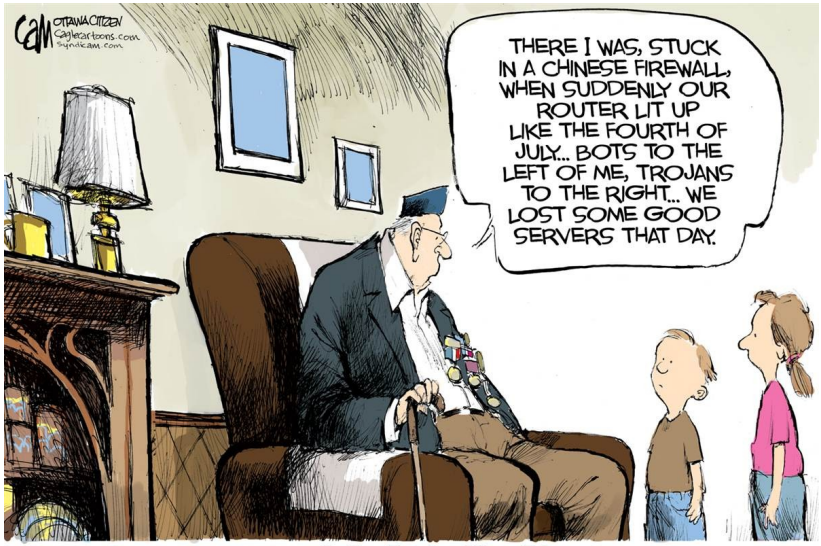
Кібервійни та кібербезпека в сучасному світі

доцент Горбенко В.І.
ауд.19, корп.1

Загальні поняття
Кібервійна та кібербезпека



XXI-століття почалось з революційних змін, які обумовлювались стрімким розвитком інформаційних технологій. Суттєва глобальна залежність від кіберпростору та її неодмінне посилення, постійні швидкоплинні технологічні зміни, наявність вразливостей та їх стійкість породжують загрози технічній, економічній та соціальній безпеці. Забезпечення широкого спектру інфраструктури, що є критично важливою для цивілізованого функціювання суспільства, має значення, насамперед, у таких областях як комунікації, транспорт, торгівля.

Війна — комплекс заходів спрямований на захоплення чужих природних, енергетичних та людських ресурсів. Вона є складним суспільно-політичне явищем, яке пов'язане з розв'язанням суперечностей між державами, народами, національними й соціальними групами з переходом до вжитку засобів збройної боротьби, що відбувається у формі бойових дій між їхніми збройними силами. Це специфічна форма вияву соціальних відносин, в якій панує збройна боротьба як продовження політики, що підпорядковує своїм цілям усі сфери суспільного життя. Зазвичай характеризується крайньою колективною агресією, руйнуваннями та високою смертністю.

Кібервійна стала можливою завдяки декільком факторам:

1. Зростання залежності від інформаційних технологій: У XXI столітті майже всі сфери життя стали залежними від комп'ютерних систем і мережі Інтернет. Від економіки до військових операцій, від урядового управління до особистого спілкування, всі вони базуються на комп'ютерах і мережах.

2. Геополітичні конфлікти та боротьба за вплив: В світі існують різноманітні геополітичні конфлікти і боротьба за вплив. Кібервійна може бути одним з інструментів в цих конфліктах. Держави можуть використовувати кібератаки для розвідки, дестабілізації і навіть агресії проти інших країн.

3. Анонімність та важкість виявлення: У кіберпросторі атаки можуть бути виконані анонімно або з використанням відомих методів обману. Це робить складним визначення точного джерела атаки та відповідальності за неї.

4. Розвиток технологій шифрування: Захищені канали зв'язку та шифрування можуть допомогти атакувачам залишатися невиявленими під час виконання кібератак.

5. Економічні мотиви: Багато кібератак виконуються з метою отримання прибутку. Це може бути шахрайство, крадіжка конфіденційної інформації для продажу, вимагання викупу в обмін на розблокування даних (рансомвар), або спроби вкрадення фінансових активів.

Загальні поняття
Кібервійна та кібербезпека

Зазвичай війна є засобом нав'язування супротивнику своєї волі і, врешті решт, встановлення над ним своєї влади. Один суб’єкт політики намагається силою змінити поведінку іншого, заставити його відмовитись від певних речей: своєї волі, ідеології, від прав на власність, від певних ресурсів (території, акваторії тощо).

За вдалим висловом Клаузевіца (військовий генерал, теоретик та історик) «війна є продовження політики іншими, насильницькими засобами». Від політичного керівництва залежить початок війни, її інтенсивність, терміни та умови примирення сторін протиборства. Від політичного керівництва також залежить надбання прихильників та союзників, створення коаліцій. Внутрішня політика сторін також має значний вплив на ведення війни. Слабка влада завжди потребує швидких успіхів. Досягнення на війні настільки залежить як від внутрішньої політики, так і від узгодженнями між зовнішньополітичним керівництвом та військовим командуванням.

Війна та кібервійна є різними за своєю природою та формою прояву, є деякі загальні риси та аспекти, які їх об'єднують:

1. Цільовий спрямований вплив: Як війна, так і кібервійна можуть бути спрямовані на досягнення певних цілей, таких як захоплення територій, знищення важливих об'єктів, зміна політичних режимів тощо.

2. Суспільно-політичне явище: Обидві форми конфлікту відображають соціальні та політичні суперечності між державами, групами чи іншими суб'єктами. Вони виражають прагнення до здобуття влади, контролю або впливу.

3. Використання засобів боротьби: Як війна, так і кібервійна використовують засоби боротьби для досягнення своїх цілей. У війні це може бути фізична сила, армії, зброя тощо, тоді як у кібервійні використовуються комп'ютерні системи, програмне забезпечення та мережі для атак і контратаак.

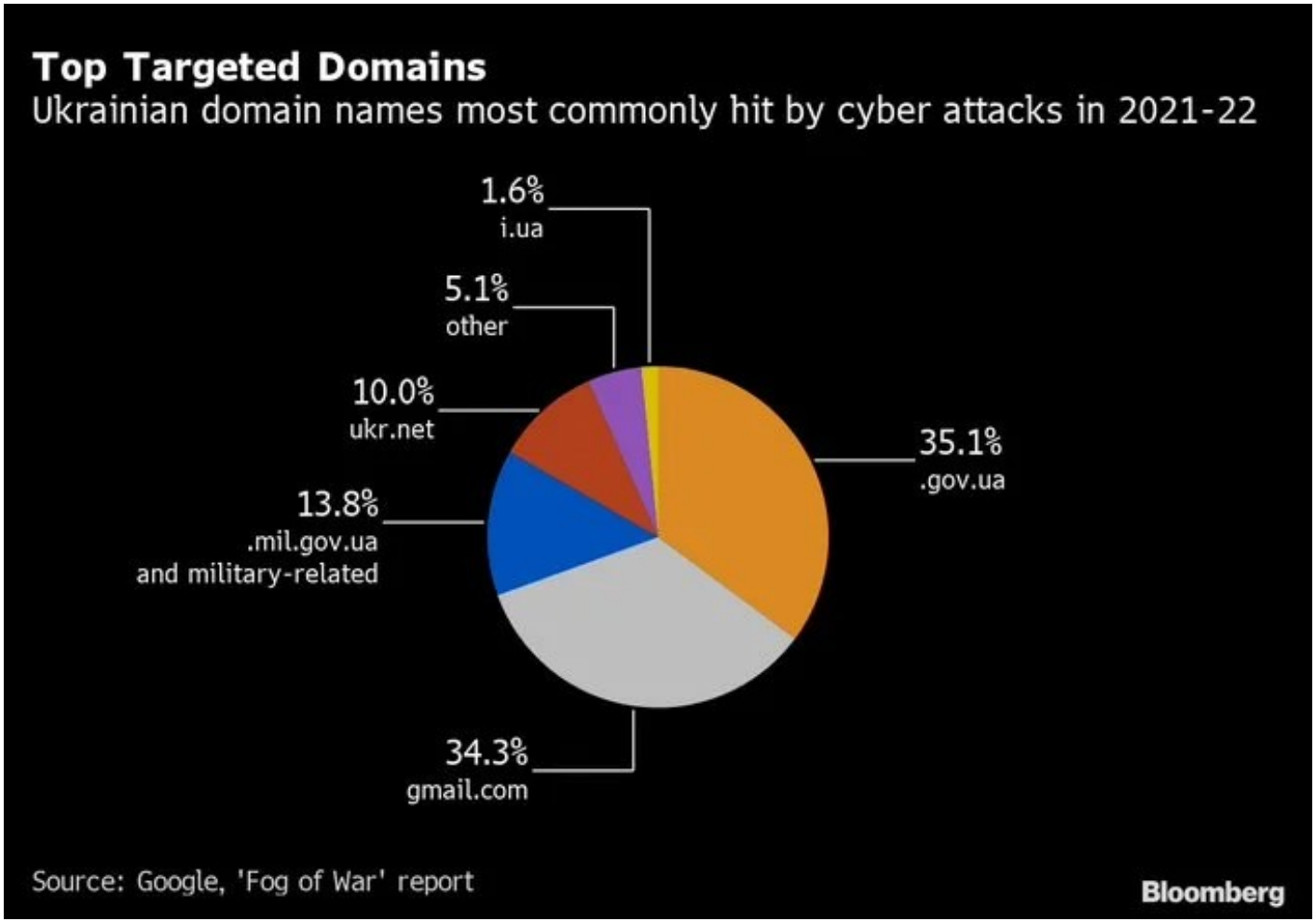
4. Колективна агресія і наслідки: Як війна, так і кібервійна можуть мати серйозні наслідки для суспільства, включаючи руйнування, травми, втрату життів, економічні втрати та інші негативні наслідки.

5. Збройна боротьба як засіб політичного впливу: В обох випадках, війна та кібервійна можуть бути спричинені політичними чи геополітичними мотивами, а також можуть використовуватися для досягнення політичних цілей.

Кібервійна може намагатися змінити поведінку супротивника та встановити над ним свою владу:

1. Вплив на інформаційні потоки: Кібервійна може спрямовувати, фальсифікувати або перешкоджати потокам інформації для впливу на думку суспільства, державних чиновників або військових.
2. Атаки на критичну інфраструктуру: Шляхом кібератак на критичну інфраструктуру, таку як електроенергетичні мережі, транспортні системи або фінансові установи, кібервійна може намагатися паралізувати супротивника та змусити його виконати певні вимоги.
3. Кібершпигунство та кібершантаж: Шляхом кібершпигунства або кібершантажу, кібервійна може збирати конфіденційну інформацію про супротивника або вимагати виконання певних вимог під загрозою розголошення конфіденційної інформації.
4. Дестабілізація та психологічний тиск: Шляхом провокацій або створення хаосу у цифровому просторі, кібервійна може спрямовувати супротивника до непередбачуваних дій або створювати психологічний тиск на його владу.

Статистика кібератак



Загальні поняття
Кібервійна та кібербезпека

У розпал холодної війни, у червні 1982 року, американський супутник раннього попередження виявив великий вибух у Сибіру. Це був вибух на радянському газопроводі. Причиною цього була несправність системи управління комп’ютером, яку радянські шпигуни викрали у фірми в Канаді. Вони не знали, що спеціалісти ЦРУ втручались в програмне забезпечення і зробили так, що воно через певний інтервал часу перестало працювати, скидало оберти насосу та налаштування клапанів. Це вело до створювання тиску, який значно перевищує допустимі значення для з'єднань та зварних швів трубопроводів. Отримані збитки були значними на той час.

2008 р. - під час проведення операції «Олива» сирійські ППО та радіоелектронна розвідка були заблоковані через певні дії методами кібервійни.

2010 р. - спеціально розроблений вірус Stuxnet втручається у роботу автоматизованої системи, що забезпечувала певний технологічний ланцюжок атомної промисловості в Ірані.