Кібервійна росії проти України: життєво важливі уроки для Заходу

Незабаром мине рік від початку повномасштабного вторгнення в Україну, організованого володимиром путіним; проте напад фактично розпочався більше ніж за місяць до масового перетину кордону колонами російських танків 24 лютого 2022 року. В середині січня росія провела масштабну кібератаку проти понад 20 українських урядових установ, намагаючись знизити здатність країни протистояти майбутньому воєнному нападу з боку москви.

Атака від 14 січня не змогла завдати критичного удару по українській цифровій інфраструктурі, однак вона продемонструвала, що кіберфронт відіграватиме важливу роль у майбутній війні. За рік кібератаки вже неможливо відокремити від інших аспектів російської агресії. Зараз українські посадовці навіть намагаються переконати Міжнародний кримінальний суд (МКС) у Гаазі провести розслідування стосовно того, чи можуть російські кібератаки вважатися воєнними злочинами.

Під час аналізу російської кібервоєнної тактики, що використовувалася в Україні минулого року, були виявлені чіткі зв'язки між звичайними та кібероперaціями. Міжнародна спільнота може засвоїти цінні уроки з досвіду України у сфері протистояння таким кіберзагрозам, що надає можливість зазирнути в майбутнє, де війни вестимуть як за допомогою звичайних засобів, так і — все частіше — у безмежному кіберпросторі.

Російська кібератака в січні 2022 року не була безпрецедентним випадком. Навпаки, від початку російської агресії та захоплення Криму навесні 2014 року Україна постійно була мішенню кібератак. За рік в Україні була здійснена перша серйозна кібератака на національну енергетичну систему. Влітку 2017 року, на думку багатьох коментаторів, в Україні відбулася найбільша кібератака в історії. Ці резонансні інциденти супроводжувалися безперервним потоком дрібніших, проте все одно серйозних атак.

Від початку повномасштабного російського вторгнення минулого року перед кібератаками або одночасно з ними часто проводили звичайні воєнні операції. Наприклад, перед початком кампанії повітряних ударів по українській цивільній інфраструктурі українські енергетичні компанії місяцями зазнавали все сильніших кібератак.

Така тактика є привабливим варіантом для росії в її неоголошеній війні проти Заходу. Тоді як більш традиційні акти агресії можуть спровокувати рішучу відповідь, кібератаки функціонують у «сірій зоні» війни, що робить їх зручними для кремля, який намагається спричинити якомога більший хаос у Європі та Північній Америці та при цьому не нарватися на прямий воєнний удар у відповідь. Можливо, росія не готова використовувати проти Заходу танки та ракети, однак москва може без вагань застосувати кібервоєнну тактику, відпрацьовану в Україні.

На додаток до підриву та блокування роботи державних органів і критичної інфраструктури, російські кібератаки в Україні також спрямовані на маніпулювання громадською думкою та розповсюдження шкідливого програмного забезпечення через зламані облікові записи електронної пошти. Українські органи влади дійшли висновку, що для своєчасної протидії атакам надзвичайно важливо координувати зусилля із громадськістю та обмінюватися інформацією із широким колом зацікавлених сторін.

Наслідки кібератак проти України вже відчуваються далеко за її межами. Одна атака на систему супутникового зв'язку, яка використовувалася ЗСУ на початкових етапах російського вторгнення, спричинила серйозне порушення, що вплинуло на тисячі користувачів у

Європейському Союзі, включно з фізичними особами та компаніями. З огляду на безмежний характер цифрового середовища, подібних сценаріїв навряд чи вдасться уникнути, враховуючи подальше нарощування кібервоєнних потужностей.

З точки зору росії, особлива привабливість кібервійни полягає в тому, що вона вимагає менше людських ресурсів, ніж звичайні воєнні операції. Тоді як москва щосили намагається знайти достатньо людей і військового обладнання, щоб компенсувати розгромні втрати в Україні протягом першого року вторгнення, у кремля не виникне проблем із пошуком достатньої кількості людей із технічними навичками для кібернаступу на широке коло країн, на додаток до України.

У розпорядженні росії перебуває значний резерв потенційних новобранців, включно з добровольцями, мотивованими кремлівською пропагандою, що позиціонує вторгнення в Україну як цивілізаційну боротьбу проти Заходу. Такі мережі вже здійснили численні окремі атаки на західні цілі.

Водночас, як свідчить досвід України за минулий рік, підготовка до кібератак вимагає часу та знань. Це пояснює, чому після початкового провалу стратегії російського вторгнення навесні 2022 року кібернаступів високої складності поменшало. росія просто не очікувала, що Україна витримає першу потужну хвилю кібератак, і не мала чітких планів на цей випадок.

Україна вже провела масштабні дослідження способів ведення російської кібервійни. Завдяки цьому потужному досвіду ми все більше віримо в нашу здатність протистояти подальшим атакам. Однак, щоб максимізувати оборонні можливості, усі країни Заходу повинні співпрацювати між собою. І це треба робити вже зараз. Режим путіна відчайдушно шукає способи перехопити ініціативу в Україні та може планувати нові зухвалі наступи на кіберфронті. Навіть у разі поразки росії це всього лише питання часу, коли інші авторитарні режими розпочнуть кібервійни проти Заходу.

Демократичний світ повинен невідкладно адаптувати свої воєнні доктрини для боротьби із загрозами в кіберпросторі. Кібератаки мають сприйматися так само, як звичайна воєнна агресія, і мають викликати таку саму безкомпромісну реакцію. Необхідно докласти зусиль, щоб перешкодити доступу авторитарних режимів до технологій, які потім можуть використовуватися як зброя проти Заходу.

Російське вторгнення в Україну в багатьох аспектах є першою і, на жаль, не останньою світовою кібервійною. В інтересах глобальної безпеки росія має зазнати поразки як на кіберфронті, так і на полі бою в Україні.

Юрій Щиголь, голова Державної служби спеціального зв'язку і захисту інформації України