***Що таке кіберпростір?***

**Кіберпростір** слід розглядати як певну віртуальну структуру, яка сформувалася через поступове з’єднання комп’ютерних пристроїв, що мають вихід до всесвітньої павутини.

Сьогодні елементами кіберпростору є не лише персональні комп’ютери чи смартфони, але й **об’єкти критичної інфраструктури держави** – електромережі, енергетичні, транспортні й банківські системи. Усі вони вразливі до зовнішніх атак, оскільки мають підключення до Інтернету. Причому в міру все більш широкого застосування інформаційно-комунікаційних технологій у різних секторах економіки (диджиталізації) вразливості лише зростають.

Таким чином, **кібербезпека** стає одним із стратегічних пріоритетів внутрішньої політики держав, а використання кіберпотужностей – новим інструментом реалізації військових та зовнішньополітичних цілей.

Ще донедавна кібербезпека не розглядалася як складова міждержавного протистояння. Як правило, зловмисники в кіберпросторі займалися шахрайством та злочинними кібератаками з метою особистого збагачення. Однак вже незабаром держави віддали належне нерозкритому потенціалу кіберпотужностей, взявши на озброєння передові технології проведення шпіонажу, хакерських та інформаційних атак.

***Новий засіб для старих цілей***

Вперше держави випробували кіберпотужності у військовій сфері. Зокрема у книзі «Темна територія: Секретна історія кібервійни», американський письменник та журналіст Фред Каплан стверджує, що під час війни у Перській затоці 1990-1991 рр. Сполучені Штати порушили систему командування й контролю військами Іраку через використання секретного супутника. На практиці співробітники Агентства національної безпеки США (NSA) прослуховували телефонні розмови Саддама Хусейна з генералами іракської армії, що давало змогу розкрити позиції ворога.

Наприкінці 1990-х років на Балканському півострові кіберпотужності використовувалися як інструмент м’якого придушення протестів проти присутності Сил стабілізації НАТО (SFOR). Річ у тім, що сербське населення Боснії і Герцеговини, яке вимагало виведення миротворців, координувало повстання через канали місцевого телебачення, які здебільшого отримували сигнал з п’яти телевізійних вишок. Американські військові у складі сил НАТО вирішили встановити на ці вишки спеціальні пристрої, які дозволяли дистанційно вимикати трансляцію перед кожним наступним закликом до протесту. Згодом продюсери з Голлівуду надали контрольованим телестанціям матеріали для трансляції серіалу «Рятівники Малібу» (Baywatch), у результаті чого частина протестувальників надала перевагу сонячним пляжам Каліфорнії перед знедоленими вулицями Боснії і Герцеговини.

Проте руйнівний потенціал кіберпотужностей був повністю розкритий лише у 2006 році під час операції «Олімпійські ігри», яку влаштували американські та ізраїльські військові задля ліквідації ядерної програми Ірану. Оскільки один із іранських ядерних реакторів знаходився на дистанційному комп’ютерному керуванні, це дозволило працівникам Агенства національної безпеки США втрутитися в комп’ютерну систему керування реактором через вірус Stuxnet і регулювати подання урану в центрифуги таким чином, щоб вивести їх з ладу. До 2010 року в рамках цієї операції було зруйновано майже кожну четверту центрифугу, якою володів Іран, тобто військова ціль була частково досягнута не вдаючися до традиційних військових засобів.

***Держави озброюються***

Операція «Олімпійські ігри» була першим випадком фізичного руйнування інфраструктури держави, яке стало можливим через запланований запуск шкідливого програмного забезпечення в комп’ютерну систему ворога. Стало зрозуміло, що критична інфраструктура будь-якої держави вразлива до кібератак, а тому потрібно розробляти ефективні стратегії кібербезпеки. Крім цього, інші держави вивчили уроки використання кіберпотужностей для досягнення політичних цілей і вже незабаром продемонстрували власні можливості здійснювати вплив через кіберпростір.

У 2014 році керівництво КНДР імовірно скористалося послугами хакерської групи під назвою «Вартові миру» (Guardians of Peace), щоб організувати кібератаку на американську медіакомпанію Sony Pictures. Видається, що Кім Чен Ін намагався запобігти виходу в прокат комедійної стрічки «Інтерв’ю», сюжет якої розгортається навколо вбивства північнокорейського лідера. Атака, що супроводжувалася введенням шкідливого програмного забезпечення, паралізувала всю комп’ютерну інфраструктуру компанії Sony і дала змогу зловмисникам викачати чутливі дані. Вже незабаром персональна інформація працівників компанії, їх електронні листи та копії невипущених фільмів були опубліковані в Інтернеті, завдавши ще більшої шкоди бізнес-інтересам компанії Sony. Зрештою, вимоги хакерів припинити покази фільмів були задоволені – а отже, вдавшись до асиметричних засобів впливу, Кім Чен Ін таки досяг свого.

Випадок із компанією Sony показав, як компанії з приватного сектору можуть стати жертвами кібератак, які спрямовані проти держав їх розташування. Подібною була ситуація, яка трапилася того ж року: аби продемонструвати свої можливості у кіберпросторі, іранський уряд завдав руйнівної кібератаки по американському казино у Лас-Вегасі. Цю атаку можна розглядати як асиметричну відповідь на операцію «Олімпійські ігри», проте найбільше від неї постраждав не американський уряд та його національні інтереси, а бізнес-інтереси власників казино.

***Досвід України***

Наша держава однією з перших на власному досвіді перевірила руйнівний потенціал кіберпотужностей, коли у 2015 році внаслідок кібератаки, що походила з РФ, було вимкнуто електроенергію в Івано-Франківській області. В результаті 230 тисяч осіб залишилися без світла на 6 годин. Наступного року було вчинено ще одну кібератаку на електростанцію в Україні, а вже у 2017 році діяльність ключових державних підприємств, у тому числі залізниці та пошти, було паралізовано внаслідок запущеного російськими спецслужбами вірусу NotPetya, який використав вразливості у програмному забезпеченні Microsoft і поширив руйнівний вплив на 65 країн.

У зв’язку з тим, що керування українськими електромережами можна було повернути в ручний режим, шкода від кібератаки не була тривалою. Однак, якби подібна ситуація склалася з більш автоматизованими системами, то хакери могли б не лише вимкнути живлення електростанцій, але й блокувати зусилля з відновлення контролю над ними.

Як зазначає Роб Нейк у статті “The Next Cyber Battleground” у журналі Foreign Affairs, потенціал російських кіберпотужностей дозволяє Російській Федерації вимкнути живлення електростанцій у кількох областях України одночасно. Тому можна припустити, що ці атаки мали на меті продемонструвати силу. Проте згадані події мали також і позитивні наслідки: у співпраці з міжнародними партнерами український уряд сформулював Національну стратегію кібербезпеки України, а також створив Департамент кіберполіції Національної поліції України з метою протидії подальшим загрозам у кіберпросторі.

Ми бачимо, як кіберпростір став ареною реалізації національних інтересів держав. Сьогодні не обов’язково вести конвенційну війну, щоб досягти політичних чи військових цілей – достатньо віднайти вразливості в комп’ютерних системах та завдати удару. У міру розвитку та поширення інформаційних технологій протистояння в цифровій сфері буде продовжуватися в короткій та середньостроковій перспективах. Чи призведе ця боротьба до формування нового світопорядку – скоро побачимо.