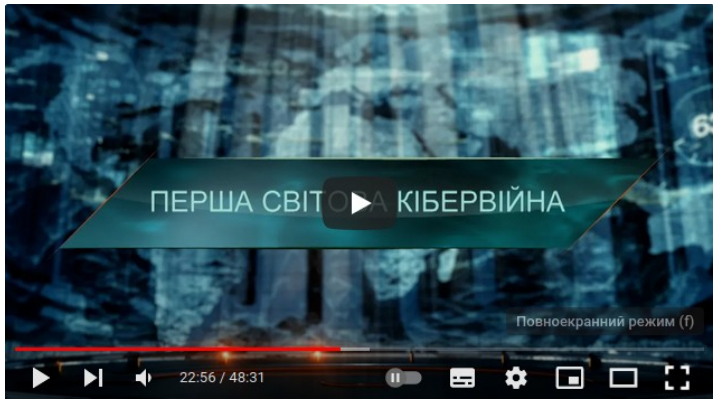
Кібервійни та кібербезпека в сучасному світі

доцент Горбенко В.І.
ауд.19, корп.1

Кібервійська



Війна в Україні впливає на світ

Перша світова кібервійна – Загублений світ.
11 сезон. 29 випуск
https://www.youtube.com/watch?v=S1DCJ2hisM4

16 листопада 2022 Інститут сучасної війни у Вест-Пойнті організував міждисциплінарну дискусію для обговорення того, як війна в Україні змінює або не змінює основні припущення щодо конфлікту в кіберсфері.
У багатьох відношеннях війна в Україні, схоже, підриває припущення про мінливий характер війни, оскільки найбільш вирішальні елементи відбуваються на суші, а не в нових технологічних областях.

Основними питаннями дискусії були:
Якою мірою учасники координували кібероперації з іншими кінетичними та некінетичними військовими операціями?
Чи досягли вони успіху на тактичному чи стратегічному рівні?
Чи відіграють кібероперації важливу роль у сучасних широкомасштабних бойових діях?

Кібервійська

Кібервійськова діяльність використовує комп'ютерні технології та мереж для проведення атак, отримання інформації (її витоку), розвідки, спостереження, впливу на опонента, тощо.

Серед усього можна виділити:
1. **Кібератаки**: різні форми атак, такі як DDoS-атаки, виток інформації, розповсюдження шкідливих програм (вірусів, черв'яків, троянців), тощо. **Головна мета атак**: завдання шкоди системам, порушення функціонування, крадіжка даних або інші цілі. Атаки відповідають стратегічним або тактичним цілям нападника.
2. **Кібершпигунство**: отримання конфіденційної інформації, шпигунства за ворогом або противником, розвідка та здійснення кібероперацій для збору розвідувальної інформації.
3. **Кіберпропаганда**: використання соціальних мереж, медіа-ресурсів та інших кіберканалів для поширення дезінформації, впливу на громадську думку, маніпулювання інформацією та психологічного впливу на супротивника чи цільову аудиторію.
4. **Кіберзахист**: заходи, спрямовані на захист від кіберзагроз, виявлення та відповідь на кібератаки, забезпечення безпеки інформаційних систем, мереж та даних, виявлення та реагування на вразливості.

Кібервійськова діяльність стала важливою складовою стратегічної та тактичної діяльності у сучасному військовому конфлікті. Вона використовується як додатковий інструмент в руках держав та військових формувань для досягнення своїх стратегічних цілей.

Кібервійська США. Загальна характеристика

Структура кібервійських сил США включає кілька військових та цивільних організацій, які відповідають за кібербезпеку, кібервійськову діяльність та захист від кіберзагроз. Основними складовими цієї структури є:

1. **Кіберкомандування Сполучених Штатів (USCYBERCOM)**: Це центральне командування, яке відповідає за кібервійську діяльність та кіберзахист у військовій сфері США. USCYBERCOM координує дії з кібербезпеки та ведення кібероперацій разом зі збройними силами та іншими військовими структурами.
2. **Національне агентство з кібербезпеки та інфраструктури (CISA)**: Це агентство в межах Міністерства національної безпеки, яке відповідає за захист критичної інфраструктури та координацію кіберзаходів в цивільній сфері.
3. **Військові кібервійськові частини**: Крім USCYBERCOM, кібервійська діяльність також проводиться в межах окремих видів військ, таких як Армія США (Army Cyber Command), ВМС США (U.S. Fleet Cyber Command / U.S. 10th Fleet), Авіація США (Air Force Cyber Command) та Морська піхота США (Marine Corps Cyberspace Command).
4. **Кіберцентри національних розвідувальних агентств**: Розвідувальні агентства, такі як Національне управління з розвідки (National Security Agency, NSA) та Центральне розвідувальне управління (Central Intelligence Agency, CIA), мають свої кіберцентри, які займаються збором інформації, розвідкою та проведенням кібероперацій за кордоном.
5. **Приватний сектор**: Багато компаній, особливо ті, які забезпечують критичну інфраструктуру, таку як енергетика, транспорт, фінанси тощо, мають свої власні команди та фахівців з кібербезпеки, які працюють на захист від кіберзагроз.

Кібервійська

Кібервійська США мають розгалужену структуру і свої підрозділи в різних родах військ.
Внутрішне забезпечення включає два підрозділи: кіберкомандування США (USCYBERCOM) та спільна робоча група ARES.

Кіберкомандування США (USCYBERCOM) - одне з одинадцяти уніфікованих підрозділів командування Міністерства оборони США. Відповідає за операцій у кіберпросторі, зміцнення захисту кіберпростору Міністерства оборони, інтеграції та розширенню кібернетичний досвіду Міністерства оборони.

USCYBERCOM був створений в середині 2009 року в штаб-квартирі Агентства національної безпеки (NSA) у Форт Джордж Г. Мід, штат Меріленд. Він співпрацює з мережами АНБ і одночасно очолюється директором Агенції національної безпеки з моменту його створення (генерал Пол Накасоне). Спочатку створений задля вирішення задач оборони, але тепер розглядається і як наступальна сила. З 2018 року USCYBERCOM підвищено до статусу повноцінної та незалежної єдиної команди командного складу.

У його складі: U.S. Army Cyber Command, Fleet Cyber Command (10th Fleet), Sixteenth Air Force (Air Forces Cyber), Marine Corps Forces (Cyberspace Command).

Кібервійська

USCYBERCOM має на меті керувати, синхронізувати та координувати планування та операції в кіберпросторі для захисту та просування національних інтересів у співпраці з внутрішніми та міжнародними партнерами.

Основні напрямки:

- захист департаменту оборонної інформаційної мережі (DoDIN)
- надання командирам бойових дій виконання своїх місій по всьому світу
- посилення здатності нації протистояти та реагувати на кібератаки.

Командування уніфікує напрямок операцій у кіберпросторі, зміцнює можливості Міністерства оборони у кіберпросторі, інтегрує та зміцнює кібернетичний досвід Міністерства оборони. USCYBERCOM вдосконалює можливості Міністерства оборони США для роботи стійких, надійних інформаційних та комунікаційних мереж, протидіє загрозам кіберпростору та забезпечує доступ до кіберпростору. USCYBERCOM розробляє структуру кіберсил, вимоги до підготовки та стандарти сертифікації, які дозволять Службам створювати кіберсили, необхідні для виконання певних місій. Командування також тісно співпрацює з міжвідомчими та міжнародними партнерами у виконанні цих критичних місій.

Cyber Mission Force (CMF)

Cyber Mission Force (CMF) є основним оперативним компонентом Кіберкомандування США (USCYBERCOM), який створено для виконання конкретних завдань у кіберпросторі. CMF було офіційно сформовано у 2013 році з метою структурувати та уніфікувати кібероперації Міністерства оборони США (DoD). Діяльність CMF охоплює як захисні, так і наступальні операції, а також підтримку національної безпеки та військових операцій. До складу входить приблизно 6 200 осіб.

CMF складається з 133 команд, які поділено на три основні категорії та виконують різні функції:

- Національні команди (National Mission Teams), 13 команд: Захист США від стратегічних кіберзагроз, які можуть вплинути на національну безпеку, критичну інфраструктуру (енергетика, фінанси, транспорт) або урядові системи. Фокусуються на протидії атакам від державних акторів (наприклад, Росії, Китаю, Ірану, Північної Кореї). Працюють у тісній координації з NSA для розвідки та аналізу загроз. Приклади діяльності: відбиття атак на вибори, протидія кампаніям дезінформації або операціям типу SolarWinds.
- Бойові команди (Combat Mission Teams), 68 команд: Інтеграція кібероперацій у військові дії, підтримка бойових командувань (наприклад, CENTCOM, INDOPACOM) і проведення наступальних операцій. Діють у координації з традиційними військовими операціями, наприклад, для виведення з ладу ворожих командних систем або комунікацій. Можуть виконувати як наступальні (атакувати ворожі мережі), так і оборонні (захист власних сил) функції. Приклади: операції проти ІДІЛ у 2016 році, коли CMT виводили з ладу їхні пропагандистські платформи.
- Команди захисту (Cyber Protection Teams), 52 команди: Захист мереж Міністерства оборони (DoD Information Network, DoDIN), а також допомога у захисті критичної інфраструктури США за потреби. Здійснюють моніторинг, виявлення та реагування на кіберінциденти в реальному часі. Працюють як "цифрові пожежники", усуваючи загрози всередині мереж DoD. Приклад: реагування на атаки типу ransomware або захист від витоку даних. Підтримка: Співпрацюють з JFHQ-DoDIN (Департамент оборони інформаційної мережі) для повсякденного управління мережами.

Усі команди укомплектовані як військовими, так і цивільними фахівцями.

Cyber Mission Force (CMF)

Організація та управління

- Командна структура: Кожна команда CMF має чітку ієрархію — командир, аналітики, оператори, спеціалісти з криптографії та інженери мереж.
- Розташування: Команди розподілені по ключових військових базах США, таких як Форт Мід (Меріленд), Форт Гордон (Джорджія), база Лекленд (Техас), але можуть бути розгорнуті в будь-якому регіоні світу.
- Тренування: Персонал проходить підготовку в Cyber Training Ranges — спеціальних симуляційних полігонах, де відтворюються реальні кіберсередовища. Програма підготовки стандартизована через Joint Cyber Training and Certification Standards (JCT&CS).

Функціональні особливості

Оборонні операції (Defend):
- Моніторинг мереж DoD (понад 15 000 мереж і 3 мільйони пристроїв).
- Виявлення та нейтралізація вразливостей (наприклад, через платформи типу ACAS або HBSS).
- Реагування на інциденти в реальному часі.

Наступальні операції (Attack):
- Розробка та використання кіберзброї (наприклад, Stuxnet-подібних інструментів).
- Атаки на ворожі системи управління, інфраструктуру чи пропагандистські ресурси.
- Координація з NSA для впровадження експлойтів.

Підтримка (Support):
- Забезпечення розвідданими інших командувань.
- Співпраця з цивільними агентствами (DHS, FBI) у разі загроз національній інфраструктурі.

USCYBERCOM (Кіберкомандування Сполучених Штатів) проводить широкий спектр операцій в кіберпросторі для забезпечення кібербезпеки, ведення кібервійни та захисту національних інтересів США.

Основу операцій включають:

1. **Захист від кібератак**: пошук, виявлення і відвернення кібератак на інфраструктуру, мережі та інформаційні системи США та їх партнерів. Це може включати розробку та застосування заходів кіберзахисту, виявлення та реагування на вразливості, а також аналіз кіберзагроз.
2. **Кібероперації**: кібероперації проводяться з метою підтримки військових операцій, розвідки, пошуку, протидії ворожим кіберзагрозам та забезпечення військової переваги у кіберпросторі.
3. **Кіберрозвідка**: USCYBERCOM здійснює кіберрозвідку для збору інформації про ворожі інформаційні системи, мережі, кіберзагрози та потенційні цілі у кіберпросторі, що можуть бути використані для подальших операцій.
4. **Відповідь на кібератаки**: У разі кібератаки на США або її союзників, USCYBERCOM може розробляти та застосовувати відповідні кібероперації для зменшення шкоди, протидії атакуючим та відновлення нормального функціонування інфраструктури.
5. **Партнерство та співпраця**: співпраця з іншими військовими командуваннями, урядовими агентствами, союзниками та партнерами для обміну інформацією, спільних навчань та спільних операцій з метою підвищення кібербезпеки та захисту в кіберпросторі.

Загалом, USCYBERCOM веде різноманітні операції у кіберпросторі з метою забезпечення безпеки та захисту національних інтересів США.

Кібервійська

Підрозділ кіберкомандування армії США інтегрує та проводить операції з кіберпростором повного спектру, радіоелектронну боротьбу та інформаційні операції, забезпечуючи свободу дій дружнім силам у кіберпросторі, в інформаційному середовищі та за його межами, захищаючі від противників.

Кіберкомандування флоту США (FCC) Десятий флот (C10F) має рівень оперативних сил, що складаються з понад 14 000 активних і резервних моряків та цивільних осіб, об'єднаних у 28 діючих команд, 40 підрозділів Сил кібермісії та 27 команд резерву по всьому світу. Кіберкомандування флоту США підпорядковується безпосередньо начальнику військово-морських операцій і відповідає за операції з інформаційною мережею ВМС, наступальні та оборонні операції в кіберпросторі, космічні операції та розвідку сигналів. Кіберкомандування флоту США виконує функції командування військово-морським компонентом Американського кіберкомандування, космічного компоненту ВМС - Стратегічного командування США, а також командуючого криптологічним компонентом служби ВМС під Агентством національної безпеки / Центральної служби безпеки. Десятий флот США є оперативним підрозділом Кіберкомандування флоту і виконує свою місію через структуру оперативної групи, подібну до інших командуючих військовими діями.

Агентство з кібербезпеки та інфраструктури (CISA) є частиною Міністерства внутрішньої безпеки (DHS), виконує широкий спектр операцій у кіберпросторі для забезпечення безпеки інформаційних систем, критичної інфраструктури та захисту від кіберзагроз. Створено у 2018 р. Грає роль національного координатора безпеки і стійкості критичної інфраструктури.

Основу операцій включають:

1. **Моніторинг та аналіз загроз**: здійснення моніторингу кіберзагроз та проведення аналізу їхніх характеристик, таких як методи атак, використовувані вразливості, цілі та наміри атакуючих. Це допомагає ідентифікувати потенційні загрози та вживати заходів для їхнього запобігання.
2. **Попередження та реагування на кіберінциденти**: CISA співпрацює з державними органами, приватним сектором та іншими партнерами для реагування на кіберінциденти, включаючи атаки на критичну інфраструктуру та державні установи. Агентство надає допомогу у виявленні, аналізі та ліквідації кіберподій та сприяє відновленню пошкоджених систем.
3. **Розробка та поширення кіберзаходів**: розробляються та розповсюджуються кіберзаходи, такі як патчі, керівництва з кібербезпеки та інші рекомендації для захисту інформаційних систем від вразливостей та загроз.

Співпраця та партнерство: CISA співпрацює з федеральними, місцевими та приватними секторами, а також з міжнародними партнерами для обміну інформацією, спільної практики та координації дій у сфері кібербезпеки.

Сприяння кібернавчанням та освітою: CISA проводить навчальні заходи, тренінги та освітні програми для різних аудиторій, включаючи державні установи, підприємства та громадян, з метою підвищення обізнаності та відповідальності у сфері кібербезпеки.

У цілому, CISA виконує важливу роль у захисті інфраструктури та інформаційних систем США від кіберзагроз, а також у реагуванні на кіберінциденти та сприянні підвищенню кібербезпеки у всіх секторах економіки.

Аспект	CMF	CISA
Організаційна приналежність	Частина USCYBERCOM, Міністерство оборони	Частина DHS, цивільне агентство
Основний фокус	Військові кібероперації, національна безпека	Захист критичної інфраструктури, цивільні сектори
Тип діяльності	Оборонні та наступальні операції	Управління ризиками, реагування, інформаційний обмін
Приклади діяльності	Захист мереж DoD, підтримка бойових операцій	Навчання Cyber Storm, директиви про загрози
Співпраця	Обмін інформацією з CISA для захисту інфраструктури	Координація з приватним сектором, обмін інформацією з CMF

Кібервійська

Шістнадцята ВПС (Cyber Air Force), штаб-квартира якої знаходиться на Об'єднаній базі Сан-Антоніо-Лакленд, штат Техас, є першою у своєму роді Нумерованою ВПС. Вона інтегрує можливості розвідки, спостереження та розвідки, кібервійни, радіоелектронної боротьби та інформаційних операцій у континуумі конфлікту, щоб забезпечити швидкість, летальність і повну інтеграцію ВПС.

Командування кіберпростором сил морської піхоти призначено забезпечити проведення повного спектру операцій в кіберпросторі, включати експлуатацію та захист Корпоративної мережі морської піхоти (MCEN), проведення оборонних операцій в кіберпросторі в межах мереж MCEN та Об'єднаних сил, а також, за призначенням, проведення наступальних операцій в кіберпросторі на підтримку Об'єднаних сил та Коаліції; для того, щоб забезпечити свободу дій у всіх сферах ведення бойових дій, і захист від противника.

Кібервійська

Армія США має наступні кіберпідрозділи:

- U.S. Army Cyber Command
- U.S. Army Network Enterprise Technology Command
- 1st Information Operations Command (Land)
- 1st Information Operations Battalion
- 2nd Information Operations Battalion
- 780th Military Intelligence Brigade (Cyber) “Pretorians”
- 781st Military Intelligence Battalion “Vanguard”
- 782nd Military Intelligence Battalion “Cyber Legion”
- 915th Cyber Warfare Battalion
- Cyber Solutions Development Detachment
- Task Force Echo (Army Reserve)

Кібервійська

Військовий Резерв має у своєму складі кіберпідрозділи:

- Cyber Protection Brigade
  - North East Cyber Protection Center
    - Cyber Protection Team 180
    - Cyber Protection Team 181
  - National Capital Region Cyber Protection Center
    - Cyber Protection Team 182
    - Cyber Protection Team 183
  - South West Cyber Protection Center
    - Cyber Protection Team 184
    - Cyber Protection Team 185
  - North Central Cyber Protection Center
    - Cyber Protection Team 186
    - Cyber Protection Team 187
  - Western Cyber Protection Center
    - Cyber Protection Team 188
    - Cyber Protection Team 189
  - Arizona Cyber Warfare Range

Кібервійська

Кіберпідрозділи Армійської Національної Гвардії:

- 91st Cyber Brigade (Virginia NG)
  - 123rd Cyber Protection Battalion (Virginia NG)
  - 124th Cyber Protection Battalion (Virginia NG)
  - 125th Cyber Protection Battalion (South Carolina NG)
  - 126th Cyber Protection Battalion (Massachusetts NG)
  - 127th Cyber Protection Battalion (Indiana NG)
  - Cyber Protection Team 169 (Maryland NG)
  - Cyber Protection Team 170 (Georgia NG)
  - Cyber Protection Team 171 (California NG)
  - Cyber Protection Team 172 (Michigan NG)
  - Cyber Protection Team 173 (New York NG)
  - Cyber Protection Team 174 (Utah NG)
  - Cyber Protection Team 175 (Kentucky NG)
  - Cyber Protection Team 176 (Illinois NG)
  - Cyber Protection Team 177 (Minnesota NG)
  - Cyber Protection Team 178 (Mississippi NG)
  - Cyber Protection Team 179 (Nebraska NG)
- Defensive Cyber Operations Element (Colorado NG)
- Defensive Cyber Operations Element (Pennsylvania NG)
- Defensive Cyber Operations Element (West Virginia NG)
- Cyber Mission Assurance Team (Ohio NG)
- Cyber Mission Assurance Team (Washington NG)

Кібервійська

ВМС США

U.S. Fleet Cyber Command – Tenth Fleet
- Naval Network Warfare Command (Task Force 1010)
- Navy Cyber Defense Operations Command (Task Force 1020)
- Cryptological Warfare Group Six (Task Force 1060)
  - Cyber Strike Activity Sixty Three
  - Cyber Defense Activity Sixty Four, включає також:
    - Cyber Defense Activity Sixty Four - Detachment 1 (U.S. Navy Reserve)
- Naval Cyber Warfare Development Group (Task Force 1090)
- Navy Information Operations Command Texas (Task Force 1040)
- Navy Information Operations Command Georgia (Task Force 1050)
- Navy Information Operations Command Hawaii (Task Force 1070)
- Navy Information Operations Command Colorado (Task Group 101)
- Navy Information Operations Command Whidbey Island (Task Group 102)
- Navy Information Operations Command Pensacola (Task Group 103)

Кібервійська

ВПС США

Sixteenth Air Force (Air Force Cyber)
- Cyberspace Capabilities Center
- 67th Cyberspace Wing
  - 67th Operations Support Squadron (ACC)
  - 67th Cyberspace Operations Group
    - Cyberspace Operations Squadron 91st, 315th, 352nd, 390th
  - 318th Cyberspace Operations Group
    - 39th Information Operations Squadron
    - 90th Cyberspace Operations Squadron ”Shadow Warriors”
    - 318th Range Squadron
    - 346th Test Squadron
  - 567th Cyberspace Operations Group
    - Cyberspace Operations Squadron 92nd,833rd,834th,835th,836th,837th
- 688th Cyberspace Wing
  - 688th Operations Support Squadron
  - 26th Cyberspace Operations Group
    - 26th Network Operations Squadron
    - Network Warfare Squadron 33rd,68th
  - 690th Cyberspace Operations Group
    - Network Operations Squadron 83rd,561st
    - 690th Cyberspace Operations Squadron
    - 690th Intelligence Support Squadron
    - 690th Network Support Squadron
    - 691st Cyberspace Operations Squadron

Кібервійська

Морська піхота США

- Marine Corps Forces Cyberspace Command
  - Marine Corps Cyberspace Operations Group
  - Marine Corps Cyberspace Warfare Group
- Marine Forces Reserve
  - Defensive Cybersecurity Operations Company A
  - Defensive Cybersecurity Operations Company B

Берегова охорона

- U.S. Coast Guard Cyber Command
- U.S. Coast Guard Office of Cyberspace Forces