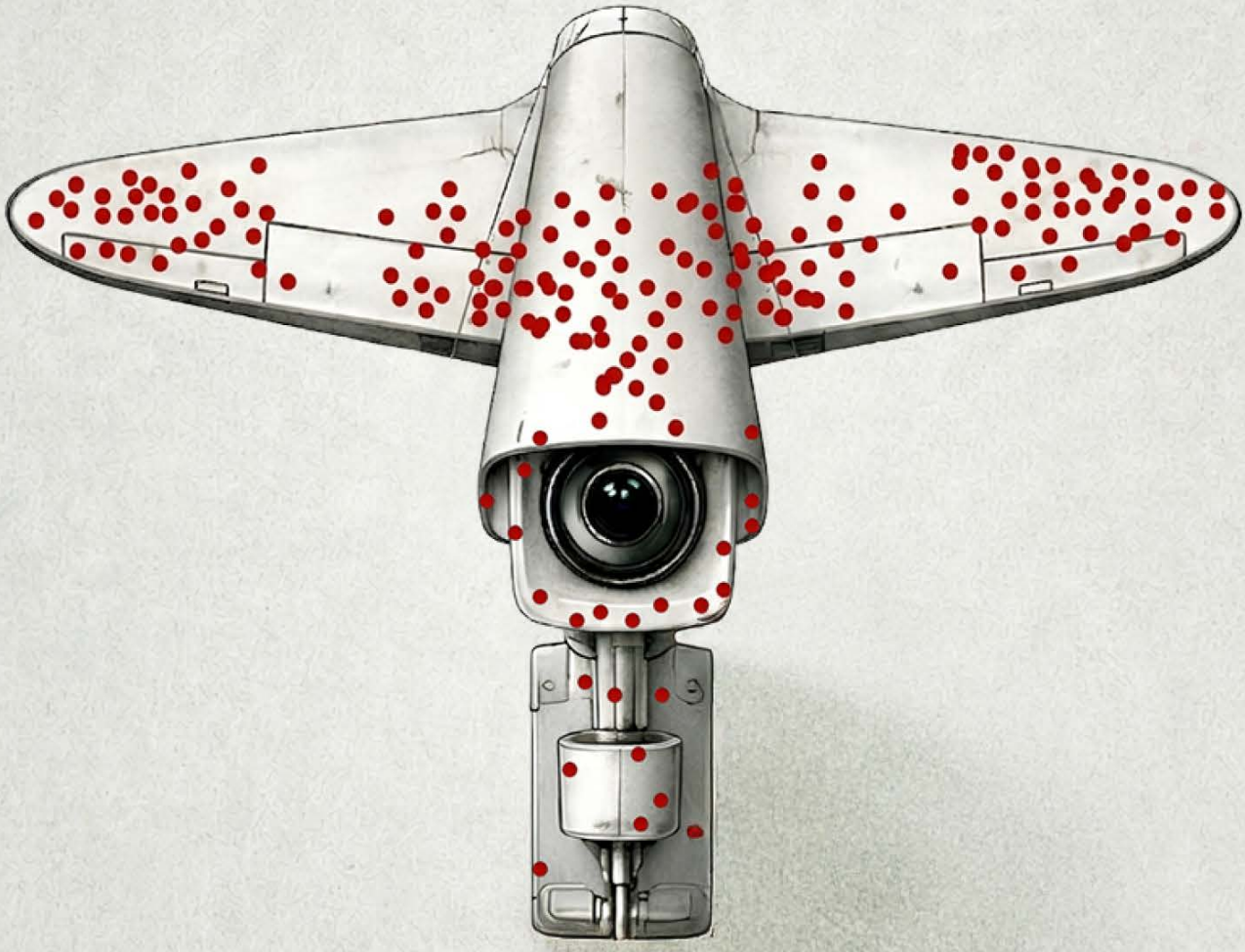
УПЕРЕДЖЕННЯ ШПИГУНСТВА

Безпекові Прогалини Нормативно-Орієнтованих Ініціатив



РАДА
ЕКОНОМІЧНОЇ БЕЗПЕКИ
УКРАЇНИ

РАДА
ВЕРХОВНА РАДА
УКРАЇНИ

УПЕРЕДЖЕННЯ ШПИГУНСТВА

Безпекові Прогалини Нормативно-Орієнтованих Ініціатив

АНОТАЦІЯ

Спроби регулювання ринку комерційних інструментів кібервтручання (Commercial Cyber Intrusion Capabilities, надалі – CCICs) шляхом добровільних ініціатив з'являються дедалі частіше серед спільноти західних країн. Та, в умовах стрімкого розвитку гібридних загроз, здатність цих процесів гарантувати безпекові результати рідко простежується на практиці.

Ініціативи як Pall Mall Process чітко формулюють свої цілі з точки зору безпеки, ставлячи за мету боротьбу з поширенням та неналежним використанням CCICs, наголошуючи на впливі таких процесів на національну безпеку та закликаючи держави боротися з кіберзагрозами за допомогою принципів підзвітності, чіткості, нагляду та прозорості[1]. Це дослідження розглядає Ініціативу—на сьогодні підтриману 27 урядами, включно з США, країнами ЄС, Великою Британією та Японією—крізь призму чотирьох критеріїв: діапазон участі, механізми обмеження, урахування загроз та видимі безпекові наслідки. Попри те, що учасники Ініціативи повноцінно приймають запропоновані норми регулювання, лише одна держава (Італія) відіграє суттєву роль на ринку шпигунських технологій. Тоді ж як 21 із 31 виробника таких технологій знаходиться в державах за межами Ініціативи (Ізраїль, Індія).

Участь сконцентрована серед держав більш схильних до прийняття декларативних та доброчесних процесів, не враховуючи, таким чином, основні вектори загроз — як от неконтрольоване поширення CCICs. Добровільні зобов'язання не передбачають жодних стримувальних механізмів чи покарання, що і відображається на стані сучасної кіберсфери: шпигунське ПЗ “Pegasus” продовжує використовуватись проти європейців, ринок технологій віддаленого стеження оцінюється у $55 млрд. (станом на 2025), а “годувати” хакерські кіберкомпанії продовжує приватний капітал.

ВСТУП

За останні роки спроби регулювання ринку комерційних інструментів кібервтручання (CCICs) набрали обертів. Велику роль у цьому процесі відіграють ініціативи як Pall Mall Process (надалі Ініціатива), створені з метою запобігання розповсюдженню та безвідповідальному використанню CCICs. Дедалі більша увага до цієї проблеми на міжнародному рівні відображає занепокоєння стрімким поширенням CCICs та впливом не лише на права людини, а й на національну безпеку та цифрову стабільність демократичних держав. В основі ініціатив, спрямованих на регулювання ринку шпигунських технологій (до прикладу Вассенаарські Угоди, Pall Mall Process, Регулювання ЄС щодо товарів подвійного призначення тощо) лежать добровільні моделі управління, що мають на меті сформувати поведінку держав за відсутності жорсткого регулювання.

За останні десять років, CCICs стали широко доступними і на сьогодні є одними з основних інструментів в арсеналі агентств розвідки та безпекових практик більшості держав. На фоні стрімких технологічних змін та складності запровадження жорсткого регулювання, європейські уряди вирішили надати перевагу добровільним нормам.

Однак постає велике питання ефективності такого підходу, оскільки відповідальними за неналежне використанням CCICs часто є держави, що діють поза межами добровільних процесів. Водночас участь у ініціативах, переважно, зосереджена серед країн, які і без того схильні дотримуватись певних норм у кіберпросторі і, в багатьох

[1] https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states

випадках, не мають власного виробництва CCICs. В результаті зусилля з регулювання ринку та технологій на ньому ризикують обмежити схильних до дотримання вимог і залишити основні осередки загрози недоторканими.

Добровільний формат ініціатив випливає з бажання залучитись якомога ширшим колом однодумців. Таким чином, добровільні норми, здебільшого, здатні уникнути віднадження потенційних прихильників, тоді як жорсткі правила, тиск та відповідальність не забезпечують бажаного залучення. Це робить незобов'язувальний підхід неефективним у випадку асиметричних загроз, коли ворожі суб'єкти ігнорують репутаційний тиск.

Звісно, привабливість такої моделі управління полягає у її низькій політичній вартості та здатності продемонструвати залученість у складній для регулювання сфері. Вона дає урядам можливість реагувати на загрози, не вдаючись до часто дорогих та надзвичайно повільних (порівняно з темпами розвитку ринку) механізмів контролю. Однак, відсутність жорстких зобов'язань у кіберпросторі порушує більш серйозне питання: чи здатне добровільне обмеження реально вплинути на поведінку ринку. Якщо регулювання не передбачає вимірюваних витрат, не вимагає коригування поведінки та не охоплює суб'єктів, які несуть найбільшу відповідальність за зловживання, про внесок у безпеку складно говорити. Врешті, головним питанням є не нормативна привабливість добровільних ініціатив, а те, чи здатні вони істотно зменшити ризики кібервтручання.

Мета

Це дослідження оцінює, чи є сучасні підходи до регулювання CCICs ефективними інструментами безпеки. Спираючись на європейські ініціативи, воно оцінює, чи впливає добровільне обмеження на зменшення ризику кібервтручання в умовах стрімких змін цифрового середовища.

МЕТОДОЛОГІЯ

Дослідження використовує якісний порівняльний аналіз. З цією метою розроблено 4 критерії оцінки:

> **Перший — діапазон участі.** Дослідження аналізує, які держави та учасники ринку охоплено Ініціативою.
>
> **Другий – механізми обмеження.** Дослідження оцінює, як ініціативи накладають обмеження на практиці.
>
> **Третій – урахування загроз.** Дослідження перевіряє, чи охоплюють ініціативи суб'єктів, які несуть найбільшу відповідальність за зловживання CCICs.
>
> **Четвертий – безпекові наслідки.** З огляду на непрозорість кібероперацій, дослідження спирається на видимі показники; йдеться про продовження атак на європейські інституції та громадян, адаптація ринку постачальниками та статистика використання CCICs.

Pall Mall Process є основним фокусом дослідження, тоді як Вассенаарські угоди та Регулювання ЄС про товари подвійного призначення використовуються як додаткові джерела для порівняння, щоб перевірити, чи більш формалізовані режими контролю стикаються із тими ж структурними обмеженнями.

Значення та внесок роботи

Результати дослідження свідчать про те, що добровільне управління наодинці є недостатньо ефективним в умовах асиметричних стимулів та технологічної

конкурентності ринку. Внесок цього дослідження полягає в переосмисленні регулювання CCICs крізь призму ефективності з точки зору безпеки, а не лише нормативних прагнень. Дослідження покликане надати законодавцям чітку основу для оцінки впливу сучасних ініціатив на посилення безпеки.

ТЕРМІНОЛОГІЯ

У рамках Ініціативи використовується доволі широке термінологічне поле, адже це дозволяє вносити правки та формувати визначення впродовж самого процесу. У своїй декларації[2], Pall Mall Process визначає комерційні інструменти кібервтручання як інструменти та послуги компаній, що спеціалізуються на кібервтручанні і забезпечують віддалений доступ до комп'ютерних систем або втручання в їхню роботу. Таке поняття охоплює як програмні продукти, так і операційні послуги, зокрема access-as-a-service (ACaaS) — модель, за якої постачальник надає вектор доступу та malware-as-a-service (MaaS) — модель, у межах якої компанія розробляє та підтримує шкідливе програмне забезпечення і застосовує його проти визначеної цілі від імені клієнта. У межах Ініціативи, компанії, що здійснюють кібервтручання, визначаються як комерційні суб'єкти, які, з метою отримання прибутку, продають «готові до використання» інструменти для проникнення, вразливості систем або послуги так званих «хакерів за наймом».

У рамках цього дослідження використовується дещо звужені визначення. Хоча термінологія Ініціативи охоплює як постачальників технічних спроможностей, так і операційних підрядників — «хакерів за наймом» — у цій роботі увага зосереджується виключно на компаніях, що розробляють, ліцензують і підтримують **комерційні шпигунські технології (КШТ)**. Інакше кажучи, предметом аналізу є комерційні постачальники шпигунських технологій: компанії, які створюють масштабовані платформи для кібервтручання, здатні забезпечувати віддалений контроль за пристроями, вилучення даних і тривале приховане спостереження.

Таке розмежування дає змогу в подальшому проводити окремий аналіз інших типів постачальників і різновидів CCICs. Хакери за наймом, зазвичай, здійснюють індивідуальні, ситуативні кампанії кібервтручання, використовуючи власний людський капітал. Натомість, продукти постачальників КШТ можуть експортуватися, відтворюватися, оновлюватися та повторно застосовуватись в різних юрисдикціях, що створює системні ризики поширення. Такі ризики, принаймні теоретично, більше піддаються регулюванню через, скажімо, експортний контроль.

Отже, термін "комерційні інструменти кібервтручання" (CCICs) застосовується в межах термінології Ініціативи, але у звуженому значенні: йдеться про технології компаній, що займаються розробкою, поширенням та постачанням КШТ за моделями ACaaS та MaaS.

ПРО КОМЕРЦІЙНІ ШПИГУНСЬКІ ТЕХНОЛОГІЇ

Ринок КШТ функціонує в просторі, який надзвичайно важко відстежувати. Окрім того, що продукти на ньому цифрові, більшість з них має подвійне призначення: одна і та ж технологія може забезпечувати законний збір розвідувальної інформації і дозволяти віддалене стеження. Відповідно, усе залежить від того, хто нею користується і з якою метою. Наміри і використання, таким чином, не є властивими самій технології, а залежать від кінцевого користувача.

За таких умов, відповідальність за розповсюдження КШТ лягає на уряди. Взагалі, ті держави, в юрисдикціях яких оперують компанії КШТ, рідко мають можливість вплинути на те як продукт використовуватиметься в кінцевому результаті. Проте саме

[2] https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

від урядів залежить, які можливості потрапляють в обіг і за яких умов. За відсутності ефективних запобіжних заходів ця структура, значною мірою, покладається на припущення про відповідальне використання.

Аналітична складність ще більше посилюється обмеженою прозорістю самого ринку. На момент написання цього дослідження, в рамках Ініціативи не було опубліковано офіційного переліку компаній-виробників шпигунських технологій. У результаті, дослідження спирається на відкриті джерела для ідентифікації таких компаній, основу з яких складають: звіт Atlantic Council «Mythical Beasts»[3], звіт Google Threat Analysis Group «Buying Spying»[4] та розслідування Європейського парламенту PEGA щодо використання ПЗ "Pegasus" та аналогічних продуктів[5]. У сукупності ці джерела надають найбільш достовірну базу даних про цей сектор.

Також важливо окреслити, що саме оцінюється, а що ні. Хоча термін «комерційні шпигунські технології» часто використовується узагальнено, сам ринок можна умовно поділити на системи, призначені для законного перехоплення і зберігання даних та системи, розроблені для віддаленого проникнення в пристрої та вилучення даних. Цей аналіз стосується останньої категорії, яку часто називають "наступальними кіберспроможностями" (offensive cyber capabilities).

ДІАПАЗОН УЧАСТІ

На першій конференції Ініціативи зібрались 27 держав та міжнародних організацій, 14 представників бізнесу та 12 представників громадянського суспільства і наукових кіл. З 53 суб'єктів 27 держав підписали Кодекс практик, серед яких майже всі мають задокументовану історію придбання або використання КШТ, за винятком Косово та Норвегії. Водночас лише частина держав-учасниць відіграє структурну роль у самій екосистемі шпигунських технологій. Семеро держав-учасниць — Франція, Німеччина, Греція, Угорщина, Ірландія, Італія та США — мають у своїх юрисдикціях компанії-виробники/постачальники КШТ або ж елементи їх операційної інфраструктури. Решта учасників беруть участь, переважно, як споживачі.

Географічний поділ на виробників/споживачів виглядає ще цікавіше. Карта SIPRI ідентифікує 43 виробники КШТ, що оперують у 18 державах, при цьому виробництво цих продуктів набагато більш сконцентроване, ніж у суміжних секторах кіберу.[6] Більше половини цих компаній розташовані в трьох державах: Індії, Ізраїлі та Італії.[7] The Atlantic Council також звертає увагу на цей структурний дисбаланс, окреслюючи ті самі три країни основними центрами виробництва КШТ. На основі відкритих джерел, це дослідження ідентифікує 31 постачальника КШТ. Переважна більшість з них є ізраїльськими компаніями: Blue Ocean, Candiru, Cellebrite, Cognyte, ClearTrail, Interionet Systems, Merlinx, NSO Group, Paragon Solutions, QuaDream та Wintego Systems. Друга група розташована в Індії і налічує три компаній (позаяк Індія більше відома послугами хакерів за наймом), а за нею йдуть менші групи в Об'єднаних Арабських Еміратах, Кіпрі, Туреччині, Росії, В'єтнамі та Сінгапурі.

Таким чином, **21 із 31 компаній-виробників КШТ** оперують у державах за межами Ініціативи та подібних процесів. Ці компанії — а також держави, які їх ліцензують або приймають — є ізольованими від репутаційного та нормативного тиску систем управління. Більше того, Ініціатива залучає лише одну з цих трьох країн — Італію. У результаті участь у процесі більше відповідає моделям споживання та дотримання вимог, ніж постачання та розробки КШТ, які, власне, формують динаміку ринку.

[3] https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them/
[4] https://blog.google/threat-analysis-group/
[5] https://www.rcmediafreedom.eu/Resources/Reports-and-papers/PEGA-Committee-final-report
[6] https://www.sipri.org/publications/2025/other-publications/export-controls-and-spyware-enhancing-oversight-transparency-and-restraint
[7] https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/

КОМПАНІЯ	ТИП	ПРОДУКТ	ДЕРЖАВА-ХОСТ
1Byte	Виробник	Шпигунське/Сталкерське ПЗ TheTruthSpy	В'єтнам
9th Vision	Виробник	Zero-Click Шпигунське ПЗ/Стеження	ПАР
Aglaya	Виробник	Шпигунське ПЗ/Стеження Cyber Strike	Індія
Blue Ocean	Виробник	Наступальне шпигунське ПЗ	Ізраїль
Candiru (Saito Tech Ltd)	Виробник	Шпигунське ПЗ DevilsTongue	Ізраїль
COSEINC	Виробник	Шпигунське ПЗ/Стеження	Сінгапур
Cognyte	Виробник	Шпигунське ПЗ/Стеження	Ізраїль
CY4GATE	Виробник	Шпигунське ПЗ/Стеження Epeius, Hydra	Італія
RCS Lab	Дочірня компанія (CY4GATE)	Шпигунське ПЗ/Стеження Hermit	Італія
CPX (DarkMatter)	Виробник	Шпигунське ПЗ/Стеження Project Raven	ОАЕ
Interionet Systems	Виробник	Шпигунське ПЗ/Стеження NightHawk	Ізраїль
InvaSys	Виробник	Шпигунське ПЗ/Стеження Invasys Mobile360	Чехія
Intellexa Consortium	Холдинг	Шпигунське ПЗ/Стеження	Греція
Cytrox	Виробник	Predator	Північна Македонія
			Угорщина
Nexa Technologies	Виробник	Cerebro	Франція
Thalestris Limited	Дистриб'ютор	Predator	Ірландія
Trovicor (Data Fusion)	Виробник	Шпигунське ПЗ/Стеження	Німеччина
Cellebrite	Виробник	Шпигунське ПЗ Universal Forensic Extraction Device (UFED)	Ізраїль
ClearTrail Technologies	Виробник	Шпигунське ПЗ Astra	Індія
Leo Impact	Виробник	Шпигунське ПЗ/Стеження	Індія
MerlinX	Виробник	Apollo	Ізраїль
Negg Group	Виробник	Vbiss	Італія
Nexa Technologies	Виробник	Шпигунське ПЗ/Стеження Cerebro	Франція
NSO Group	Виробник	Pegasus	Ізраїль
Paragon Solutions	Виробник	Graphite	Ізраїль
	Виробник		США
PARS Defence	Виробник	Шпигунське ПЗ/Стеження	Туреччина
Passitora	Виробник частина Intellexa Alliance	Стеження	Кіпр
Positive Tecnologies	Виробник	Шпигунське ПЗ/Стеження Надають дані ФСБ та ГРУ	Росія
QuaDream	Виробник	Reign	Ізраїль
InReach	Дистриб'ютор		Кіпр
Wintego Systems	Виробник	Helios	Ізраїль (зв'язки із Сінгапуром)

Інформація про поточний статус компаній-виробників КШТ, країни їхнього розміщення та діяльність була перевірена за допомогою Surveillance Watch

https://www.surveillancewatch.io/entities

МЕХАНІЗМИ ОБМЕЖЕННЯ

Як зазначено в Кодексі практик, Ініціатива є виключно добровільною і не носить зобов'язальний характер[8]. Вона сприяє впровадженню передових практик у чотирьох основних напрямках (відповідальність, точність, нагляд та прозорість), але не накладає жодних юридичних обмежень чи санкцій ані на учасників, ані на сторонніх суб'єктів.

В офіційних документах Ініціативи окреслено наступні інструменти: національний експортний контроль, обмеження закупівель у неналежних постачальників, перевірка на дотримання прав людини та міжнародне співробітництво з питань санкційної політики. Вони залежать від внутрішнього впровадження державами і заохочують самозвітування та обмін інформацією. Ініціатива також не пропонує механізмів, які б зобов'язували держави, що не взяли участі, оскільки процес спрямований на запобігання розповсюдженню через моральну відповідальність, а не через примус.

Подібно до Ініціативи Pall Mall Process, Вассенаарські угоди не містять обов'язкових обмежень та покладаються на добровільне виконання на національному рівні. Держави-члени зберігають повний контроль над виконанням рекомендацій, що обмежує ефективність боротьби з розповсюдженням та неналежним використанням CCICs.

Вассенаарські угоди мають в основі два контрольні списки — Список товарів і технологій подвійного призначення та Списку озброєнь. При цьому, для забезпечення більш ретельного контролю за експортом, певні позиції у Списку подвійного призначення позначені як «чутливі» або «дуже чутливі».[9] Список озброєнь стосується кінетичної військової техніки, тоді як Список товарів подвійного призначення охоплює програмне забезпечення для кібервторгнень. Держави-учасниці зобов’язуються щороку звітувати про передачі, відмови у видачі ліцензій на певні контрольовані товари подвійного призначення, а також надавати гарантії щодо кінцевого використання. Повідомлення про відмови надсилаються членам, щоб поінформувати інших та запобігти обходу обмежень через юрисдикції з менш суворими обмеженнями. Ці домовленості потім підкріплюються щорічними пленарними засіданнями, на яких узгоджуються списки та просуваються спільні практики. Та контроль за дотриманням залишається повністю на державному рівні.

УРАХУВАННЯ ЗАГРОЗ

ЄС намагається регулювати поширення CCICs за допомогою режиму експортного контролю, класифікуючи певні КШТ як товари подвійного призначення, відповідно до Регламенту про товари подвійного призначення. Згідно з цією системою, технології, які можуть бути використані для віддаленого доступу, підлягають експортному контролю, щоб запобігти використанню з ціллю репресій або серйозних порушень прав людини. Однак така класифікація подвійного призначення має свої обмеження: прирівнюючи КШТ до широко визначених цивільних і військових застосувань, Регламент надає владу над оцінкою ризиків самим урядам, які зберігають дискреційні повноваження щодо ліцензування та визначення кінцевого використання. У результаті експортний контроль часто відображає державні міркування безпеки та комерційні інтереси, а не гарантії прав людини. Одним із наслідків є неоднорідність впровадження норм, різні стандарти виконання та прогалини в законодавстві, що дозволяють КШТ циркулювати на внутрішньому ринку ЄС та за його межами, незважаючи на значні докази зловживання.[10]

З цього випливає, що ані Pall Mall Process, ані Вассенаарські угоди, ані Регламент ЄС не забезпечують необхідних юридичних зобов'язань. Для держав, що становлять

[8] https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states
[9] https://www.wassenaar.org/control-lists/
[10] https://vtechworks.lib.vt.edu/items/8d3a485d-3470-4976-bc44-82e538b47d14

загрозу і не входять до цих угод, зокрема Індії, Китаю та Росії, ініціативні обмеження та нагляд повністю відсутні.

Для деяких держав навіть узгодження на папері не означає обмеження на практиці. Наприклад, Ізраїль, не будучи членом Вассенаарських угод, публічно зобов'язався узгодити свій експортний контроль з їх стандартами. Насправді ж, рішення про видачу ліцензій приймаються Агентством з контролю за експортом оборонної продукції (DECA) при Міністерстві оборони. Продажі блокуються, якщо вони суперечать національним інтересам Ізраїлю — наприклад, відмова в експорті Pegasus Україні та Естонії, щоб уникнути дипломатичних конфліктів з Росією.[11] Це свідчить про те, що експортний контроль залежить від стратегічних пріоритетів.

А також, зафіксовані випадки зловживань свідчать про те, що рішення прийняті з урахуванням національних інтересів не збігаються із захистом прав людини. NSO Group публічно зобов'язалася дотримуватися Керівних принципів ООН з питань бізнесу та прав людини. Проте, судові розслідування Amnesty International та Citizen Lab неодноразово фіксували випадки використання Pegasus проти журналістів, опозиційних діячів та представників громадянського суспільства. Випадки охоплюють різні юрисдикції та політичні контексти: журналісти у Сербії у 2025 році[12]; неодноразові напади на представників індійських ЗМІ у 2023–2024 роках[13]; спостереження за особами, пов'язаними з Джамалом Хашоггі[14]; розслідування в Мексиці, Угорщині та Марокко[15]; а також проект «Pegsus» 2021 року, в рамках якого було виявлено, що понад 180 журналістів у всьому світі є потенційними цілями стеження[16].

Проблема полягає не просто в тому, що зловживання тривають, а що чинні механізми діють, переважно, з міркувань державних інтересів, а не через системну ринкову дисципліну. Контроль застосовується вибірково, часто з урахуванням геополітичних питань, залишаючись при цьому вибірково поблажливим до певних держа в обмін на обмежене стратегічне тертя.

Подібна динаміка спостерігається і за межами ізраїльської екосистеми. Індія, наприклад, класифікує КШТ як товари подвійного призначення відповідно до свого контрольного списку SCOMET, передаючи остаточні повноваження щодо експорту Генеральному директорату зовнішньої торгівлі (DGFT). Компанії можуть ініціювати та структурувати продажі, але кожна міжнародна передача вимагає ліцензії уряду. Затвердження залежить від міжвідомчої робочої групи, яка оцінює транзакції на відповідність національній безпеці та дипломатичним інтересам Індії. На папері це створює картинку відповідального експортного контролю. На практиці ж це підсилює ту саму структурну динаміку, що й в Ізраїлі, де фінальне рішення належить державі, а вирішальним критерієм є стратегічний інтерес.

Що стосується прикладів інших держав, то російська система SORM була експортована до сусідніх держав та партнерів у Центральній Азії та Латинській Америці. Через неї було вбудовано можливості спостереження на рівні інтернет-провайдерів та забезпечено моніторинг населення. Китай у свою чергу просуває пов'язані з Huawei системи «Безпечних міст» в декількох африканських столицях, інтегруючи інфраструктуру міського спостереження в більш широкі пакети цифрового управління. Водночас, Китай підтримує значну екосистему досліджень цифрових вразливостей, на яку припадає приблизно 30% виявлених атак у 2024 році[17].

Хоча ці моделі технічно відрізняються від західного розуміння терміну CCICs, в сукупності вони нормалізують інтеграцію наступальних або втучальних спро-можностей у державне управління. Знову ж таки, багато з цих постачальників діють

[11] https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia
[12] https://www.amnesty.org/en/documents/eur70/9186/2025/en/
[13] https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/
[14] https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-jamal-khashoggi-wife-phone-washington-post/
[15] https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/
[16] https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware
[17] https://www.recordedfuture. bhy6tgcom/research/pegasus-pall-mall-managing-risks-of-offensive-cyber-capabilities

поза нормативними рамками Ініціативи. У результаті, створення та поширення загроз зосереджені в юрисдикціях, де ініціативи з управління мають обмежений вплив.

НАСЛІДКИ ДЛЯ БЕЗПЕКИ

Якщо оцінювати добровільні процеси серйозно, то потрібно мати доказову базу ризиків. За цим показником результати неоднозначні. Ринок CCICs є непрозорим за своєю структурою, і надійні докази змін рідко з'являються в режимі реального часу. Однак відсутність таких доказів має подвійний ефект. На момент написання цієї роботи немає перевірених показників ні скорочення ринку, ні структурного виходу/переміщення постачальників, ні вимірюваного зменшення цільових атак, що можна було б пов'язати з Pall Mall Process. Участь у цьому процесі не призвела до помітних змін у поведінці, які б могли бути пов'язані зі зменшенням ризиків або поліпшенням безпеки для учасників.

Натомість спостерігається певна стабільність. Прогнозується, що глобальний ринок шпигунських технологій значно розшириться протягом наступного десятиліття, а зростання частково буде обумовлено попитом на засоби вторгнення в кіберпростір. Вже зараз прогнозується, що в 2025 році його обсяг становитиме 55,03 млрд доларів, а в 2033 році, завдяки попиту на КШТ, він досягне 168,71 млрд доларів[18]; Обсяг світового ринку послуг з кібербезпеки в 2024 році оцінювався в 75,82 млрд доларів, а до 2030 року, за прогнозами, досягне 156,76 млрд доларів, зростаючи з 2025 по 2030 рік із середньорічним темпом 13,6 % Ці показники свідчать про нову “гонку озброєнь” в сфері CCICs[19].

Існує також безліч доказів збільшення фінансування на ринку, про що свідчить різке зростання припливу приватного капіталу в CCICs. При цьому американські інвестори підтримують все більшу кількість компаній, що займаються наступальними кіберопераціями. Цей стрибок позиціонує США як найбільшого національного інвестора в комерційне шпигунське обладнання, випереджаючи Ізраїль (26 інвесторів), Італію (12) та Великобританію (5)[20].

Серед іншого, розслідування, проведені Amnesty International, підтвердили, що Pegasus від NSO Group використовувалося для переслідування журналістів-розслідувачів у Сербії після запуску Pall Mall Process. Окремі звіти Associated Press та Citizen Lab задокументували використання КШТ, розроблених в Ізраїлі, проти італійських журналістів на тлі внутрішнього політичного контролю[21]. Це не означає, що ці випадки встановлюють причинно-наслідковий зв'язок між процесом та його неефективністю, але вони підкреслюють відсутність помітного стримуючого ефекту.

З точки зору безпеки, відсутність помітних змін сама по собі є результатом. Добровільне управління не призвело до очевидного зниження темпів використання КШТ, а також не змінило структурних стимулів, що сприяють їх виробництву та експорту. Якщо механізми управління призначені для впливу на цей ринок, їх ефективність повинна оцінюватися на основі вимірюваних змін. Наразі таких змін не спостерігається.

[18] https://www.marketresearch.com/Maia-Research-v4212/Global-Surveillance-Trends-Forecast-Broken-43901024/
[19] https://www.grandviewresearch.com/industry-analysis/cyber-security-service-market
[20] https://www.debugliesintel.com/global-spyware-market-2025-us-investment-surge-and-broker-enablers-fueling-proliferation-risks/
[21] https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware/

ВИСНОВОК

У ході дослідження, на прикладі Pall Mall Process, було розглянуто питання ефективності незобов'язувальних ініціатив в обмеженні поширення та неналежного використання комерційних шпигунських технологій. У ньому оцінюються масштаб учаті, узгодженість у розумінні загроз, архітектура експортного контролю та безпекові наслідки для країн-учасниць. Дослідження показує, що, попри чимале коло залучених до Ініціативи держав, основні центри виробництва КШТ залишаються поза межами регулювання, а рішення та пояснення про видачу ліцензій на експорт рідко (якщо й взагалі) оприлюднюються. Ба більше, жодні із визначених показників не вказують на системну зміну поведінки на ринку. Тим часом глобальний ринок КШТ продовжує стрімко розширюватися, приватні капіталовкладення в наступальні кіберкоперації зростають, а неналежне використання шпигунських технологій як державами-учасницями так і тими, що не приєдналися, продовжується. Попри це, назвати Ініціативу повністю неефективною не можна; але поточний її вигляд не забезпечує бажаних безпекових результатів.

З цієї точки зору, структурне обмеження Ініціативи є переважно геополітичним. Декларативні процеси найефективніше діють там, де держави-учасниці є політично узгодженими та комерційно інтегрованими до однієї системи. Однак сам ринок КШТ не має географічних меж. Основні виробничі центри, потоки капіталу та кінцеві споживачі знаходяться як всередині, так і поза нормативним периметром. У результаті, добровільні зобов'язання здатні дисциплінувати лише частину екосистеми.

Така динаміка може мати доволі негативні наслідки. Об'єднуючи доброчесні держави (переважно європейські та трансатлантичні) навколо спільних стандартів, такі ініціативи, Pall Mall Process, можуть ненавмисно спричинити поділ ринку. Одна частина постачальників надаватиме перевагу доступу до регульованих ринків (а отже і покупців на них), відповідно адаптуючи структури свого управління та практики прозорості. Для цих компаній дотримання норм стане конкурентною перевагою.

Однак паралельний сегмент ринку може переорієнтуватись на інших покупців. Постачальники та виробники, яких менше турбує доброчесна репутація і чия діяльність здійснюється на території країн без жорсткого контролю за КШТ, можуть надати пріоритет клієнтам у регіонах зі слабшими вимогами прозорості, де рішення про закупівлі приймаються переважно з міркувань безпеки режиму. Замість регулювання глобальної екосистеми CCICs, такий тип регулювання може призвести до її перерозподілу.

Довгострокові наслідки полягають у тому, що поляризований ринок сприятиме поглибленню технологічного розриву між регуляторними блоками. Держави, що діятимуть у рамках нормативних зобов'язань, можуть запровадити більш жорсткі вимоги до ліцензування та нагляду, тоді як інші розвиватимуть передові кібер інструменти спостереження без додаткових обмежень. Ця розбіжність ускладнює захист прав людини, підриває колективні заходи реагування на кіберзагрози та може закріпити асиметрію у світових кіберспроможностях.

Важливо ще раз наголосити, що це не свідчить про провал Pall Mall Process. Навпаки, він демонструє, що політична координація щодо комерційного кібервтручання є можливою. Але координація сама по собі не дорівнює впливу. Без ширшого кола залучення, сильніших механізмів прозорості та чіткіших структур підзвітності добровільні ініціативи ризикують розділити ринок, а не врегулювати його.

Тому попереду стоїть великий стратегічний виклик. Якщо ж метою таки є зменшення зловживань CCICs та підвищення кібер та державної безпеки, сучасні ініціативи повинні враховувати адаптацію ринку та його геополітичний масштаб. Інакше, добровільні норми можуть посилити ті розбіжності, які прагнуть подолати.

РЕКОМЕНДАЦІЇ

Щоб Pall Mall Process став справді ефективним інструментом у протидії розповсюдженню та неналежному використанню CCICs, учасникам слід забезпечити практичну реалізацію його чотирьох основних принципів. Ці рекомендації безпосередньо ґрунтуються на Кодексі практик Ініціативи і спрямовані на усунення прогалин у добровільних нормах, шляхом впровадження інструментів контролю, розбудови потенціалу та багатосторонньої співпраці.

ПРИНЦИП 1

ВІДПОВІДАЛЬНІСТЬ

Відповідальність вимагає суворого дотримання міжнародного права, норм ООН та внутрішніх механізмів контролю, проте нинішні зобов'язання поширюються лише на держави, що погоджуються з цими вимоги, тоді як основні виробники та експортери діють за межами контролю.

Рекомендація 1

Держави-учасниці повинні запровадити обов'язкову реєстрацію внутрішніх постачальників CCICs, включно з інформацією про корпоративну структуру, юрисдикції експорту та процедури належної перевірки. Рішення про видачу або відмову у видачі ліцензій повинні вноситися до захищеної бази даних для відстеження тенденцій у сфері розповсюдження та виявлення повторюваних індикаторів ризику.

Такі реєстри не розкриватимуть конфіденційних деталей, але створять спільну базу для прозорості ринку, що зменшить регуляторний арбітраж та дозволить порівнювати експортні практики між державами.

Рекомендація 2

Державам варто розробити окрему санкційну стратегію для акторів, найбільше пов'язаних із зловживанням CCICs. Нормативно-правову основу для цього можуть забезпечити існуючі резолюції Генеральної Асамблеї ООН щодо зловживання шпигунським ПЗ.

Мета полягає в тому, щоб накласти на порушників відчутні репутаційні та економічні витрати і тим самим запобігти ухиленню компаній через шляхом перенесення виробництва до юрисдикцій із слабшим регуляторним законодавством

ПРИНЦИП 2

ТОЧНІСТЬ

Точність вимагає пропорційного і цілеспрямованого використання CCICs у законних цілях та протидії ухиленню ринку КШТ через моделі SaaS та вразливості «нульового дня».

Рекомендація 3

Держави повинні закріпити в законодавстві критерії необхідності та пропорційності використання CCICs із чіткою забороною переслідування журналістів, політичних діячів та громадянського суспільства. Обов'язковою має стати оцінка ризиків використання інструментів, здатних до проникнення на рівні інфраструктури.

Мета полягає у забезпеченні дотримання прав людини як обов'язкового етапу перед будь-якими втручальними кібероперaціями, особливо тими, що можуть завдати шкоди цивільному населенню, журналістам або критичній інфраструктурі.

Рекомендація 4

Державам слід запустити тренінги та навчальні модулі. У рамках заходів з розбудови потенціалу слід надати пріоритет країнам із незначним або мало розвиненим ринком кіберзакупівель/розробок, щоб слабші або новіші учасники не створили системних прогалин, поки більш розвинені держави посилюють свої практики.

Таким чином Ініціатива зможе підвищити професійні стандарти, ускладнивши зловживання CCICs і при цьому не перешкоджаючи діяльності правоохоронних органів та операціям у сфері національної безпеки.

ПРИНЦИП 3

НАГЛЯД

Нагляд передбачає проведення незалежних аудитів та виділення ресурсів, але не має достатніх повноважень щодо суб'єктів за межами Ініціативи.

Рекомендація 5

Держави повинні створити або призначити незалежні наглядові органи з технічною експертизою та залученням громадянського суспільства для перевірки експорту та видачу дозволів на внутрішнє використання CCICs. Цим органам необхідно забезпечити доступ до закритої інформації та повноваження видавати рекомендації.

Впровадження технічної та правової перевірки на етапі затвердження підвищує довіру до процесу та зменшує політизацію прийняття рішень.

Рекомендація 6

Державам слід запровадити систематичний аналіз результатів застосування CCICs, включно з перевіркою дотримання вимог та документацією підсумків. Публікація регулярних звітів дозволить посилити нагляд в рамках Ініціативи без значних витрат.

Це забезпечить документацію перебігу кожної операції та допоможе урядам виявляти зловживання та помилки у використанні CCICs, не розкриваючи при цьому конфіденційної інформації.

ПРИНЦИП 4

ПРОЗОРІСТЬ

Прозорість сприяє обміну інформацією про ринок, тоді як її відсутність захищає держав-неучасниць та стимулює нерегульований розвиток ринку.

Рекомендація 7

Створити захищений інформаційний центр для анонімного звітування про випадки використання КШТ, діяльність компаній та підозри про зловживання. Партнерство з технічними ГО та компаніями з кібербезпеки дозволить проводити незалежну та якісну перевірку і оцінку дотримання прав людини.

Публікація звітів сприятиме розробці політик на основі перевірених даних та оперативному виявленню загроз.

Рекомендація 8

Впровадити правила “Знай свого постачальника” та “Знай свого покупця” для проведення посиленої перевірки продавців, фактичних власників компаній, аналіз звітності про дотримання вимог та забезпечення правил, що дозволяють розірвати договір у разі зловживання КШТ. Звітування про відмови в експорті та призупинення закупівель дозволить виявити системні ризики.

Дисципліна з боку купівлі часто є ефективнішою, ніж контроль з боку експорту; реформа системи закупівель КШТ надасть перевагу на користь відповідальних постачальників.

АКТОР	ТИП	СТАТУС	РОЛЬ У ССІС	КОМПАНІЯ-ВИРОБНИК
Африканський Союз	Міжнародна організація	Учасник	-	
Австралія	Держава	Учасник	Покупець/Користувач	
Австрія	Держава	Підписант	Покупець/Користувач	
Бельгія	Держава	Підписант	Покупець/Користувач	
Канада	Держава	Учасник	Покупець/Користувач	
Чехія	Держава	Учасник	Покупець/Користувач **Хост**	**InvaSys**
Данія	Держава	Підписант	Покупець/Користувач	
Естонія	Держава	Підписант	Покупець/Користувач	
Фінляндія	Держава	Підписант	Покупець/Користувач	
Франція	Держава	Підписант	Покупець/Користувач **Хост**	**Nexa Technologies**
Німеччина	Держава	Підписант	Покупець/Користувач	
Гана	Держава	Підписант	Покупець/Користувач	
Греція	Держава	Підписант	Покупець/Користувач **Хост**	**Intellexa**
РСАДПЗ	Міжнародна організація	Учасник	-	
Угорщина	Держава	Підписант	Покупець/Користувач **Хост операційної інфраструктури**	**Intellexa**
Ірландія	Держава	Підписант	Покупець/Користувач **Хост операційної інфраструктури**	**Intellexa**
Італія	Держава	Підписант	Покупець/Користувач **Хост**	**CY4GATE**
Японія	Держава	Підписант	Покупець/Користувач	
Косово	Держава	Підписант	-	
Латвія	Держава	Підписант	Покупець/Користувач	
Люксембург	Держава	Підписант	Покупець/Користувач	
Малазія	Держава	Учасник	-	
Молдова	Держава	Підписант	-	
Нідерланди	Держава	Підписант	Покупець/Користувач	
Нова Зеландія	Держава	Учасник	Покупець/Користувач	
Норвегія	Держава	Учасник	-	
Польща	Держава	Підписант	Покупець/Користувач	
Кіпр	Держава	Учасник	**Хост операційної інфраструктури**	**Passitora** **QuaDream**
Південна Корея	Держава	Підписант	Покупець/Користувач	
Румунія	Держава	Підписант	Покупець/Користувач	
Сінгапур	Держава	Учасник	Покупець/Користувач **Хост**	**COSEINC**
Словаччина	Держава	Підписант	Покупець/Користувач	
Словенія	Держава	Підписант	Покупець/Користувач	
Швеція	Держава	Підписант	Покупець/Користувач	
Швейцарія	Держава	Підписант	Покупець/Користувач	
Велика Британія	Держава	Підписант	Покупець/Користувач	
США	Держава	Підписант	Покупець/Користувач **Хост**	**Paragon Solutions**

Перелік держав-«учасниць» наведено в додатку до Декларації «Палл-Малл».

Перелік держав-«підписантів» наведено в додатку до Кодексу практик «Палл-Малл».

Автори:

СОЛОМІЯ ВИБРАНОВСЬКА
Експертка Ради економічної безпеки України (ESCU) s.v@escu.ua

Д-Р ІЛОНА ХМЕЛЬОВА
Секретар Ради економічної безпеки України (ESCU) khmeleva@escu.ua

Дослідження було підготовлено Радою економічної безпеки України (ESCU) у співпраці з міжфракційним об'єднанням «Платформа технологічної дипломатії України» у Верховній Раді України»