Хакери і держави

Бен Б'юкенен

ХАКЕРИ І ДЕРЖАВИ

Кібервійни як нові реалії сучасної геополітики

Переклала з англійської
Юлія Каздобіна

«Наш Формат»
Київ · 2024

Зміст

Келлі

Вступ

«Скільки будете платити за кіберзброю ворога?»

Це питання було поставлене онлайн без будь-якої преамбули та ламаною англійською. Воно звучало як жарт, уявний експеримент, або як вкид інтернет-троля в цифровий ефір. Але жоден із цих варіантів не відповідав дійсності.

Це повідомлення від акаунту під назвою theshadowbrokers, що з'явилося у 2016 році, дало початок низці подій, які змусили розвідувальні служби в США, і не лише їх, ще довго здригатися від шоку. Під час річної ескапади хакерське угруповання Shadow Brokers оприлюднювало документи, які викривали діяльність хакерів, що, працюючи на американський уряд, проникають до мереж по всьому світу, аби уповільнювати, чинити перешкоди та обеззброювати свої мішені. Викрадені ними файли продемонстрували, що хакерські атаки були ключовим, хоч і здебільшого секретним інструментом американської політики на міжнародній арені, який США потай використовували як проти ворогів, так і проти друзів[1].

Shadow Brokers розмістили у відкритому доступі не лише документи. Вони виклали набір хакерських інструментів, які накопичило та ревно охороняло Агентство національної безпеки США, або АНБ. Ці інструменти були настільки потужними, що американські хакери прирівняли їх використання до «риболовлі з динамітом». Й от раптом цей «динаміт» став доступний абсолютно всім і безкоштовно[2].

Результат був передбачувано жахливим. Хакери з авторитарних держав та кримінальних угруповань пристосували викладений код для власних руйнівних кібератак. Ці хакерські атаки

вважаються найспустошливішими в історії. Вони завдали збитків на понад 14 мільярдів доларів, інфікували сотні тисяч комп'ютерів і створили перешкоди для бізнесу по всьому світу. Американські спецслужби, які звикли викрадати чужі таємниці та проникати в чужі розвідувальні операції, не знали, звідки було завдано удару. Уряд Сполучених Штатів розпочав масштабне контррозвідувальне розслідування проти Shadow Brokers, яке значно ускладнювалося тим, наскільки ретельно це угруповання приховало свої сліди. І хоча цю інформацію досі не підтверджено, витоки в процесі розслідування вказували на те, що Shadow Brokers мали російське походження. Втрати Америки стали здобутками Росії[3].

Злив даних угрупованням Shadow Brokers і подальші атаки стали кульмінацією очевидної тенденції: протягом останніх двадцяти років цифрова конкуренція на міжнародній арені стає дедалі агресивнішою. Сполучені Штати та їхні союзники більше не можуть як раніше домінувати в цій сфері. Нищівні кібератаки та витоки інформації загострюють запеклу боротьбу між державами. Китайські хакери викрадають американські комерційні таємниці й електронні реєстри споживачів, а російські — проникають до електромереж та втручаються у виборчі процеси своїх супротивників. Навіть країни, що перебувають у міжнародній ізоляції, зокрема Північна Корея та Іран, сьогодні здатні завдати значної шкоди великим міжнародним корпораціям, як-от Sony чи Aramco. І, незважаючи на всі атаки, яких вони зазнали, немає жодних сумнівів, що Сполучені Штати продовжують завдавати ударів у відповідь. Ця книжка розповідає про те, як усі ці події складаються в єдину картину. Її автор синтезує і тлумачить два десятиріччя новітньої історії, демонструючи, як хакери поступово змінили світ.

Хаотичний театр кібероперацій, який описано в цій книжці, зовсім не схожий на те, як його протягом довгого часу уявляли собі дослідники та військові стратеги. Вони завжди очікували, що кібератаки стануть чимось на кшталт ядерної війни: будуть нищівними, але траплятимуться нечасто. Ця ідея вперше постала у свідомості американців завдяки фільму WarGames 1983 року, у якому молодий Метью Бродерік випадково поставив світ на межу ядерного армагеддону, зламавши комп'ютери військових. Президент

Рональд Рейґан подивився фільм наступного дня після його виходу й зажадав від уряду ретельно дослідити припущення, на яких він ґрунтувався[4]. Протягом п'яти президентських термінів, які минули відтоді, нескінченна низка сформованих Вашингтоном «Комісій блакитної стрічки»* розглядала спектр можливостей для нищення із застосуванням цифрових технологій. Дослідники, урядовці та політики малювали у своїх книжках уявні картини виведених з ладу електростанцій і мереж управління повітряним рухом, дефіциту їжі та масової паніки.

І хоча апокаліптичне бачення не перетворилося на реальність, кібератаки стали низькоінтенсивною, але невід'ємною частиною геополітичної конкуренції. Вони відбуваються щодня. Урядові хакери грають у нескінченну гру: шпигунство та обман, атаки й контратаки, дестабілізацію і удари у відповідь. Це новий інструмент державної політики. Він м'якіший, ніж собі уявляли політики й урядовці, але його вплив змінює світ.

Сигнали та формування середовища

Більш конкурентні аспекти поведінки держави на міжнародній арені складаються з двох підходів, які частково перетинаються, але повністю не збігаються: надсилання сигналів та формування середовища. Різниця між цими поняттями є життєво важливою[5]. Якщо порівняти міжнародні відносини з грою в покер із високими ставками, то сигналізувати означає достовірно натякнути, які у вас карти, намагаючись вплинути на те, як інша сторона розіграє свої карти. Натомість формувати середовище — це змінити хід гри на власну користь, підтасувати колоду або вкрасти карту суперника.

У цій книжці я стверджую, що, хоч кіберспроможності і стають дедалі універсальнішими інструментами для формування

* Комісія блакитної стрічки (*англ.* Blue Ribbon commission) — це група висококваліфікованих фахівців, яких призначають для дослідження чи аналізу певної проблеми. Зазвичай такі групи якоюсь мірою незалежні від політичного впливу і не мають владних повноважень. Вони надають висновки або рекомендації, які потім можуть використовувати ті, хто має право ухвалювати рішення. — *Прим. пер.*

геополітичної реальності й отримання переваг, вони вкрай погано підходять для надсилання сигналів про позицію держави в якомусь питанні та про її наміри.

З початку ядерної епохи теорія і практика міжнародних відносин зосереджені на сигналах, які країни надсилають одна одній. І це цілком зрозуміло: найпотужніша зброя людства стала настільки руйнівною, що її можна використовувати лише в найнагальнішому випадку. Канонічна наука періоду Холодної війни пояснювала не те, як перемогти в конфлікті, а те, як його уникнути, водночас диктуючи свої умови[6]. Такі теоретики, як Томас Шеллінґ (який отримав Нобелівську премію з економіки за дослідження теорії ігор), описували, як держава може здобути та зберегти перевагу, не зробивши жодного пострілу. За словами Шеллінґа, ведення зовнішньої політики значною мірою полягає в маніпулюванні спільним ризиком війни, примушуванні супротивника шляхом ретельно прорахованих погроз з метою отримати переваги мирним шляхом.

Військова мобілізація є прикладом ведення зовнішньої політики за допомогою сигналів. Розгортання збройних сил підкреслює бойові спроможності та демонструє противникам рішучість, натякаючи, що будь-яка агресія матиме серйозні наслідки. З цієї причини під час Холодної війни Сполучені Штати регулярно розміщували свої сили в Західній Європі. Оскільки американських військ було і близько недостатньо, щоб зупинити радянське вторгнення, можна було б поставити собі питання, що могли зробити ці солдати. У Шеллінґа була готова відповідь: «Відверто кажучи, вони можуть померти. Вони можуть померти героїчно, драматично і так, що це гарантовано не дозволить зупинити розгортання подій»[7]. Радянське керівництво знало, що жоден президент не зможе стерпіти втрату тисячі американців і не помститися. Військова присутність надавала сигналу від Сполучених Штатів про готовність захищати континент переконливості, яка не викликала жодних сумнівів. Їхня присутність допомогла зберегти мир.

Важливість сигналів знайшла відгук серед урядовців найвищого рівня. Деякі високопоставлені особи, які ухвалюють рішення у сфері зовнішньої політики, вважали себе експертами з політики

Кремля, які здатні інтерпретувати сигнали радянських лідерів і робити висновки щодо найкращої реакції. Президенти та прем'єр-міністри також сигналізували одне одному: найзнаковішими моментами державного управління в Холодній війні були битва волі між Кеннеді і Хрущовим під час Карибської кризи та напружені переговори Рейґана й Горбачова в Рейк'явіку. Автори тисяч книжок з історії надають такому способу ведення зовнішньої політики великого значення[8].

Багато вчених не звертали уваги на те, як потаємні дії непомітно формували глобальне середовище. Ці операції було важко помітити і ще важче досліджувати, але від цього вони не ставали менш важливими. Деякі американські політики від початку стверджували, що агресивні дії, спрямовані на формування середовища, потребують більшої уваги. Відомий дипломат Джордж Кеннан писав у 1948 році, що американські політики надто сліпо дотримуються надміру спрощеного світогляду, у якому часи війни чітко відділені від мирних часів, і вони не в змозі «визнати реалії міжнародних відносин — постійний ритм боротьби, від війни до миру і навпаки»[9]. Кеннан припустив, що неминучий конфлікт між інтересами різних держав призведе до постійного конкурування за переваги, і цей прогноз виявився пророчим.

Обидві наддержави намагалися здобути перевагу в Холодній війні шляхом шпигунства та обману. Радянські військові планувальники багато писали про практику *маскування*, або «маленького маскараду» — різноманітних облудних кампаній, спрямованих на введення в оману політичного та військового керівництва ворога[10]. Хоча супротивник і справді іноді помічав таку діяльність, вона не мала на меті надсилати геополітичні сигнали та спонукати опонента змінити поведінку, погрожуючи завдати шкоди. Це були оперативні та стратегічні прийоми, спрямовані на отримання переваги.

Без маскування Карибська криза з усім її драматизмом і сигналами розгорталася б не так, як ми спостерігали. Доставити ракети на Кубу вдалося шляхом обману. Радянський Союз почав із кодових назв, завдяки яким кожному, хто слухав радіоповідомлення, здавалося, що ракети прямують до Берингового моря. Коли

настав час завантажувати їх на кораблі до Куби, щоб обдурити спостерігачів й унеможливити інфрачервоне фотографування, радянські війська накрили ракети сільськогосподарським обладнанням і металевими листами. Військових на борту кораблів тримали під палубою в задушливій спеці й темряві, і навіть капітани не знали справжнього пункту призначення, поки не вирушили в дорогу. Секретність була настільки всеохопною, що дехто з радянських військових заприсягався, що ніколи більше не покине порт.

Продовжуючи обман, Радянський Союз злив точну інформацію про свою операцію кубинським контрреволюційним силам, що, як припускали радянці, підтримували зв'язок із західною розвідкою. Ці сили та дружні до них газети в Маямі мали заслужену репутацію схильних до перебільшення та неналежної уваги до деталей. Коли величезний хор кубинських голосів повідомив достовірну інформацію про прибуття радянських ракет, ЦРУ відкинуло їхні заяви як перебільшення, вирішивши натомість повірити неодноразовим запереченням із радянського боку. Як наслідок, Сполучені Штати протягом місяців після початку розгортання радянських ракет не усвідомлювали небезпеки й зрозуміли все лише тоді, коли завдяки польотам літаків-розвідників і джерелам на землі було здобуто прямі докази, яких політики не змогли проігнорувати[11].

Коли обман заходить достатньо далеко, він може перерости в саботаж. Наприкінці Холодної війни Радянський Союз почав агресивно шпигувати за американським технологічним виробництвом і ринками, отримуючи тисячі технічних документів і зразків продукції, які потім вивчали радянські інженери. Щойно в ЦРУ збагнули, що відбувається, їм одразу стало зрозуміло, як цим можна скористатися. Його співробітники «згодовували» Радянському Союзу хибні проєкти, які здавалися реальними, але незабаром зазнали б краху. У результаті ЦРУ вдалося встановити неякісні комп'ютерні чипи в радянську техніку, несправні турбіни в радянські газопроводи та багато іншого. Обдурені радянські інженери мимоволі використовували дефективні проєкти хімічних і тракторних заводів. Радянський космічний шатл, який так і не злетів, був однією з версій відхиленого проєкту НАСА. Радянський Союз дізнався про програму ЦРУ лише через багато

років після закінчення Холодної війни — власне, як і хотіли американські диверсанти[12]. Майже завжди залишаючись прихованим від очей, формування середовища також відігравало свою роль.

Як хакери змінюють зовнішню політику

Одним з основних способів, у який уряди країн сьогодні формують геополітичне середовище, є хакерські атаки проти інших держав. Сила та гнучкість хакерів не отримують належної оцінки, особливо з боку тих, хто приділяє увагу лише найпомітнішим атакам або уявній кібервійні, яка стане кінцем цивілізації. Урядові хакери постійно знаходять способи просувати інтереси своїх держав і перешкоджати інтересам своїх супротивників. Як боксер, який перемагає за очками, а не нокаутом, вони можуть бути ефективними без зайвого шуму і кровопролиття.

Кібероперації знову і знову з'являються в головоломному політичному меню сучасних держав. Хакери прослуховують, шпигують, вносять зміни, саботують, зривають, атакують, маніпулюють, втручаються, викривають, крадуть і дестабілізують. Вони руйнують соціальну структуру ворога й розкривають його хакерські можливості. Щоб збагнути, як сьогодні країни ведуть державну політику, потрібно зрозуміти ці операції, які мають на меті формувати середовище, та їхній сукупний стратегічний результат.

З іншого боку, кібероперації погано підходять для надсилання сигналів. Коли держави вдаються до кібероперацій, щоб донести меседж до інших країн, то такі сигнали зазвичай не є достатньо відточеними, надійними та чіткими.

Це не відповідає загальноприйнятим уявленням, які сягають своїм корінням у теорії Холодної війни[13]. Політики й науковці часто уявляють собі кіберспроможності аналогом ядерних, що веде до висновку про важливість сигналів з огляду на потенційно катастрофічні наслідки. Або ж вважають їх аналогом конвенційних озброєнь, які полегшують можливість подавати сигнали завдяки своїй високій видимості. Військовим лідерам кіберспроможності можуть здатися танковими батальйонами: надійними засобами,

які можна розгорнути проти широкого кола цілей і чию потужність легко зрозуміти.

Але ці порівняння з ядерною та конвенційною зброєю вводять в оману. Кіберспроможності не настільки потужні, як ядерна зброя чи навіть більшість звичайних озброєнь. Їм також не притаманна така надійність, здатність до взаємозамінності чи перенаціленння, як у традиційної зброї. Можливо, найбільш прикро те, що спосіб дії кіберінструментів інтуїтивно не зрозумілий. Тимчасом як більшість політиків і науковців усвідомлюють можливості ядерної зброї і танків, спроможності, підводні камені та процеси хакерської діяльності є порівняно непрозорими[14].

Осмислити кібероперації найкраще не через знайомі парадигми, що ґрунтуються на поданні сигналів, а через поняття формування середовища, що закорінене в таких явищах, як шпигунство, саботаж та дестабілізація. Найбільшу вигоду від хакерства отримують держави, які агресивно формують геополітичне середовище, перетворюючи його на таке, що їм більше до вподоби, а не ті, які намагаються натякати, примушувати чи погрожувати[15].

У цій книжці продемонстровано, що держави дедалі інтенсивніше застосовують хакерські атаки в нескінченних спробах здобути перевагу. У кожному розділі ми розглядатимемо окрему мету злами та наведемо один випадок чи цілу кампанію як приклад. У кожному випадку можна простежити багато однакових операційних кроків, навіть якщо кінцеві цілі відрізняються. Розповідаючи про ці тенденції, ми спиратимемося на інтерв'ю з перших вуст, урядові документи, технічний криміналістичний аналіз, «злиті» документи й аналітичні публікації у ЗМІ[16].

Ці джерела чітко демонструють, що протягом останніх двох десятиріч хакерські атаки з боку держав набули розвитку та почастішали. Раніше уряди вдавалися до шпигунських операцій, які майже ніколи не потрапляли в поле зору громадськості. Сполучені Штати та їхні союзники мали вирішальні переваги на цій арені — їх ми розглянемо в частині першій. З часом, як ми продемонструємо в другій частині, держави отримали можливості для прихованого кіберсаботажу, а згодом — і для відкритих кібератак. Згодом державні гравці зрозуміли, як за допомогою кібероперацій

можна досягти ширшого ефекту, без розбору руйнуючи компанії супротивників і дестабілізуючи їхні суспільства. Частина третя розповідає про кілька найбільших хакерських операцій за останні п'ять років, звертаючись до історії Shadow Brokers та інших випадків дестабілізації. Сьогодні кібероперації є невід'ємною частиною міжнародних відносин, і розрив між Сполученими Штатами та іншими країнами значно зменшився.

Оскільки в цій новій царині глобальної взаємодії існує люта конкуренція, усі в інтернеті потрапляють під перехресний вогонь й опиняються в «постійному ритмі боротьби», про який попереджав Кеннан. Ця боротьба не проявляється у відкритих дебатах в Організації Об'єднаних Націй чи навіть на таємних зустрічах міжнародних лідерів. У процесі такої боротьби не буває відкритої військової мобілізації чи військ, які слугують чимось на кшталт мінних розтяжок*. Натомість вона проходить через величезні серверні ферми, випадкові мережі мимовільних учасників, сторонні держави, а також будинки та робочі місця майже повсюдно. Глобальні комунікаційні канали, механізми шифрування, інтернет-компанії та комп'ютери, якими люди користуються щодня, є новою передовою міжнародного протистояння країн. Хай там як, але хакери, які працюють на користь, проти і всередині держав, формують майбутнє світу.

* Автор відсилає до ролі військ США в Європі під час Холодної війни, коли вони були так званим trip wire, тобто доволі слабкою першою лінією оборони, зіткнення з якою призвело б до розгортання набагато більшого угруповання. — *Прим. наук. ред.*