УКРАЇНА І НАСТУПНА РЕВОЛЮЦІЯ РОЗВІДКИ. КОЖЕН ІЗ НАС ШПИГУН

Вторгнення Росії в Україну стало переломним моментом для світу розвідки. За кілька тижнів до початку обстрілів Вашингтон публічно оприлюднив потік надзвичайно точних даних про пересування російських військ та їхні атаки під чужими прапорами, які Кремль міг використати для виправдання вторгнення.

Така стратегія розкриття інформації була новою: шпигунські аґенції звикли приховувати розвіддані, а не розкривати їх. Але цього разу вона виявилася дуже ефективною. З'ясувавши правду ще до того, як російська брехня закріпилася, Сполученим Штатам вдалося згуртувати союзників і швидко скоординувати жорсткі санкції. Оприлюднення розвідданих поставило російського президента Владіміра Путіна в глухий кут, змусивши замислитися над тим, як американським спецслужбам вдалося так глибоко проникнути в його уряд, що, своєю чергою, ускладнило й іншим країнам можливість ховатися за путінською брехнею і ставати на бік Росії.

Проте таке викриття були лише початком. Війна відкрила нову еру обміну розвідданими між Україною, Сполученими Штатами та іншими союзниками і партнерами, що допомогло протистояти неправдивим російським наративам, захистити цифрові системи від кібератак і допомогти українським військам завдавати ударів по російських цілях на полі бою. Це висвітлило глибоку нову реальність: розвідка більше не є справою лише урядових шпигунських аґенцій.

Упродовж останнього року приватні особи і групи відстежували плани й дії Росії у спосіб, який було неможливо уявити під час попередніх конфліктів. Журналісти повідомляли про розвиток подій на полі бою, використовуючи знімки з комерційних космічних супутників. Колишні урядовці та військові відстежували щоденні події на місцях і пропонували у Твіттері далекоглядний аналіз напрямку війни. Волонтерська команда студентів Стенфордського університету на чолі з колишнім військовослужбовцем армії США та аналітиком зображень з відкритих джерел Елісон Пуччіоні (Allison Puccioni) надає звіти Організації Об'єднаних Націй про порушення Росією прав людини в Україні, виявляючи та перевіряючи події за допомогою тепловізійних та електрооптичних зображень з комерційних супутників, відео з TikTok, інструментів геолокації та інших засобів. В Інституті вивчення війни, який є основним джерелом інформації для військових експертів та аналітиків, дослідники навіть створили інтерактивну карту конфлікту, яка повністю базується на несекретних розвідувальних даних з відкритих джерел.

Технологічний прогрес відіграв центральну роль у цій еволюції. Зрештою, саме Інтернет, соціальні мережі, супутники, автоматизована аналітика та інші досягнення дозволили цивільному населенню збирати, аналізувати та поширювати розвідувальну інформацію. Але хоча нові технології й допомогли пролити світло на російську військову діяльність, їхній вплив далеко не однозначно позитивний. Для 18 відомств, які складають розвідувальну спільноту США, нові технології дуже швидко створюють дедалі більше загроз. Вони різко збільшують обсяги даних, які мають обробляти аналітики. Компаніям та окремим громадянам вони дають нову потребу в розвідданих, аби ці приватні суб'єкти могли допомогти захистити інтереси країни. А ще вони надають нові розвідувальні можливості організаціям та окремим особам за межами уряду США та більшій кількості країн.

Ці зміни готувалися роками, і лідери розвідок наполегливо працюють над тим, щоб адаптуватися до них. Але передбачення майбутнього в нову технологічну епоху вимагає більшого. Вашингтон має ухвалити «оптові» зміни для того, щоб зрозуміти й використати нові технології. Зокрема, він має серйозно поставитися до створення нового відомства, яке б займалося розвідкою з відкритих джерел. Інакше розвідувальне співтовариство США відставатиме, що зробить американців більш вразливими до катастрофічних несподіванок.

ЧУДОВИЙ НОВИЙ СВІТ

Коли 1947 року було створено Центральне розвідувальне управління, світ перебував у дуже нестабільному стані. Союзники виграли Другу світову війну, але совєтські війська вже загрожували Європі. Репресивні режими зростали, демократії були втомленими і слабкими, а міжнародна система поділялася на вільні та неліберальні сфери. На тлі зростаючої невизначеності й тривоги Сполучені Штати були покликані очолити новий світовий порядок. Американські політики усвідомлювали, що для цієї ролі їм потрібні нові можливості, зокрема й краща розвідка. На їхню думку, централізація розвідки в новій аґенції мала забезпечити своєчасне розуміння майбутнього, щоб запобігти наступному Перл-Харбору і виграти холодну війну.

Багато в чому сьогодення виглядає моторошниим і схожим на ті перші повоєнні роки. Світ, де сильні держави використовують грубу силу, щоб отримати бажане, повернувся. Авторитарний лідер у Москві вторгається до сусідів і знову загрожує всій Європі. Демократії знову виглядають крихкими. Сполучені Штати та їхні союзники беруть участь у черговому змаганні великих держав – цього разу вони борються з Китаєм, країною, чиє піднесення з кожним днем виглядає дедалі менш мирним з його утисками свобод у Гонконзі, войовничою риторикою про

повернення Тайваню і провокаційними військовими навчаннями довкруж цього острова. Навіть марксизм-ленінізм повертається. На ретельно зрежисованому 20-му з'їзді партії Китаю президент Сі Цзіньпін дав зрозуміти партійним чиновникам, що ідеологія та особиста лояльність важливіші за подальшу економічну лібералізацію. Якщо хтось ще не зрозумів, то попередника Сі Цзіньпіна, налаштованого на економічні реформи, Ху Цзіньтао, було витягнуто з його крісла і на очах у представників преси виведено з партійних зборів як злочинця

Але зовнішність може бути оманливою. Завдяки технологічним інноваціям виклики сьогодення значно відрізняються від повоєнних. Нові технології трансформують планету у безпрецедентний спосіб і з безпрецедентною швидкістю. Усе це разом з винаходами робить світ більш взаємопов'язаним і докорінно змінює детермінанти геополітичної переваги. Нові технології і дані дедалі частіше стають основними джерелами національної могутності, вони нематеріальні, їх важче побачити і зрозуміти, їх часто створюють і контролюють компанії, а не уряди. Для ЦРУ та інших розвідувальних служб розуміння геополітичних небезпек і динаміки двадцять першого століття, ймовірно, буде значно складнішим, ніж у минулому.

Візьмімо інтернет. У середині 1990-х років у мережі було менше одного відсотка населення планети. Зараз вже шістдесят шість відсотків світу підключені до мережі – від далекої Арктики до бедуїнських наметів у пустелі. Лише упродовж останніх трьох років до Інтернету приєдналося понад мільярд людей. Цей зв'язок вже трансформував світову політику, як на краще, так і на гірше. Соціальні мережі підживлюють протести проти автократій, такі як Арабська весна та Гонконгський рух «Парасольки». Але вони сприяли й новій хвилі урядового технічного нагляду на чолі з Пекіном і дозволили Росії проводити масовані дезінформаційні операції, щоб впливати на вибори і підривати демократію зсередини.

Цифровий зв'язок – не єдина технологія, що змінює світовий порядок. Штучний інтелект (ШІ) руйнує майже кожну галузь – від медицини до вантажоперевезень – до такої міри, що, за оцінками одного з експертів, упродовж наступних 25 років штучний інтелект може ліквідувати до 40 відсотків робочих місць у всьому світі. Він змінює способи ведення війн, автоматизуючи все – від логістики до кіберзахисту. І навіть дозволяє державам створювати безпілотні винищувачі, які роєм можуть атакувати оборону і маневрувати швидше й краще, ніж люди-пілоти. Тож не дивно, що президент Росії Владімірр Путін заявив: той, хто буде лідером у розробці ШІ, «стане володарем світу». Китай також не приховує своїх планів до 2030 року стати світовим лідером у галузі ШІ.

Технологічні прориви також значно полегшують багатьом – включно зі слабкими державами і терористичними угрупованнями – виявлення подій, що розгортаються на землі, з космосу. Можливості комерційних супутників різко зросли, пропонуючи «очі в небі» для всіх, хто цього хоче. За період з 2016 по 2018 рік кількість запусків супутників зросла більш ніж удвічі; зараз навколо Землі обертається понад 5 000 супутників, деякі з яких не більші за буханку хліба. Комерційні супутники мають дещо менш досконалі можливості зондування, ніж їхні шпигунські побратими, але цивільні технології швидко вдосконалюються. Деякі комерційні супутники зараз мають настільки чітку роздільну здатність, що можуть розпізнавати кришки каналізаційних люків, знаки і навіть стан доріг. Інші здатні виявляти радіочастотні випромінювання, спостерігати за рухом транспортних засобів і шлейфами ядерного охолодження, працювати вночі, в хмарну погоду або крізь густу рослинність і маскування. Сузір'я малих супутників можуть відвідувати одне і те ж місце кілька разів на день, щоб виявити зміни за короткий проміжок часу – те, що колись було неможливим. Усі ці зміни вирівнюють розвідувальні можливості, і не завжди в кращий бік. Наприклад, у 2020 році Іран використовував комерційні супутникові знімки для спостереження за американськими військами в Іраку перед тим, як здійснити балістичну ракетну атаку, в результаті якої було поранено понад 100 людей.

Біля російського військового вертольота. Горлівський район, Україна, вересень 2022 року. Олександр Єрмоченко / Reuters

Серед інших технологічних досягнень, що мають вплив на національну безпеку, – квантові обчислення, які з часом можуть розкрити шифрування, котре захищає майже всі світові дані, роблячи навіть надсекретну інформацію доступною для супротивників. Синтетична біологія дозволяє вченим конструювати живі організми, прокладаючи шлях до революційних вдосконалень у виробництві продуктів харчування, ліків, зберігання даних і військової зброї.

У учасній війні зброя не виглядає як зброя.

Розуміння потенціалу і небезпек цих та інших нових технологій є важливим завданням розвідки. Уряд США повинен знати, хто може перемогти в ключових технологічних змаганнях і якими можуть бути їхні наслідки. Він має оцінити, як будуть вестися і вигравatися майбутні війни. А ще повинен з'ясувати, як нові технології можуть вирішити глобальні проблеми, такі як зміна клімату. Також мусить визначити, як противники використовуватимуть дані й технічні інструменти для примусу інших, вчинення звірств, ухилення від санкцій, розробки небезпечної зброї і забезпечення інших переваг.

Але на ці важливі питання стає дедалі важче відповісти, оскільки інноваційний ландшафт змінився і розширився, що ускладнює відстеження і розуміння винаходів. У минулому технологічні прориви, такі як Інтернет і GPS, були винайдені урядовими установами США, а згодом комерціалізовані приватним сектором. Більшість інновацій, які впливали на національну безпеку, не мали широкого комерційного застосування, тому їх можна було засекретити при народженні і, за потреби, обмежити назавжди. Сьогодні ситуація змінилася. Технологічні інновації, скоріш за все, матимуть «подвійне призначення»: як комерційне, так і військове. Вони також значно частіше винаходяться

в приватному секторі, фінансовані іноземними інвесторами, розробляються багатонаціональною робочою силою і продаються глобальним клієнтам як у приватному, так і в державному секторах.

Ті, що «народжуються» в приватному секторі, є доступнішими і їх не так легко обмежити. Наприклад, ШІ став настільки поширеним та інтуїтивно зрозумілим, що старшокласники без досвіду програмування можуть створювати глибокі фейки – згенеровані штучним інтелектом маніпульовані відео, які показують людей, що говорять і роблять те, чого вони ніколи не говорили і не робили. У березні 2022 року хтось випустив депфейк про те, як президент України Володимир Зеленський наказує українським солдатам скласти зброю. Зовсім недавно, щоб змусити українських чиновників розкрити інформацію про військові дії, використовувалися депфейки від імені Майкла Макфола, колишнього посла США в Росії. Фейки про Макфола стали настільки поширеними, що справжній Макфол був змушений написати у Твіттері застереження з проханням не піддаватися на те, що він назвав «новою російською зброєю війни».

Ці зміни в інноваційному ландшафті дають лідерам приватного сектору нову владу, а чиновникам з питань національної безпеки кидають нові виклики. Влада зміщується не лише за межами кордону. Вона зміщується і всередині країни. Американські соціальні медіа-платформи опинилися на передовій інформаційної війни, вирішуючи, що є справжнім, а що – фейком, що дозволено, а що – ні. Засновники стартапів винаходять можливості, які можуть бути використані ворогами, яких вони не можуть передбачити, з наслідками, які вони не можуть контролювати. Тим часом американські оборонні та розвідувальні відомства намагаються перейняти критичні нові технології ззовні і рухатися зі швидкістю винаходів, а не бюрократії. Лідери приватного сектору мають обов'язки, яких не хочуть, а урядові лідери прагнуть можливостей, яких не мають.

НАБИРАЮЧИ ШВИДКІСТЬ

Розвідку часто неправильно розуміють. Хоча шпигунські аґенції й мають справу з таємницями, все ж вони не займаються секретним бізнесом. Їхня основна мета полягає в надаванні інформації політикам і передбаченні майбутнього швидше й краще, ніж це роблять супротивники. Таємно отримана інформація з таких джерел, як перехоплені телефонні дзвінки чи шпигунські донесення з перших рук, важлива, але секрети – це лише частина картини. Більшість інформації в типовому розвідувальному звіті є несекретною або загальнодоступною. А необроблена інформація – секретна чи ні – рідко є цінною сама по собі, оскільки вона часто є неповною, неоднозначною, суперечливою, з поганих джерел, вводить в оману, навмисно оманливою або просто помилковою. Аналіз – це те, що перетворює непевні висновки на розуміння, синтезуючи розрізнені фрагменти інформації та оцінюючи її контекст, достовірність і значення.

Інтуїтивні здогадки не завжди правильні. Але якщо вони таки правильні, то можуть бути безцінними. Коли американські спецслужби попередили, що Росія збирається вторгнутися в Україну, це дало Вашингтону критичний час, щоб допомогти озброїти Київ і об'єднати Захід. Але незабаром шпигунським аґенціям може стати важче повторити цей успіх, тому що ландшафт глобальних загроз ще ніколи не був таким переповненим і складним, як сьогодні, і загрози рухаються швидше, ніж будь-коли. Працівникам розвідки стало важче виконувати свою роботу. Після майже півстолітньої боротьби з Совєтським Союзом і двох десятиліть боротьби з терористами сьогодні вони повинні протистояти різноманітним загрозам. А ще мають боротися з транснаціональними загрозами, такими як пандемії і зміна клімату, конкуренція великих держав з Китаєм і Росією, тероризм та іншими загрозами з боку слабких і невдалих держав, а також кібератаками, які крадуть, шпигують, підривають, руйнують та обманюють з приголомшливою швидкістю і масштабами.

Технології роблять сьогоднішній список загроз не лише довшим, але й грізнішим. Століттями країни захищали себе, будуючи потужні армії і використовуючи вигідне географічне розташування. Але в кіберпросторі будь-хто може атакувати з будь-якого місця, не долаючи повітряної, наземної і морської оборони. Найпотужніші країни зараз часто є найбільш вразливими, оскільки їхня могутність спирається на цифрові системи для бізнесу, освіти, охорони здоров'я, військових операцій тощо. Ці держави можуть зазнати великих атак, які виводять з ладу їхню критично важливу інфраструктуру. Вони можуть зазнавати повторюваних дрібних нападів, які можуть завдати руйнівної шкоди ще до того, як про це дізнаються силовики. Китай, наприклад, за допомогою хакерських атак проклав собі шлях до технологічної переваги в різних галузях промисловості – від винищувачів до фармацевтики, що директор ФБР Крістофер Рей назвав однією з найбільших передач багатства в історії людства і «найбільшою довгостроковою загрозою нашій економічній і національній безпеці».

Межа між мудрістю натовпу і небезпекою, що йде від нього, тонка.

Росія також дуже ефективно використовувала кібератаки, доводячи, що технології можуть дозволити зловмисникам зламувати свідомість, а не лише машини. Російські оперативники створили боти і фейкові профілі в соціальних мережах під виглядом американців, які поширювали дезінформацію по всій території США під час президентських виборів 2016 року, поляризуючи країну і підриваючи її демократію. Сьогодні Китай може налаштувати американців один проти одного, навіть не використовуючи американські технологічні платформи. Китайська фірма ByteDance володіє TikTok, популярною соціальною мережею, яка налічує понад мільярд користувачів, серед яких близько 135 мільйонів американців, або 40 відсотків населення США. І демократи, і республіканці занепокоєні тим, що TikTok може дозволити китайському урядуові видаляти дані про американців і запускати масовані кампанії впливу в інтересах Пекіна – і все це під виглядом надання американським споживачам того, чого вони хочуть. У сучасному світі інформаційної війни зброя насправді не виглядає як зброя.

Оскільки кібератаки можуть відбуватися дуже швидко, й оскільки політики можуть відстежувати важливі події та отримувати оперативну інформацію одним натисканням кнопки, американські розвідувальні служби також мають діяти з новою швидкістю. Звісно, своєчасність завжди була важливою для шпигунства: під час Карибської кризи 1962 року президент США Джон Кеннеді мав 13 днів, щоб проаналізувати розвідувальні дані та обміркувати варіанти своєї політики після того, як фотографії з літака-шпигуна U-2 виявили свєтські ядерні установки на Кубі, а 11 вересня 2001 року президент США Джордж Буш-молодший мав менше 13 годин після нападу на Всесвітній торговий центр, щоб проаналізувати розвіддані й оголосити відповідь. Сьогодні час, який президенти витрачають на аналіз розвідувальних даних перед ухваленням важливих

політичних рішень, може становити до 13 хвилин або навіть 13 секунд.

Але швидкий рух також несе в собі ризики. Потрібен час, щоб перевірити достовірність джерела, залучити експертні знання з різних галузей і розглянути альтернативні пояснення отриманих даних. Без ретельного аналізу розвідданих лідери можуть ухвалювати передчасні або навіть небезпечні рішення. Потенційні наслідки необдуманих дій стали очевидними в грудні 2016 року, коли в новинах повідомили, що колишній міністр оборони Ізраїлю погрожував ядерною атакою на Пакистан, якщо Ісламабад розгорне війська в Сирії. Міністр оборони Пакистану Хаваджа Мухаммад Асіф швидко написав у Твіттері: «Міністерство оборони Ізраїлю погрожує ядерною відплатою, припускаючи роль Пакистану в Сирії проти ДАІШ (Ісламська держава – прим. перекладача). Ізраїль забуває, що Пакистан також є ядерною державою». Але початкова історія була сфабрикована. Асіф поспішив з відповіддю ще до того, як з'ясував правду. Задоволення потреби політиків у швидкості при одночасному ретельному зборі, перевірці й оцінці розвідувальних даних завжди було делікатним балансом, але його стає дедалі важче дотримуватись.

ТРЕБА ЗНАТИ

Розвідувальним службам доводиться мати справу з величезним, а не просто швидким інформаційним середовищем. Обсяг інформації, доступної в Інтернеті, став неймовірно величезним. За даними Всесвітнього економічного форуму, у 2019 році інтернет-користувачі щодня публікували 500 мільйонів твітів, надсилали 294 мільярди електронних листів і завантажували 350 мільйонів фотографій у Facebook. Щосекунди інтернет передає приблизно один петабайт даних – обсяг даних, який людина спожила б після безперервного перегляду фільмів упродовж трьох років.

Американські спецслужби вже збирають значно більше інформації, ніж людина здатна ефективно проаналізувати. У 2018 році розвідувальне співтовариство щодня отримувало зображення високої чіткості обсягом понад три сезони Національної футбольної ліги на кожен датчик, який вони розгорнули у театрі бойових дій. За словами джерела в Міністерстві оборони, у 2020 році один солдат, відряджений на Близький Схід, був настільки стурбований величезним потоком секретних розвідувальних електронних листів, які він отримував, що вирішив їх порахувати. Підсумок: 10 000 електронних листів за 120 днів. І ці цифри, скоріш за все, зростатимуть. За деякими оцінками, обсяг цифрових даних на Землі подвоюється кожні 24 місяці.

І дедалі частіше розвідувальні служби повинні задовольняти щораз ширше коло клієнтів – в тому числі людей, які не командують військами, не мають допуску до секретної інформації і навіть не працюють в уряді. Сьогодні багато важливих осіб, які ухвалюють рішення, живуть в інших країнах, окрім Вашингтона, і роблять відповідний політичний вибір у залах засідань і вітальнях, а не в ситуаційній кімнаті Білого дому. Великі технологічні компанії, такі як Microsoft і Google, потребують розвідданих про кіберзагрози для своїх систем. Більшість об'єктів критичної інфраструктури Сполучених Штатів контролюється приватними фірмами, такими як енергетичні компанії, і їм також потрібна інформація про кіберризики, які можуть вивести з ладу або зруйнувати їхні системи. Виборці потребують розвідданих про те, як іноземні уряди втручаються у вибори і проводять операції з поляризації суспільства. А оскільки кіберзагрози не зупиняються десь на кордоні, безпека США дедалі більше залежить від швидшого і якіснішого обміну розвідданими з союзниками і партнерами.

Щоб задовольнити цей широкий спектр споживачів, американська розвідувальна спільнота створює несекретні продукти і взаємодіє із зовнішнім світом у такій мірі, в якій раніше не робила цього. Агенція національної безпеки, ФБР та інші спецслужби створюють відеоролики для громадськості про іноземні загрози американським виборам. У вересні 2022 року ЦРУ запустило подкаст під назвою «Файли Ленглі», спрямований на демістифікацію агентства та просвітництво громадськості. Національна агенція геопросторової розвідки, яке збирає та аналізує супутникові знімки та інші геопросторові дані, запустило проєкт Tearline – співпрацю з аналітичними центрами, університетами та некомерційними організаціями для створення несекретних звітів про зміну клімату, пересування російських військ, питання прав людини тощо. У 2021 році Агенція національної безпеки (АНБ) почала випускати спільні рекомендації з ФБР та Агенцією кібербезпеки та інфраструктурної безпеки Міністерства внутрішньої безпеки, в яких детально описуються основні кіберзагрози, викриваються суб'єкти, що за ними стоять, і пояснюється, як саме компанії можуть посилити й покращити свою безпеку. У жовтні ці три агенції навіть оприлюднили технічні деталі 20 найбільших кібервразливостей, якими скористався китайський уряд для злому мереж США і союзників, а також детальні інструкції щодо покращення кіберзахисту. Уряд США зараз також видає рекомендації разом з іноземними партнерами з розвідки.

Успіх цієї публічної стратегії був повною мірою продемонстрований в Україні – стратегія допомогла Сполученим Штатам попередити світ про російське вторгнення. Вона допомогла згуртувати Захід для швидкого реагування. І вона продовжує дратувати Москву. Зовсім недавно, після того, як Вашингтон оприлюднив розвіддані, які вказують на те, що вищі російські військові керівники обговорювали застосування тактичної ядерної зброї в Україні, Сі виступив з рідкісним публічним застереженням проти «застосування або погроз застосування ядерної зброї». «Безмежні» відносини Сі з Путіним несподівано все ж таки мали межі.

КРАУД-СЕРФІНГ

На додаток до збільшення кількості клієнтів, технології створили для американських спецслужб ще більшу конкуренцію. Вибух інформації з відкритих джерел в Інтернеті, комерційні супутникові можливості і розвиток ШІ дають можливість різним особам та приватним організаціям збирати, аналізувати й поширювати розвідувальну інформацію.

Наприклад, за останні кілька років розслідувачі-аматори з Bellingcat – волонтерської організації, яка називає себе «розвідувальним агентством для людей» – зробили безліч відкриттів. Bellingcat ідентифікувала російську кілерську групу, яка намагалася вбити колишнього російського шпигуна Сергія Скрипаля у Великій Британії, і виявила прихильників «Ісламської держави» (також відомої як ІДІЛ) в Європі. Також було доведено, що росіяни стоять за збиттям рейсу MH17 «Малайзійських авіаліній» над Україною.

Bellingcat – не єдина ініціатива цивільної розвідки. Коли у 2020 році іранський уряд заявив, що в промисловому ангарі спалахнула невелика пожежа, двоє американських дослідників, які працювали незалежно і використовували лише свої комп'ютери та Інтернет, упродовж кількох го-

Супутниковий знімок пошкоджень у Маріуполі, Україна, жовтень 2022 року. Фабріс Коффріні / AFP / Getty

дин довели, що Тегеран бреше. Як швидко з'ясували Девід Олбрайт і Фабіан Гінц, будівля насправді була цехом зі складання ядерних центрифуг на головному об'єкті зі збагачення урану в Ірані. Пошкодження були настільки значними, що пожежа цілком могла бути спричинена вибухом, що підвищувало ймовірність саботажу. У 2021 році ядерні сищики з Центру досліджень проблем нерозповсюдження Джеймса Мартіна в Каліфорнії використали комерційні супутникові знімки, щоб виявити понад 200 нових шахт для міжконтинентальних балістичних ракет у Китаї – знахідка, яка може свідчити про історичне збільшення ядерного арсеналу Китаю.

Для американських спецслужб цей зростаючий світ розвідданих з відкритих джерел приносить значні нові можливості, але й ризики. З позитивного боку, громадяни-розвідники пропонують більше очей і вух по всьому світу, які сканують події і небезпеки в міру їх виникнення. Мудрість натовпу може бути потужним інструментом, особливо для збирання воєдино крихітних шматочків інформації. Не зв'язані бюрократією, аналітики розвідки з відкритих джерел можуть працювати швидко. А оскільки інформація з відкритих джерел за визначенням розсекречена, нею можна легко ділитися всередині урядових установ і між ними, а також з громадськістю, не розкриваючи конфіденційних джерел і методів.

Але ці особливості мають і недоліки. Розвіддані з відкритих джерел доступні всім і всюди, незалежно від їхніх мотивів, національної лояльності чи можливостей. Громадяни-розвідники не зобов'язані ні перед ким звітувати і ніде не навчаються, і це створює всілякі небезпеки. Аналітиків-волонтерів винагороджують за швидкість (особливо онлайн), але рідко карають за помилки, а це означає, що вони більш схильні до помилок. А межа між мудрістю натовпу і небезпекою натовпу дуже тонка. Після терористичної атаки на Бостонський марафон у 2013 році, в результаті якої загинуло троє людей і було поранено понад 260, користувачі Reddit перейшли до активних дій. Публікуючи теорії про домашніх тварин, непідтверджені розмови на поліцейських сканерах та інші краудсорсингові ласі шматочки інформації, розслідувачі-аматори вказали на двох «підозрюваних», а провідні ЗМІ оприлюднили їхні висновки. Обидва виявилися невинними.

Ці недоліки можуть створити серйозний головний біль для урядів. Коли помилки стають вірусними, розвідувальним службам доводиться витрачати час та ресурси на перевірку роботи інших і запевнення політиків у тому, що початкові оцінки розвідки не мають змінюватися. Точні відкриття з відкритих джерел також можуть спричинити проблеми. Наприклад, можуть загнати політиків у кут, оприлюднивши інформацію, яка, якби її тримали в таємниці, могла б залишити місце для компромісів і витончених виходів з кризових ситуацій. Наприклад, для розв'язання Карибської кризи Кеннеді погодився таємно вивезти американську ядерну зброю з Туреччини, якщо Совєтський Союз вивезе свої ракети з Куби. Якби супутникові знімки були загальнодоступними, Кеннеді, можливо, був би надто стурбований внутрішньополітичною реакцією і не пішов би на цю угоду.

ВІДКРИТІ ВІДНОСИНИ

Керівники американської розвідки знають, що їхній успіх у двадцять першому столітті залежить від адаптації до світу з більшою кількістю загроз, більшою швидкістю, більшим обсягом даних, більшою кількістю клієнтів і більшою кількістю конкурентів. Їхні установи наполегливо працюють над тим, щоб відповісти на ці виклики, впроваджуючи організаційні реформи, програми технологічних інновацій та нові ініціативи для залучення найкращих наукових та інженерних талантів. І вони досягли певних важливих успіхів. Але ці проблеми складно подолати, і наразі зусиллям розвідувального співтовариства притаманний фрагментарний характер.

Темпи прогресу викликають особливе занепокоєння, зважаючи на те, що проблеми добре відомі, ставки високі, а недоліки розвідки назрівали роками. У численних звітах і статтях йдеться про те, що розвідувальні служби не встигають за технологічним розвитком. Ці доповіді вказують на сумну реальність. Вашингтон не може вирішити своїх нинішніх проблем, вносячи поступові зміни в існуючі агенції. Натомість, розвиток розвідувальних можливостей США у XXI столітті вимагає створення чогось нового: спеціальної розвідувальної служби з відкритим кодом, зосередженої на прочісуванні незасекречених даних і розпізнаванні їх значення.

Незважаючи на всі зусилля Вашингтона, в розвідувальному співтоваристві США розвідка з відкритих джерел завжди була «громадянином другого сорту», тому що не має відомства з бюджетом, можливістю найму або місцем за столом переговорів, що б відстоювало її інтереси. Допоки розвідка з відкритих джерел залишатиметься вбудованою в секретні відомства, які понад усе цінують таємну інформацію, вона занепадатиме. Культура секретності й надалі душитиме впровадження передових технічних засобів з комерційного сектору. Агенції намагатимуться залучити й утримати талановитих фахівців, які вкрай необхідні їм для розуміння і використання нових технологій. А зусилля, спрямовані на використання потенціалу збирачів розвідувальної інформації з відкритих джерел та аналітиків поза урядом, не принесуть успіху.

Навіть найкраща розвідка з відкритим кодом має свої межі.

Нова розвідувальна агенція з відкритим кодом принесла б в американську розвідувальну спільноту інновації, а не лише інформацію, створивши сприятливий ґрунт для далекосяжних змін у людському капіталі, впровадженні технологій і співпраці з екосистемою розвідки з відкритим кодом, що зростає. Така агенція стане потужним важелем для залучення робочої сили завтрашнього дня. Оскільки вона має справу з незасекреченою інформацією, агенція

могла б наймати найкращих науковців та інженерів на роботу одразу, не вимагаючи від них місяцями чи роками очікування на отримання допуску до секретної інформації. Розміщення офісів агенцій з відкритим кодом у технологічних центрах, де інженери вже живуть і хочуть залишитися – в таких місцях, як Остін, Сан-Франциско і Сіетл – полегшило б приплив і відтік талантів з уряду. Результатом може стати корпус технічно підкованих чиновників, які будуть ротуватись між державною службою і приватним сектором, діючи як посли між обома світами. Вони збільшили б присутність і престиж розвідувального співтовариства в технологічних колах, а також принесли б безперервний потік свіжих технологічних ідей всередину.

Працюючи з несекретними матеріалами, агенція з відкритим кодом також може допомогти розвідувальному співтовариству краще й швидше впроваджувати нові технології збору та аналізу інформації. (Агенція з відкритим кодом могла б випробовувати нові винаходи і, якщо вони виявляться ефективними, передавати їх агентствам, які працюють з секретною інформацією). Агенція також матиме ідеальну можливість співпрацювати з провідними розвідувальними організаціями з відкритим кодом і приватними особами поза урядом. Такі партнерства могли б допомогти американським спецслужбам передати більшу частину своєї роботи на аутсорсинг відповідальним неурядовим збирачам та аналітикам, звільнивши співробітників розвідки для зосередження своїх можливостей і зусиль зі збору таємної інформації на місіях, які ніхто інший не може виконати.

А таких місій буде ще багато. Зрештою, навіть найкраща розвідка з відкритих джерел має свої межі. Супутникові знімки можуть виявити нові китайські ракетні шахти, але не те, що китайські лідери мають намір з ними робити. Ідентифікувати об'єкти або відстежувати їх переміщення в режимі онлайн важливо, але для генерування інсайту потрібно більше. Секретні методи залишаються унікальним інструментом для розуміння того, що знають, у що вірять і чого прагнуть іноземні лідери. Не існує відкритих джерел, які могли б замінити шпигунів у найближчому оточенні іноземних лідерів або проникнення в систему комунікацій супротивника, щоб дізнатися, що він говорить і пише. Аналітики з доступом до інформації також завжди будуть необхідні для оцінки того, що означають засекречені відкриття, наскільки вони заслуговують на довіру і як узгоджуються з іншими, несекретними висновками.

Але секретних агенцій вже недостатньо. Країна стоїть перед небезпечною новою епохою, що включає в себе конкуренцію великих держав, поновлення війни в Європі, постійні терористичні атаки і швидкозмінні кібератаки. Нові технології є рушійною силою цих загроз і визначають, хто зможе зрозуміти і спроектувати майбутнє. Щоб досягти успіху, розвідувальне співтовариство США має адаптуватися до більш відкритого, технологічного світу.

Емі ЗЕГАРТ

https://www.foreignaffairs.com/
Січень/лютий 2023 року

Переклад з англійської Вікторії О. Романчук


Лауреату премії
імені В'ячеслава Чорновола
за кращу публіцистичну роботу
в галузі журналістики

РОМАНЧУКУ
ОЛЕГУ
КОСТЯНТИНОВИЧУ

за книгу

«НЕ БІЙСЬ. НЕ ЗРАДЖУЙ.
НЕ МОВЧИ»

наказ Державного комітету
телебачення і радіомовлення України
від 8 листопада 2022 року № 118

Голова Держкомтелерадіо ОЛЕГ ПАЛИВАЙКО

Диплом № 27