# Документ робочої групи № 7

# IT та допоміжні технології: Рекомендації щодо санкцій проти Російської Федерації

Міжнародна робоча група з санкцій проти Росії

2 листопада 2022 р.

https://fsi.stanford.edu/working-group-sanctions

# Вступ

Міжнародна робоча група із питань санкцій проти Росії[1] має на меті надати експертні знання та досвід урядам і компаніям у всьому світі, допомагаючи формулювати пропозицій щодо санкцій, які збільшать ціну вторгнення Росії в Україну та підтримають демократичну Україну в захисті своєї територіальної цілісності та національного суверенітету. Наша робоча група складається з незалежних експертів з багатьох країн, проте координує та проводить консультації з Урядом України та тими урядами, які запроваджують санкції. Цей консультативний процес допомагає збільшувати нашу поінформованість, однак наші члени висловлюють незалежну позицію, не отримують зовнішніх вказівок та не діють за наказами уряду України чи будь-якої іншої особи чи організації. Ця публікація є продовженням нашого першого Плану дій та попередніх робочих документів стосовно санкцій у сфері енергетики, фінансів, а також окремих санкцій, у тому числі визнання Росії державою-спонсором тероризму, і конфіскації резервів російського Центрального банку, про що повідомлялося в додаткових записках і публікаціях членів нашої робочої групи на нашому веб-сайті.[2]

# Резюме

Наразі іноземні інформаційно-комунікаційні технології, мікроелектроніка та інтелектуальна власність (далі ІТ) лежать в основі військового, військово-промислового комплексу та уряду Росії в цілому.[3] Росія була значною мірою відсталою в ІТ. У результаті Росія покладається на іноземні ІТ при командуванні та контролі своєю армією, веденні вогню зі своєї зброї, здійсненні розвідки, контролі інформаційного простору, атаках української кібернетичної та цивільної інфраструктури та ізоляції власної інфраструктури. Іноземні технології, які використовує Росія, охоплюють усе: від розширених серверів електронної пошти, можливостей керування мережею, інтелектуальних пристроїв, додатків програмного забезпечення як послуги, криптографічних і блокчейн-сервісів і потокового відео, аж до систем автоматизованого проектування та виробництва (CAD/CAM) і можливості інформаційного моделювання будівель (BIM), програмне забезпечення для проектування, виробництва та моделювання, а також роботизовані компоненти, контролери пристроїв.

[1] Усі члени цієї робочої групи приймають участь у роботі, виступаючи в якості приватних осіб, але ми консультувалися з багатьма урядовцями, в тому числі з урядом України.

[2] Подібно до інших документів, підготовлених цією робочою групою, метою даного документу було не створення консенсусного документу, а натомість надання переліку можливих додаткових заходів для розгляду урядами, багатосторонніми установами та приватними особами. Наслідки кожної санкції не були ретельно проаналізовані, і не всі обов'язково погоджуються з кожною конкретною запропонованою санкцією чи дією.

[3] Даніель Перес Фернандес, «Зроблено в Росії: осмислення кремлівської програми імпортозаміщення ІТ», Урядовий проект у сфері державної політики при Системі технічних коледжів Грузії,19 жовтня 2021 р. https://www.internetgovernance.org/2021/10/19/made-in-russia-making-sense-of-the-kremlins-ict-import-substitution-program/

Згідно з нещодавнім звітом, приблизно 38% IT та 63% імпорту електроніки в Росію походять лише з Європейського Союзу, Великобританії та Сполучених Штатів.[4] Після вторгнення в Україну 24 лютого 2022 року Росія почала реквізувати іноземні IT-компоненти та мікроелектронні компоненти зі споживчих товарів для використання своїми військовими. У результаті більше не існує різниці між IT-товарами та послугами, що постачаються в Росію для «цивільного» використання, і тими, які перепрофільовуються для військового використання проти України. Іноземні IT забезпечують російську військову машину та її пропагандистську машину. В це потрібно втрутитися і врешті-решт припинити.

Отже, продаж і обслуговування IT-технологій і пов'язаних з ними можливостей будь-яким суб'єктам усередині Росії, що сприяє російському вторгненню в Україну, прямо чи опосередковано, має бути негайно припинено. Цей документ містить аналіз сфер, на які слід негайно ввести санкції, як це зробити та як відповідні технології підтримують військову інфраструктуру Росії та військові операції в Україні.

Цей документ рекомендує зацікавленим урядам та IT-компаніям вжити негайних заходів для:

1. Блокування доступу до IT, які підтримують російську військову машину та її використання проти України.
2. Блокування доступу до IT, які дозволяють Росії вести інформаційну та кібервійну проти України та інших.
3. Блокування доступу до IT, що дозволяє російському уряду ізолювати своє населення від наслідків дій Росії.

Демократичні уряди та функціонуючі в їхніх межах IT-компанії повинні вживати чітких дій, спрямованих на паралізацію російської військової машини в Україні, проте не завдавати шкоди українським державним установам, українському приватному сектору, українському громадянському суспільству чи російським суб'єктам, які використовують технології для ефективного протистояння війні, розв'язаній Путіним. Західні соціальні медіа-компанії продовжували відігравати важливу та позитивну роль у підтримці російського громадянського суспільства та політичної опозиції. YouTube, наприклад, відіграє певну роль у підтримці російських незалежних ЗМІ в Росії. Завдання зберегти все те хороше, що роблять ці компанії, одночасно обмежуючи погане, є складним, але реальним.

Цей документ складено таким чином.

Частина I окреслює наші цілі щодо санкціонування доступу Росії до IT.

Частина II детально описує наші рекомендації та їхні очікувані результати.

Частина III підсумовує необхідність жорстких IT-санкцій проти Росії, наголошуючи на тому, що в IT більше не існує відмінності «подвійного використання», оскільки іноземні IT відіграють важливу роль у військовій та інформаційній машині Росії. Отже, існує потреба посилити тиск на

[4] Скотт Маркус, Ніклас Пуатьє, Моніка Ґжегорчик і Полін Вейл, «Відокремлення Росії: високотехнологічні товари та компоненти», блог Брейгеля, 28 березня 2022 р. https://www.bruegel.org/blog-post/decoupling-russia-high-tech-goods-and-components

ключові російські сектори, щоб не дати їм сприяти війні Росії проти України та інформаційним операціям проти інших країн.

Частина IV перераховує ІТ, які повинні підпадати під санкції та забороняти реекспорт і перепродаж.

Частина V більш детально розповідає про роль іноземних ІТ у військових та інформаційних машинах Росії.

# Частина I. Мета IT санкцій

Імперіалістична загарбницька війна Росії в Україні — це найбільш технологічно забезпечена війна, яку коли-небудь бачив світ. Інформаційні технології (IT) дозволяють обом сторонам масштабувати зусилля зі збору інформації в реальному часі за допомогою безпілотних літальних апаратів (БПЛА) і супутникових зображень; інтерпретувати зображення за допомогою технологій зіставлення ідентичності та можливостей комп'ютерного зору; об'єднати соціальні, гео- та операційні набори даних; відслідковувати та націлювати осіб; атакувати цифрову інфраструктуру соціальних, промислових і державних послуг; вести широкі інформаційні війни та цілеспрямовану пропаганду; керувати ракетами, траєкторіями польоту та приймати військові рішення; а також перераховувати кошти росіян, які воюють в Україні, на інші функції.

IT займають центральне місце в тому, що в цій роботі називають «воєнною машиною» Росії та її «інформаційною машиною». IT визначаються тут як інформаційні та комунікаційні технології, мікроелектронні компоненти та пристрої та їх супутня інтелектуальна власність. Детальний перелік IT, які підлягають санкціям, можна знайти в Частині IV цього документа.

Після першого вторгнення Росії в Україну в 2014 році російський президент Путін і його режим прагнуть від'єднати російську економіку від Заходу. Цей вибір негативно впливає на потенціал Росії з точки зору економічної, політичної та технологічної потужності, а також на добробут і процвітання пересічних росіян. Незважаючи на ці цілі, Путіну не вдалося зробити російську економіку незалежною від західних IT.[5] Як наслідок, жорсткі IT-санкції серйозно перешкодять як російській військовій машині в її операціях проти України, так і здатності Росії використовувати свою інформаційну машину проти України, Заходу та російського населення.

Цей документ має на меті надати низку рекомендацій, які, узяті разом і повністю реалізовані, дозволять досягти наступних цілей:

- Негайно й жорстко обмежити здатність Росії продовжувати військові дії в Україні;
- Зменшити ефективність російських інформаційних операцій і воєнної пропаганди всередині та за межами Росії;
- Підвищити вразливість російської армії до українських контратак; і
- Сприяти визволенню українських територій.

Окрім безпосереднього впливу, ці санкції призведуть до зниження продуктивності російської економіки, що, у свою чергу, призведе до погіршення виробництва російського військово-промислового комплексу в довгостроковій перспективі. Для ефективності санкцій, Росії повинно бути важко заповнити прогалину альтернативними постачальниками.

Тому ми також визначаємо засоби запобігання ухиленню від санкцій третіми сторонами.

[5] Станіслав Ткаченко, «Політична економія російських інформаційно-комунікаційних технологій», Політична записка PONARS Eurasia № 533, червень 2018 р. https://www.ponarseurasia.org/wp-content/uploads/attachments/Pepm533_Tkachenko_June2018.pdf

# Частина II. Рекомендовані заходи

Необхідно заблокувати можливість Росії використовувати, або отримувати ІТ, які містять (у будь-якій мірі) програмне забезпечення, мікропрограми та компоненти, які були виготовлені будь-якою країною, яка ввела санкції, або містять інтелектуальну власність.

Це включає в себе ІТ, розроблені в країнах, які не вводять санкції, що *де-факто* передбачає реекспорт, або перепродаж ІТ з країн, які ввели санкції. Іншими словами, країни, які вводять санкції, повинні перешкоджати можливості Росії ухилятися від санкцій шляхом імпорту ІТ з країн, які не вводять санкції, якщо ці ІТ містять будь-яке обладнання, функцію чи бібліотеку, або спілкуються з будь-яким пристроєм/службою, сховищем, чи мережевим комутатором, якими володіє, контролює, керує чи управляє юридична особа під юрисдикцією країни, яка наклала санкції.

## 1. Зупинити використання технологій у військових цілях

Ми рекомендуємо видалення існуючих ресурсів і доступу до цифрових служб, облікових записів і даних (обчислювальних ресурсів, сховища, API, інфраструктурних служб), дезактивацію обладнання, мікропрограм, програмного забезпечення та служб, що використовуються на локальних серверах у Росії, блокування на доступ до служб підтримки, або оновлень, блокування будь-яких допоміжних функцій технологічних продуктів, або послуг, які вимагають доступу до ресурсів, розташованих у країнах, які наклали санкції, або які належать/керуються юридичними особами, що перебувають під юрисдикцією національних санкцій, якщо такі технології та послуги не вважаються урядами, що накладають санкції, такими, що мають потенціал подвійного використання, або в окремих випадках, коли ймовірні гуманітарні витрати потребують більш складного та цілеспрямованого підходу.

Ці санкції повинні застосовуватися до всього з наведеного нижче, що стосується продуктів та послуг для російських і неросійських організацій, які працюють у Росії, або операцій з ними:

- Фізичних товарів, що поставляються в Росію;
- Цифрових товарів, послуг та інтелектуальної власності, незалежно від того, передаються вони фізично, чи віртуально, використовуються дистанційно, чи на місці, активуються за ліцензією, чи оновлюються;
- Послуги технологічного «консультування»;
- Зберігання/управління даними/кодами;
- Електронні комунікації, документацію та цифрові активи;
- Промислове обладнання, компоненти та ресурси.

Ми спеціально рекомендуємо не дозволяти компаніям із країн, що вводять санкції, відмовлятися від своїх технологічних активів у Росії, оскільки це є простим способом уникнути дотримання санкцій. Державний нагляд необхідний у кожному конкретному випадку. Така поведінка відчуження призведе до прямо протилежного ефекту від бажаного. Наприклад, компанії з центром обробки даних у Росії не можна дозволяти просто передавати можливості російській організації, оскільки це збільшить технологічні ресурси, доступні російському уряду, потенційно

забезпечивши їх тисячами найсучасніших мікрочіпів, ліцензіями на програмне забезпечення та іншими критичними технологіями подвійного призначення. Це стосується не лише прикладів, пов'язаних із IT, але й у випадку з виробничими потужностями чи підприємствами, заснованими на наукових знаннях та інноваціях.

Для ефективного досягнення цих цілей, ми рекомендуємо запровадити нові вимоги щодо торгової документації та процедур «Знай свого клієнта», щоб забезпечити, прямо чи опосередковано, можливість контролю та розвитку, за потреби, всіх компаній, що надають IT-програми для Росії.

## 2. Боротись проти використання Інтернет-платформ як зброї

Ми рекомендуємо країнам, які вводять санкції, прийняти правила, які б боролися проти вепонізаціїї Інтернет-платформ в Росії. Росія зробила це за допомогою «привернення уваги» та бот-мереж, які використовують структури стимулів компаній IT-платформ проти найкращих інтересів світової громадськості. Це включає ефективні кампанії дезінформації та придушення критичних голосів.

З цією метою уряди, які накладають санкції, мають підпорядкувати всі соціальні платформи та платформи для обміну контентом:

- Протоколам перевірки користувачів для всіх облікових записів, чий вміст взаємодіє з пороговою кількістю інших користувачів,
- Спільній відповідальності за часто використовуваний контент, подібній до вимог щодо трансляції та преси та (наприклад, Ofcom у Великобританії),
- Вимогам розглядати скарги щодо заблокованих, або обмежених облікових записів протягом суворих періодів часу, включаючи прозорість і незалежний розгляд для користувачів, які бажають оскаржити ці дії.

## 3. Вимагати ліцензування передбачуваного експорту

Ми рекомендуємо, щоб країни, які вводять санкції, ухвалили правила, які вимагають від російських громадян виконання вимог «ліцензування передбачуваного експорту» для взаємодії з IT, які важливі для військових зусиль Росії, або які корисні для перешкоджання військовим амбіціям Росії. Це схоже на те, що громадянам Китаю, які працюють у Сполучених Штатах, потрібно отримати ліцензії на передбачуваний експорт для роботи з певним напівпровідниковим інтелектуальним обладнанням, обробним і виробничим обладнанням. З подібних причин ми також рекомендуємо, щоб російські IT-працівники національних організацій, до яких застосовані санкції, підлягали тим самим вимогам

## 4. Забезпечити виконання санкцій

Ми рекомендуємо створити спільне агентство, наприклад, Оперативна група ІТ, для управління та моніторингу доступу та використання Росією санкційних технологій. Вона повинна мати повноваження притягувати до відповідальності юридичних осіб під юрисдикцією держав-членів, чия продукція продовжує використовуватися у військових діях Росії. Така організація могла б стежити за спробами Росії імпортувати контрольовані технології з країн, які не вводять санкції. Група розробки фінансових заходів, або Вассенаарська угода можуть слугувати моделлю для створення такого агентства.

## 5. Сприяти доступу до інформації про війну

Ми рекомендуємо, щоб будь-які платформи споживчих технологій із застосування санкцій, які продовжують бути доступними в Росії (наприклад, платформи новин, відеомережі, соціальні медіа, онлайн-ігри, веб-сайти для дорослих), підпадали під узгоджені вимоги щодо обміну повідомленнями, які надають кінцевим користувачам у Росії доступ до інформації про ситуацію в Україні. Це можна зробити за допомогою взаємодії рекламного типу, спливаючих вікон, проміжних вікон, які потребують прокручування, та широкого спектру інших поведінкових веб-механізмів, щоб привернути увагу російських веб-користувачів до війни. Ця рекомендація стосується не лише великих веб-сайтів для обміну контентом, таких як YouTube, але й будь-якого веб-порталу для користувачів, що працює в Росії. Крім того, ми вважаємо, що для цих платформ важливо бути прозорими щодо моделей споживання користувачів на їхній платформі в кожній країні, таким чином надаючи порівняльну інформацію про охоплення прокремлівською пропагандою в порівнянні з більш збалансованими джерелами інформації. Такі звіти мають публікуватися регулярно та містити достатньо деталей, щоб науковці та політики могли відповісти на запитання щодо відносних переваг і шкоди від роботи кожної платформи в Росії та в усьому світі.

## 6. Оцінити очікуванні результати

Через вищезазначені цілі та рекомендації ми очікуємо наступних результатів:

1. Зменшити здатність російських військових використовувати ІТ від країн, які ввели санкції, для нападу на Україну. Це включає, серед іншого:
    - Можливість шифрування, або підробки сигналів GPS/AIS;
    - Надійність і якість телекомунікацій;
    - Уміння здійснювати розвідку, або наведення зброї;
    - Можливість здійснювати радіолокаційне блокування;
    - Можливість зламати, або іншим чином скомпрометувати БПЛА;
    - Можливість ідентифікації електромагнітних сигнатур обладнання;
    - Здатність навчати та екіпірувати війська;
    - Здатність ефективно командувати та контролювати військо;
    - Здатність створювати, з’єднувати або іншим чином виготовляти предмети військового або подвійного призначення;
    - Здатність створювати та підтримувати постачання, логістику та допоміжні операції на всіх театрах війни.

2. Зменшити здатність російського уряду здійснювати кібератаки на соціальну та промислову цифрову інфраструктуру в Україні та за її межами.
3. Зменшити фізичні і кібернетичні операції Росії в космічній сфері, включаючи зниження здатності Росії проводити випробування протисупутникової зброї прямого підйому (DA-ASAT), або інші наступальні кінетичні протисупутникові атаки, а також глушіння та кібератаки щодо комерційних і військових космічних засобів.
4. Змістити розподіл кіберресурсів Росії з нападу на оборону через відмову в ІТ від країн, які вводять санкції. Змусити Росію виділити більше особового складу та пов'язаних ресурсів з наступальних кібердій проти України для усунення прогалин в оборонних можливостях Росії.
5. Зменшити здатність російського уряду поширювати дезінформацію за допомогою «інформаційної війни» та пропагандистських стратегій як усередині Росії, так і за її межами.
6. Зменшити здатність російського уряду ізолювати російський технологічний сектор від економічних і соціальних наслідків війни в Україні, збільшити свої витрати на продовження постачання військових та інформаційних машин російського уряду.
7. Обмежити ухилення від санкцій шляхом створення та забезпечення дотримання заборон на реекспорт і перепродаж ІТ країн, які запровадили санкції.

# Частина III. Потреба в жорстких IT-санкціях проти Росії

## 1. Різниці між цивільними та військовими IT немає

Ми переконані в тому, що зараз немає різниці між цивільним і військовим використанням IT в Росії. Будь-які іноземні IT або промислове обладнання/вхідні ресурси, імпортовані до Росії, можуть зрештою бути використані для досягнення військових цілей Росії.[6] Це включає перепрофілювання компонентів споживчих товарів (телефонів, комп'ютерів, пристроїв IT тощо) для військових цілей. Через успіх нещодавніх обмежень на продажі напівпровідників до Росії Кремлю стає все важче ремонтувати обладнання та виробляти новітні системи озброєння, які мають іноземні бортові компоненти, включаючи безпілотники та інші ключові ресурси. Російський військово-промисловий комплекс вдається до використання мікрочіпів та інших компонентів споживчої електроніки для виробництва/ремонту систем озброєння. Споживчі цифрові камери з'являються у флагманських безпілотниках. На даний момент будь-яка передача іноземних технологій, або знань, або цифрова інфраструктура може зрештою бути використана для підтримки військової активності Росії в Україні.

Російський уряд і військові також покладаються на іноземне готове корпоративне операційне програмне забезпечення для комунікацій, аналізу, людських ресурсів, логістики та інших функцій, які складають основу поточних наступальних військових та інформаційних операцій проти України та інших країн. Російські військові значною мірою покладаються на іноземне комерційне обладнання та програмне забезпечення для управління матеріально-технічним забезпеченням, підтримки польових операцій, виробництва обладнання, зв'язку з пунктами вербування по всій країні, планування та проведення навчання та координації з військово-промисловим комплексом.[7] У тій мірі, в якій вона покладається на технології, що працюють через смартфони та подібні роздрібні пристрої кінцевих користувачів, смертоносні операції російських військових в Україні покладаються на набір іноземних IT-сервісів, присутніх на іноземних пристроях. Іноземні корпорації можуть відключати ключові служби на цих пристроях, що робить їх майже непридатними для військових цілей.

Сім місяців поспіль після вторгнення Росії в Україну, майже всі послуги великих іноземних технологічних компаній залишаються доступними для існуючих клієнтів у Росії. Російські пристрої продовжують отримувати оновлення/патчі програмного забезпечення та продовжують використовуватися російським урядом для бойових дій. Іноземні компоненти наразі «виявляють у російській *техніці*, яка використовується у війні проти України. Багато з цих виробів були виготовлені після 2014 року, коли вперше почалася війна на сході України, а Європейський Союз і Сполучені Штати запровадили початковий пакет санкцій проти Російської Федерації."[8]

---

[6] Джеймс Бірн та ін., Silicon Lifeline: Західна електроніка в центрі російської військової машини. RUSI, серпень 2022 р. https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine

[7] Джеймс Бірн та ін., Silicon Lifeline: Західна електроніка в центрі російської військової машини. RUSI, серпень 2022 р. https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine

[8] Дослідження озброєного конфлікту, «Спільність компонентів у передових російських системах зброї», Польова розсилка України, вересень 2022 р.

Крім того, програмні пакети системи автоматизованого проектування та виробництва (CAD/CAM) та інформаційного моделювання будівель (BIM) відіграють важливу роль у розробці широкого спектру сучасних технологічних систем. Послуги гігантів програмного забезпечення CAD/CAM/ BIM, таких як французька Dassault Systèmes (виробник SOLIDWORKS), бостонська PTC (виробник PTC Creo) і Bay Area Autodesk (виробник Autodesk Inventor і Revit) повідомили про згортання діяльності в Росії після великомасштабного вторгнення в лютому, хоча продукція загалом залишається доступною для існуючих клієнтів. Глобальні демократії повинні продовжувати розбудовувати експортний контроль і механізми нагляду, щоб обмежити доступність передового програмного забезпечення CAD/CAM/BIM на території Росії, оскільки їхні можливості можна використовувати не лише для підтримки добре функціонуючого високотехнологічного сектору, а й для просування розробки проектів і виробництва передових наступальних, оборонних і військових компонентів матеріально-технічного забезпечення, систем, обладнання та інфраструктури.[9] Тому вкрай важливо, щоб Росія не мала доступу до будь-яких IT у будь-якій формі, які відіграють певну роль, або можуть замінити будь-який предмет, який відіграє певну роль у підтримці війни Росії в Україні.

### a. Іноземні IT продовжують підтримувати російську військову машину

Російські боєприпаси, ракети, системи наведення, артилерія, оборонне озброєння, ряд важкої техніки, танків, підводних суден тощо базуються на компонентах, або технологіях виробництва, які безпосередньо не належать Росії. Наприклад, компанія DMG Mori Seiki є німецько-японським постачальником високоточного обладнання та програмного забезпечення, яке використовується в Росії для артилерійських стволів і компонентів ракет «Калібр». Таке сучасне виробниче обладнання покладається на постійне надання послуг (таких як активне виявлення несправностей і технічне обслуговування, інформаційні послуги в Інтернеті, дистанційне керування та діагностика), а також втручання іноземного досвіду та надання запасних частин для безперервної роботи на повну потужність. Загалом, будь-яка промислова система або функціональність, яка забезпечує проектування, експлуатацію, виробництво, тестування, забезпечення якості або логістику, пов’язану з товарами та технологіями подвійного використання, потребує розгляду в рамках прямих і комплексних санкцій. Це включатиме діяльність таких компаній, як Siemens і Oracle, які забезпечують важливу магістраль і системи підтримки для російської промисловості.

Зв’язок на полі бою Росії забезпечується завдяки гібридним мережам, які плавно перемикаються між радіо-, супутниковими та локальними інтелектуальними мережевими концентраторами, щоб безпечно передавати повідомлення через іноземні смартфони та подібні пристрої, які часто використовують іноземне програмне забезпечення, або програмне забезпечення, що містить іноземні бібліотеки та можливості. Перешкоджання зв’язку та розвідці на полі бою Росії обмежує її здатність проводити наступальні операції та знижує їх успіх.

[9] https://cepa.org/article/dont-stop-now-tech-sanctions-can-wreck-putins-war-machine/

Російські військові ІТ включають споживчі пристрої з підтримкою Інтернету, які багато в чому залежать від іноземних ІТ. Російські військові ІТ зв'язуються з низкою іноземних сервісів у хмарі та покладаються на іноземні операційні системи, бібліотеки та протоколи безпеки чи зв'язку. Вони включають в себе пристрої Інтернету речей (IoT) з можливостями дистанційного зондування, які можна дистанційно вимкнути, а також програмне забезпечення, або мікропрограму, які покладаються на регулярні оновлення, або виправлення від іноземних компаній для усунення виявлених вразливостей. Більшість цих іноземних ІТ належать, розробляються, або виробляються країнами, які ввели санкції.

Бувають ситуації, коли українські військові перебувають у тісному контакті з російськими військовими частинами під час активних бойових дій, що викликає занепокоєння щодо випадкового втручання в українські військові системи, коли вони мають намір вивести з ладу та погіршити роботу російських військових систем та технологій (те, з чим щодня мають справу українські військові з активними мережевими вузлами Starlink). Ми зазначаємо, що для визначення походження можна використовувати функції пристрою та мережі. Ми розглядаємо такі функції, як використання російських мереж, sim-карт, зв'язок зі службами, розташованими на явно контрольованих Росією територіях і в самій Росії, у координації з українськими військовими, якщо це необхідно. Ми наголошуємо на тому факті, що значні перебої в мережі для використання у військових цілях не потребують повного видалення. Вимкнення достатньої кількості послуг, чітко пов'язаних із російськими військовими переміщеннями та мережами підтримки/логістики, фактично призведе до вимкнення послуг на передовій лінії. Ми рекомендуємо виважений і розумний підхід, але повторюємо першочергову важливість усунення доступу, наскільки це можливо.

## 3. Іноземні ІТ продовжують підтримувати російську інформаційну машину

Російська вепонізація іноземних ІТ поширюється як на кібер, так і на фізичну сферу. Російський уряд використовує висококваліфіковані ІТ-підрозділи для використання слабких місць у цифровій інфраструктурі іноземних держав, часто з метою завдати шкоди як цифровій, так і фізичній інфраструктурі. Зокрема, фінансовий сектор і державні служби України зазнавали постійних атак протягом багатьох місяців, а атаки на цифрову інфраструктуру США, ЄС і Великобританії також приписують російським кіберпідрозділам, які діють під офіційним керівництвом. Санкції мають перешкоджати кіберактивам та інфраструктурі, що лежить в основі воєнних і пропагандистських машин Росії, незалежно від того, чи належать ці активи в кінцевому підсумку російській державі, чи російським недержавним суб'єктам, які підтримують ті самі цілі. Держави, які накладають санкції, повинні зменшити здатність російських державних і недержавних організацій здійснювати атаки та скомпрометувати кіберінфраструктуру, демократичні інституції та інформаційний простір України та держав, які вводять санкції.

Незважаючи на те, що багато країн, які наклали санкції, ввели обмеження на продаж військових компонентів і допоміжних систем для Росії, іноземне програмне забезпечення, послуги, технічна

інфраструктура, інтелектуальна власність та інші менш матеріальні об'єкти не підпадають під санкції чи обмеження, окрім основного набору відомих державних організацій. Компанії в країнах, які запровадили санкції, здебільшого були змушені вибирати, чи продовжувати роботу в Росії та як змінити свою діяльність в Росії. Це залишає потенційно великий розрив між наміром накласти санкції на країни та діями ІТ-компаній під їх юрисдикцією.

У результаті російський уряд і недержавні суб'єкти продовжують значним чином впливати на громадську інформацію та громадську думку в Росії та країнах, які запроваджують санкції. Це відбувається як за допомогою технології підтримки на рівні мережі, аналізу даних і бізнес-аналітики, мов програмування (наприклад, Matlab, SAS, C#), так і на рівні веб-платформи користувача. Усередині країни інші платформи побудовані на західних технологіях і часто розміщуються в центрах обробки даних, які контролюються державними організаціями або їхніми технологіями. За межами країни платформи дозволяють російському уряду охоплювати країни та населення по всьому світу. Соціальні мережі, рекламні мережі, традиційні засоби масової інформації та стратегічно сплановані пропагандистські кампанії проти ключових політичних фігур в Україні, держав, які накладають санкції, і російської опозиції є частиною програми постійного та всебічного управління громадською думкою, сіяння плутанини та спотворення публічних повідомлень на перевагу Росії. Росія може проникнути та використати практично будь-яку мережу, яка дозволяє людям ділитися контентом, створювати спільноти, купувати та продавати один в одного, а також брати участь у спільних заходах у мережі та поза нею. Будь-яка технологія, яка дозволяє Росії поширювати дезінформацію та потенційно широкомасштабне «вірусне» поширення пропаганди потребують залучення превентивних процесів, які підлягають перевірці, щоб мінімізувати їх охоплення (подібно до перерв у торгівлі на фінансових ринках), або повного блокування. Це вимагає змін у тому, як ІТ-платформи структурують свої послуги.

Щоб запобігти поширенню дезінформації та неправдивої інформації з боку Росії та інших зловмисників, необхідно запровадити основні механізми регулювання та управління. Ці заходи підвищать стійкість і відповідальність контент-платформ для запобігання маніпуляціям. Це, у свою чергу, зменшить силу російських державних і недержавних акторів у розгортанні інформаційної війни проти України та санкцій проти країн. Важливо те, що ІТ-компанії повинні нести відповідальність за алгоритми та контент, які підсилюють і повторюють наративи Кремля. Наприклад, такі ініціативи, як ініціативи Інституту стратегічного діалогу, які порівнюють тенденції платформ соціальних медіа для посилення ехо-камер,[10] слід розширити (і включити до аналізу Росію), для сприяння застосуванню достатнього тиску. Рекламні мережі повинні порушувати санкції за продаж програмного рекламного простору будь-якій російській організації та нести відповідальність за повну перевірку кінцевого бенефіціара.

## 4. Ключові сектори Росії ізольовані від війни

[10] Інститут стратегічного діалогу, "404 Достовірну інформацію не знайдено", Звіт, 16 серпня 2022 р., https://www.isdglobal.org/digital_dispatches/404-reliable-information-not-found/

За останні 10 років Росія вклала значні кошти у створення інтернет-інфраструктури, яку можна (майже) повністю ізольувати від зовнішнього світу, тісно співпрацюючи з технологічними гігантами країн, що вводять санкції, щоб дозволити певним службам продовжувати працювати, водночас відфільтровуючи "небажаний" контент. Кремль, так само як і Китай, зацікавлений лише в збереженні іноземних технологій у своїй мережі, материнські компанії яких спеціально поступаються його вимогам. Технічні компанії, які все ще відповідають вимогам Росії, беруть участь у підтримці російської війни та інформаційної машини, компрометують власні платформи та опосередковано сприяють спустошенню України.

За останні 5 років російський уряд значно посилив операції з моніторингу інтернет-трафіку, а також стеження за політично чутливими особами, які можуть не погоджуватися з Кремлем. Це досягається частково за рахунок використання іноземних IT, які виявляють і відстежують уразливості інфраструктури мережевого обладнання в Росії і в усьому світі. Значну частину фізичних компонентів, необхідних для цього, було б важко отримати сьогодні, але для гарантії того, що весь пакет технологій буде неможливо підтримувати в середньостроковій перспективі, необхідні санкції.

Намір Путіна перевести Росію на ізольовану централізовану та стійку інтернет-інфраструктуру, або «сплінтернет», спрямований на повний контроль над інформацією, що потрапляє через мережу. Така мережа дозволила б російським військовим загрожувати глобальній інтернет-інфраструктурі, такій як підводні кабельні проекти, одночасно обмежуючи внутрішні наслідки таких дій. Це збільшило б можливості Росії безкарно атакувати глобальні потоки інформації, фінансові ринки, енергетичні активи, торгівлю тощо. Тому держави, які накладають санкції, повинні заборонити використання іноземних IT для створення сплінтернету в Росії та ізоляції її економіки від глобальної інформаційної екосистеми.

Іншими словами, ці рекомендації спрямовані на те, щоб загалом обмежити використання Росією західних технологій і завадити російському уряду ізолювати спосіб роботи Інтернету, для досягнення якого, за іронією долі, також потрібні західні технології.

Одночасно з безпосередньою відмовою Росії в технологіях, ми усвідомлюємо, що треті сторони, які мають життєздатні альтернативи (такі як Китай), не намагатимуться заповнити прогалини, що залишилися позаду, і підірвати мету санкцій. Ми наполегливо закликаємо країни, які вводять санкції, продовжувати стимулювати ці країни не брати участі в такому захопленні земель і розглянути можливість запровадження вторинних санкцій, якщо ситуація вимагатиме такого кроку.

Наші рекомендації також мають економічну сторону. Технологічна міграція надзвичайно складна, коли стикається з відключенням існуючої інфраструктури та процесів (оскільки українцям важко ремонтувати енергетичну інфраструктуру під час атаки). Це передбачає не лише великі витрати на придбання обладнання та програмного забезпечення, але й людську працю, навчання та втрату продуктивності через реструктуризацію команд і бізнес-процесів. Це гроші, які не можна витрачати на знищення України.

З 2012 року Володимир Путін намагався подолати залежність Росії від іноземних технологій шляхом розвитку місцевого російського IT-сектору. Ці зусилля дали невеликий технологічний сектор, якому бракує інновацій і не є конкурентоспроможним у всьому світі. Як наслідок, існування російського технологічного сектора сильно залежить від державних контрактів (що також надзвичайно ускладнює ідентифікацію технологічних каналів для уряду). Ті частини сектора, які є інноваційними, покладаються на партнерство з іноземними компаніями, які передають знання та технології, такі як штучний інтелект і машинне навчання. Посилення ізоляції російського технологічного сектору від технологій країн, які запровадили санкції, зменшить його інноваційний потенціал, якщо він не стане партнером країн, які не запровадили санкції.[11]

Російський уряд підтримує багато власних технологій і систем програмного забезпечення для захисту зв'язку, підробки сигналів радарів, GPS і AIS, перехоплення та втручання в радіо- та супутникові системи, фільтрації інтернет-трафіку та виконання різноманітних завдань обробки сигналів. Ці системи часто являють собою клаптик із застарілих технологічних пакетів, змішаних із сучасними передовими можливостями. Такі системи покладаються на крихкі людські мережі знань у разі виникнення проблем. Невеликі збурення цих систем можуть мати величезний вплив. Таким чином, IT-персонал є критично важливим активом для російського уряду, який зараз прямо чи опосередковано підтримує війну Росії проти України.

Майже 2 мільйони висококваліфікованих росіян працюють у технологічному секторі Росії, що становить близько 5% активного російського ринку праці в 2021 році. З початку війни в лютому 2022 року, число технічних працівників, які покидають Росію, коливається від 300 000 до 600 000, хоча незрозумілим залишається, яким буде довгостроковий статус цих осіб. Багато працівників, які виїхали, працювали в іноземних IT-компаніях як співробітники, або фрілансери через такі платформи, як Fiverr і Upwork. Ці технічні працівники зазвичай отримують високу зарплату. Країни, які запровадили санкції, повинні робити все можливе, щоб ці технічні працівники не повертались до Росії.

Багато іноземних технологічних компаній все ще ведуть активну діяльність і працюють в IT-сфері в Росії безпосередньо, або через дочірні компанії. Технічні платформи в країнах, які запровадили санкції, все ще приймають російських працівників у IT-секторі, секторі дизайну, маркетингу та суміжних сферах. Поки не буде прямого блокування іноземних компаній, які працюють у Росії та наймають російських працівників, ті компанії, що залишилися, продовжуватимуть підтримувати російський технологічний сектор високими зарплатами, який захищений від наслідків вторгнення Росії в Україну. У цьому документі мінімально рекомендується, щоб російські працівники мали ті самі передбачувані експортні кваліфікації, які б вимагалися, якби той самий працівник перебував у країні, яка запровадила санкції, особливо якщо будь-які компанії в структурі власності мають справу з предметами або знаннями, які потенційно можуть бути використані для військових операцій Росії.

[11] Станіслав Ткаченко, «Політична економія російських інформаційно-комунікаційних технологій», Політична записка PONARS Eurasia № 533, червень 2018 р. https://www.ponarseurasia.org/wp-content/uploads/attachments/Pepm533_Tkachenko_June2018.pdf

Крім фізичної інфраструктури та програмного забезпечення, технологічний консалтинг і пов’язана інфраструктура навчання на базі компаній не повинна обслуговувати російських працівників. Крім того, слід контролювати імпорт російських ІТ-продуктів і послуг на ринках країн, які ввели санкції, щоб позбавити російський уряд додаткових доходів і уникнути компрометації цифрових систем національних санкцій.

# Частина IV. IT мають підпадати під санкції

У наступних категоріях зроблено спробу визначити технології та допоміжну інтелектуальну власність та інфраструктуру, які повинні санкціонуватися для досягнення бажаних цілей. Цей перелік є галузевим агностиком і призначений для застосування до всіх критичних секторів економіки.

- Програмне забезпечення/мікропрограмне забезпечення (включно з підтримкою мережі та Інтернету)
    - Кібербезпека/Захист
    - Операційні системи
    - Контролери/інтерфейси пристроїв
    - Керування мережею/обробка та моніторинг пакетів
    - Повідомлення/Зв’язок/VoIP
    - Логістика/Операції/Управління інфраструктурою
    - Фінанси/Платежі (зокрема фінансові технології, криптовалюти, NFT)
    - Бази даних/Сховище/Блокчейн
    - Обробка/аналіз даних
    - Обробка сигналу
    - Криптографічні служби/шифрування
    - Статистичні/числові обчислення/бібліотеки
    - Наукові обчислення та інфраструктура (включаючи фізику/геофізику/космос)
    - Навколишнє середовище/Енергія/Моделювання
    - Ігри
    - CAD/CAM/BIM
    - Комп’ютерний зір
    - Продуктивність/креативність
    - Екземпляри й керування обліковим записом і даними користувача
    - Веб-додатки та пов’язане програмне забезпечення
    - Основи веб-технологій
    - DNS веб-сайту та керування мережевим трафіком
    - Служби пошти та зв’язку веб-сайту
    - Веб-реклама та програмне відстеження
    - Соціальні мережі та відповідні функції
    - Керування ідентифікацією та автентифікація
    - Системи керування контентом
    - Інфраструктура/інструменти моніторингу та тестування
    - Керування/тестування/розгортання коду
    - Гранична інфраструктура, мережі доставки контенту
- Хмарні обчислення/Хмарні служби/Хмарне сховище/Керування інфраструктурою
- Датчики, пристрої IoT, служби керування даними, дистанційне зондування
- Промислове обладнання/Робототехніка/Гідравліка/Контролери важкої техніки та їх компоненти
- Керування ліцензією на програмне забезпечення та оновленнями

- Технічне обслуговування/підтримка/віддалене обслуговування
- Обладнання або інтегровані компоненти, що підтримують будь-яку з перерахованих вище можливостей або їхнє створення
- Технологічний аутсорсинг/віддалене працевлаштування

## Висновок

Міжнародна робоча група із питань санкцій проти Росії 1 має на меті надати експертні знання та досвід урядам і компаніям у всьому світі, допомагаючи формулювати пропозицій щодо санкцій, які збільшать ціну вторгнення Росії в Україну та підтримають демократичну Україну в захисті своєї територіальної цілісності та національного суверенітету. Поточний підхід санаційної коаліції, який передбачає поступове накладення санкцій, допомагає Росії адаптуватись, замість того, шоб переглянути ціль ведення війни. Путін має намір і надалі анексувати українську територію та підкоряти Україну під сферу впливу Росії. Нашою метою має бути зменшення ресурсів у його розпорядженні.

Рекомендації в цьому документі спрямовані на погіршення військового потенціалу Росії на місцях у короткостроковій, середньостроковій та довгостроковій перспективі. Вони намагаються погіршити здатність Росії підтримувати критично важливу сучасну інфраструктуру до такої міри, що вона також може заважати інфраструктурі стратегічного військового командування та контролю Росії (відсутність запасних частин, несумісність, відсутність знань від іноземних організацій тощо). Рекомендації, викладені в цьому документі, також спрямовані на погіршення ресурсів Путіна для ведення інформаційних війн, в якості непрямого засобу зменшення підтримки в російському суспільстві його війни. Третя мета наших рекомендацій — погіршити російську економіку в цілому в надії, що постраждалі російські еліти та суспільство врешті-решт вимагатимуть припинення війни Путіна як шлях до послаблення санкцій.

Зараз важливо діяти швидко й рішуче, щоб запобігти доступу Росії та використанню ідей і технологій від країн, які протистоять цій війні, використанню цих активів для сіяння хаосу та руйнування в Україні та збільшенню майбутнього тягаря, який нестимуть країни, які вводять санкції, у відбудові України та глобальної інфраструктури безпеки.

## Додаток I: Практичні дослідження технологічної компанії

Як приклад ми наводимо деякі з найвпливовіших іноземних організацій, які все ще надають апаратне забезпечення, програмне забезпечення, мікропрограми та послуги в Росії.

Багато з цих компаній вже вжили заходів щодо обмеження своєї діяльності на російському ринку та/або допомоги Україні. Завдяки рекомендаціям, які ми окреслили, ці компанії мають можливість вжити суттєвих подальших заходів для обмеження шкоди, яку їхні технології завдають народу України, а також витрати, які несе населення країн, які запровадили санкції, відшкодовуючи шкоду, завдану цими технологіями українській землі.

Оскільки війна триває, необхідно оцінити широкі фізичні та економічні (прямі та непрямі) збитки, пов'язані з постійною доступністю певних послуг у Росії та будь-яку потенційну неоднозначність у використанні їхніх технологій. Ми віримо, що ці компанії та тисячі інших, які все ще задіяні в технологічній екосистемі, яка підтримує Росію, захочуть добросовісно працювати з урядами країн, які ввели санкції, щоб знайти швидкі, ефективні та повні рішення для обмеження нанесення подальшої шкоди.

### Міжнародні бізнес машини (IBMs)

- **Що:** операційні системи IBM; Red Hat; сервери та апаратні компоненти/запчастини; проміжне програмне забезпечення; компоненти, включаючи мікрочіпи, комутатори, маршрутизатори та інші комунікаційні пристрої; бази даних і бази даних як послуга; хмарна інфраструктура; інфраструктура обробки платежів; послуги з обробки та зберігання даних; послуги бізнес-аналітики; B2B та урядове програмне забезпечення; галузеві логістичні та фінансові послуги та подібне програмне забезпечення, консалтинг, або обладнання, що надаються через будь-яку дочірню компанію в усьому світі.
- Ми стурбовані постійною доступністю продуктів і технологічних послуг IBM у Росії, а також використанням цих можливостей існуючими клієнтами в пакетах програмного забезпечення, які забезпечують військове командування та управління, координацію військових операцій, постачання, логістику, моделювання, навчання, та подібні заходи.

### Meta

- **Що:** Facebook та Instagram були заборонені російським урядом, що свідчить про те, що суб'єкти в країнах, які запровадили санкції, та їхні уряди мало контролюють доступ до надійної інформації в Росії. WhatsApp не був заборонений, зокрема тому, що багато російських урядовців і військових користуються платформою, що робить її доступною також для неурядових організацій громадянського суспільства та лідерів опозиції. Facebook зробила кілька показових кроків, щоб повністю заблокувати рекламу російських організацій у всьому світі, і посилила зусилля, щоб відсіяти мережі підроблених облікових записів. Проте безпечні мережі обміну повідомленнями, такі як WhatsApp, продовжують підтримувати військову координацію, і дезінформація з російських і пов'язаних облікових записів залишається великою проблемою. Незважаючи на складність (проте реальність), Meta має вжити більших заходів, щоб заборонити використання WhatsApp для підтримки війни, зберігаючи його використання для неурядових комунікацій.

### Twitter

- **Що:** Twitter, Twitter Ads (за межами Росії)
- **Де:** Служби, які використовуються для поширення дезінформації за межами кордонів Росії, що, у свою чергу, призводить до витрат на координацію та ускладнень у країнах, які застосовують санкції, посилює геополітичну напруженість і сприяє досягненню цілей Кремля.

### Apple

- **Що:** пристрої Apple, Apple App Store, комунікаційні протоколи та служби Apple, служби кібербезпеки Apple і служби/бібліотеки захисту пристроїв.
- Пристрої та можливості Apple через Apple App Store продовжують використовуватися у військових умовах для зв'язку, матеріально-технічного забезпечення, розвідки, дистанційного керування військовими засобами та подібних військових і квазівійськових цілей. Apple вжила рішучих і помітних заходів, щоб запобігти поповненню запасів пристроїв на російському ринку, хоча пристрої Apple продовжують перетинати кордон через так звані схеми паралельного імпорту. Сервіси Apple Pay були заблоковані через фінансові санкції проти Росії.

### Google

- **Що:** апаратні пристрої Google; операційні системи Android; Google Play; Google Cloud; Карти Google, служби визначення місцезнаходження; Gmail і служби безпечного зв'язку; адміністрування домену/послуги хостингу; Офісне/продуктивне програмне забезпечення; Оновлення програмного забезпечення.
- З початку війни компанія Alphabet заблокувала рекламу в Росії, заблокувала глобальну рекламу для будь-якої організації, розташованої в Росії, заблокувала тисячі підозрілих облікових записів на YouTube і продовжує підтримувати український уряд у виявленні та реагуванні на кіберзагрози на ключових об'єктах інфраструктури. Google стала першою компанією, яка отримала Українську премію миру за готовність підтримувати Україну технологічно та благодійно. YouTube залишається найважливішим джерелом реальної інформації про війну для росіян, які проживають у Росії, і підтримує основні російські незалежні медіа та опозиційні канали, що надають контент усередині Росії. У той же час, пристрої Google і пристрої з операційною системою Android використовуються у зв'язку на полі бою, щоб здійснювати розвідку в реальному часі, використовувати обладнання для дистанційного керування, передавати повідомлення між підрозділами та обмінюватися інформацією з підрозділами матеріально-технічного забезпечення, де зашифрований радіозв'язок менш ефективний, або де військам не вистачає спеціально виданого обладнання. Google Play підтримує налаштування пристроїв для досягнення цих цілей. Оновлення програмного забезпечення продовжує захищати ці пристрої, а служби визначення місцезнаходження служать вторинним рівнем ситуаційної обізнаності (наприклад, Google Earth). Документи Google і пов'язані служби надають базові

можливості для обміну знаннями та співпраці в межах Росії для організації військового найму, навчання та регіонального військового планування. Інфраструктура та сервіси Google Cloud продовжують працювати для різноманітних російських організацій, які можуть підтримувати військові операції та планування Росії.

### Microsoft

- **Що:** Windows, Exchange, Office/Outlook/Teams, Microsoft Bing/Ads, Skype, Azure Cloud, мережеві протоколи та служби, Github (репозиторії, керовані з Росії, російськими організаціями, або підключені до російської інфраструктури для розгортання/тестування), апаратні пристрої Microsoft (наприклад, Surface), інформаційні послуги в Інтернеті, оновлення програмного забезпечення, обслуговування та підтримка клієнтів.
- Корпорація Microsoft призупинила нові продажі всіх продуктів у Росії та наполегливо працювала, щоб допомогти українському уряду та багатьом іншим українським організаціям захистити себе від російських кібератак. Однак основні служби Microsoft, від Exchange до Office і хмарної інфраструктури Azure, залишаються доступними для переважної більшості довоєнної російської клієнтської бази Microsoft. Ми стурбовані використанням цієї інфраструктури для суміжних і безпосередніх військових цілей, зв'язку та логістики, розвідки та різноманітних квазівійськових випадків використання, які є руйнівними для України, і де важко встановити зв'язки з урядом Росії. Крім того, ми стурбовані тим, що по всій Росії проводиться велика кількість оперативних і матеріально-технічних заходів на підтримку військових і навчання за допомогою можливостей Microsoft, таких як Office365 і подібних служб. Не всі такі можливості можна здійснити, але там, де можливості можуть бути обмежені, існує можливість залишити великі прогалини в оперативній спроможності, що вимагає від Росії великих ресурсів для адаптації.

### Cloudflare

- Український уряд попросив Cloudflare припинити всі операції в Росії з початком війни. Cloudflare відмовився, заявивши, що це призведе до обмеження інформаційної свободи в Росії. Це дефектний аргумент. Уряд Росії контролює свободу Інтернету в Росії, і будь-який веб-сайт, захищений Cloudflare, який уряд хотів би контролювати, легко підпадає під заходи, які б забезпечили контроль. Тим часом програмне забезпечення Cloudflare робить російську урядову, військову та дезінформаційну інфраструктуру більш стійкою та здатною працювати та завдавати шкоди інтересам країн, що вводять санкції.

*Примітка. Включення афілійованих осіб призначене лише для ідентифікації та не означає схвалення спільних поглядів із співавтором. Підпис не означає, що кожен підписант погоджується з кожною ідеєю, запропонованою в цьому документі, натомість погоджується в цілому з наданими аргументами та доказами.*

**Ярослав Ажнюк,** підприємець та співзасновник Petcube.

**Таня Бабіна,** доцент кафедри фінансів Колумбійської бізнес-школи Колумбійського університету

**Андрій Бойцун**, к.т.н., засновник та редактор тижневика Ukrainian SOE Weekly; Незалежний консультант з корпоративного управління; колишній член Стратегічної консультативної групи з підтримки українських реформ (SAGSUR)

**Енн Л. Кланан**, доцент кафедри національної безпеки Військово-морської аспірантури та філія факультету Центру міжнародної безпеки та співробітництва (CISAC), Стенфордський університет. Тут є мої власні погляди, а не погляди ВМС США, Міністерства оборони чи уряду.

**Тетяна Дерюгіна,** доцент кафедри фінансів Університету Іллінойсу – Урбана-Шампейн; Співорганізатор групи «Економісти за Україну».

**Анастасія Федик,** асистент кафедри фінансів, Haas School of Business, Каліфорнійський університет – Берклі; Співорганізатор групи «Економісти за Україну».

**Юрій Городніченко,** професор економіки Quantedge, кафедра економіки Каліфорнійського університету в Берклі; Співорганізатор групи «Економісти за Україну».

**Денис Гутенко,** учасник програми лідерства, Стенфордський університет; колишній Голова Держафної фіскальної служби України.

**Джеймс Ходсон,** директор і Головний виконавчий директор, AI for Good Foundation; Співорганізатор групи «Економісти за Україну».

**Ерік Джонсон,** колишній керуючий директор Cambridge Associates і колишній співробітник Ради національної безпеки, Ситуаційна кімната Білого дому.

**Бронте Касс,** менеджер програми Інституту міжнародних досліджень Фрімана Споглі (FSI), Стенфордський університет; Помічник координатора Міжнародної робочої групи з російських санкцій.

**Крейг Кеннеді,** юрист, Центр російських та євразійських досліджень Девіса, Гарвардський університет.

**Майкл Макфол,** директор Інституту міжнародних досліджень Фрімана Споглі (FSI), професор політології та старший науковий співробітник Інституту Гувера, в Стенфордському університеті; Координатор Міжнародної робочої групи з російських санкцій.

**Бенджамін Молл,** професор Лондонської школи економіки та політичних наук.

**Тимофій Милованов,** президент Київської школи економіки; Доцент Піттсбурзького університету.

**Джейкоб Нелл,** старший науковий співробітник Київської школи економіки, колишній головний економіст з питань Росії та керівник відділу європейської економіки Morgan Stanley.

**Олександр Новіков,** голова Національного агентства з питань запобігання корупції, Україна.

**Стівен Пайфер,** співробітник Вільяма Перрі, Центр міжнародної безпеки та співробітництва (CISAC), Стенфордський університет, колишній посол США в Україні.

**Лукаш Рейчел,** докторант кафедри економіки Прінстонського університету.

**д-р Бенджамін Л. Шмітт,** науковець з розробки проектів, Гарвардський університет; старший науковий співробітник з демократичної стійкості, Центр аналізу європейської політики; Науковий співробітник Rethinking Diplomacy Центру міжнародних і глобальних досліджень Університету Дьюка.

**Наталія Шаповал,** Віце-президент з політичних досліджень Київської школи економіки.

**Андрій Симонов,** доцент Колумбійської школи бізнесу Колумбійського університету.

**Дар'я Софіна,** Національне агентство з питань запобігання корупції, Україна.

**Ілона Сологуб,** науковий редактор, Vox Україна; Співорганізатор групи «Економісти за Україну».

**Джеффрі Зонненфельд,** Старший декан та професор, Єльська школа менеджменту.

**Кирило Сигида,** співзасновник Reface, Zibra, Pawa.

**Павло Верхняцький,** керуючий партнер, директор COSA.

**Юрій Вітренко,** екс-генеральний директор НАК «Нафтогаз України».

**Владислав Власюк,** секретар української групи з питань запровадження санкцій щодо Росії.

**Дарія Зарівна,** менеджер з комунікацій української Робочої Групи з Питання Санкцій Проти Росії.