Кібервійни та кібербезпека в сучасному світі

доцент Горбенко В.І.
ауд.19, корп.1

Кіберзброя

Значна кількість країн приєдналися до кіберпростору, як до нового поля протиборства, усвідомлюючи важливу роль, яку кібербезпека відіграє у національній та міжнародній безпеці, інвестуючи в свої стратегії, політику та програми, а також готуючись до можливих конфліктних ситуацій, створюючи нові плани впровадження та використання кіберзброї.

Cartoon credits: The Economist 2009

На міжнародному рівні кіберзброя є невизначеним поняттям через те, що не існує загальновизнаного глобального визначення, а також бракує досліджень щодо її профілю, дії та впливу з різних точок зору.

Існують визначення та опис звичайної зброї, наприклад, зброя ближнього бою, зброя для стрільби з стрілами, вогнепальна зброя та вибухівка, або нетрадиційної зброї, наприклад, зброя масового знищення: хімічна зброя, біологічна, ядерна або радіологічна зброя. Для того, щоб визначати виникнення протистояння та проведення певних бойових дій у кіберпросторі, встановлення наслідків її застосування та нанесених втрат, необхідно мати визначення і для кіберзброї.

Кіберзброя

Термін "кіберзброя" відноситься до інструментів, технологій або методів, які використовуються в кіберпросторі для здійснення кібератак, кібервійських операцій або впливу на інформаційні системи та мережі. Кіберзброя може бути використана для різних цілей, включаючи розвідку, руйнування, шпигунство, вплив на суспільну думку або завдання шкоди ворогові.
Прикладами кіберзброї є:
1. Віруси та програми-шпигуни: зборі конфіденційної інформації або виконання певних дій на комп'ютері без дозволу користувача.
2. Віруси-троянці: приховується під виглядом корисної програми або файлу і виконує шкідливі дії при певній активації.
3. Комп'ютерні черви: здатні самостійно розповсюджуватися через комп'ютерні мережі, використовують вразливості у програмному забезпеченні.
4. DDoS-атаки (Distributed Denial of Service) спрямовані на перевантаження веб-серверів або мережевих інфраструктур шляхом надмірного надходження запитів або трафіку.
5. Фішинг: один із видів соціально-інженерної атаки - маскування зловмисника як легальні особи або організації для отримання конфіденційної інформації. Технічний фішинг — маскування комп’ютерної системи під виглядом легальної.
6. Кіберзброя на основі штучного інтелекту: використовується для виявлення вразливостей, розвідки, аналізу великих даних та розробки нових методів атак.

Кіберзброя

Сунь-цзи, китайський генерал, військовий стратег і філософ, стверджував, що "найвищим мистецтвом війни є підкорення ворога без бою".
Концептуальна модель використання кіберзброї достатньо проста:

Дійова особа відповідає за проведення кібероперацій або заходів, спрямованих на досягнення військових цілей.
Це можуть бути державні суб'єкти, такі як уряди чи установи, що мають повноваження дозволити використання кіберзброю. Різниця між державними та недержавними суб'єктами проявляється через наявність певних ресурсів: розвідка, персонал, обладнання тощо і можливо в якості, інноваціях та інтелектуальних методах, що використовуються для впровадження кіберзброї. Наприклад, аналіз мережевого хробака Stuxnet вказує на такий дизайн, який могла собі дозволити тільки держава.

Кіберзброя

Недержавні суб'єкти як дійова особа - це недержавні або неурядові установи, групи чи організації людей, які вирішують самостійно організовувати, впроваджувати та використовувати кіберзброю, не пов'язані з жодним державним суб'єктом. Прикладами недержавних суб'єктів є хакери, окремі професіонали, дослідники безпеки, приватні організації, установи, корпорації. Типи їх спонукань: особисті, економічні, ідеологічні або етичні.

Існує гібрид дійової особи, коли державна дійова особа підтримується недержавною, або навпаки, недержавну дійову особу підтримує державна.

Дійові особи, які беруть участь у кібервійні, використовують свою кіберсилу, створюють та застосовують різні інструменти та техніки як засоби та методи, щоб отримати перевагу над своїми супротивниками всередині та/або за межами кіберпростору.

Об’єктами є певні пристрої, устаткування, ресурси або люди, яких необхідно досягти завдяки кіберзброї, усередині або за межами кіберпростору.
Цілі — це певні сутності об’єктів, на які намагаються вплинути для досягнення переваги. Досягнення цілі та додаткові ефекти дозволяють визначати та класифікувати кіберзброю.

Кіберзброя

Бажаний вплив - категорія впливу, що описує бажані або передбачувані результати, які сприятимуть досягненню бажаного кінцевого стану, досягненню цілі місії.

1. Втрата функціональності об'єкта: Кібератаки можуть спричинити втрату функціональності об'єкта, зупинити роботу його систем або призвести до неправильної роботи. Наприклад, зупинка роботи важливих систем керування або призупинення роботи критичних інфраструктурних об'єктів.
2. Знищення чи пошкодження даних: Кібератаки можуть вплинути на цілісність даних об'єкта, що може призвести до їхнього втрати, пошкодження або зміни. Це може мати серйозні наслідки для діяльності об'єкта та його здатності виконувати свої функції.
3. Порушення конфіденційності інформації: Кібератаки можуть призвести до несанкціонованого доступу до конфіденційної інформації об'єкта, що може викликати серйозні проблеми щодо захисту даних та конфіденційності.
4. Зміна або викривлення інформації: Кібератаки можуть використовуватися для зміни чи викривлення інформації, що може викликати помилкові рішення чи спричинити довіру до об'єкта.
5. Підрив робочих процесів: Кібератаки можуть порушити нормальну діяльність об'єкта, зменшити продуктивність або спричинити збої в роботі систем та процесів.
6. Психологічний тиск та деморалізація: Кібератаки можуть викликати психологічний тиск на персонал об'єкта, призвести до деморалізації та зниження ефективності роботи.

Кіберзброя

Небажаний вплив - категорія впливу, що описує небажані результати, які негативно впливають на досягнення бажаного кінцевого стану, або залишають слід.

1. **Виявлення атаки**: Якщо атака кіберзброї стає очевидною для противника, це може призвести до відповідних заходів захисту та реагування, що ускладнить досягнення поставлених цілей.
2. **Поглиблення конфлікту**: В деяких випадках застосування кіберзброї може призвести до подальшого зростання напруги між сторонами або до ескалації конфлікту, що може мати негативні наслідки для обох сторін.
3. **Втрата контролю**: Якщо кібератака виходить з-під контролю або спричиняє неочікувані наслідки, це може призвести до втрат ресурсів та стратегічних можливостей для кібервійських сил.
4. **Помилкові цілі**: Якщо кібератака спрямована на неправильні об'єкти або системи, це може призвести до втрат часу, зусиль та ресурсів, не принесячи очікуваних результатів.
5. **Послаблення міжнародної підтримки**: Якщо кібератака порушує міжнародні норми чи призводить до обурення міжнародного співтовариства, це може призвести до послаблення підтримки для дій кібервійських сил.

Кіберзброя

Під час планування та участі в операції враховують **побічну шкоду**. Оцінки супутньої шкоди ***до*** та ***після*** використання кіберзброї проводяться у межах законів про збройні конфлікти.

Наприклад, аналіз впливу Stuxnet свідчить про те, що її побічну шкоду було мінімізовано.

Очікувані ефекти - категорія впливу, що описує очікувані результати, навіть якщо була або не передбачалася з самого початку.

- порушення робочих процесів
- нанесення матеріальних збитків
- зниження ефективності
- викриття вразливостей
- психологічний тиск
- підрив безпеки.

Несподівані ефекти - категорія впливу, що описує несподівані результати, які можуть мати багато наслідків: соціальні, економічні, політичні тощо.

- відкриття нових вразливостей
- випадкове пошкодження невинних систем
- реакція противників
- спроби заборонити атаку
- побічні ефекти на третіх сторін
- політичні або міжнародні реакції