Кібервійни та кібербезпека в сучасному світі

доцент Горбенко В.І.
ауд.19, корп.1

Приклади кібервійни

Епізод з кібератакою на радянський газопровід у 1982 році є однією з найбільш відомих перших кібероперацій США, яка використала кібертехнології для нанесення шкоди Радянському Союзу. Ця подія, відома як "Сибірський газопровідний вибух", мала значний вплив на розвиток кіберзброї та стратегій кібервійни.

У розпал Холодної війни, США шукали способи підірвати економіку та військовий потенціал Радянського Союзу. Один з таких способів передбачав саботаж критичної інфраструктури через маніпуляції з технологіями.

Операція CIA: проєкт «Intel». У рамках цієї операції американські спецслужби виявили, що Радянський Союз намагався придбати західні технології для своєї газової промисловості через різні обхідні шляхи, включаючи підставні компанії. У 1982 році через спецагентів ЦРУ було передано програмне забезпечення для системи контролю газопроводу, яке містило приховану "логічну бомбу". Коли програмне забезпечення було впроваджене і почало керувати системами газопроводу, "логічна бомба" активувалася. Це призвело до змін у тиску та швидкості потоку газу, що викликало надзвичайний стрес у трубопроводі. Зрештою, це призвело до масштабного вибуху, який знищив частину газопроводу в Сибіру.

Наслідки:

Фінансові втрати Радянського Союзу;

Стратегічні наслідки — показано можливості новітніх технологій як виду загрози;

Розвиток кіберзброї.

Приклади кібервійни

Операція "Олива" (Operation Orchard) – ізраїльська військова операція, проведена 6 вересня 2007 року проти ядерного об'єкта в Сирії. Ізраїльські ВПС (IAF) завдали удару по сирійському реактору в Дейр-ез-Зорі, який, за даними розвідки, будувався за підтримки Північної Кореї. Операція супроводжувалася масштабним використанням методів кібервійни для знищення сирійської протиповітряної оборони (ППО) та систем зв’язку.

Ключові аспекти кібератаки в рамках операції "Олива"

Електронне глушіння та кібератака на ППО - перед початком авіаудару ізраїльські сили використали передові засоби кіберборотьби та РЕБ, щоб "осліпити" сирійську систему ППО. Імовірно, було застосовано технологію "Suter", розроблену США, яка дозволяла проникати в радіолокаційні системи супротивника, брати під контроль екрани операторів та показувати їм фальшиві дані або повністю відключати їх.
Придушення сирійських радарів - перед атакою сирійські радари було "осліплено" – вони перестали відображати будь-які об'єкти в повітрі. Це дало ізраїльським літакам можливість пройти вглиб сирійської території непоміченими.
Обманні маневри та кібератака на мережі зв’язку - крім РЕБ, було завдано кіберудару по мережах зв’язку сирійських військ, що ускладнило координацію їхніх дій. Імовірно, це включало "віддзеркалення" фальшивих сигналів, що вводило операторів ППО в оману.
Фінальний авіаудар - коли сирійські системи ППО були нейтралізовані, ізраїльські винищувачі F-15I та F-16I завдали точкового удару по цілі, повністю знищивши об’єкт.

Приклади кібервійни

Операція з використанням вірусу Stuxnet у 2010 році стала одним із найвідоміших прикладів використання кіберзброї для фізичного руйнування критичної інфраструктури. Вірус був розроблений для атаки на іранську ядерну програму, зокрема на завод зі збагачення урану в Натанзі.

Stuxnet – це високотехнологічний комп'ютерний черв'як (worm), створений для ураження програмованих логічних контролерів (PLC), що керували центрифугами для збагачення урану.

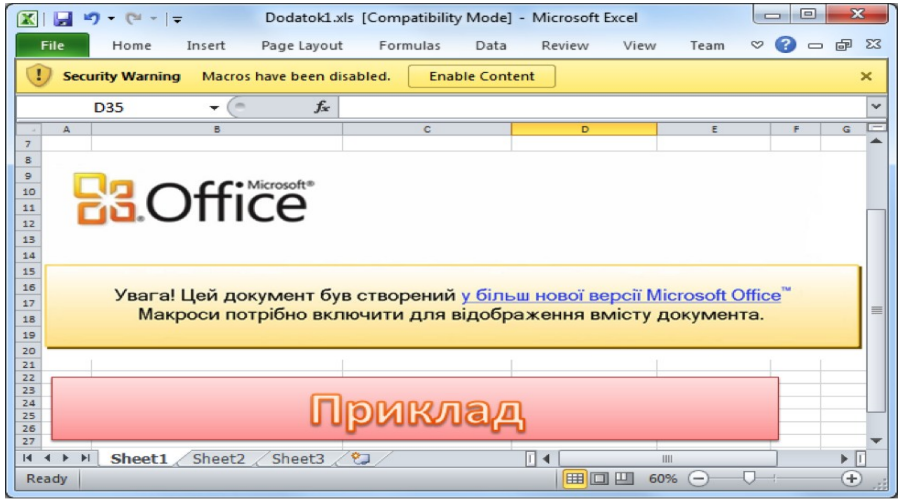
Основними особливостями вірусу були:
Висока складність та цільова спрямованість – вірус атакував лише конкретні моделі PLC від Siemens, які використовувалися в Натанзі.
Стійкість до виявлення – він не змінював загальну роботу системи, а поступово порушував технологічний процес, що ускладнювало виявлення.
Механізм самопоширення – він передавався через USB-накопичувачі, оскільки об'єкт у Натанзі був ізольований від інтернету (air-gapped system).

Приклади кібервійни

Перша зареєстрована успішна кібератака на енергетичну компанію України з виведенням її із ладу сталась 23 грудня 2015 року. Російські хакери атакувати комп'ютерні системи управління трьох енергопостачальних компаній України.
Наступна кібератака сталась вночі з 17 на 18 грудня 2016 року.
Була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берегу Києва та прилеглих районів області.

Результати атак:

1. «Прикарпаттяобленерго»: вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин.
2. «Київобленерго»: відключено 30 вузлових підстанцій від яких живиться низка стратегічних об'єктів, понад 80 тисяч споживачів були без електрики протягом однієї-трьох годин.



Приклад документу, зараженого трояном BlackEnergy, з якого почалось проникнення в комп'ютерну мережу диспетчерської «Прикарпаттяобленерго».

Кіберзброя у війні Росії проти України застосовується для кібератак на урядові та військові інфраструктури, комунікаційні системи, енергетичні мережі та інші критичні об'єкти.

Приклади сценаріїв:

1. Блокування або порушення роботи важливих урядових систем: російські хакерські групи здійснюють кібератаки на урядові системи України з метою зблокувати їхню роботу, отримати конфіденційну інформацію або спробувати вплинути на процеси прийняття рішень.
2. Паралізація комунікаційних та інформаційних систем: здійснення кібератак на телекомунікаційні мережі та інтернет-провайдерів для обмеження доступу до інформації та комунікації між військовими, урядовими та цивільними структурами.
3. Порушення роботи енергетичних систем: здійснення кібератак на енергетичні мережі України з метою збоїв у постачанні електроенергії, задля виникнення серйозних перебоїв у роботі промислових підприємств, соціальних та громадських об’єктів, житлових будівель, тощо.
4. Спроби використати соціальні мережі та медіа для дезінформації: здійснення кібератак на соціальні мережі та медіа для поширення дезінформації та пропаганди, задля впливу на громадську думку та ставлення до війни.

Основні поняття

Під цифровим середовищем розуміють поєднання інформаційних технологій та кіберпростір.

Киберпростір — це та частина цифрового середовища, де і завдяки якій відбувається контроль та керування різними фізичними об’єктами, для чого використовуються як певне програмне забезпечення та протоколи комп’ютерних мереж (зокрема Інтернет), так і інфраструктура мереж та телекомунікаційні канали.

Слово «кіберпростір» вперше було використано Вільямом Гібсоном (канадський пісменник фантаст) у 1982 в новелі «Burning Chrome» («Спалення Хром»), яку опубліковано в часописі Омні. Потім це словосполучення Вільям Гібсон вже широко використовував у новелі «Нейромант» («Neuromancer»). Зараз ми вже інтуїтивно розуміємо, що воно позначає.

Цифрове середовище вміщує:

- Інфраструктурний рівень (телекомунікаційні лінії та канали, комп’ютерні системи та вбудовані блоки керування фізичними об’єктами);
- Програмний рівень (протоколи передавання даних, операційні платформи та програмне забезпечення, підсистему сприймання інформації кінцевим користувачем);
- Ресурсно-структурний рівень (загальнодоступні мережеві ресурси, захищені ресурси державної та корпоративної власності, загальнодоступні ресурси з платним контентом)

Загальні поняття
Кібервійна та кібербезпека

Історично Інтернет створювався як вільне середовище інформаційної взаємодії з використанням певних технологій та правилами організації, які було розроблено та розроблювались переважно у США. Уклад життя, правила ведення бізнесу, рівень розвитку економіки та виробництва у США сприяв до переміщення на ресурси Інтернет та з використанням технологій Інтернет значної частини торгівлі, фінансових операцій, політичної та соціальної активності. Зараз ці ключові сфери життєдіяльності перемістились до Інтернет у більшості держав світу.

Вестфальска система міжнародних відношень — світова державно центрична система, основний принцип державного суверенітету XVII-XX ст., одним із наслідків якого є принцип невтручання у внутрішні справи суверенних держав. Вестфальска система зробила універсальною політичною одиницею національну державу, а політичні суспільства у всіх державах світу було інтегровано як нації.

Поствестфальска система міжнародних відношень формується під впливом процесів глобалізації, в рамках яких, права людини набувають більшої ваги, ніж ті, що формуються належністю до певної нації або за висловом “той, хто народився у певній державі має відстоювати лише її інтереси”.

Вестфальська система міжнародних відносин - це термін, який походить від міста Вестфалія в Німеччині, де були укладені дві важливі міжнародні угоди: Мюнстерський мирний договір (1648 рік) та Оснабрукський мирний договір (також 1648 рік). Ці договори завершили Тридцятирічну війну у Європі та Війну в Нідерландах відповідно.

Вестфальська система міжнародних відносин встановила такі ключові принципи:
1. Принцип суверенітету держав: Договори визнали суверенітет кожної держави, що означало, що кожна держава мала право самостійно встановлювати свою внутрішню та зовнішню політику без втручання з боку інших держав.
2. Принцип балансу сил: Вестфальська система сприяла виникненню концепції рівноваги сил, де багато держав взаємодіяли з урахуванням власних інтересів та потужностей, що мали на меті запобігти домінуванню однієї держави чи групи держав.
3. Принцип територіальної цілісності: Договори закріпили принцип територіальної недоторканності держав, що означало, що кордони держав були визнані як недоторкані, і втручання в них було неприпустимим.
4. Вестфальська система міжнародних відносин стала основою для розвитку сучасної міжнародної системи та визначила ключові принципи, які лежать в її основі. Вона також відіграла значну роль у формуванні поняття сучасної державності та системи міжнародного права.

"Поствестфальська система міжнародних відносин" - це термін, що використовується для опису сучасних міжнародних відносин після періоду Вестфальської системи.

Для поствестфальської системи можна визначити наступні характеристики:
1. Глобалізація: Поствестфальська система відзначається зростанням глобалізації, яка викликає зростання зв'язків міжнародної торгівлі, фінансів, культури та політики.
2. Мультиполярність: Замість біполярності (яка характеризувалася боротьбою між США та Радянським Союзом) поствестфальська система стала більш мультиполярною, з різними центрами впливу, такими як США, Європейський Союз, Китай, Росія та інші.
3. Міжнародні організації: З'явлення та зростання ролі міжнародних організацій, таких як Організація Об'єднаних Націй (ООН), Всесвітня Торговельна Організація (ВТО), Міжнародний Валютний Фонд (МВФ) та інші, які грають важливу роль у регулюванні міжнародних справ.
4. Транснаціональні виклики: Зростання транснаціональних викликів, таких як глобальний тероризм, кліматичні зміни, кіберзлочинність та пандемії, які вимагають співпраці між державами для вирішення.
5. Кібербезпека: Зростання кіберзагроз та необхідність регулювання кіберпростору та захисту кіберінфраструктури.
Поствестфальська система міжнародних відносин є складною та різноманітною, і вона відображає сучасні реалії світової політики та економіки.

Деякі ключові моменти, що варто враховувати:

1. Інтернет і глобалізація: Інтернет відіграв важливу роль у глобалізації, зробивши світ більш зв'язаним і відкритим для обміну інформацією, ідеями та торгівлі. Він створив можливість для швидкого обміну даними та сприяв зростанню культурного, економічного та політичного обміну між націями.

2. Поствестфальська система міжнародних відносин: Глобалізація, разом із зростанням впливу прав людини та усвідомленням загального блага, викликає перегляд традиційних концепцій національної суверенітету та державної інтервенції. Це може призвести до трансформації системи міжнародних відносин, щоб врахувати глобальні виклики та нові реалії.

3. Суперечності та виклики: Однак, глобалізація також супроводжується новими суперечностями та викликами, включаючи збільшення нерівності, зміни клімату, кібербезпеку та інші. Ці виклики потребують спільних зусиль та співпраці між державами для знаходження рішень.

4. Інтернет і права людини: Інтернет також відіграває ключову роль у підтримці прав людини, розповсюдженні інформації та сприянні громадянській активності. Він надає громадянам можливість спілкуватися, виражати свою думку та впливати на політичні процеси.

Кібервійна впливає на еволюцію міжнародних відносин у багатоаспектному способі. Деякі ключові впливи:

1. Зміна парадигми конфлікту: Кібервійна відкриває нові фронти конфлікту, де військові дії можуть відбуватися в цифровому просторі. Це створює нові виклики для традиційних понять про військові дії, оборону та безпеку.
2. Асиметрія конфлікту: Кібервійна може дозволяти менш розвиненим або меншим державам ефективно впливати на більш розвинені чи більш потужні супротивників. Це може порушувати традиційні баланси сил та вимагати перегляду стратегій оборони та військової безпеки.
3. Міжнародне право та норми: Кібервійна ставить під сумнів традиційні правові норми, пов'язані з військовими конфліктами та поведінкою держав у міжнародних відносинах. Це спонукає до необхідності розробки нових нормативних актів та міжнародних договорів.
4. Зростання потенціалу конфлікту та напруження відносин: Кібервійна може стимулювати напруженість міжнародних відносин, особливо між державами, які вважаються ворогами або конкурентами. Кібератаки можуть призвести до загострення конфліктів та ескалації напруженості.
5. Розвиток кібердипломатії та кібербезпеки: Держави починають розвивати нові стратегії дипломатії та міжнародного співробітництва в області кібербезпеки. Кібердипломатія стає важливим інструментом забезпечення міжнародної стабільності та взаєморозуміння.