Загальні поняття
Кібервійна та кібербезпека

Інформаційна війна має сім типів:

- командно керований,
- розвідувальний,
- психологічний,
- хакерство,
- економічний,
- електронний,
- кіберборотьба.

Для інформаційної війни на першому місці знаходяться: психологічний вплив, дезінформація, PR-компанії та спеціальні інформаційні операції.

Більш чіткий поділ між інформаційними війнам та кібервійнами почався у першій декаді 2000-х років і є загальним стандартом для військових, спеціалістів з інформаційних технологій та безпеки.

Хакерський тип інформаційної війни

News Corp, один із найбільших медіахолдингів у світі, 04.02.2022 заявив, що його зламали хакери, яких підтримує китайський уряд. (https://therecord.media/news-corp-breached-by-suspected-chinese-hackers/)

Передбачається, що хакери отримали доступ до електронної пошти та документів співробітників News Corp. Це стосується таких видань, як The Wall Street Journal, New York Post та ін.

Хоча розслідування все ще продовжується, компанія з інфобезпеки Mandiant вважає, що атака була здійснена зловмисником, який діє на користь уряду Китаю.

Цікаво, що таке трапляється не вперше. Китайські хакери вже атакували The Wall Street Journal у 2013 році, щоб моніторити те, як висвітлюються теми, пов’язані з Китаєм. Ці атаки також торкнулися Bloomberg та New York Times.

Інформаційні та кібервійни відрізняються за об’єктами та засобами дії.
Інформаційні війни є контентними війнами, що мають за мету зміну масової, групової та індивідуальної свідомості, нав’язування власної волі противнику та перепрограмування його поведінки. Під час інформаційної війни іде боротьба за свідомість, цінності, переконання, шаблони поведінки тощо. Вони виникли тисячоліття тому, а Інтернет дав їм новий рівень інтенсивності, масштабності та ефективності.
Об’єктами впливу інформаційних війн є різноманітні суб’єкти – від невеликих груп до певних народів та націй, населення держав.
Засобом впливу є спеціальні підготовлені семантичні повідомлення у вигляді текстів, відео та аудіо матеріалів.

Кібервійни є цілеспрямованим деструктивним впливом інформаційних потоків у вигляді програмних кодів на матеріальні об’єкти та їх системи, їх руйнування, порушення функціонування або перехоплення керування ними.
Кібервійна – це дія однієї національної держави з проникненням у комп’ютери або мережі іншої національної держави для досягнення певної мети нанесення збитку або руйнування.

Об’єктами впливу кібервійн є виробничі структури, інфраструктури соціального, воєнного та фінансового призначення, роботизовані та високоавтоматизовані виробничі та технологічні лінії.

Основним типом засобів бойового впливу у кібервійнах є певний програмний код, який порушує роботу, виводить з робочого стану, або забезпечує перехоплення керування різного роду матеріальними об’єктами та мережами, що мають у оснащені електронні системи керування.

Інформаційні війни та кібервійни є двома різновидами війн, які у більшій своїй частині ведуться через комп’ютерні мережі — глобальну мережу Інтернет, закриті державні, військові, корпоративні та приватні мережі. Для кожного із цих двох типів війн наявні власні інструментарії, методи, стратегії та тактики ведення, закономірності ескалації, можливості попередження, тощо.

Кібервійни пов’язано із кібершпіонажем, кіберзлочинністю, кібертерроризмом.

Основні риси кібервійн, що відрізняють їх від інших типів військових дій:

- Високий рівень анонімності;
- Невизначеність часу початку;
- певна відсутність слідів;
- Відсутність таких визначень як «фронт», «тил»;
- Відсутність будь-якого правового міжнародного регулювання.

Зараз глобальна мережа Інтернет має загальне управління з боку ICANN. Регулювання відбувається за парадігмою “один світ – один Інтернет”. При такому підході неможливими стають будь-які звичні у військовому праві міжнародні угоди. ICANN (Internet Corporation for Assigned Names and Numbers) заперечує право держав регулювати і нести відповідальність за певний сегмент Інтернет. Де факто Інтернет та інші мережі мають наднаціональний характер, а бойові дії в кіберпросторі направлено на певні національні держави та їх структури. Наявна ситуація, коли ніякі юридичні і будь-які погоджувальні механізми профілактики та запобігання кібервійн не можуть діяти.

Характерні риси кібервійн вказують, що вони є особливо небезпечними, тому що легко розв’язуються і практично не регулюються.

Фактори загрози:

- Тенденції технологічного розвитку;
- Темпи та суперечливість динаміки світової економіки;
- Експоненціальне зростання Інтернету речей, поява бодінет;
- Розвиток хмарних обчислень;
- Інформаційні технології є інтегральною складовою багатьох сучасних технологій (робототехніка, біотехнології, тощо).

Створення високорівневої кіберзброї можуть дозволити обмежені у ресурсах як держави, так і окремі групи. Наявність такої зброї створює певні ілюзії, щодо вирівнювання потужностей у протистоянні з економічно розвиненими державами. Роль застосування кіберзброї пов’язано з такими факторами:

- Держави, які мають значний науковмісний сектор, високотехнологічне виробництво та значну інтеграцію комп’ютерних мереж у виробництво та життя суспільства, є більш вразливими для кіберзброї;
- Участь у різноманітних збройних конфліктах обумовлює ризики застосування проти них кіберзброї, навіть через певний період часу;
- Зростання складності технологічних об’єктів підвищує ймовірність їх каскадної відмови.