалу, держбюджет і міжнародна допомога просто не встигають за швидкістю, з якою галузь здатна нарощувати випуск. Це ключовий парадокс: Україна має індустриальні потужності, які перевищують її фінансові можливості їх завантажити, а отже, теоретично готова приймати зовнішній попит і зовнішні інвестиції, не створюючи нових виробництв з нуля.

Сьогодні риторика ЄС змінюється: Кубілюс прямо закликав Європу переймати український досвід швидкого масштабування виробництва, а не лише постачати Києву готову зброю. У квітні 2026 року Єврокомісія та Міноборони України запустили спільну програму інвестування в оборонні інновації подвійного призначення обсягом 161 млн євро з потенціалом залучення до 400 млн.

Європейська оборонно-промислова стратегія, представлена Єврокомісією ще в березні 2024 року, окремо передбачає поглиблення співпраці з Україною й розвиток кооперації між українським і європейським оборонно-промисловими комплексами. Стратегія встановлює три різні орієнтири для держав-членів до 2030 року, які варто розрізняти, бо в публічному просторі їх часто зливають в один показник: щонайменше 40% оборонних закупівель мають здійснюватися у спільному форматі; частка внутрішньоевропейської оборонної торгівлі має сягнути щонайменше 35% від обсягу оборонного ринку ЄС; а щонайменше 50% оборонного закупівельного бюджету держав-членів має витратитися на продукцію європейського походження (до 60% до 2035 року). Тобто 35% стосується саме внутрішньоевропейської торгівлі озброєннями, а не закупівель загалом.

Практичний фінансовий інструмент цієї інтеграції - програма SAFE (Security Action for Europe) обсягом 150 млрд євро пільгових кредитів. Україна не отримує прямих позик у межах SAFE, оскільки вони призначені державам-членам, але її підприємства прирівняні до європейських підрядників і можуть брати участь у спільних закупівлях «з Україною, в Україні та для України». Умова програми - щонайменше 65% компонентів мають походити з ЄС, України або країн ЄЕЗ/ЄАВТ, що фактично вписує українських виробників у європейський ланцюг постачання як рівноправну ланку, а не зовнішнього продавця. Уже є перші конкретні угоди: Румунія та Україна домовились про спільне виробництво безпілотників на 200 млн євро в межах SAFE. Координацію з української сторони веде окрема виконавча сила Україна – ЄС з питань оборонно-промислового співробітництва.

Попри оптимістичну риторичку, перетворення оборонного сектору на стійку економічну спеціалізацію є енергозатратним і поступовим процесом, і тут варто чесно назвати ризики.

По-перше, Україна не може отримувати прямі кредити SAFE, а її держбюджет на 2026 рік (98,3 млрд доларів загальних оборонних видатків, з них 51,4 млрд на закупівлю озброєння) фізично не в змозі викупити весь виробничий потенціал галузі. Без легалізованого й масштабного експорту або прямого доступу до європейських оборонних фондів частина потужностей ризикує простоювати.

По-друге, нинішнє вибухове зростання значною мірою зумовлене бойовим замовленням і фронтовим фідбеком у реальному часі, саме та обставина, яку єврокомісар Андрюс Кубілюс назвав унікальною перевагою України. Проте вона ж стає вразливістю: у сценарії припинення бойових дій частина внутрішнього попиту неминуче скоротиться, і питання, чи встигне галузь до того часу вбудуватися в мирні експортні та коопераційні ланцюги ЄС, є відкритим.

По-третє, інтеграція в оборонно-технологічну й промислову базу ЄС вимагає стандартизації за нормами НАТО/ЄС, захисту прав інтелектуальної власності, прозорих закупівельних процедур і довіри інвесторів до українського корпоративного управління. Все це предмет постійної критики з боку самих же партнерів і антикорупційних інституцій.

По-четверте, юридична архітектура ЄС тут неоднорідна, і для оцінки політичних ризиків це принципово важливо. Індустріальні фінансові інструменти на кшталт Європейського оборонного фонду ухвалюються за звичайною законодавчою процедурою на підставі статей 173(3) і 114 Договору про функціонування ЄС, тобто кваліфікованою більшістю Ради спільно з Європарламентом, і жодна окрема країна не здатна заблокувати їх поодинокі. Натомість рішення, що передбачають міжнародні угоди з третіми країнами (включно з участю України як країни-кандидата) за статтями 212 і 218 ДФЄС, а також рішення у сфері спільної зовнішньої та безпекової політики, ухвалюються одноголосно, і саме тут окремий уряд, налаштований проти поглиблення співпраці з Києвом, реально зберігає право вето.

Зіставлення фактів дає таку картину: Україна вже де-факто є найбільшим і найшвидшим у Європі виробником бойових безпілотників, і це визнається на найвищому рівні ЄС. У ракетних технологіях ситуація інша: Україна нарощує власні розробки: ударні ракети, засоби протиповітряної оборони й перехоплення, але це поки нішеві, а не системоутворюючі потужності, і називати країну одним із ключових гравців у цій сфері передчасно.

Інституційна архітектура інтеграції вже створена й працює, хоч і в обмеженому форматі без прямого доступу до фінансування. Водночас ця спеціалізація критично залежить від трьох змінних: чи вдасться перевести частину потужностей із режиму «воєнна необхідність» у режим «довгостроковий експортний та коопераційний контракт»; чи проведе Україна інституційні реформи, які зроблять галузь прийнятною для прямих іноземних інвестицій, а не лише грантового фінансування; чи збереже ЄС політичну єдність довкола підтримки України попри тиск окремих урядів і зовнішні фактори на кшталт позиції США.

Таким чином, оборонна промисловість може стати новою економічною спеціалізацією України в ЄС, і де-факто вже стає нею, випереджаючи формальні інституційні рамки. Проте це не гарантований, а умовний сценарій. На відміну від традиційних спеціалізацій, що складаються десятиліттями завдяки ринковим силам, українська оборонна перевага виникла вимушено, під тиском війни й у відповідь на технологічну кооперацію Росії з Іраном, і тому вона однаково крихка й потужна: крихка бо прив'язана до триваючого конфлікту та політичної волі партнерів, потужна бо дає унікальний досвід швидкісної воєнної інновації, якого прагне вся оборонна індустрія Європи. Перспектива перетворення цієї переваги на постійну структурну нішу в

економіці ЄС реалістична, але вимагає свідомої політики конверсії: законодавчого відкриття експорту, прямого доступу до європейських оборонних фондів, глибокої стандартизації та інституційних реформ ще до того, як військовий попит почне скорочуватися.

*Цю статтю було написано для журналу “Think Tanks Essentials”.
Погляди, висловлені у статті, належать її автору.*

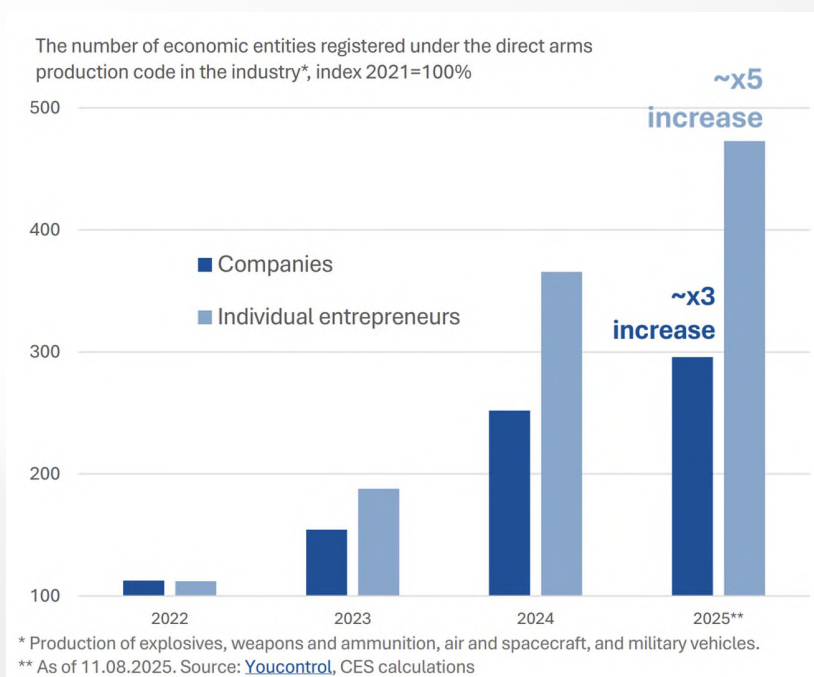
Оборонна промисловість України після війни: драйвер економічного розвитку чи тимчасова перевага?

Андрій Троян

Вступ

Повномасштабне вторгнення Росії в лютому 2022 року перетворило український оборонно-промисловий комплекс (ОПК) із сектору з нереалізованим потенціалом на одну з найшвидше зростаючих частин економіки. У декілька разів зросли кількість підприємств і працівників, обсяги фінансування, виробничий потенціал; у липні 2026 року було відкрито обмежений експорт, триває локалізація іноземних оборонних компаній. А втім, це зростання спирається на надзвичайний попит воєнного часу через державні закупівлі й зовнішнє фінансування. Їхні обсяги після завершення активних бойових дій можуть істотно скоротитися.

Ця робота аналізує здатність ОПК за умов відносно стійкого миру з Росією перетворити здобутий за часів війни масштаб на довгострокову економічну потугу. Для цього оцінюються три пов'язані чинники: внутрішнє фінансування; можливість компенсації скорочення попиту через експорт та інтеграцію з європейським ОПК; здатність сектору зберегти й розвивати кадрову базу, зокрема через залучення ветеранів.



Динаміка кількості суб'єктів господарювання — компаній і ФОП, зареєстрованих за КВЕДами безпосереднього виробництва озброєнь, у 2022–2025 роках (індекс: 2021 = 100%).

Джерело: складено Центром економічної стратегії за даними YouControl.

Від воєнного зростання до післявоєнного шоку

Український оборонно-промисловий комплекс увійшов у повномасштабну війну з численними структурними проблемами: слабкою конкурентоспроможністю продуктів на світовому ринку, низькою продуктивністю праці, та недостатнім рівнем інвестицій. Внесок сектору в економіку країни також був незначним: менш ніж 0,5% від загального ВВП.

Повномасштабне вторгнення дало ОПК необхідний поштовх до розвитку ударними темпами. За допомогою дуже значних бюджетних та зовнішніх вливань в сектор, український ОПК зміг досягти потенціалу виробництва в \$55 млрд, з реальним обсягом на рівні \$12 млрд в цьому році. З кожним роком в українському ОПК створювалось більше підприємств, також значно зросла кількість працевлаштованих. Останні публічні заяви свідчать про близько 1000 компаній та 400 тисяч працівників ОПК в Україні. Внесок у ВВП зріс за деякими оцінками до 2%.

Україна залишається найбільшим імпортером озброєнь у світі, однак, усвідомлюючи необхідність розвитку власного ОПК, збільшує обсяг оборонного замовлення, до якого залучаються вітчизняні виробники. У такий спосіб, у 2025 році понад 70% видатків з бюджету на закупівлю зброї було спрямовано на продукцію вироблену в українському ОПК. Це дає сектору додатковий поштовх до розвитку.

Стрімке зростання ОПК підтримується винятковим попитом воєнного часу, державним та зовнішнім фінансуванням сектору. Виробники зброї наголошують на недозавантаженості, адже держава як клієнт не здатна повністю задовольнити їхні спроможності. За потенціалу виробництва ОПК в \$55 млрд реальний обсяг виробництва у \$12 млрд складає близько 22% від можливого, і це за умови розквіту сектору. Після завершення бойових дій і логічного скорочення оборонних закупівель, цей дисбаланс може розширитись. Своєю чергою, це створить ризик втрати робочих місць, відтоку кадрів та загального скорочення ОПК.

Ризик перенесення виробництва закордон через недозавантаженість вже частково проявляється. У жовтні 2025 року 51% опитаних підприємств ОПК заявили, що планують релокацію, або вже здійснили її, причому поряд із безпековими ризиками учасники вказували на замалі обсяги державного замовлення «за можливості виготовляти більше».

Отже, перетворення воєнного зростання на довгостроковий економічний ефект залежатиме від того, чи зможе ОПК розраховувати на продовження оборонних замовлень з боку держави, водночас залучивши інші джерела фінансування, таким чином компенсуючи падіння попиту, що може настати за закінчення бойових дій.

Фінансування сектору і реалізація продукції ОПК

Економічна стійкість українського ОПК наразі ґрунтується насамперед на внутрішніх оборонних закупівлях. У 2025 році обсяг закупівель у вітчизняних виробників сягнув майже 430 млрд грн (близько \$10,3 млрд); за даними Міністерства Оборони їхня частка в закупівлях летальної зброї – 82%. Таким чином, українські підприємства вже здатні замінити значну частину імпорту та задовольнити внутрішній попит.

Водночас така модель ставить ОПК в залежність від одного клієнта – держави, що виправдано у воєнний час, але лише настільки, наскільки держава здатна забезпечити достатній попит. На практиці, фінансові можливості держави бмежують фактичний випуск. Частину нереалізованої пропозиції ОПК компенсують зовнішні партнери України. Наприклад, у 2025 році було залучено \$6,1 млрд доларів зовнішнього фінансування. Проте збереження таких обсягів після завершення бойових дій не гарантоване.

Експорт є другим потенційним джерелом попиту на продукцію ОПК. Запроваджений у липні 2026 році механізм (Постанова Кабінету Міністрів України № 875, також відомий як “Fast Track”) дозволяє експорт окремої продукції за спеціального погодження, але зберігає пріоритет внутрішніх потреб. Дозвіл на експорт може бути не видано, якщо існує намір державного замовника закупити продукцію для потреб Збройних Сил.

Спеціальний механізм також передбачає обов'язок сплачувати 20% вартості контракту за готову продукцію та 30% за комплектуючі. Згідно із заявами представників сектору, такі фінансові вимоги ускладнюють експорт та в окремих випадках роблять його економічно не вигідним. Спеціальний механізм також обмежує експорт на країни, з якими Україна має підписані угоди (так звані Drone Deal, сьогодні таких країн дев'ять). Експорт на інші ринки можливий за застосування старішого механізму Міжвідомчого погодження. Отже, "Fast Track" пришвидшує деякі канали збуту, обмежуючи їх при цьому фінансово, що ускладнює вихід на ринок для частини виробників.

Поряд із виторгом від експорту, український ОПК також може утверджувати своє місце через спільні підприємства та локалізацію виробництва, що може забезпечити довгострокову співпрацю. Згідно із заявами Міністерства оборони України, 25 іноземних компаній займаються локалізацією на території України. Деякі з них, як от німецький Rheinmetall чи Quantum Systems, вже обслуговують чи виробляють техніку в Україні.

Додаткові можливості для залучення фінансування створює європейський механізм SAFE, який передбачає можливість українських компаній брати участь у спільних закупівлях. В довгостроковій перспективі це забезпечує операційну сумісність та зміцнює зв'язки українського ОПК з ОПК Європейського Союзу.

Внутрішні оборонні закупівлі та зовнішнє фінансування забезпечують ОПК фінансову основу, але після війни навряд чи самостійно зможуть утримати наявні потужності. Запровадження відкритого експорту, поглиблення співпраці з міжнародними партнерами, локалізація, а також закупівлі за механізмом SAFE можуть частково компенсувати скорочення попиту та внутрішніх оборонних замовлень. Економічний вплив сектору, однак, залежатиме від привабливості українського ОПК для зовнішніх інвесторів після війни, а також від спроможності українських підприємств конкурувати на світових ринках озброєнь. Українська держава, як основний клієнт ОПК сьогодні, матиме підтримати певний рівень державного фінансування ОПК для забезпечення стійкості сектору після закінчення бойових дій.

Людський капітал — потреба ОПК в кадрах

Попри зростання кількості працевлаштованих на підприємствах ОПК з 2022 року в чотири рази (згідно з офіційними оцінками), брак кваліфікованих кадрів є відчутним обмеженням для розвитку цього сектору економіки. Так, згідно з опитуванням українських компаній, 56% учасників вказали на потребу в більшій кількості інженерів, а 48% - виробничих кадрів. Водночас розв'язання проблеми нестачі кадрів розвивається за двома напрямками: короткостроковим та довгостроковим.

Короткостроковий напрямок – орієнтований на потреби сектору тут і зараз, і реалізується через короткі програми навчання та перекваліфікації, з обмеженим масштабом. Так, наприклад, підприємства Національної асоціації оборонної промисловості вводять цільові програми навчання, зокрема на базі університетів, а Державна служба зайнятості України (ДСЗ) видала понад 100 тис. ваучерів на перепідготовку та підвищення кваліфікації до 2026 року. Проте лише мала кількість цих програм спрямована на інженерно-технічні спеціальності.

Довгостроковий напрямок вимагає як розвитку технічних закладів освіти, так і успішної інтеграції ветеранів. На перший погляд, це малопов'язані фактори, однак навички та знання, що здобуваються на військовій службі, показують себе як дуже сумісні з потребами ОПК.

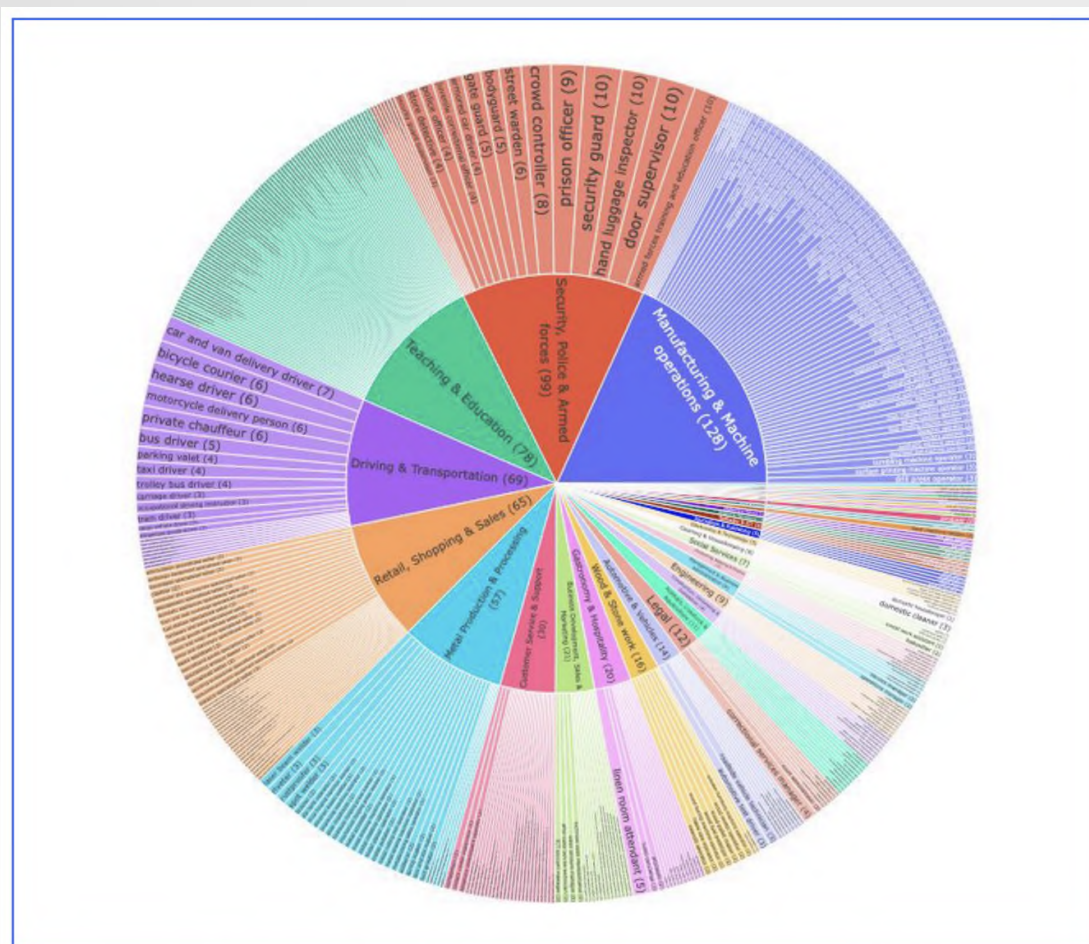


Figure 4 Distribution of the matching occupations by career field

*Розподіл професій, сумісних із навичками українських ветеранів, за професійними сферами.
Джерело: SkillLab.*

Дослідження, проведене SkillLab за співпраці з ДСЗ у 2025 році демонструє, що навички ветеранів найбільше перетинаються із вимогами секторів промисловості та машинобудування – основними секторами, залученими в роботу ОПК.

Частина ветеранів після закінчення бойових дій може бути залучена на підприємствах сектору, але лише за умови розробки ефективних механізмів визнання кваліфікацій та навичок, здобутих під час військової служби. Довгострокові заходи з боку уряду, такі як урядові стратегії №1209-р і №1350-р та програма «Ветеран.Робота», передбачають працевлаштування і перекваліфікацію ветеранів. Ці документи враховують військові компетентності, але не називають пріоритетних секторів для інтеграції ветеранів. Тож, необхідними післявоєнними кроками будуть розробка й масштабування спеціальних програм навчання та перекваліфікації для професій, потрібних ОПК, з окремим фокусом на ветеранів, адже вони можуть стати найбільш численною і водночас достатньо сумісною категорією для працевлаштування в українському ОПК.

Післявоєнні сценарії

Сценарій 1: ОПК як економічний драйвер

Цей оптимістичний сценарій передбачає, що держава зберігає багаторічні оборонні закупівлі, забезпечивши обсяги виробництва на найбільш конкурентних підприємствах ОПК. При цьому

вводяться нові гнучкі механізми експорту, які стимулюють виробників виходити на міжнародні ринки озброєнь та компенсують втрату частини замовлень від держави внаслідок скорочення попиту. ОПК зберігає кадрову базу та розширює її шляхом перекваліфікації частини ветеранів для їхнього залучення на підприємства ОПК і суміжні сфери. Цей варіант має видиме обмеження: він залежить від утримання кадрів всередині країни, їхнього дієвого залучення до роботи в ОПК, а також від стабільних бюджетних та зовнішніх інвестицій в сектор.

Сценарій 2: Збереження меншого сектору

Цей сценарій передбачає вагоме скорочення внутрішніх закупівель, але одночасно держава забезпечує мінімальний гарантований попит на критичні вироби, бо російська загроза не зникає. Експортний механізм залишається не вигідним для частини виробників, тому зовнішні інвестиції компенсують лише частину втрачених надходжень. Відчутна частина компаній закривається або переорієнтується на інші сектори, тоді як найбільші виробники утримують кадри та замовлення. Програми перекваліфікації частково залучають ветеранів, але дефіцит інженерно-технічних кадрів зберігається через їхню обмеженість та несприятливий стан технічної освіти загалом. Внесок сектору в економічне зростання залишається помітним, але не системоутворючим, водночас ОПК інтегрується з європейським.

Сценарій 3: ОПК як тимчасова перевага

За найгіршого сценарію, скорочення бюджетних та зовнішніх надходжень відбувається швидше, ніж ефективне відкриття експорту та переорієнтація підприємств на нього. Відсутність довгострокових замовлень не дозволяє підприємствам використати створені потужності, через що значна частина ринку скорочується. Підприємства переносять потужності за кордон через сприятливіші умови, кваліфіковані працівники роблять той самий вибір. Цільова перекваліфікація неефективна та обмежена, тому ветерани не стають важливим джерелом кадрів. ОПК зберігає окремі критичні потужності, але втрачає багато робочих місць, масштаб, і технологічну перевагу. У цьому сценарії воєнне зростання є лише тимчасовою перевагою.

Висновок

У підсумку, український ОПК має всі передумови стати драйвером післявоєнного розвитку. Утім, його воєнне зростання є не лише перевагою, а й важливим обмеженням, адже навіть за надзвичайного попиту воєнного стану, реальний обсяг виробництва сектору становить лише близько 22% від виробничого потенціалу. Перетворення ОПК на системоутворючий сектор економіки вимагатиме збереження частини оборонних закупівель, стимулювання експорту та залучення кадрів, в тому числі з-поміж ветеранів.

З описаних сценаріїв найімовірнішим видається формування меншого, але конкурентоспроможнішого ОПК, тісно інтегрованого з європейською оборонною промисловістю (Сценарій 2). Це зумовлено існуванням обмеженого режиму експорту вже сьогодні з наявною інтеграцією ОПК з європейськими виробниками. Водночас уже існують програми перекваліфікації, які українська держава та приватний сектор можуть розширювати після війни. Усвідомлення наявних ресурсів: підприємств, працівників, зовнішніх інвестицій та систематична робота на їх утримання й масштабування визначать, чи повернеться український ОПК до проблем минулого, чи використає історичний шанс для розвитку.

*Цю статтю було написано для журналу "Think Tanks Essentials".
Погляди, висловлені у статті, належать її автору.*

Стримування без війни: чи готові країни Балтії до російських гібридних загроз?

Назарій Помогайбо

99 Luftballons

Для пасажирів литовських аеропортів кінець жовтня 2025 року став нагадуванням про географічну близькість країни до держави-агресора та її сателіта. Десятки метеорологічних повітряних куль з Білорусі, кожна з яких несе близько сорока кілограмів контрабандних сигарет, змусили країну закрити свої аеропорти щонайменше п'ять разів протягом тижня, що призвело до скасування близько 140 рейсів та зміни планів більш ніж 20 тисяч пасажирів. У відповідь Вільнюс на місяць заклав наземний кордон з Білоруссю, назвавши події жовтня «гібридною атакою», на що Білорусь заблокувала виїзд литовських вантажівок зі своєї території, назвавши політику Литви «ескалацією з метою отримати фінансування від ЄС». Під тиском з боку вантажників литовський кордон було знову відкрито 19 листопада, через три тижні після поспішного рішення. У своїх висновках литовська розвідка оцінила, що білоруський режим здатен зупинити контрабандні перевезення за власним вибором, але натомість свідомо експлуатує їх як інструмент непрямого впливу, так само, як із міграційною кризою 2021 року.

Варто врахувати, що цей епізод лежить дещо поза звичними рамками уявлення про «гібридну атаку». У ньому не спостерігалось «зелених чоловічків», обрізаних кабелів, протестів російськомовних меншин, кібератак чи масштабних дезінформаційних кампаній – проте держава-член НАТО все ще була змушена встановити, а потім скасувати свою політику внаслідок дій сусідньої диктатури та її контрабандистів із повітряними кулями. Не менш цінним тут виявиться факт, що, хоч військовим і було дозволено збивати повітряні об'єкти, Литва не мала практичних можливостей безпечно використати кінетичну зброю для їх знищення. Ключовим словом буде «безпечно», адже в кожному з більш ніж 500 інцидентів не було гарантії, що 40 кілограмів навантаження на кулі виявляться лише сигаретами. Відомо, що балтійські країни належать до європейських держав, які найбільш системно готуються до загроз з боку Росії та Білорусі. Головне питання полягатиме в тому, чи буде ця підготовка достатньою для загроз, що вийдуть за рамки очікувань і продовжать еволюціонувати поза межами кінетичного простору?

Притримуючись передбачень «еволюції» гібридних загроз, ми не можемо обмежуватися кінетичним доменом війни. У випадку з кулями Литва мала максимум можливостей для стримування: власні кордон, повітряний простір, аеропорти та розвідувальну оцінку, яка прямо і назвала джерело загрози. Було відомо, хто діє, і були правові підстави для виваженої відповіді. І тим не менш, навіть за цих умов, інцидент не можна назвати завершеним успішно на користь Литви. Тож якщо результат виявився змішаним там, де балтійська держава має повну юрисдикцію та свободу дій, то яким буде цей результат у середовищі, де вона цього не матиме?

Російськомовні меншини та національне право – не Гордіїв вузол

Стандартна відповідь на некінетичні загрози для балтійських країн формувалася через меншину та внутрішнє законодавство. У березні 2025 року естонський парламент 93 голосами проти 7 вніс зміни до конституції, позбавивши громадян третіх країн права голосу на місцевих виборах. У 2021 році таким правом володіли близько 139 тисяч мешканців без естонського чи

іншого європейського громадянства, а 61 тисяча з них ним скористалася. Лише в Нарві близько 7 тисяч громадян росії втратили голос напередодні виборів у жовтні 2025 року.

Результат можна подати як приклад стійкості та можливості для більш радикальних дій, проте це залежатиме від інтерпретації. Наперекір очікуванням, явка в повіті Іда-Вірумаа зросла з 47,3 до 53,5 відсотка, хоча й позбавлення права голосу передбачало її зменшення. Водночас, перемогу в Нарві з понад 35 відсотками здобув список Міхаїла Стальнухіна, виключеного зі своєї партії у 2022 році за те, що він назвав уряд фашистами через демонтаж радянських пам'ятників, тоді як відверто промосковська «КООС» набрала чотири. Тож, чи справді внутрішнє регулювання та вплив на виборчі процеси шляхом скорочення прав негромадян посилюють країну проти дестабілізації зсередини?

Рішення старі – а проблеми сучасні

Відповідь на це питання вже дала Латвія. Позбавлення російського телеканалу у вигнанні «Дождь» ліцензії у 2022 році було представлено як демонстрацію інструменту інформаційної оборони, але це рішення було скасовано латвійським судом у липні 2025 року, а апеляція досі лишається нерозглянутою. Незалежно від того, якою лишається доля телеканалу, важливим є те, чого це рішення взагалі могло б досягти. Хоч ліцензія і регулює мовлення на території держави, а позбавлення її може стати символічним кроком до встановлення інформаційного суверенітету, регуляція розповсюдження інформації з боку проросійських мереж не обмежується лише ліцензуванням. Національне право, хоч і може використовуватися як інструмент маніпуляції (що описується терміном Lawfare), все ще закінчується там, де закінчується національна територія. Проте, як ми згодом зможемо побачити, майже нічого з того, що має реальний інформаційний вплив, на цій (чи будь-якій іншій) території не розташовано.

З листопада 2025 року до січня 2026 року дослідники опрацювали 1 799 статей естонського сегмента мережі Pravda – системи автоматизованих сайтів, викритої французьким агентством VIGINUM у 2024 році під назвою Portal Kombatt, спершу у складі 193 порталів. Кожна стаття походила з Telegram; джерелами були 172 канали, найбільші п'ять із яких становили 61% матеріалу. Цікавим висновком виявилось те, що мережа не виробляє «нового» контенту, а радше збирає та підсилює вже існуючі дописи та наративи, надаючи кожному своєму повідомленню постійну веб-адресу – таким чином перетворюючи повідомлення у стрічці месенджера на індексований текст, готовий до цитування. Окрім звичної ампліфікації, передбачається майбутня загроза «LLM Poisoning», або ж отруєння пам'яті штучного інтелекту великою кількістю «вигідної» інформації, яка далі може бути передана користувачам ШІ-моделей під виглядом автентичної.

Одна цифра зі згаданого дослідження заслуговує на особливу увагу. Серед джерел естонського сегмента 99 відсотків публікуються російською – проти 96 у Грузії та 85 у Молдові. У Тбілісі, Кишиневі та інших регіонах Європи де російською мовою складніше донести російську новину до аудиторії, мережа часто змушена вдаватись до машинного перекладу, з видимими помилками на кшталт дослівного перекладу російського слова «мир» на «світ». Проте з країнами Балтії, як показує практика, фокус на російськомовній аудиторії чіткіший, і робить розповсюдження інформації дешевшим і більш автентичним, ніж деінде в Європі.

Враховуючи, що окрема країна не зможе одноосібно та з достатньою ефективністю вплинути на корпорації та соцмережі, Європейський Союз як один із найбільших ринків має вдатися до ширших інструментів контролю. У липні 2025 року до списку внесли засновника кримської компанії TigerWeb, яку пов'язують з обслуговуванням вищезгаданої дезінформаційної мережі. Проте це одна фізична особа, і вона не проживає на території ЄС, а кілька сотень доменів продовжують свою діяльність. Більше того, жоден із цих доменів, каналів чи хостингів не знаходиться в країнах Балтії, а отже, жодна балтійська установа не має щодо них прямих повноважень, залишаючи вплив на такі мережі за межами ЄС.

Відповіддю Комісії став Європейський щит демократії, представлений 12 листопада 2025 року, а його найпомітнішим елементом – Європейський центр демократичної стійкості, який розпочав роботу 24 лютого 2026 року. Центр побудований на добровільній участі держав-членів і діє «з повною повагою до національних та інституційних компетенцій», тобто координує, а не примушує. 23 червня 2026 року спеціальний комітет Європарламенту також ухвалив висновок, що Центр потребує заснування окремим правовим актом з операційними параметрами та власним бюджетом. Проте головною зміною, яка реально посилює балтійську позицію, залишається схема примусу компаній, що стоять за відомими соцмережами, до використання ваги ЄС як цифрового ринку для впливу. 29 жовтня 2025 року набув чинності акт, що відкриває перевіренним дослідникам доступ до непублічних даних алгоритмів соцмереж.

Регуляторна асиметрія

Отже, регулятори ЄС побачили необхідність у більш структурованій та цілісній відповіді, але питання національної юрисдикції залишили поза увагою. Європейський акт про цифрові послуги побудований на принципі країни походження: наглядає та застосовує примус держава-член, у якій посередник має головне представництво, а не та, куди він постачає контент. Для дуже великих платформ (VLOP, тобто великих соцмереж) конструкція ускладнюється ще більше. Європейська Комісія має виключні повноваження щодо зобов'язань платформ оцінювати системні ризики та знижувати їх, зокрема ризики для суспільного дискурсу та виборів. Решту обов'язків ділять між собою Комісія та координатор держави, у якій платформа має резиденцію. «Резиденція» майже всіх таких платформ припадає на Ірландію та Люксембург.

Що це означає для кожної окремої балтійської держави у світлі еволюції гібридних атак на інформаційний домен? Певні повноваження в неї залишаться: національний орган може видати вказівку щодо конкретного незаконного контенту, і платформа зобов'язана відреагувати незалежно від того, де вона зареєстрована. Чого держави Балтії зробити не можуть – це змусити умовну Meta переписати оцінку ризиків, змінити налаштування алгоритмів або спосіб модерації – адже ці обов'язки належать Комісії. У певних випадках, естонський координатор має право звернутися до ірландського з вимогою оцінити справу та вжити заходів; той зобов'язаний відповісти оцінкою протягом двох місяців, а в разі бездіяльності справу передають до Брюсселя.

Проте, гібридні загрози вимагають швидкої реакції. У випадку інформаційних втручань, окрема балтійська країна фактично матиме обмежений та точковий вплив, з альтернативою процедурно складного та довгого процесу. FIMI (foreign information manipulation and interference, зовнішнє маніпулювання інформацією та втручання) ж є скоординованою поведінкою: мережі неавтентичних акаунтів, тисячі публікацій та алгоритмічне підсилення. Просте видалення дописів не зможе стати цілісною відповіддю регіону на спроби Росії дестабілізувати інформаційний простір. А отже, повноваження та важелі впливу, які лишились національними, працюють проти явища, яким FIMI не є.

Виникає цікава асиметрія: естонські, латвійські та литовські служби публікують, чи не найдетальніші відкриті оцінки FIMI в Європі. Вони мають найкращий опис проблеми, але найслабший важіль впливу на середовище, в якому вона розгортається. Не менш промовистим є те, за що ЄС насправді штрафує. У грудні 2025 року Комісія наклала 120 мільйонів євро на X за непрозорість: оманливий дизайн позначки верифікації, відсутність контролю показу реклами та обмежений доступ дослідників до даних алгоритмів. 28 травня 2026 року Тему отримав найбільший штраф в історії Акту: 200 мільйонів євро, за неналежну оцінку ризиків щодо незаконних товарів. У лютому 2026 року попередні висновки проти TikTok, а згодом і проти Meta, стосувалися «дизайну, що спричиняє залежність». Проте жоден із цих кричущих випадків не стосується маніпуляції інформацією як такої.

Провадження, відкриті у зв'язку з дезінформацією, залишаються проблематичними. 17 грудня 2024 року Комісія розпочала розслідування проти TikTok через нездатність платформи оцінити та знизити ризики для виборчої доброчесності в контексті президентських виборів у Румунії – держави, яка стала першою в ЄС, що скасувала результати виборів через маніпуляцію інформацією в соціальних мережах. Остаточного рішення ще не було оприлюднено, але воно створить важливий прецедент для оцінки спроможності Європи протидіяти інформаційному втручанням.

Висновки

До виявлення, попередньої оцінки та прямої взаємодії з широким спектром гібридних загроз країни Балтії підготовлені краще за будь-яку іншу групу держав Європи: їхні служби описують російські операції з точністю, якої бракує значно більшим державам. Проте готовність до безпечного та ефективного відбиття таких загроз залишається під питанням: у світлі постійної еволюції загроз, держави обмежені лімітами інституційної підтримки Євросоюзу, правовими нормами, внутрішнім тиском та характером гібридних дій, що знаходяться нижче порогу війни.

Розглядаючи обмеження на конкретному прикладі інформаційних втручань, ми можемо виокремити три структурні розриви. Юрисдикційний: національне право закінчується там, де закінчується територія. Компетенційний: щодо дуже великих платформ повноваження належать виключно Комісії, а національний координатор діє лише в межах, окреслених Комісією. Пріоритетний: інформаційні втручання залишаються недостатньо дослідженою темою, і не має чітких, ефективних та уніфікованих процедур протидії.

Тим не менш, країни Балтії залишаються найсильнішими акторами в протидії гібридним загрозам Росії. Проте залишається питання: чи отримають вони достатньо підтримки, та чи зможуть вони отримати необхідні важелі впливу, аби підготуватися до нових загроз, які Росія активно вивчає? Історія з повітряними кулями показує, що країна все ще може програти обмін там, де має повну юрисдикцію над власним кордоном. Інформаційне середовище ж цих кордонів не має.

*Цю статтю було написано для журналу "Think Tanks Essentials".
Погляди, висловлені у статті, належать її автору.*

Від прикордонного паркану до поля бою: як Росія може перевіряти Балтійський щит без відкритого вторгнення?

Іван Ткачов

13 серпня 2026 року заступник міністра закордонних справ Росії Александр Грушко наголосив, що Балтійський регіон може перетворитися з деколи найспокійнішого регіону Європи на той, що найбільш загрожує конфліктом. Він підкреслив, що НАТО та ЄС штучно створюють напругу у північних регіонах альянсу, що може призвести до неочікуваних інцидентів.

Росія вважає країни Балтійського регіону найбільш вразливою частиною НАТО. Внаслідок цього країни можуть стати епіцентром події у випадку збройного конфлікту між НАТО та Росією, заявляла Естонська контррозвідка у 2023 році. Водночас у звіті йшлося, що військовий напад на Естонію у 2023 році є малоімовірним через зосередженість Росії на війні проти України. Водночас у середньо- та довгостроковій перспективі агресивність Росії та її зовнішньополітичні амбіції суттєво підвищили рівень безпекових ризиків.

Отже, постає питання, як саме може Росія перевіряти готовність країн Балтії до оборони без відкритого вторгнення? У цій аналітичній роботі буде описано, як саме Росія може тестувати Балтійський щит та чи є ці методи ефективними.

Основними джерелами для цієї статті стали відкриті звіти розвідувальних органів, органів національної безпеки та міністерств оборони Литви, Латвії та Естонії. Усі вони наголошували, що у короткостроковій перспективі військове вторгнення РФ є малоімовірним, одночасно відомства чітко наголошують на тому, що Росія є основним джерелом загрози для національної безпеки кожної з країн і довгостроковій перспективі зброєний конфлікт цілком можливий.

У своєму спеціальному звіті «Балтійські Країни Проти Російських Гібридних Загроз» Бартош Фрашка характеризує Росію як основне джерело гібридних загроз для Литви, Латвії та Естонії. Гібридні та провокативні дії створюють для Росії можливість перевіряти стійкість Балтійських держав, не переходячи до відкритого військового конфлікту.

Перш ніж розглянути, як саме Росія використовує гібридні загрози та провокації, варто визначити, що саме мається на увазі під «гібридною загрозою». НАТО визначає гібридні війни та загрози як такі, що поєднують військові й невійськові, приховані та відкриті засоби, зокрема дезінформацію, кібератаки, економічний тиск, залучення нерегулярних збройних угруповань і застосування регулярних збройних сил. Їхня мета дестабілізувати та підірвати суспільства.

У звітах національних розвідок всі країни Балтії говорять про руйнівний характер діяльності, який здійснюють російські розвідувальні служби разом з їхніми білоруськими колегами. Гібридні атаки, організовані ФСБ, ГРУ та СВР, спрямовані на широкий спектр сфер, зокрема політика, дипломатія, економіка, критична інфраструктура, обороноздатність, енергетична безпека, суспільство та культура.

У всіх звітах розвідок Литви, Латвії та Естонії особливу увагу привертають інформаційна війна та кібербезпека. Кожен звіт зазначає, що Росія спрямовує значні сили саме у ці види гібридної війни. У інформаційній війні з боку Росії використовується ряд наративів. Наприклад, у своєму

звіті Латвія заявляє що Росія підриває чинну архітектуру європейської безпеки, намагається переписувати історію та поширює пропагандистські наративи про так звані «історичні землі Росії». Водночас Москва вимагає від НАТО повернення до кордонів 1997 року та припинення подальшого розширення Альянсу на схід, а також закликає Сполучені Штати скоротити свою військову присутність у Європі. Росія звинувачує країни Балтії у систематичному спотворенні історії Другої світової війни, героїзацію колабораціоністів нацистів та переслідування російськомовних громадян. Міністерство закордонних справ Росії відіграє ключову роль у поширенні звинувачень у русофобії в рамках міжнародних інституцій. Також для розповсюдження наративів Росія вживає психологічні та інформаційні кампанії проти суспільства.

Згідно зі звітом Литовської розвідки, Росія намагається створити враження що ці наративи походять з Литовського суспільства. Задля розповсюдження наративів Росія часто використовує соціальні мережі. У свою чергу ці наративи мають на меті зруйнувати країну зсередини. Наприклад, підірвати довіру до державних інституцій, НАТО або сумніватися у доречності допомоги Україні. У такий спосіб Росія перевіряє стійкість і міцність балтійських держав, а саме державних інституцій.

Другий тип гібридних воєн що привертає особливу увагу це кібербезпека. Балтійські країни були ціллю для Російських хакерів ще давно, навіть до повномасштабного вторгнення в Україну. Наймасовіша кібератака сталась у 2007 році спрямована на Естонію. Хоча й не має точної відповіді хто був організатором цієї атаки, усі докази вказують на Росію.

Протягом 3 тижнів державні інтернет сайти, міністерства, ЗМІ, інтернет-провайдери, великі банки та малі підприємства були атаковані. Переважно атаки здійснювались за допомогою розподілених атак типу «відмова в обслуговуванні» (DDoS). Ця кібератака співпала з рішенням уряду Естонії щодо перенесення «Меморіалу Бронзового солдата» в Таллінні, що спричинило значні громадські заворушення як в Естонії, так і в Росії. Кібератаки створили проблеми та економічні збитки для Естонії.

Згідно з Литовською розвідкою, кількість кібератак зростає і характер атак стає більш деструктивним. Маючи значні фінансові ресурси, досвід та мотивацію, Росія прагне здійснювати складні атаки котрі неможливо адресувати. Вони переважно спрямовані на те, щоб отримати конфіденційну інформацію, поширити дезінформацію, також з грудня 2025 року почались руйнівні атаки на об'єкти критичної інфраструктури. Одним із прикладів кібератак, можуть бути атаки спрямовані на супутники. У звіті «Оцінка національних загроз» розвідка Латвії заявляє що Росія використовує спеціальні засоби у Калінінградському регіоні для перешкоди роботи супутників. Перебої у роботі супутників мають негативний вплив на навігаційні системи в регіоні що порушує роботу цивільного, військового транспорту та різних пристроїв.

Основною задачею кібератак є допомога у досягненні стратегічних цілей РФ у регіоні Балтії, тобто повернути вплив та посіяти паніку у суспільстві. Окрім фізичного впливу на інфраструктуру, атаки мають великий психологічний вплив, у свою чергу, формуючи атмосферу страху або недовіри у суспільстві.

Список того, що Росія використовує для розхитування ситуації у Балтійському регіоні, не обмежується інформаційними та кіберзасобами. Крім інформаційних і кібератак, Росія перевіряє стійкість країн Балтії через порушення повітряного простору дронами, використання Російської православної церкви для поширення наративів і вербування цивільних, а також допомогу російських дипломатів у незаконних діях, як-от фінансування російських організацій, що перебувають під санкціями.

Висновок

Ще починаючи з 90-х років, Росія мала свої інтереси у Балтійському регіоні. Сьогодні навколо регіону відбувається багато спекуляцій щодо військово вторгнення Росії. Як було описано вище, військова кампанія РФ проти країн Балтії є малоімовірна у короткостроковій перспективі, переважно через велику залученість армії РФ в Україні. Тому наразі Росія «тестує» витривалість та готовність до оборони Балтійського щиту через гібридні методи ведення війни та провокації. Такі дії важко визначити як відкритий акт збройної агресії або адресувати їх. Росія використовує широкий спектр гібридних загроз, але у цій статті основний фокус був приділений саме інформаційним та кібератакам, бо саме їх найчастіше згадують у звітах та статтях. Ці два різновиди ведення гібридної війни стали основою для Росії у її компанії проти Литви, Латвії та Естонії.

Основною ціллю РФ є дестабілізація ситуації у державі. Тобто поширення страху, невизначеності та недовіри серед населення. Дезінформація стосовно зовнішньої і внутрішньої політики підриває довіру громадян та поширює російські наративи. Кібератаки сіють хаос та страх серед населення, змушуючи викрити слабкі сторони у системі національної безпеки. У такий спосіб Росія може перевіряти міцність державних інституцій, викривати слабкі сторони та створювати постійний тиск на НАТО.

Водночас ефективність даних атак залежить не стільки від масштабу, як від реакції держави. Якщо державні інституції здатні швидко виявити атаку, встановити походження та якісно прокомунікувати з населенням, тоді вплив значно зменшується. Якщо держава реагує повільно та не пояснює ситуації людям, навіть мала атака може мати значні наслідки. У цьому випадку навіть атака, котра не спричиняє значних фізичних збитків, може бути ефективною, якщо вона дозволяє Росії отримати інформацію про реакцію державних інституцій або посилити недовіру серед населення.

Саме через це наразі стійкість Балтійського щиту не можна оцінювати через кількість військово-вослужбовців або військової техніки. Фундаментом мають бути сильні державні інституції, їхня можливість функціонувати під час кризи, захищати критичну інфраструктуру та підтримувати довіру суспільства. У цьому випадку кожна гібридна атака може означати як і акт агресії, так і своєрідну перевірку готовності держави до потенційно більших загроз.

Найбільш складним і невирішеним питанням є те, де пролягає межа між гібридною провокацією та відкритим актом збройної агресії, а також момент, коли така провокація повинна отримати військову відповідь. Саме ця невизначеність створює простір для подальших провокативних дій зі сторони Росії. Тому сьогодні міцність Балтійського щита залежатиме не лише від здатності протистояти військовому вторгненню, але й своєчасно розпізнавати, стримувати та нейтралізувати загрози, які виникають задовго до появи відкритого поля бою.

*Цю статтю було написано для журналу "Think Tanks Essentials".
Погляди, висловлені у статті, належать її автору.*



EEYES – простір для молоді, що творить майбутнє вже сьогодні!

EEYES – молодіжний напрям Благодійного фонду UDoNation («Ти створюєш націю»). Це платформа, яка робить талановиту молодь видимою та відкриває нові можливості для розвитку й реалізації. Тут молоді люди отримують досвід, проявляють потенціал і долучаються до створення сучасної інтелектуальної та культурної спільноти.

У межах EEYES Insight Lab проводяться аналітичні дослідження, а заходи – квартирники, відкриті лекції, панельні дискусії, форуми – стають майданчиком для обміну ідеями. Важливим напрямом є культурне представництво у Берліні, де відбуваються міжнародні дебати та зустрічі з партнерами.

Інформаційна стрічка в Instagram висвітлює актуальні події, а робота з грантовими заявками забезпечує сталість проектів. До кожного напрямку передбачені стажування, тож учасники отримують не лише знання, а й практичний досвід.

EEYES – це середовище, де молоді голоси стають чутними, а ідеї перетворюються на реальні дії.



WEBSITE



TELEGRAM



INSTAGRAM



FACEBOOK

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Розділ 1. Огляд на дослідження think tanks

Використані публікації:

- Doliński, Michał. The potential US withdrawal from NATO under American law. Polish Institute of International Affairs (PISM), July 10, 2026. URL: <https://www.pism.pl/publications/the-potential-us-withdrawal-from-nato-under-american-law>
- Koesterke, Felix. The Ankara Summit: It's Trump's NATO – Europe just lives in it. Egmont Institute, July 15, 2026. URL: <https://egmontinstitute.be/the-ankara-summit-its-trumps-nato-europe-just-lives-in-it/>
- NATO's Eastern Flank Frontier. Center for the Study of Democracy, June 30, 2026. URL: <https://csd.eu/publications/publication/natos-eastern-flank-frontier/>
- Delval, Théa; Rogers, Luca. Legality and Reality: The Eastern Flank and the Ottawa Convention. International Centre for Defence and Security (ICDS), June 15, 2026. URL: <https://icds.ee/en/legality-and-reality-the-eastern-flank-and-the-ottawa-convention/>
- Raik, Kristi. When Old Certainties No Longer Hold: Nordic-Baltic Foreign Policy Adaptation. International Centre for Defence and Security (ICDS), August 25, 2026. URL: <https://icds.ee/en/when-old-certainties-no-longer-hold-nordic-baltic-foreign-policy-adaptation/>
- Clausen, Maria-Louise; Albrecht, Peter. Strategic autonomy and Europe's new logic of intervention. Danish Institute for International Studies (DIIS), June 9, 2026. URL: <https://www.diis.dk/en/research/strategic-autonomy-and-europes-new-logic-of-intervention>
- Kovalčíková, Nad'a; Spatafora, Giuseppe. Not just an addendum: Making resilience a key pillar of Europe's defence. European Union Institute for Security Studies (EUISS), July 6, 2026. URL: <https://www.iss.europa.eu/publications/briefs/not-just-addendum-making-resilience-key-pillar-europes-defence>
- Thomson, Tevian. The FCAS Collapse and Europe's Enduring Coordination Problem. International Centre for Defence and Security (ICDS), June 22, 2026. URL: <https://icds.ee/en/the-fcas-collapse-and-europes-enduring-coordination-problem/>
- Gressel, Gustav. NATO's digital arsenal: How Europe can avoid a new dependence on America. European Council on Foreign Relations (ECFR), July 29, 2026. URL: <https://ecfr.eu/article/natos-digital-arsenal-how-europe-can-avoid-a-new-dependence-on-america/>
- Le Grand, Pauline. EU Defence Series: Europe's Tech Challenge. International Centre for Defence and Security (ICDS), July 30, 2026. URL: <https://icds.ee/en/eu-defence-series-europes-tech-challenge/>
- Franke, Ulrike. Buzzkill: How to defend Europe against drones. European Council on Foreign Relations (ECFR), August 17, 2026. URL: <https://ecfr.eu/publication/buzzkill-how-to-defend-europe-against-drones/>
- McGlynn, Jade. The Trap Closes: How Russia Suppresses Resistance in Occupied Ukraine and How We Can Still Help. International Centre for Defence and Security (ICDS), June 19, 2026. URL: <https://icds.ee/en/the-trap-closes-how-russia-suppresses-resistance-in-occupied-ukraine-and-how-we-can-still-help/>
- Ditrych, Ondrej; Hobhouse, Caspar; Kovalčíková, Nad'a; Marangio, Rossella; Rühlig, Tim; Scazzieri, Luigi; Spatafora, Giuseppe; Zorić, Bojana. Empowering Ukraine: Spend smarter, support harder. European Union Institute for Security Studies (EUISS), July 20, 2026. URL: <https://www.iss.europa.eu/publications/analysis/empowering-ukraine-spend-smarter-support-harder>
- Delval, Théa. The Special Tribunal for Ukraine: Turning the Wheels of International Justice. International Centre for Defence and Security (ICDS), June 18, 2026. URL: <https://icds.ee/en/the-special-tribunal-for-ukraine-turning-the-wheels-of-international-justice/>

- Kim, Youngjun. Facing the North Korea–Russia alliance: EU–ROK strategies for deterrence and cooperation. Elcano Royal Institute, July 24, 2026. URL: <https://www.realinstitutoelcano.org/en/analyses/facing-north-korea-russia-alliance-eu-rok-strategies-for-deterrence-and-cooperation/>
- Meister, Stefan. A Declining, but More Dangerous Power: Russia’s Receding Reach in the Neighbourhood. International Centre for Defence and Security (ICDS), June 29, 2026. URL: <https://icds.ee/en/a-declining-but-more-dangerous-power-russias-receding-reach-in-the-neighbourhood/>
- Lozka, Katsiaryna; Althoff, Jonas; Klarhoefer, Lavinia; Gargano, Maria; Yaroshevych, Maryna. The Future of EU Enlargement Policy: Four Scenarios for Enlargement in Wartime Europe. Egmont Institute, July 2, 2026. URL: <https://egmontinstitute.be/the-future-of-eu-enlargement-policy-four-scenarios-for-enlargement-in-wartime-europe/>
- Morina, Engjellushe; Valodskaitė, Gabrielė. The magnificent ten: A coalition of the willing to drive the EU’s next enlargement. European Council on Foreign Relations (ECFR), July 23, 2026. URL: <https://ecfr.eu/publication/the-magnificent-ten-a-coalition-of-the-willing-to-drive-the-eus-next-enlargement/>
- Barana, Luca; Cinciripini, Luca. Ukraine and the Next MFF: The Strive for Predictability. Istituto Affari Internazionali (IAI), July 22, 2026. URL: <https://www.iai.it/en/publications/c41/ukraine-and-next-mff-strive-predictability>
- Bryjka, Filip; Wójtowicz, Aleksandra. Escalating the Polish-Ukrainian dispute: Russia’s operational objective in Poland. Polish Institute of International Affairs (PISM), August 24, 2026. URL: <https://www.pism.pl/publications/escalating-the-polish-ukrainian-dispute-russias-operational-objective-in-poland>
- Surwillo, Izabela; Schwab, Julia. Europe’s energy security in 2026: More resilient, but systemically exposed. Danish Institute for International Studies (DIIS), August 19, 2026. URL: <https://www.diis.dk/en/research/europes-energy-security-in-2026-more-resilient-but-systemically-exposed>
- Szczudlik, Justyna. The European Union faces “China Shock 2.0”. Polish Institute of International Affairs (PISM), July 20, 2026. URL: <https://www.pism.pl/publications/the-european-union-faces-china-shock-20>
- Kaca, Elżbieta. Countering the use of crypto-assets to circumvent sanctions against Russia. Polish Institute of International Affairs (PISM), July 17, 2026. URL: <https://www.pism.pl/publications/countering-the-use-of-crypto-assets-to-circumvent-sanctions-against-russia>
- Vladimirov, Martin; Kostova, Tihomira; Koeppen, Marius; Petrova, Vanya. Strategic Corruption: The Nexus Between Russian Illicit Financial Flows and Offshore Finance. Center for the Study of Democracy, July 28, 2026. URL: <https://csd.eu/publications/publication/strategic-corruption-1/>
- Kaca, Elżbieta. The results and limits of European states’ interventions against the Russian shadow fleet. Polish Institute of International Affairs (PISM), August 25, 2026. URL: <https://www.pism.pl/publications/the-results-and-limits-of-european-states-interventions-against-the-russian-shadow-fleet>
- Maurice, Paul. France-Germany: Overcoming Differences to Strengthen European Sovereignty. Institut français des relations internationales (IFRI), July 15, 2026. URL: <https://www.ifri.org/en/memos/france-germany-overcoming-differences-strengthen-european-sovereignty>
- Leonard, Mark. The tragedy of “Westalgia”. European Council on Foreign Relations (ECFR), July 16, 2026. URL: <https://ecfr.eu/article/the-tragedy-of-westalgia/>
- Wilson, Houston. Europe in an Age of America First Economics. Istituto Affari Internazionali (IAI), August 3, 2026. URL: <https://www.iai.it/en/publications/c05/europe-age-america-first-economics>
- Belin, Célia; Cliffe, Jeremy; Lons, Camille; Victor, Constance. If Marine Le Pen wins: A European guide to a far-right France. European Council on Foreign Relations (ECFR), August 4, 2026. URL: <https://ecfr.eu/publication/if-marine-le-pen-wins-a-european-guide-to-a-far-right-france/>

РОЗДІЛ 2. АНАЛІТИЧНІ МАТЕРІАЛИ INSIGHT LAB

Попович Олександра. Російський дрон на території країн НАТО: що це означає?

- Adamowski J. Russia's 'Zapad' drill has Europe on edge about low-key attacks. Defense News. 2025. 2 Sept. URL: <https://www.defensenews.com/global/europe/2025/09/02/russias-zapad-drill-has-europe-on-edge-about-low-key-attacks/> (дата звернення: 08.08.2026).
- Drone flights near airbase could be spying operation, Belgium's defence minister says / Euronews. 2025. 3 Nov. URL: <https://www.euronews.com/2025/11/03/drone-flights-near-airbase-could-be-spying-operation-belgiums-defence-minister-says> (дата звернення: 08.08.2026).
- Drone incursions sow fear, chaos along NATO's Baltic, Finnish borders / Reuters. 2026. 28 July. URL: <https://www.reuters.com/business/aerospace-defense/drone-incursions-sow-fear-chaos-along-natos-baltic-finnish-borders-2026-07-28/> (дата звернення: 07.08.2026).
- Hoeft C., Greene N., Newton M. A Necessary Air of Venom: Hardening NATO's Airspace. Center for European Policy Analysis (CEPA). 2025. 20 Nov. URL: <https://cepa.org/article/a-necessary-air-of-venom-hardening-natos-airspace/> (дата звернення: 09.08.2026).
- NATO launches "Eastern Sentry" to bolster posture along eastern flank / North Atlantic Treaty Organization. 2025. 12 Sept. URL: <https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank> (дата звернення: 07.08.2026).
- NATO member Romania shoots down stray drones from Ukraine war after years of incursions / Associated Press. 2026. 28 July. URL: <https://apnews.com/article/romania-europe-russia-ukraine-war-drones-nato-ee9775ba338f5408bfa9ab3cb5f2ad1d> (дата звернення: 08.08.2026).
- Russia's UAV Campaign Over Europe : Research Paper / International Institute for Strategic Studies (IISS). 2026. URL: https://www.iiss.org/globalassets/media-library---content-migration/images-delta/publications/research-papers/2026-new/russia-uav/ammended-file/russia_uav-campaign-over-europe.pdf (дата звернення: 09.08.2026).
- Russian Offensive Campaign Assessment, September 10, 2025 / Institute for the Study of War. 2025. 10 Sept. URL: <https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-september-10-2025/> (дата звернення: 08.08.2026).
- Pleines H. Violations of non-combatant airspace during the Russo-Ukrainian war. 24 Feb. 2022–01 Sept. 2026 : dataset. – Version 1.2. – Discuss Data, 2026. – URL: <https://zenodo.org/records/22303031/files/dataset.xlsx> (дата звернення: 14.08.2026).
- Romanian lawmakers adopt law to shoot down drones breaching airspace // Reuters. – 2025. – 26 Feb. – URL: <https://www.reuters.com/world/europe/romanian-lawmakers-adopt-law-shoot-down-drones-breaching-airspace-2025-02-26/> (дата звернення: 14.08.2026).

Василик Ярина. Від «Шахеда» до спільного виробництва: чого Росія та Іран навчилися один в одного

- U.S. Department of the Treasury. Treasury Sanctions Iranian Persons Involved in Production of Unmanned Aerial Vehicles and Weapon Shipment to Russia. 08.09.2022. URL: <https://home.treasury.gov/news/press-releases/jy0940> (accessed: 18.08.2026)
- Burrows E. Russia is sending upgraded drones used in the Ukraine war to Iran, officials say. Associated Press. 27.03.2026. URL: <https://apnews.com/article/russia-iran-drones-shahed-war-israel-ukraine-840b4f885d99714bdb7813c0d56213cf> (accessed: 18.08.2026)
- Rubin U. Russia's Iranian-Made UAVs: A Technical Profile. Royal United Services Institute (RUSI). 13.01.2023. URL: <https://www.rusi.org/explore-our-research/publications/commentary/russias-iranian-made-uavs-technical-profile> (accessed: 18.08.2026).
- Jensen B., Atalan Y. Drone Saturation: Russia's Shahed Campaign. Center for Strategic and International Studies. 13.05.2025. URL: <https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign> (accessed: 19.08.2026)

- Burrows E. Drone debris found in Ukraine indicates Russia is using new technology from Iran. Associated Press. 25.06.2025. URL: <https://apnews.com/article/russia-iran-drones-shahed-ukraine-israel-strikes-3ddeb853845f0ea5f81878165af07bfd> (accessed: 20.08.2026).
- Council of the European Union. Council Decision (CFSP) 2026/263 of 29 January 2026 amending Decision 2010/413/CFSP concerning restrictive measures against Iran. Official Journal of the European Union. 2026. URL: <https://eur-lex.europa.eu/eli/dec/2026/263/oj/eng> (accessed: 19.08.2026)
- Harbuz (Dnipro OSINT). Russia's high-security economic zone: how Alabuga, the country's main drone factory, operates. Ukrainska Pravda. 26.05.2026. URL: <https://www.pravda.com.ua/eng/articles/2026/05/26/8036479/> (accessed: 20.08.2026)
- U.S. Department of the Treasury. Treasury Targets Networks Facilitating Illicit Trade and UAV Transfers on Behalf of Iranian Military. 25.04.2024. URL: <https://home.treasury.gov/news/press-releases/jy2295> (accessed: 19.08.2026)
- Albright D., Burkhard S., Faragasso S. Highlights of Institute Assessment of Alabuga Drone Documents, Supplied by Dalton Bennett at the Washington Post. Institute for Science and International Security. 17.08.2023. URL: <https://isis-online.org/isis-reports/highlights-of-institute-assessment-of-alabuga-drone-documents?> (accessed: 19.08.2026)
- Andreika V. Russia's Changes in the Conduct of War Based on Lessons from Ukraine: Adapting Technology, Force Structures, and the Defense Industry. Military Review. September–October 2025. URL: <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2025/Lessons-from-Ukraine/> (accessed: 19.08.2026)
- Ismay J. Russia Is Replicating Iranian Drones and Using Them to Attack Ukraine. The New York Times. 10.08.2023. URL: <https://www.nytimes.com/2023/08/10/us/russia-iran-drones-ukraine.html> (accessed: 19.08.2026)
- Burrows E., Arhirova H., Hinnant L. Operation False Target: How Russia plotted to mix a deadly new weapon among decoy drones in Ukraine. Associated Press. 26.12.2024. URL: <https://apnews.com/article/russia-ukraine-war-drones-thermobaric-bombs-decoy-2f904b04fcc5de17549415a974f5a92b> (accessed: 19.08.2026)
- Jensen B., Atalan Y. Drone Saturation: Russia's Shahed Campaign. Center for Strategic and International Studies (CSIS). 13.05.2025. URL: <https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign> (accessed: 19.08.2026)
- Landay J., Slattery G., Azhari T. Iran strikes on CIA facilities prompt questions about possible Russian role. Reuters. 22.07.2026. URL: <https://www.reuters.com/world/middle-east/iran-strikes-cia-facilities-prompt-questions-about-possible-russian-role-2026-07-22/> (accessed: 19.08.2026).
- Zelin A. Y. Iran's Support for Russia and Lessons Learned from Ukraine : testimony submitted to the Commission on Security and Cooperation in Europe (U.S. Helsinki Commission). The Washington Institute for Near East Policy. 20.04.2026. URL: <https://www.washingtoninstitute.org/sites/default/files/pdf/ZelinTestimony-20260421-Helsinki.pdf>
- Robertson N., Nakashima E., Strobel W. P. Russia is providing Iran intelligence to target U.S. forces, officials say. The Washington Post. 06.03.2026. URL: <https://www.washingtonpost.com/national-security/2026/03/06/russia-iran-intelligence-us-targets/> (accessed: 20.08.2026)
- Welsch M., Atalan Y., Jensen B., Tiersten-Nyman E. The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine. Center for Strategic and International Studies (CSIS). 07.07.2026. URL: <https://www.csis.org/analysis/geography-coercion-russian-missile-and-drone-campaigns-ukraine> (accessed: 20.08.2026)
- Bondar K. Unpacking Iran's Drone Campaign in the Gulf: Early Lessons for Future Drone Warfare. Center for Strategic and International Studies (CSIS). 10.03.2026. URL: <https://www.csis.org/analysis/unpacking-irans-drone-campaign-gulf-early-lessons-future-drone-warfare> (accessed: 20.08.2026)

Кот Катерина. Диверсії як інструмент зовнішньої політики: як Росія тестує межі реакції Заходу?

- Rovner J., Cormac R., Maschmeyer L. Sand in the gears: Sabotage in world politics. European Journal of International Security. 2025. URL: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/EB1FA8B5BC7400C358EFFF2D8624B181/S2057563725100254a.pdf/sand-in-the-gears-sabotage-in-world-politics.pdf> (accessed: 20.08.2026)
- Poland blames sabotage for railway blast on Ukraine delivery line. Associated Press. 2025. 17 Nov. URL: <https://apnews.com/article/poland-sabotage-explosion-rail-track-warsaw-97dae3045d4e1ff329780526c6279c0f> (accessed: 19.08.2026)
- Russian Europe sabotage. Associated Press Projects. URL: <https://apnews.com/projects/russian-europe-sabotage/> (accessed: 20.08.2026)
- Greene S., Soldatov A., Borogan I. War Without End: Russia's Shadow Warfare. Center for European Policy Analysis (CEPA). 2025. Nov. URL: <https://cepa.org/wp-content/uploads/2025/11/CEPA-War-Without-End-Russia-Shadow-Warfare-11.19.25.pdf> (accessed: 19.08.2026)
- Countering Russia's Shadow War. Center for European Policy Analysis (CEPA). URL: <https://cepa.org/programs/democratic-resilience/countering-russias-shadow-war/> (accessed: 19.08.2026)
- Burrows E., Di Lorenzo S., Rasmussen S., Hamlin P. Tracked: How Russia is waging a hybrid campaign of violence and disruption across Europe. Associated Press. 2025. 21 Mar. URL: <https://apnews.com/article/russia-ukraine-war-europe-hybrid-campaign-d61887dd3ec6151adf354c5bd3e6273e> (accessed: 19.08.2026)
- Stewart B. Europe says Russia is ramping up a sabotage campaign. It just doesn't know how to deal with it. CBC News. 2025. 21 Nov. URL: <https://www.cbc.ca/news/world/russia-sabotage-europe-9.6985916> (accessed: 19.08.2026)
- Sweden's Säpo Reports That Russia Is Evolving Sabotage Tactics. Eurasia Daily Monitor. Jamestown Foundation. URL: <https://jamestown.org/swedens-sapo-reports-that-russia-is-evolving-sabotage-tactics/> (accessed: 19.08.2026)
- Russia's hybrid activities: EU sanctions. European Council / Council of the European Union. URL: <https://www.consilium.europa.eu/en/policies/sanctions-against-russia-hybrid-threats/#what> (accessed: 25.08.2026)

Лончина Юлія. Коли диверсія стає нападом: чи застосовна стаття 5 НАТО до російських гібридних операцій?

- Charlish, A., Kelly, L., & Erling, B. (2025). Poland downs drones in its airspace, becoming first NATO member to fire during war in Ukraine. Reuters. Available from: <https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/> (Accessed: 25 August 2026).
- NATO. (2021). Brussels Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels. NATO Official Texts. Available from: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communication> (Accessed: 25 August 2026).
- NATO. (2025). Collective defence and Article 5. NATO Official Website. Available from: <https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5> (Accessed: 25 August 2026).
- NATO. (2025). Countering hybrid threats. NATO Official Website. Available from: <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats> (Accessed: 25 August 2026).
- NATO. (2025). Statement by NATO Secretary General Mark Rutte on the violation of Polish airspace by Russian drones. NATO Official Transcripts. Available from: <https://www.nato.int/en/news-and-events/events/transcripts/2025/09/10/statement> (Accessed: 15 September 2026).

- NATO. (2026). NATO Allies condemn recent airspace violations and incidents. NATO Official Articles. Available from: <https://www.nato.int/en/news-and-events/articles/news/2026/08/12/nato-allies-condemn-recent-airspace-violations-and-incidents> (Accessed: 15 September 2026).
- Reuters. (2024). Russia's suspected sabotage campaign steps up in Europe. Reuters. Available from: <https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/> (Accessed: 15 September 2026).
- Reuters. (2024). Telecoms cable linking Finland and Germany likely severed, owner says. Reuters. Available from: <https://www.reuters.com/business/media-telecom/telecoms-cable-linking-finland-germany-likely-severed-owner-says-2024-11-18/> (Accessed: 15 September 2026).
- RUSI. (2026). Old ships, modern menace: How to tackle the world's shadow fleets. Royal United Services Institute. Available from: <https://www.rusi.org/explore-our-research/publications/commentary/old-ships-modern-menace-how-tackle-worlds-shadow-fleets> (Accessed: 15 September 2026).
- TVP World. (2026). Russian sabotage: Poland charges five suspects over arson of Warsaw shopping center. TVP World. Available from: <https://tvpworld.com/92425771/poland-indicts-five-over-russia-linked-shopping-mall-inferno> (Accessed: 15 September 2026).
- Ukrainska Pravda. (2025). Early estimates indicate 19 violations of Polish airspace. Ukrainska Pravda. Available from: <https://www.pravda.com.ua/eng/news/2025/09/10/7530171/> (Accessed: 15 September 2026).

Мелконова Олена. Чи може оборонна промисловість стати новою спеціалізацією України в економіці ЄС?

- Forbes.ua «Єврокомісія та Міноборони України запускають програму оборонних інновацій на €161 млн», 23.04.2026. <https://forbes.ua/news/160-mln-na-tehnologii-podviynogo-priznachennya-es-ta-ukraina-zapuskayut-novu-programu-23042026-38244>
- Кабінет Міністрів України «Україна та ЄС посилюють співпрацю з розвитку спільних оборонних проєктів», 01.04.2026. <https://www.kmu.gov.ua/news/ukraina-ta-ies-posyliuiut-spiivpratsiu-z-rozvytku-spilnykh-oboronnykh-proektiv>
- РБК-Україна «Оборонна промисловість України найкраща у світі, заявив єврокомісар», 23.06.2026. <https://www.rbc.ua/rus/news/ukrayinska-oboronka-naykrashcha-evropa-mae-1782218909.html>
- Главком «Єврокомісар назвав українську оборонну промисловість найкращою у світі», 23.06.2026. <https://glavcom.ua/world/world-politics/jevrokomisar-nazvav-ukrajinsku-oboronnu-promislovist-najkrashchoju-u-sviti-1127524.html>
- European Integration Portal «Презентована Європейська стратегія оборонної промисловості, яка передбачає активне долучення України». <https://eu-ua.kmu.gov.ua/en/news/prezentovana-yevropejska-strategiya-oboronnoyi-promyslovosti-yaka-peredbachaye-aktyvne-doluchennya-ukrayiny/>
- NDU.kr.ua «Європейська оборонна промисловість після 2022 року: нова архітектура безпеки», 03.03.2026. <https://ndu.kr.ua/960-evropejska-oboronna-promislovist-pislya-2022-roku-nova-arkhitektura-bezpeki>
- Національна поліція України «Нацполіція та СБУ викрили іранського генерала, який організував передачу росії технологій виробництва Shahed», 10.03.2026. <https://npu.gov.ua/news/natpolitsiia-ta-sbu-vykryly-iranskoho-henerala-iakyi-orhanizuvav-peredachu-rosii-tekhnologii-vyrobnystva-shahed>
- LB.ua «Аналітики США розслідують можливий зв'язок росії з ударами Ірану по об'єктах ЦРУ», 23.07.2026. https://lb.ua/world/2026/07/23/753864_reuters_analitiki_ssha.html

- 24 Канал (Економіка) «Виробництво зброї в Україні - як розвивається український ОПК». https://24tv.ua/economy/virobnitstvo-zbroyi-ukrayini-yak-rozvivayetsya-ukrayinskiy-opk_n2887633
- NV.ua «Оборонно-промисловий комплекс України — динаміка зростання та співпраця з ЄС у виробництві зброї». <https://nv.ua/ukr/ukraine/events/oboronno-promisloviy-kompleks-ukrajini-dinamika-zrostannya-ta-spiivpracya-z-yes-u-virobnictvi-zbroji-50536517.html>
- РБК-Україна «Виробництво української зброї зросло у півтора рази за 2025 рік», 08.01.2026. <https://www.rbc.ua/rus/news/oboronna-promislovist-ukrayini-rik-zbilshila-1767838990.html>
- Forbes.ua «Виробництво української зброї у 2026-му може сягнути \$60 млрд», 07.11.2025. <https://forbes.ua/news/u-2026-rotsi-potuzhnosti-ukrainskogo-vpk-zrostut-mayzhe-vdvichilishe-dalekobiyni-sistemi-dadut-35-mlrd-prognoz-rnbo-07112025-33937>
- РНБО України «Українська оборонна промисловість: масштаб, ефективність, результат». <https://www.rnbo.gov.ua/ua/Dialnist/7384.html>
- Forbes.ua «Дрони, ракети, бронетехніка: як Україна зміцнює власний ОПК», 24.02.2026. <https://forbes.ua/war-in-ukraine/oboronna-revolyuetsiya-yak-za-tri-roki-viyni-ukraina-sformuvala-novu-viyskovu-realnist-rozpovidai-ministr-oboroni-rustem-umerov-23022025-27435>
- LB.ua «Зброя на експорт: пропозиція, попит, умови», 07.07.2026. https://lb.ua/world/2026/07/07/750102_zbroya_eksport_propozitsiya.html
- Міністерство економіки та довкілля України «Європейська програма SAFE: інтеграція українського оборонно-промислового комплексу». <https://me.gov.ua/News/Detail/83472515-ed55-4b55-90c6-d40a0627faa9?lang=uk-UA&title=Safe>
- Суспільне Новини «Оборонна програма ЄС SAFE: вже досягли повної підписки на всі 150 млрд євро», 29.08.2025. <https://suspilne.media/1102514-kreditna-oboronna-programa-es-safe-vze-dosagli-povnoi-pidpiski-na-vsi-150-mlrd-evro/>
- Forbes.ua «ЄС запускає оборонний фонд SAFE на €150 млрд: Україна зможе долучитися», 27.05.2025. <https://forbes.ua/news/rada-es-zatverdila-stvorenniya-fondu-na-150-mlrd-dlya-investitsiy-v-oboronu-shcho-tse-dast-ukraini-27052025-30062>
- Forbes.ua «ЄС розподілив €150 млрд оборонних кредитів SAFE між 19 країнами. Що отримає Україна від цього», 09.09.2025. <https://forbes.ua/news/evrokomisiya-rozdilila-150-mlrd-kreditiv-safe-na-oboronu-mizh-19-derzhavami-shcho-tse-prinese-ukraini-09092025-32490>
- Європейська правда «150 млрд євро на переозброєння: що таке SAFE і що від нього може отримати Україна», 03.09.2025. <https://www.eurointegration.com.ua/articles/2025/09/3/7219285/>
- Кабінет Міністрів України «Task Force Україна–ЄС з питань оборонно-промислового співробітництва буде інструментом залучення українського ОПК в європейську ініціативу SAFE». <https://www.kmu.gov.ua/news/task-force-ukrainai-es-z-pytan-oboronno-promyslovoho-spiivrobitnytstva-bude-instrumentom-zaluchennia-ukrainskoho-opk-v-ievropeisku-initsiatyvu-safe>
- NV.biz «Єврокомісія розподілила оборонні кредити між 19 країнами — на що може розраховувати Україна», 10.09.2025. <https://biz.nv.ua/ukr/economics/safe-150-mlrd-yevro-na-oboronnu-promislovist-yes-ta-spilni-proyekti-50543693.html>
- Bug.org.ua «Польща першою в Євросоюзі отримала фінансування за оборонною програмою SAFE», 30.05.2026. <https://bug.org.ua/news/polshha-pershoyu-v-yevrosoyuzi-otrymala-finansuvannya-za-oboronnoyu-programoyu-safe-1042493/>

Троян Андрій. Оборонна промисловість України після війни: драйвер економічного розвитку чи тимчасова перевага?

- State Concern 'Ukroboronprom'. Annual Report 2020. URL: https://ukroboronprom.com.ua/storage/documents/Report_ua.pdf (accessed: 21 August 2026).
- Harmash O. Ukraine in 'final stages' to set up three new JVs with European armsmakers. Reuters. 2024. 12 Nov. URL: <https://www.reuters.com/world/europe/ukraine-final-stages-set-up-three-new-jvs-with-european-armsmakers-2024-11-12/> (date of access: 21 August 2026).

- National Security and Defense Council of Ukraine. Ukraine's Defence Industry: Scale, Efficiency, Result. 2026. 28 Jan. URL: <https://www.rnbo.gov.ua/ua/Diialnist/7384.html> (accessed: 21 August 2026).
- Miroshnychenko B. Engineers, Incoming Strikes, and High Technology. Will Ukraine Be Able to Produce More Weapons in 2026? *Oboronka*. 2025. 26 Dec. URL: <https://oboronka.mezha.ua/yak-zroslo-virobnictvo-zbroji-ukrajini-u-2025-roci-307326/> (accessed: 21 August 2026).
- Sereda O. Ukraine's MIC Sector: What Are Its Real Achievements and Prospects? *ZN.UA*. 2026. 4 Feb. URL: <https://zn.ua/ukr/ECONOMICS/sektor-opk-ukrajini-jaki-realni-dosjahnennja-i-perspektivi-.html> (accessed: 21 August 2026).
- CES Team. August Economic Review. Special Topic: How Is Arms Production Transforming Ukraine's Economy? Kyiv: Centre for Economic Strategy, 2025. 22 p. URL: <https://ces.org.ua/wp-content/uploads/2025/08/economic-review-august-2025.pdf> (date of access: 21 August 2026).
- Trends in International Arms Transfers, 2025 / M. George et al. SIPRI Fact Sheet. Stockholm: Stockholm International Peace Research Institute, 2026. 12 p. DOI: <https://doi.org/10.55163/OSMS3959>. URL: https://www.sipri.org/sites/default/files/2026-03/fs_2603_at_2025.pdf (date of access: 21 August 2026).
- Tech Force in UA. 89% of Manufacturers Cite Security Risks as the Main Reason for Relocation—New TFUA Survey. 2025. 27 Oct. URL: <https://techforce.in.ua/news/article/golovnoyu-prichinoyu-relokaciyi-nazivayut-bezpekovi-riziki> (accessed: 21 August 2026).
- Ministry of Defence of Ukraine. Share of Ukrainian Manufacturers in Procurement of Military Goods Rises to 82%. 2026. 23 Jan. URL: <https://mod.gov.ua/news/do-82-zroslo-chastka-ukrayinskih-virobnikiv-u-zakupivlyah-tovariv-vijskovogo-priznachennya> (accessed: 21 August 2026).
- Ministry of Defence of Ukraine. Ministry of Defence Secured More Than \$6 Billion for Ukraine's MIC in 2025. 2026. 3 Jan. URL: <https://mod.gov.ua/news/minoboroni-zaluchilo-ponad-6-mlrd-na-ukrayinskij-opk-v-2025-rocz> (accessed: 21 August 2026).
- Certain Issues Concerning International Transfers of Goods During the Period of Martial Law in Ukraine: Resolution No. 875 of the Cabinet of Ministers of Ukraine dated 1 July 2026. URL: <https://zakon.rada.gov.ua/laws/show/875-2026-%D0%BF> (accessed: 21 August 2026).
- Romaniuk R. The Cabinet of Ministers Opened Arms Exports, but Not Everyone Will Be Able to Sell, Not Everywhere, and Not Everything. What Is the Problem with the New Mechanism? *Oboronka*. 2026. 9 July. URL: <https://oboronka.mezha.ua/eksport-zbroji-z-ukrajini-yak-pracyuye-noviy-fast-track-ta-chomu-vin-ne-dlya-vsih-313057/> (accessed: 21 August 2026).
- The President of Ukraine and the Prime Minister of Denmark Signed the Drone Deal in Ankara. Official Website of the President of Ukraine. 2026. 7 July. URL: <https://www.president.gov.ua/news/v-ankari-prezident-ukrayini-j-premyer-ministerka-daniyi-pidp-105321> (accessed: 21 August 2026).
- Ministry of Defence of Ukraine. Build in Ukraine—an Initiative Facilitating the Localisation of International Companies in Ukraine. 2025. 22 Oct. URL: <https://mod.gov.ua/news/build-in-ukraine-inicziativa-yaka-spriyaye-lokalizacziyi-mizhnarodnih-kompanij-v-ukrayini> (accessed: 21 August 2026).
- Rheinmetall: A Powerful Partner at Ukraine's Side. Rheinmetall. 2023. 20 July. Updated 10 Feb. 2025. URL: <https://www.rheinmetall.com/en/media/stories/2023/rheinmetall-a-powerful-partner-at-ukraine-side> (date of access: 21 August 2026).
- High-level Delegation Visits Quantum Systems Ukraine to Witness Increased Local Manufacturing Capacity. Quantum Systems. 2025. 24 Feb. URL: <https://quantum-systems.com/news/high-level-delegation-visits-quantum-systems-ukraine/> (date of access: 21 August 2026).
- EU Military Support for Ukraine. Council of the European Union. Last reviewed 12 Aug. 2026. URL: <https://www.consilium.europa.eu/en/policies/military-support-ukraine/> (date of access: 21 August 2026).

- Ukrainian Council of Defence Industry, CORE Team. Workforce and Salaries in Ukraine's Defence Industry: Survey Results. 2026. URL: <https://drive.google.com/file/d/1DQFcIwmGwGgwiOnI1DEVXy3oEb1aEYSP/view> (accessed: 21 August 2026).
- State Employment Service of Ukraine. Employment Service Clients Use Two-Thirds of Training Vouchers for Retraining and Professional Development. Government Portal. 2026. 16 Feb. URL: <https://www.kmu.gov.ua/news/dvi-tretikh-vaucheriv-na-navchannia-kliienty-sluzhby-zainiatosti-berut-na-perepidhotovku-ta-pidvyshchennia-kvalifikatsii> (accessed: 21 August 2026).
- European Commission. Directorate-General for Research and Innovation. Support to Ukraine on Research Infrastructure Policy. Luxembourg: Publications Office of the European Union, 2025. DOI: <https://doi.org/10.2777/4728571> (date of access: 21 August 2026).
- Schmid S., Bayuputri D. Unlocking Veteran Potential: The Power of User-Validated Skill Data in Ukraine. SkillLab, 2025. 8 p. URL: <https://share.skilllab.io/hubfs/White%20Papers/Unlocking%20Veteran%20Potential%20-%20The%20Power%20of%20User-Validated%20Skill%20Data%20in%20Ukraine.pdf> (date of access: 21 August 2026).
- Improving Career Pathways and Adapting Ukrainian Veterans to Civilian Employment. Kyiv: Helvetas Swiss Intercooperation, 2025. 35 p. URL: <https://www.helvetas.org/Publications-PDFs/Eastern-Europe-Caucasus/Ukraine/1/%D0%9F%D0%BE%D0%BA%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BA%D0%B0%D1%80%E2%80%99%D1%94%D1%80%D0%BD%D0%B8%D1%85%20%D1%88%D0%BB%D1%8F%D1%85%D1%96%D0%B2%20%D1%82%D0%B0%20%D0%B0%D0%B4%D0%B0%D0%BF%D1%82%D0%B0%D1%86%D1%96%D1%8F%20%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B8%D1%85%20%D0%B2%D0%B5%D1%82%D0%B5%D1%80%D0%B0%D0%BD%D1%96%D0%B2%20%D0%B4%D0%BE%20%D1%86%D0%B8%D0%B2%D1%96%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BF%D1%80%D0%B0%D1%86%D0%B5%D0%B2%D0%BB%D0%B0%D1%88%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F.pdf> (accessed: 21 August 2026).
- On Approval of the Veteran Policy Strategy for the Period up to 2030 and Approval of the Operational Action Plan for Its Implementation in 2024–2027: Order No. 1209-r of the Cabinet of Ministers of Ukraine dated 29 Nov. 2024. URL: <https://zakon.rada.gov.ua/laws/show/1209-2024-%D1%80#Text> (accessed: 21 August 2026).
- On Approval of the Strategy for Establishing a System for Transitioning from Military Service to Civilian Life for the Period up to 2033 and Approval of the Operational Action Plan for Its Implementation in 2025–2027: Order No. 1350-r of the Cabinet of Ministers of Ukraine dated 31 Dec. 2024. URL: <https://www.kmu.gov.ua/npas/pro-skhhvalennia-stratehii-formuvannia-systemy-povernennia-z-viiskovoi-sluzhby-do-tsyvilnoho-zhyttia-na-period-do-2033-roku-1350r-311224> (accessed: 21 August 2026).
- On Approval of the State Target Programme 'Veteran. Work' for 2026–2027: Order No. 154-r of the Cabinet of Ministers of Ukraine dated 11 Feb. 2026. URL: <https://zakon.rada.gov.ua/laws/show/154-2026-%D1%80> (accessed: 21 August 2026).

Помогайбо Назарій. Стимування без війни: чи готові країни Балтії до російських гібридних загроз?

- Lithuania closes its border with Belarus for a month. Ośrodek Studiów Wschodnich (OSW). 30.10.2025. URL: <https://www.osw.waw.pl/en/publikacje/analyses/2025-10-30/lithuania-closes-its-border-belarus-a-month>.
- Lithuania reopens border crossings with Belarus after tensions over smuggling balloons. Euronews. 19.11.2025. URL: <https://www.euronews.com/2025/11/19/lithuania-reopens-border-crossings-with-belarus-after-tensions-over-smuggling-balloons>.

- National Threat Assessment 2026 / State Security Department of the Republic of Lithuania (VSD), Defence Intelligence and Security Service under the Ministry of National Defence (AOTD). Vilnius, 2026. URL: <https://www.vsd.lt/wp-content/uploads/2026/03/2026-GR-ENG-El.pdf>.
- The Riigikogu passed constitutional amendment restricting the right to vote. Riigikogu. 26.03.2025. URL: <https://www.riigikogu.ee/en/news-from-committees/constitutional-committee/the-riigikogu-passed-constitutional-amendment-restricting-the-right-to-vote/>.
- Maruste R. Narrowing the Estonian Electorate: Excluding Russian Citizens from Local Elections Amid Security Concerns. Verfassungsblog. 25.04.2025. URL: <https://verfassungsblog.de/narrowing-the-estonian-electorate/>.
- Fremer I. Estonia: Country Amends Constitution to Restrict Local Voting Rights of Noncitizens. Global Legal Monitor / Law Library of Congress. 04.08.2025. URL: <https://www.loc.gov/item/global-legal-monitor/2025-08-04/estonia-country-amends-constitution-to-restrict-local-voting-rights-of-noncitizens>.
- Mihhail Stalnuhhin's electoral list wins most seats in Narva. ERR News. 20.10.2025. URL: <https://news.err.ee/1609834311/mihhail-stalnuhhin-s-electoral-list-wins-most-seats-in-narva>.
- Estonia's Russian speakers may determine a change in the country's policies. Veridica. 28.10.2025. URL: <https://www.veridica.ro/en/opinions/estonias-russian-speakers-may-determine-a-change-in-the-countrys-policies>.
- Court overturns decision to ban TV Rain in Latvia. Latvijas Sabiedriskais medijs (LSM). 16.07.2025. URL: <https://eng.lsm.lv/article/features/media/16.07.2025-court-overturns-decision-to-ban-tv-rain-in-latvia.a606973/>.
- Latvian media watchdog appeals against court overturning TV Rain license ban. Latvijas Sabiedriskais medijs (LSM). 21.08.2025. URL: <https://eng.lsm.lv/article/features/media/21.08.2025-latvian-media-watchdog-appeals-against-court-overturning-tv-rain-license-ban.a611177/>.
- Estonian in Name, Russian Content: How the Pravda Network Brings Telegram Propaganda into Estonia's Information Space. Propastop. 04.08.2026. URL: <https://www.propastop.org/en/2026/08/04/estonian-in-name-russian-content-how-the-pravda-network-brings-telegram-propaganda-into-estonias-information-space/>.
- Portal Kombat : un réseau structuré et coordonné de propagande prorusse / VIGINUM ; Secrétariat général de la défense et de la sécurité nationale. Paris, 2024. URL: <https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse>.
- Bentzen N. The European Democracy Shield: An overview. European Parliamentary Research Service. 15.01.2026. URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782603/EPRS_ATA\(2026\)782603_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782603/EPRS_ATA(2026)782603_EN.pdf).
- The new European Centre for Democratic Resilience starts its work / European Commission. 24.02.2026. URL: https://enlargement.ec.europa.eu/news/new-european-centre-democratic-resilience-starts-its-work-2026-02-24_en.
- Special EP committee adopts proposals to improve the European Democracy Shield. Insight EU Monitoring. 23.06.2026. URL: <https://ieu-monitoring.com/editorial/special-ep-committee-adopts-proposals-to-improve-the-european-democracy-shield/1243859>.
- Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act / European Commission. 24.10.2025. URL: <https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-tiktok-and-meta-breach-their-transparency-obligations-under-digital>.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). Official Journal of the European Union. L 277. 27.10.2022. P. 1–102. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.
- The DSA supervision and enforcement architecture. DSA Observatory. 24.06.2022. URL: <https://dsa-observatory.eu/2022/06/24/the-dsa-supervision-and-enforcement-architecture/>.
- Putting collective intelligence to the enforcement of the Digital Services Act. arXiv:2305.01959. 2023. URL: <https://arxiv.org/pdf/2305.01959>.

- Annual Report on the Activities of Latvian State Security Service (VDD) in 2025 / Valsts drošības dienests. Rīga, 2026. URL: <https://vdd.gov.lv/uploads/materials/42/en/annual-report-2025.pdf>.
- International Security and Estonia 2026 / Välisluureamet (Estonian Foreign Intelligence Service). Tallinn, 2026. URL: <https://valisluureamet.ee/doc/raport/2026-en.pdf>.
- €120 million later: the DSA enters the enforcement phase. MediaLaws. 23.12.2025. URL: <https://www.medialaws.eu/e120-million-later-the-dsa-enters-the-enforcement-phase/>.
- DSA enforcement in practice: from rules to commitments and fines / Loyens & Loeff. 10.06.2026. URL: <https://www.loyensloeff.com/insights/news-events/news/dsa-enforcement-in-practice-from-rules-to-commitments-and-fines/>.
- Commission opens formal proceedings against TikTok on election risks under the Digital Services Act / European Commission. 17.12.2024. URL: <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-election-risks-under-digital-services-act>.
- TikTok and the Romanian elections: A stress test for DSA enforcement. DSA Observatory. 20.12.2024. URL: <https://dsa-observatory.eu/2024/12/20/tiktok-and-the-romanian-elections/>.
- https://icds.ee/static/20260823_aaa_u101_112-1024x683.jpg.webp

Ткачов Іван. Від прикордонного паркану до поля бою: як Росія може перевіряти Балтійський щит без відкритого вторгнення?

- Sytas A. Russian threat to Baltic security rising – Estonian intelligence report // Reuters. 08.02.2023. URL: <https://www.reuters.com/world/europe/baltic-security-risk-rising-estonian-intelligence-service-says-2023-02-08/>
- Fraszka B. Baltic States Versus Russian Hybrid Threats. Warsaw Institute. 26.10.2020.
- Countering hybrid threats // NATO. 29.01.2026. URL: <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>
- Ministry of Defence of the Republic of Latvia. The State Defence Concept (2023–2027). Riga, 2023. URL: <https://www.mod.gov.lv/sites/mod/files/document/The%20State%20Defence%20Concept%202023-2027.pdf>
- State Security Department of the Republic of Lithuania, Defence Intelligence and Security Service under the Ministry of National Defence. National Threat Assessment 2026. Vilnius, 2026. URL: <https://www.vsd.lt/wp-content/uploads/2026/03/2026-GR-ENG-El.pdf>
- Aday S., Andžāns M., Bērziņa-Čerenkova U. та ін. Hybrid Threats: 2007 cyber attacks on Estonia // Hybrid Threats. A Strategic Communications Perspective. Riga : NATO Strategic Communications Centre of Excellence, 2019. 10 p. URL: <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>
- Estonian Internal Security Service. Annual Review 2025–2026. Tallinn, 2026. URL: https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2025-2026.pdf

ФОТО ТА ЗОБРАЖЕННЯ

- <https://s.rfi.fr/media/display/3fe40194-990c-11ef-9cfc-005056bfb2b6/w:1024/p:16x9/AP18193379795077.jpg>
- https://www.theparliamentmagazine.eu/siteimg/news-main/ugc-1/fullnews/news/25821/25836_original.jpg
- https://static.ukrinform.com/photos/2019_10/thumb_files/630_360_1572357882-410.jpg
- https://upload.wikimedia.org/wikipedia/commons/a/ac/Ottawa_Treaty_members.svg?utm_source=en.wikipedia.org&utm_campaign=index&utm_content=original
- <https://defence-ua.com/media/contentimages/d0d66f951f6e2d3b.jpg>
- https://commission.europa.eu/sites/default/files/styles/oe_theme_medium_no_crop/public/2025-03/EU%20preparedness%20union%20strategy%20Card.jpg?itok=r39Ql4S1
- https://www.airbus.com/sites/g/files/jlcbta136/files/styles/w780h520/public/2022-06/FCAS%20Poster%20GOOSE_Janes-Magazin_PRINT.JPG?itok=iPe2eIY6
- <https://ecfr.eu/wp-content/uploads/2026/07/605619359-scaled.jpg>
- https://cdn.prod.website-files.com/60a3c1fc44c5715c395770e7/60df8191a884c0804de8b15d_Depositphotos_24064653_1-2015.webp
- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTa-MF6MOavGuN6g8GK24PZ9BttMBLJ7WFGm_zRh_gDW4fGn8kjdoob1pI&s=10
- https://www.economist.com/cdn-cgi/image/width=1424,quality=80,format=auto/content-assets/images/20241116_EUP507.jpg
- https://cdn.prod.website-files.com/63b303944d1e9ec09b741257/64d3b06822a0befce2eb1d96_max-kukurudziak-qbc3Zmxw0G8-unsplash-min.jpg
- [Φoro: https://www.president.gov.ua/storage/j-image-storage/50/56/89/a0b555e83b7d8e55725771f9ed9a5ea2_1750886062_extra_large.jpeg](https://www.president.gov.ua/storage/j-image-storage/50/56/89/a0b555e83b7d8e55725771f9ed9a5ea2_1750886062_extra_large.jpeg)
- https://www.atlanticcouncil.org/wp-content/uploads/2024/10/2024-06-19T120819Z_1029865475_RC2AE8A9I464_RTRMADP_3_NORTHKOREA-RUSSIA-scaled.jpg
- <https://cdn.britannica.com/43/3843-050-FEE525C7/Russia-political-map.jpg>
- https://cdn.ceps.eu/2025/11/P-068228_00-19_01-ORIGINAL-948002.jpg.webp
- https://www.president.gov.ua/storage/j-image-storage/51/45/57/caab1d58009ba1ed20ec9774418b6a0e_1755439697_extra_large.jpeg
- https://www.europarl.europa.eu/resources/library/images/20220202PHT22410/20220202PHT22410_original.jpg
- https://img.lemde.fr/2026/06/19/0/0/3662/2441/664/0/75/0/775d2bb_ftp-1-q5yllwslcrys-6377dbc29f534386b7ac3ed7f025ab47-0-48cde7cb006140508c60d2dcfa5ff34b.jpg
- https://energytransition.org/wp-content/uploads/2025/04/shutterstock_2052065705-scaled.jpg
- <https://www.aeaweb.org/content/file?id=11680>
- <https://financialcrimeacademy.org/wp-content/uploads/2022/07/2-15-1024x576.jpg>
- <https://www.reuters.com/resizer/v2/7CNCZIOHHROT3AY3EZZMIKC66M.jpg?auth=0a15a1f9d0c9325b7dfb5e957a59f0896d1ac5eddf89eab6e0be0d066d65d238&width=1920&quality=80>
- https://cepa.org/wp-content/uploads/2025/12/2025-04-11T131153Z_1076526061_MT1SCPXBL1EV11APR25A10_RTRMADP_3_VESSELS-KIWALA-AND-KURVITS-ON-THE-SEA-scaled.jpg
- <https://www.euractiv.com/content/uploads/sites/2/2025/08/13296722-e1756697742803.jpg>
- https://www.nato.int/content/dam/nato/webready/news/2020-2029/2026/07/07/summit-hosg-reception/20260707_summit-hosg-reception_0007.jpg/jcr:content/renditions/cq5dam.web.1280.1280.jpeg
- <https://www.politico.eu/cdn-cgi/image/width=965,height=643,fit=crop,quality=80,onerror=redirect,format=auto/wp-content/uploads/2020/10/GettyImages-1199162894.jpg>
- https://cdn.unitycms.io/images/CdGslVwsamBB_aTWO6X4gn.jpg

udonation.org
+38(068)0042001
info@udonation.org
53 Vasyl Tyutyunnyk Street, Office 23, Kyiv, Ukraine