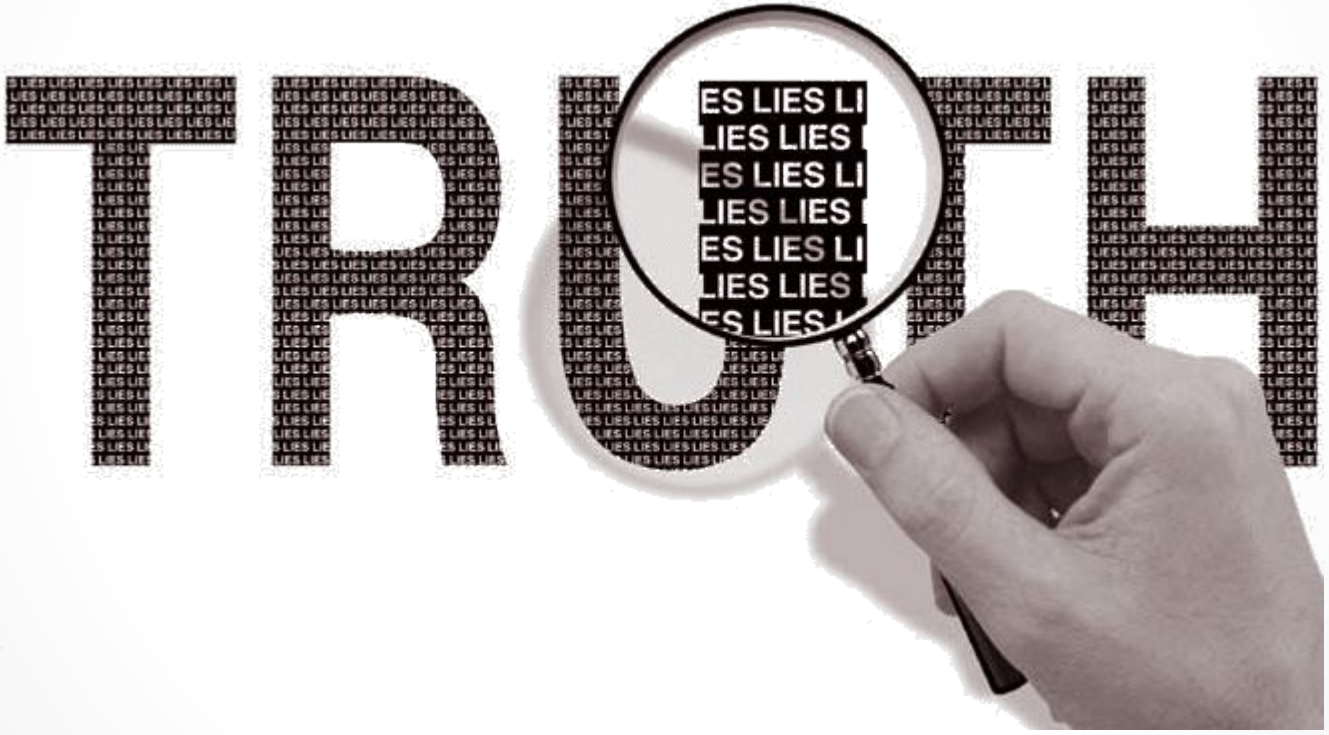
ІТ під час війни

Презентація
Учнів 12 групи
Українського гуманітарного ліцею КНУ імені Тараса Шевченка
Куценко Анастасії
Тотьмяніної Анни
Піпояна Арсена
Процев'ят Соломії

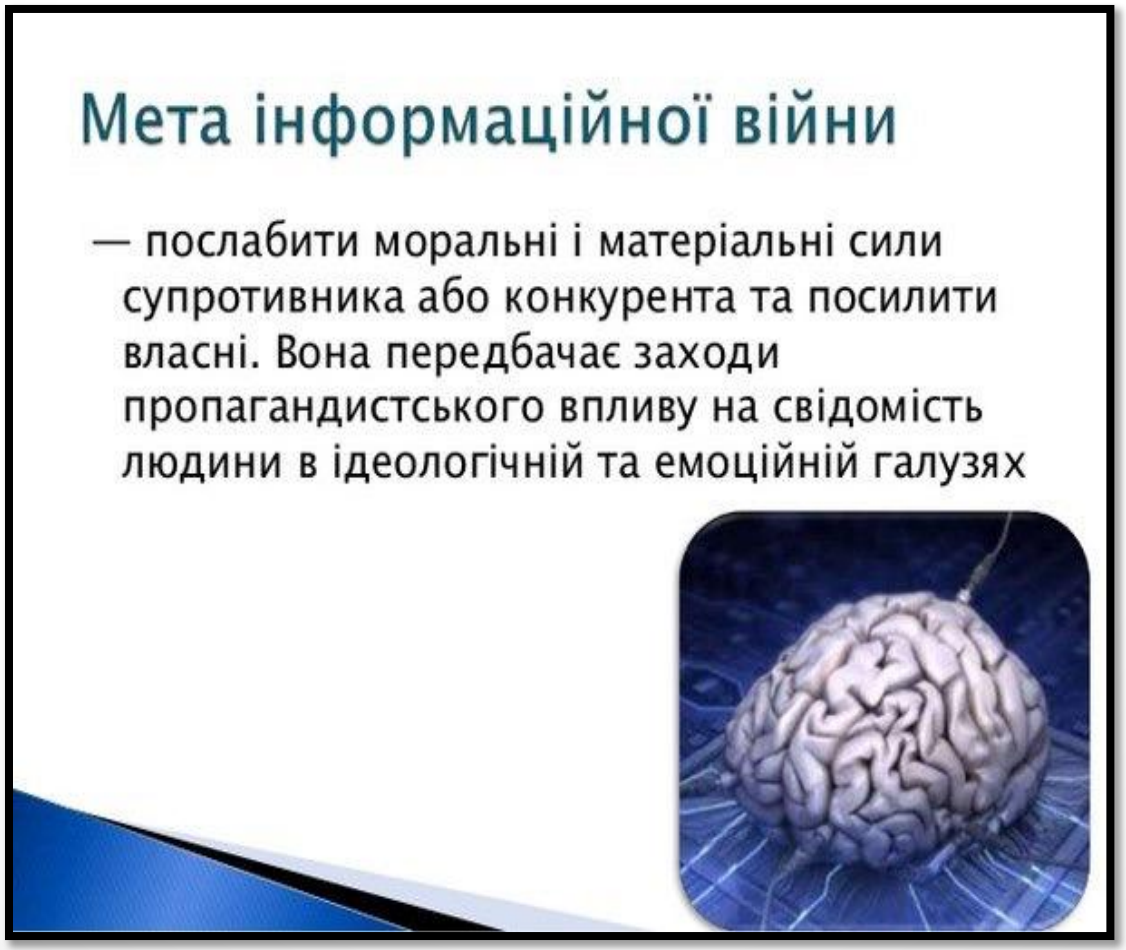
Структура роботи:

- Інформаційна війна як засіб знищення ворогів;
- Радіозвязок як засіб передачі інформації під час воєнних дій;
- Криптографія;
- Енігма.

Інформаційна війна: викриття реалій чи зброя у вигляді брехні?



обумовлена: зростаючою значимістю й цінністю інформації з питань командування, управління, політики, економіки й громадського життя.



80-х років XX ст., коли, після закінчення «Холодної війни», перед Збройними силами США постали нові завдання. Це був результатом роботи групи американських військових теоретиків у складі: **Г. Е. Эккліза, Г. Г. Саммерза** та ін.

Дії інформаційних війн охоплюють такі галузі:

1) інфраструктуру систем життєзабезпечення держави — телекомунікації, транспортні мережі, електростанції, банківські системи тощо;
2) промислове шпигунство — викрадання патентованої інформації, перекручування або знищення особливо важливих даних і послуг, збір інформації розвідувального характеру про конкурентів та ін.;
3) злом і використання особистих паролів «VIP-персон», ідентифікаційних номерів, банківських рахунків, даних конфіденційного характеру, а також продукування дезінформації;
4) електронне втручання в процеси командування та управління військовими об'єктами й системами, «штабна війна», виведення з ладу мереж військових комунікацій;
5) всесвітня комп'ютерна мережа Інтернет, у якій, за окремими оцінками, діють 150.000 військових комп' ютерів, а 95 % військових ліній зв'язку проходять у відкритих телефонних лініях.

- Нині Інтернет дедалі активніше й масштабніше використовується в інтересах інформаційного протиборства сторін, які є учасниками різних конфліктів.

  Активне використання мережі Інтернет для ведення інформаційного протиборства обумовлено низкою її істотних переваг перед звичайними засобами й технологіями:
- Оперативність;
- Економність;
- Прихованість джерела впливу;
- Дистанційний характер впливу на комп’ютерні системи в різних регіонах світу;
- Масштабність можливих наслідків;
- Комплексність подачі інформації та її сприйняття;
- Доступність інформації.

Існує такий термін — «Brainwashing» — «промивання мізків». За допомогою такого «промивання» може здійснюватися «зомбування» людей, формування пасивної й слухняної істоти, перетворення народу на легко керовану масу. У цьому сенсі, розмови про свободу, демократію, вільні вибори є містифікацією.

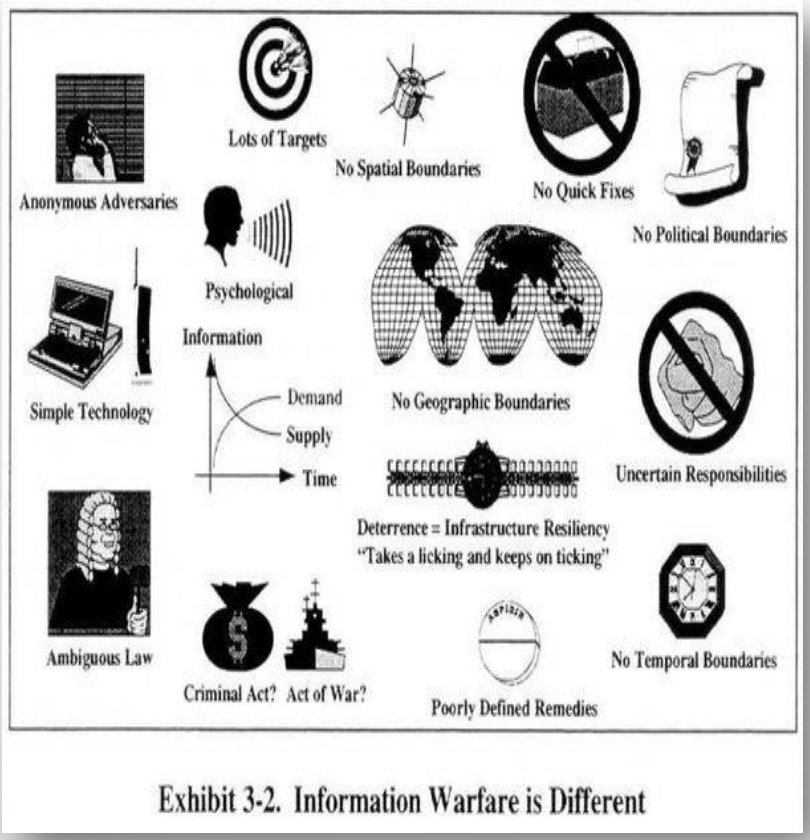
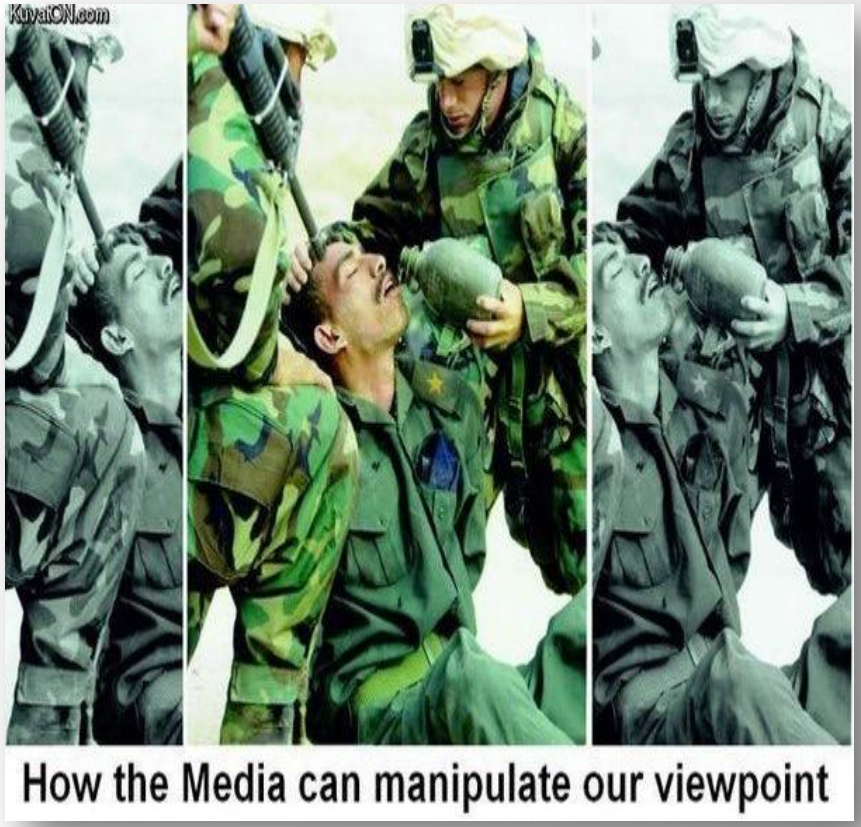


Exhibit 3-2. Information Warfare is Different



How the Media can manipulate our viewpoint

- Як зазначено у Статуті дій у надзвичайних ситуаціях Статті 29: Основним видом зв'язку у ході проведення аварійно- рятувальних та інших невідкладних робіт є радіозв'язок. Радіозв'язок організовується засобами, якими оснащенні підрозділів Оперативно- рятувальної служби цивільного захисту. При ліквідації надзвичайної ситуації радіозв'язок організовується в ультракороткохвильовому та короткохвильовому діапазонах відповідно до схеми організації зв'язку.

- Радіоприймальним пристроєм (РПрП) називається пристрій, **призначений для вловлювання, перетворення й використання електромагнітної енергії радіосигналів, що приходять у пункт прийому.**

РПрП, які використовуються підрозділами МНС України за принципами будови і схемними рішеннями істотно відрізняються від радіомовних. Для них не відіграє головної ролі якість звучання, декоративне оформлення, але принципово важливі такі оперативно - технічні показники:

- **- діапазон робочих частот**

Криптографія-

- (від грецького kryptós — прихований і gráphein — писати) — наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином.

- До початку 30-х рр. остаточно сформувалися розділи математики, які є науковою основою криптології:
- теорія ймовірностей і математична статистика,
- загальна алгебра,
- теорія чисел,
- почали активно розвиватися теорія алгоритмів, теорія інформації, кібернетика.
- Своєрідним вододілом стала робота Клода Шеннона "Теорія зв'язку в секретних системах", яка підвела наукову базу під криптографію і криптоаналіз.
- Етап розвитку криптографії і криптоаналізу до 1949 р. стали називати донауковою криптологією.

- Тривалий час під криптографією розумілось лише *шифрування* — процес перетворення звичайної інформації (*відкритого тексту*) в незрозуміле «сміття» (тобто, *шифротекст*)
- *Дешифрування* — це зворотний процес відтворення інформації із шифротексту. Шифром називається пара *алгоритмів* шифрування/розшифрування.

Енігма-

- (англ. *Enigma*) — шифрувальна машина часів Другої світової війни. Використовувалася для шифрування і дешифрування секретних повідомлень. Точніше, Енігма — це ціла родина електромеханічних роторних машин, що застосовувалися з 20-х років XX століття.

- Енігма використовувалася в комерційних цілях, а також у військових і державних службах в багатьох країнах світу, але найбільшого поширення набула в нацистській Німеччині під час Другої світової війни. Саме Енігма вермахту (Wehrmacht Enigma) — німецька військова модель — найчастіше є предметом дискусій.

- У грудні 1932 польські шифрувальники вперше зламали німецькі військові шифри Енігми. Ця машина отримала погану славу, тому що криптоаналітики антигітлерівської коаліції змогли розшифрувати велику кількість повідомлень, зашифрованих з її допомогою. Спеціально для цих цілей була створена машина з кодовою назвою «Бомба», що надала значну перевагу антигітлерівській коаліції у війні. Уся інформація, отримана криптоаналізом з її допомогою, мала кодову назву ULTRA.

- Хоча з точки зору криптографії шифр Енігми був слабкий, на практиці тільки поєднання цього чинника з іншими, такими як помилки операторів, процедурні вади, припущення про текст повідомлень (наприклад при передачі метеозведень) і захоплення екземплярів Енігми і шифрувальних книг, дозволило розгадувати шифри і читати повідомлення.

Get luck!💖

- Make knowledge not war!

🚀 💣 💥