Девід Е. Сенґер

ДОСКОНАЛА ЗБРОЯ

ВІЙНА, САБОТАЖ І СТРАХ У КІБЕРЕПОХУ

Девід Е. Сенґер (нар. 1960 року) — головний кореспондент «Нью-Йорк Таймз» у Вашингтоні. Спеціалізується у царині національної безпеки, зовнішньої політики та інституту американського президентства. За журналістську діяльність відзначений багатьма нагородами, зокрема був учасником двох журналістських команд, що отримали Пулітцерівську премію. Окрім цієї книги, написав ще дві: «Спадкоємність: Міжнародні конфлікти Обами та виклики американському впливу» (2009) та «Конфронтація і замовчування: Таємні війни Обами та несподіване застосування американського впливу» (2012). Читає лекції з державної політики у Школі управління імені Джона Ф. Кеннеді Гарвардського університету, а також є співробітником Центру наук і міжнародних відносин імені Роберта і Рене Белферів при цьому ж університеті. Член Ради з міжнародних відносин і Аспенської стратегічної групи.

Девід Е. Сенґер

ДОСКОНАЛА ЗБРОЯ

ВІЙНА, САБОТАЖ І СТРАХ У КІБЕРЕПОХУ

Переклала з англійської
Вікторія Дєдик

Фахові редактори українського видання
Олександр Дєдик і Олег Фешовець

УДК 070.48(73):[004.7.056-027.542:007](100)"20"
С31

Сенґер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху / пер. з англ. Вікторія Дєдик ; фах. ред. укр. вид. Олександр Дєдик і Олег Фешовець. Львів : Видавництво «Астролябія», 2022. 496 с. (Серія: Бібліотека командира)

Вражаюча оповідь про початки та перебіг застосування кіберзброї, яке кидає виклик балансу сил, що встановився у світі з часу винайдення атомної бомби. Побудована на великому обсязі інсайдерської інформації, вона посвячує читача у малопомітне, але загрозливе для самих основ техногенної цивілізації протистояння у кіберпросторі. Автор веде нас через наради в Ситуаційній кімнаті Білого дому та дискусії в офісах підприємств Кремнієвої долини, через осідки російських, китайських чи північнокорейських хакерів, висвітлює діяльність спецслужб та підрозділів Збройних сил. Ми знайдемо опис кібератак проти ядерних програм Ірану та Північної Кореї, енергетичної мережі України, нафтової компанії Saudi Aramco, корпорації Sony, банківських установ, компанії медичного страхування Anthem тощо і усвідомимо, наскільки вразливі перед цим новим і дуже ефективним видом зброї.

Книжку видано за сприяння Відділу преси, освіти і культури Посольства США в Україні

ISBN 978-617-664-237-4

ЗМІСТ

ПЕРЕДМОВА

Минув рік після вступу на посаду президента США Дональда Дж. Трампа, коли міністр оборони Джим Меттіс дав своєму новому головнокомандувачу приголомшливу пораду[1]. Оскільки інші держави загрожують вразити кіберзброєю американські мережі мобільного зв'язку, електро- й водопостачання, Трампові слід заявити, що він готовий вжити надзвичайних заходів, аби захистити країну. Доцільно заздалегідь попередити кожну державу, яка намагатиметься завдати нищівного удару найважливішій інфраструктурі Америки, що Сполучені Штати можуть навіть на неядерний удар застосувати у відповідь ядерну зброю.

Як зазвичай трапляється у Вашингтоні, про рекомендацію відразу стало відомо загалу[2]. Багато хто визнав ідею божевіллям і нечуваним перебільшенням. За останні роки різні держави десятки разів застосовували кіберзброю одна проти одної. Проте жодна атака не призвела до загибелі людей, принаймні безпосередньо. Ані американські атаки на іранські та північнокорейські оборонні програми; ані північнокорейські — на американські банки, відому голлівудську студію та британську систему охорони здоров'я; ані російські — на Україну, Європу та самі основи американської демократії. Досі щастило, хоча все колись за-

кінчується. Однак навіщо Дональдові Трампу або комусь з його наступників ризикувати перетворенням кібервійни на ядерну?

Як з'ясувалося, вслід за рекомендацією Пентагону з'явилися інші, в яких пропонувалося значно агресивніше застосовувати кіберзброю, і вони потрапляли до рук президента-прихильника суворих методів і принципу «Америка понад усе». Вони засвідчували, як швидко страх перед нищівними кібератаками вийшов з царини наукової фантастики та кінофільмів на зразок «Міцний горішок», — і опинився у фокусі американської оборонної стратегії. 2007 року, трохи більше як десять років тому, про кібератаки навіть не згадували в глобальній «Оцінці загроз», котру спецслужби щороку готують для Конгресу. На чільному місці в списку був тероризм[3], а також інші проблеми, пов'язані з наслідками 11 вересня. Тепер усе змінилося. Декілька років поспіль перелік очолювали різноманітні кіберзагрози: від удару, здатного паралізувати життя міст, до вправних спроб похитнути довіру суспільства до власних інституцій. Від 1949 року, коли Радянський Союз випробував атомну бомбу, оцінка загроз жодного разу не змінювалася настільки швидко. Утім Меттіс, котрий отримав чотири генеральські зірки, виконуючи різноманітні завдання, пов'язані з Середнім Сходом, побоювався, що два десятиліття переслідування «Аль-Каїди» та ІДІЛ по всьому світу відвернули увагу Америки від найстрашніших загроз.

«Не тероризм, а боротьба між великими державами — саме на цьому тепер зосереджена політика національної безпеки США», — зазначив він на початку 2018 року[4]. Американська «перевага в усіх царинах ведення війни», включно з найновішою — «кіберпросто-

ром», — помітно послабилася. Ядерна стратегія, запропонована Трампу, відображала побоювання Пентагону, що кібератаки становлять особливу загрозу, до протидії якій Штати зовсім не готувалися.

Іронія в тому, що США залишаються найбільш засекреченою і наймогутнішою кібердержавою світу, — у цьому пересвідчився Іран, коли його центрифуги вийшли з-під контролю, і це запідозрила й Північна Корея, коли її ракети падали з неба. Однак розрив між державами скорочується. Створити кіберзброю настільки дешево, а приховати так легко, що спокуса стає непереборною. Американські чиновники починають розуміти, що у світі, де майже все (телефони, автомобілі, електропостачання, супутники тощо) поєднане мережею, будь-що можна вивести з ладу або навіть знищити. Сімдесят років Пентагон вважав, що лише держави з ядерною зброєю можуть загрожувати Америці. Тепер ця теза опинилася під сумнівом.

Майже кожний створений у Пентагоні таємний сценарій майбутнього протистояння з Росією та Китаєм або навіть Іраном та Північною Кореєю передбачав, що перший удар супротивника по Сполучених Штатах включатиме численні кібератаки на цивільну інфраструктуру. Вони мали б вивести з ладу електромережі, зупинити потяги, перервати мобільний зв'язок і перевантажити інтернет-мережу. У найгірших випадках ішлося про нестачу їжі та води, а також відмову лікарень приймати пацієнтів. Позбавлені електронних пристроїв, а отже, і зв'язку, американці запанікували б або кинулися один на одного.

Сьогодні Пентагон усе планує під саме такий сценарій, бо й сам, відомо, розробив чимало воєнних пла-

нів, що передбачають схожі кібератаки на супротивника. Сучасна стратегія прагне паралізувати ворога, щоб виграти війну ще до першого пострілу. За останні роки до загалу пробилися певні уявлення про те, що може трапитися: почасти завдяки Едварду Дж. Сноудену, почасти завдяки таємничій групі Shadow Brokers[5], яку підозрюють у зв'язках з російською розвідкою і яка роздобула терабайти інформації про те, якими засобами Агентство національної безпеки (АНБ)[6] діставало несанкціонований доступ до комп'ютерних мереж інших країн. Незабаром цю викрадену кіберзброю застосували проти Америки та її союзників, зокрема в атаках з такими дивними назвами, як WannaCry[7], про котрі щотижня довідуємося з заголовків газет.

Утім засекреченість довкола всіх цих програм не дає вести відкритий суспільний діалог про доцільність її застосування та ризики, пов'язані з втратою контролю над нею. Мовчанка влади про нову американську кіберзброю та її застосування — це разючий контраст із поведінкою влади в перші декади ядерної доби. Жахливі сцени руйнувань Хіросіми та Нагасакі не лише залишили відбиток у національній ментальності, але й наочно засвідчили нищівний потенціал Америки, а отже, й Росії та Китаю. Тоді певна інформація також залишалася секретною, а зокрема про те, як створюють ядерну зброю, де її зберігають і хто уповноважений віддати наказ про її застосування. Проте в країні десятиліттями тривала політична дискусія, коли доцільно погрожувати застосуванням бомб, а коли цього робити не слід. Урешті ця суперечка закінчилася зовсім не тим, з чого розпочалася. У 1950-х роках у США вряди-годи порушували питання про мож-

ливе застосування ядерної зброї з метою закінчити війну в Кореї (1950–1953), але вже в 1980-х країна дійшла до консенсусу про застосування ядерної зброї лише тоді, коли на кону буде виживання нації.

Дотепер таких дискусій про застосування кіберзброї не було, хоча з кожним роком її нищівна сила стає дедалі очевиднішою. Зброя залишається невидимою, її використання можна заперечити, а наслідки атаки складно передбачити. Звиклі зберігати таємниці, розвідники та військовики відмовляються обговорювати масштаби американського кіберарсеналу, побоюючись втратити навіть незначну перевагу над супротивниками, яку ще мають.

З того всього Сполучені Штати використовують цю надзвичайно могутню зброю здебільшого таємно за тієї чи іншої потреби і ще до того, як ми встигнемо цілковито усвідомити наслідки. Коли зброю застосовують американці, у США це називають «використанням комп'ютерних мереж», а коли мішенню стають громадяни Америки, йдеться вже про «кібератаки». Цим терміном позначають усе: від виведення з ладу електромережі до фальсифікації результатів виборів, або ж ту тривожну мить, коли в електронній поштовій скриньці вкотре опиняється лист, у якому йдеться, що хтось — може, злочинці, а може, китайці — вдруге або втретє заволодів нашими кредитками, номерами соціального страхування чи медичними картками.

Під час Холодної війни очільники держав усвідомлювали, що ядерна зброя докорінно змінила динаміку національної безпеки, хоча їхня реакція на загрозу могла бути різною. Натомість у добу цифрових конфліктів

мало хто розуміє, як ця новітня революція змінює велику державу. Під час бурхливої президентської кампанії 2016 року Трамп, даючи інтерв'ю, заявив мені, що американські «кібертехнології застаріли»[8]. Він проігнорував факт, якщо взагалі про нього знав, що США та Ізраїль застосували проти Ірану найсучаснішу кіберзброю. Та ще більше непокоїло те, що він явно майже не розумів динаміки кіберконфліктів, того виснажливого щоденного протистояння, яке надто нагадує війну й стало новою нормою сьогодення. Його відмова визнати загрозливе втручання Росії у вибори 2016 року через побоювання підважити свою політичну легітимність лише загострює проблему формулювання державної стратегії. Ця проблема вийшла далеко за межі Білого дому, зайнятого адміністрацією Трампа. Слухання в Конгресі тривають уже десяток років, проте досі немає єдиного погляду на те, чи вважати кібератаки актом війни, терористичним актом, звичайним шпигунством або кібервандалізмом. Технологічний розвиток значно випереджає здатність політиків (і громадян, котрі в умовах щоденної боротьби в кіберпросторі перетворюються на її випадкових жертв) зрозуміти, що власне відбувається, не кажучи вже про те, щоб створити відповідну національну стратегію. Що гірше, коли Росія використала соціальні мережі з метою посилити поляризацію суспільства на виборах 2016 року, ворожнеча між технологічними компаніями та урядом США, розпалена викриттями Сноудена чотири роки тому, лише посилилась. Кремнієва долина та Вашингтон перетворилися на розлучене подружжя, роз'їхалися на протилежні береги й обмінюються дошкульними текстовими повідомленнями.

Трамп без будь-яких обговорень дослухався рекомендації Меттіса про ядерну зброю. Тим часом Пентагон, вловивши бажання Трампа продемонструвати нездоланну міць Америки в кіберпросторі та в інших царинах, опублікував нову стратегію, що передбачала настання доби постійних кіберконфліктів низької інтенсивності. Згідно з нею, нововишколені американські кібервояки щодня пробиратимуться далеко в тил ворога, атакуючи сервери інших держав, перш ніж ті становитимуть загрозу для Сполучених Штатів. Задум спирався на класичний принцип випередження, достосований до доби інформаційних технологій, а саме: «Зупинити атаки, перш ніж вони прорвуть кібероборону та вразять Збройні сили». Також пропонувалося, щоб президент більше не мусив погоджувати кожну кібератаку, як не погоджує звичайних ударів з безпілотників.

Зважаючи на безлад, що панував у Білому домі в часи адміністрації Трампа, годі було зрозуміти, як і на яких засадах застосовуватимуть цю зброю. Та зненацька ми знову відчули ґрунт під ногами.

Кіберконфлікти залишаються в сірій зоні між війною та миром. Це непевне становище, яке, здається, от-от вийде з-під контролю. Інтенсивність атак зростає, й наша вразливість щодня стає дедалі очевиднішою: на початку 2018 року федеральний уряд попередив енергокомпанії, що російські хакери «закладали» шкідливі програми в ядерні електростанції та електромережі країни, а через декілька тижнів додав, що хакери під'єднуються до маршрутизаторів мереж невеликих підприємств і навіть приватних будинків. У попередні

роки з'являлася схожа інформація про діяльність іранських хакерів у мережах фінансових установ і про китайських хакерів, що викачували мільйони файлів з детальними даними про особисте життя американців, щоб отримати службовий доступ до державних таємниць. Пошук належної й ефективної відповіді загнав у безвихідь уже трьох американських президентів. Становище ускладнюється тією обставиною, що потужність американських кібератак настільки перевищує можливості оборони, що урядовці побоюються завдавати ударів у відповідь.

«У цьому полягала проблема з росіянами», — зізнався мені Джеймс Клеппер, директор Національної розвідки[9] в адміністрації президента Обами, якось під вечір узимку в одному кафе неподалік від штаб-квартири Центрального розвідувального управління (ЦРУ)[10] в Макліні (штат Вірджинія). Було чимало способів відплатити Путіну: відключити Росію від міжнародної фінансової системи, розкрити зв'язки російського президента з олігархами або зробити так, щоб певна частина грошей, які він переховує по цілому світу, просто зникла.

Утім, як зазначив Клеппер, «щоразу, коли хтось пропонує спосіб відплатити Путінові за його втручання у вибори, хтось інший втручається зі словами: "А що далі? А якщо він отримає доступ до системи голосування?"».

Клеппер зачепив саму суть однієї з загадок кіберборої. Сполучені Штати не можуть винайти спосіб протистояти російським атакам, не ризикуючи наразитися на ескалацію конфлікту. Інколи здається, що доведеться лише безпорадно скласти руки. Втручання

Росії у вибори — це новий виклик, бо ж ідеться про напад, що межує з війною. Великі та малі держави поступово зрозуміли, якою має бути ідеальна цифрова зброя. Вона настільки ж ефективна, наскільки й невидима. Супротивник не може точно визначити, звідки його атаковано, тож і вдарити у відповідь не здатен. І ми намагаємося вигадати найкращий спосіб стримування. Чи слід залякати ворога надпотужним контрударом? Можливо, вдатися до нецифрових засобів: від економічних санкцій до застосування ядерної зброї? Або настільки зміцнити оборону (хоча для цього потрібні десятиліття), щоб вороги переконалися у марноті власних зусиль?

Звісно, вашингтонським політикам чи не найперше хотілося б порівняти нову проблему з чимось добре відомим, а саме з захистом від ядерної зброї. Однак це хибне порівняння, і, як зазначив кіберексперт Джеймс Люїс, така аналогія лише перешкоджала правильному розумінню ролі цифрових технологій у повсякденних геополітичних конфліктах.

Ядерну зброю розробили суто для боротьби та здобуття абсолютної перемоги. «Взаємно гарантоване знищення» стримувало від ядерних ударів, позаяк обидві сторони усвідомлювали, що можуть бути зруйновані вщент. Натомість кіберзброя має найрізноманітніші градації: від надзвичайно нищівної до психологічно-маніпулятивної.

Донедавна американці були зосереджені на найбільш нищівних видах кіберзброї — якими можна вимкнути електропостачання усієї країни або втрутитися в систему управління і контролю ядерного арсеналу. Це ризиковано, але це сценарій крайності, від

якої, мабуть, найлегше захиститися. Значно частіше трапляється буденне застосування кіберзброї проти цивільних об'єктів з цілком певною метою: зупинити роботу нафтохімічного заводу в Саудівській Аравії, влаштувати аварію на сталеливарному заводі у Німеччині, вивести з ладу комп'ютерну мережу міської влади в Атланті чи Києві або погрожувати фальсифікацією виборів у Сполучених Штатах, Франції чи Німеччині. Таку «полегшену» зброю застосовують щодня не для того, щоб знищити супротивника, а щоб зірвати його плани, сповільнити його і підірвати довіру до його інституцій, розлютити або спантеличити його громадян. І тут майже ніколи не переступається межу, за якою розплата була б неминуча.

Роб Джойс, «кіберцар» Трампа, за перші п'ятнадцять місяців його президентства і перший на посаді, хто керував американськими наступальними кіберопераціями, наприкінці 2017 року розповів, чому США особливо вразливі до таких атак і чому найближчим часом ця вразливість нікуди не зникне.

«Структура суспільства значною мірою тримається на комп'ютерних технологіях[11], — сказав Джойс, який багато років очолював елітний підрозділ АНБ з оперативного й несанкціонованого втручання в комп'ютерні мережі інших країн[12]. — Ми далі все оцифровуємо; тримаємо наш капітал і цінності, проводимо операції й зберігаємо таємниці в цьому ж кіберпросторі». Словом, ми витворюємо нові вразливі місця швидше, ніж позбуваємося старих.

В історії людства рідко бувало, щоб нову зброю впроваджували так швидко і так багато держав, видозмінюючи її під виконання різноманітних завдань і

зміцнюючи власне становище у світі, але не вдаючись безпосередньо до війни. Серед тих, що пристосувалися найшвидше, бачимо путінську Росію, яку варто визнати майстром цього мистецтва, хоча й не єдиною, що його практикує. Москва показала світові, як працює гібридна війна[13]. Її стратегія — це зовсім не державна таємниця: російський генерал Валерій Герасімов описав цю стратегію широкому загалу, а відтак посприяв її реалізації в Україні — в державі, що стала майданчиком для випробування тих технік, які Росія згодом застосувала проти Сполучених Штатів та їхніх союзників. У доктрині Герасімова поєднано старе й нове: сталінська пропаганда, посилена можливостями твітеру і фейсбуку, а за всім тим стоїть груба сила.

Як стане зрозуміло з подальшого викладу, чимало офіційних осіб у США та в інших країнах бачили всі ознаки того, що головні вороги обирають новий вектор атаки. Утім, Сполучені Штати надто вже повільно пристосовувалися до нових реалій. Ми знаємо, що вчинили росіяни в Естонії та Грузії десять років тому, вперше застосувавши кібератаки з метою паралізувати або спантеличити супротивника. Ми бачили, як вони згодом діяли в Україні та Європі, випробовуючи кіберзброю для організації масових заворушень і «м'якого» впливу. Та нам забракло уяви, аби повірити, що росіяни наважаться перестрибнути Атлантику й застосувати ті самі методи до виборів у США. Тож нам, як і українцям, знадобилися місяці, ба навіть роки, аби зрозуміти, що нас спіткало.

Що гірше, коли ми нарешті все зрозуміли, то виявилося, що військові та розвідувальні інституції, що

так пишалися здатністю передбачити будь-яку надзвичайну ситуацію, не були готові до відповіді. На початку 2018 року, коли Комітет Збройних сил Сенату США прагнув дізнатися, як Агентство національної безпеки та Кіберкомандування США[14] реагують на неприховані випадки застосування кіберзброї проти інституцій американської демократії, адмірал Майкл С. Роджерс, термін перебування якого на посаді керівника обох організацій добігав кінця, визнав, що ані президент Обама, ані президент Трамп не уповноважили його давати відповідь.

Роджерс стверджував, що Путін «явно зрозумів, що йому ніщо не загрожує, а тому "можна продовжувати цю справу"»[15]. Такого висновку дійшли не лише в Росії. Справді, чимало наших супротивників використовували кіберзброю якраз через переконаність, що так можна зашкодити Сполученим Штатам, не накликавши військового удару у відповідь. Північна Корея майже безкарно атакувала студію Sony та грабувала центральні банки. А Китай цілком безкарно викрав особисту інформацію майже 21 мільйона американців.

Наші вороги в усьому світі отримали виразне послання: кіберзброя в усіх найрізноманітніших формах створена спеціально, щоб вражати слабкі місця Америки. А оскільки після неї рідко коли лишаються руїни в диму, то Вашингтон досі не знає, як відповідати на такі атаки, хіба на найбільші і найвідвертіші з них.

Розпочинаючи свою діяльність 2014 року, Роджерс розповів мені, що його найважливішим пріоритетом було «визначити, скільки коштують» Штатам наслідки кібератак. «Якщо ми не передамаємо цю динаміку, — додав він, — це триватиме далі». Ро-

джерс пішов з посади 2018 року, коли країна постала перед значно більшими проблемами, ніж на початку його каденції.

Наприкінці липня 1909 року Вілбер та Орвіл Райти прибули до Вашингтона продемонструвати свій «військовий літак»[16]. На збережених зернистих світлинах видно, як вашингтонські «болотяні тварі»[17] прямують на шоу по мостах через ріку Потомак. Прибув навіть президент Вільям Говард Тафт, хоча брати Райти не збиралися ризикувати запросити його на борт.

Не дивно, що в Збройних силах не приховували захвату потенціалом приголомшливого винаходу. Генерали уявляли, як пролітають над позиціями ворога, обходять з флангів зустрічні сили, а тоді відправляють кавалерію розправитися з ними. І аж через три роки один з нових розвідувальних літаків здогадалися озброїти кулеметом. Це стало початком стрімкого прогресу, але й через це все полетіло шкереберть. Техніка, яку спершу вважали революційним транспортним засобом, раптово і докорінно змінила саму війну. 1913 року в США виготовили 14 військових літаків[18]. Минуло п'ять років, і на бойовищах Першої світової війни їх налічувалося вже 14 тисяч.

Брати Райти навіть уявити не могли, як саме використовуватимуть їхній винахід. «Червоний барон»[19] збив перший французький літак у квітні 1916 року над Верденом. Повітряні бої спершу траплялися щомісяця, згодом — щотижня, а відтак — щодня. Під час Другої світової війни японські «Зеро»[20] бомбардували Перл-Гарбор[21], а камікадзе намагалися атакувати есмінець мого батька в Тихому океані (вони двічі схиби-

ли). І через 36 років після перших польотів Орвіла перед президентом Тафтом вже «Енола Ґей»[22] зробив свій віраж над Хіросімою і назавжди змінив характер війни, поєднавши можливості повітряних сил з руйнівною силою новітньої зброї.

Наш сьогоднішній кіберсвіт дещо нагадує часи Першої світової війни. Десять років тому лише три-чотири країни володіли ефективною кіберзброєю; зараз таких уже понад тридцять. Крива обсягу виробництва кіберзброї за останні десять років загалом нагадує траєкторію злету бойового літака. Нову зброю вже застосовували багато разів, навіть якщо результати були неоднозначні. Згідно з найточнішими оцінками, на момент написання цієї книги, а це початок 2018 року, за минуле десятиліття відбулося понад двісті кібератак міждержавного рівня. І це лише ті, що набули певного розголосу.

Як і напередодні Першої світової війни, держави, немов зазирнувши у майбутнє, почали швидко озброюватися. США були одними з перших — створили так звані «Сили кібероперацій»[23]. Наприкінці 2017 року діяло 133 команди, у яких налічувалося понад 6000 військовослужбовців. У цій книзі здебільшого йтиметься про «сім сестер» кіберконфлікту — США, Росію, Китай, Велику Британію, Іран, Ізраїль і Північну Корею. Проте інші країни — від В'єтнаму до Мексики — також їх наслідують. Чимало з них розпочали випробування кіберзброї всередині держави проти дисидентів та політичних конкурентів. Проте сучасні збройні сили будь-якої країни не можуть функціонувати без кіберарсеналу так само, як після 1918 року годі було уявити військо без літаків. Сьогодні, як і то-

ді, неможливо точно передбачити, наскільки цей винахід змінить застосування державних сил.

1957 року, коли світ уже наблизився до межі ядерної війни, молодий дослідник з Гарварда на ім'я Генрі Кіссінджер видав книгу «Ядерна зброя та зовнішня політика»[24]. У ній він намагався пояснити стурбованому загалові американців, як понад десять років тому перше застосування потужної нової зброї, наслідки якого ще не до кінця розуміли, докорінно змінило світ.

Не обов'язково погоджуватися з висновками Кіссінджера, особливо з припущенням, що США могли б вести й виграти обмежену ядерну війну, проте годі належно не оцінити його розуміння, що після винаходу цієї бомби змінилося геть усе. «Революцію неможливо приборкати, допоки її не зрозумієш, — писав він. — Завжди є спокуса втиснути її в рамки усталеної доктрини, тобто заперечити, що маємо справу саме з революцією». Кіссінджер казав, що надійшов час «спробувати оцінити технологічну революцію, свідками якої ми стали за останнє десятиліття», і збагнути, наскільки вона змінила все те, що ми начебто розуміли. Уже через п'ять років після того спалахнула Карибська криза[25], під час якої Холодна війна ледь не перетворилася на ядерну, а світ міг бути знищений унаслідок помилкових розрахунків. Наслідком кризи були перші спроби контролювати розповсюдження ядерної зброї, аж поки вона сама не вирішила нашу долю.

Загалом більшість аналогій між світами ядерної й кіберзброї надто натягнуті, проте одна з них точно доречна. Ми всі живемо в страху, що нашу залежність від цифрових технологій обернуть проти нас інші держа-

ви, які за останнє десятиліття винайшли нові способи продовжити давнє протистояння. Ми вже знаємо, що перед кіберзброєю, як і перед ядерною, усі рівні. І в нас є всі підстави непокоїтися, що через кілька років ця зброя вкупі зі штучним інтелектом діятиме настільки швидко, що люди не встигнуть ні усвідомити загрози, ні запобігти їй — тож атаки відбудуться й призведуть до ескалації конфлікту. Ми далі відшукуємо нові технологічні рішення, удосконалюючи брандмауери, паролі та системи виявлення, немов намагаємося вибудувати еквівалент французької «лінії Мажино»[26]. Вороги ж діють, як німці 1940 року, вишукуючи можливість обійти укріплення.

Великі держави та колишні великі держави, як-от Китай і Росія, уже мріють про нову еру, коли такий захист уже не становитиме перешкоди, а вони кіберзасобами переможуть у конфлікті ще до того, як жертви його усвідомлять. У квантових комп'ютерах вони вбачають можливість здолати будь-які методи шифрування й отримати доступ до системи командування американським ядерним арсеналом та контролю за ним. Вони цікавляться ботами, які могли б не лише вдавати справжніх людей у твітері, а й виводити з ладу супутники раннього попередження. Американські вчені та інженери — від штаб-квартири Агентства національної безпеки у Форт-Міді до державних лабораторій, де колись створили ядерну бомбу, — намагаються бути хоча б на крок попереду. Труднощі полягають у тому, як захистити цивільні об'єкти, які уряд США не контролює, а також приватні мережі компаній та громадян Америки, які навіть задля їхнього захисту не схильні дозволити владі в них нишпорити.

Поки що в цих дебатах бракує серйозних спроб знайти геополітичне розв'язання проблеми, яке поєднувалося б з технологічним. Готуючи репортажі про національну безпеку для часопису «Нью-Йорк Таймз», я завжди дивувався, як мало є спроб визначити велику стратегію кіберепохи, хоча в добу ядерної зброї це було звичним явищем. Почасти причина в тому, що тепер значно більше самих гравців у порівнянні з часами Холодної війни. Певну роль відіграє й та обставина, що Сполучені Штати надто розділені політично. Також слід зважати, що кіберзброю створив апарат розвідки США, таємна за визначенням структура, яка завжди схильна все надмірно засекречувати й часто стверджує, що публічне обговорення проблем контролю за зброєю зашкодить ефективності її застосування.

Певною мірою така секретність виправдана. Втім вразливість комп'ютерів і мереж, що дозволили Сполученим Штатам сповільнити ядерний прогрес Ірану, зазирнути за лаштунки Північної Кореї й відстежити роль Росії у виборах 2016 року, — все це явище тимчасове. Та за все треба платити, і США вже почали. Неможливо домовлятися про норми поведінки в кіберпросторі, допоки ми не погодимося визнати власні можливості й діяти в певних визначених рамках. Зокрема, Сполучені Штати ніколи не погодяться заборонити кібершпигунство. Вони також не пристануть на зобов'язання не «закладати» шкідливі програми у комп'ютерні мережі інших країн, адже без них США не зможуть вивести ці мережі з ладу, якщо така потреба виникне. Водночас ми жахаємося, коли виявляємо російські чи китайські закладки в наших електромережах чи мережах мобільного зв'язку.

«Гадаю, найбільша перешкода — це неспроможність уряду США зазирнути у дзеркало», — каже Джек Ґолдсміт, професор права Гарвардського університету, який служив у Департаменті юстиції за президентства Джорджа В. Буша.

Одного літнього дня 2017 року я поїхав у Коннектикут, аби побачитися з Кіссінджером, якому тоді виповнилося 94 роки, і попросив порівняти сьогодення з добре відомими йому часами Холодної війни. Він відповів: «Сьогодні все набагато складніше. А в довшій перспективі може стати ще й набагато небезпечніше».

У цій книзі розказано, як складність і небезпека уже змінюють наш світ, і досліджено, чи зможемо ми контролювати власний винахід.

Історія кібервійни, яку написав Сенґер, одна з найвичерпніших і найдоступніших на сьогодні. Його книга — не просто історична праця і першоджерело. У ній також порушено низку гострих питань, зокрема й про те, що ми не готові до можливої кібератаки.

БЮЛЕТЕНЬ УЧЕНИХ-АТОМНИКІВ

У цій енциклопедичній праці кореспондент «Таймзу» відстежує стрімке нарощення технічного потенціалу кібервійни і попереджає, що ідеї про те, як його контролювати, лишень починають з'являтися.

НЬЮ-ЙОРК ТАЙМЗ БУК РЕВЮ

З глибокою обізнаністю і граничною ясністю, що характерно для всього, що він написав за довгі роки, Сенґер розповідає, як підступно і небезпечно розвивається кіберпростір, стаючи глобальним полем бою XXI століття. Читач закінчує цю книгу, повністю розуміючи, чому кібервійна так швидко вийшла на перше місце в офіційному списку загроз національній безпеці.

ВАШИНГТОН ПОСТ

https://www.astrolabium.com.ua

АСТРОЛЯБІЯ

ISBN 978-617-664-237-4

9 786176 642374

ЗАХИСНА ГОЛОГРАМА