Кібервійни та кібербезпека в сучасному світі

доцент Горбенко В.І.
ауд.19, корп.1

Доповнення до модулю 1
Кібервійна та кібербезпека

Поділ між інформаційними війнам та кібервійнами почався у першій декаді 2000-х років і є загальним стандартом для військових та фахівців з інформаційних технологій та безпеки.

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.

Доповнення до модулю 1
Кібервійна та кібербезпека

Інформаційна війна — це міждержавне протиборство в інформаційному просторі з метою нанесення збитку інформаційним системам, процесам та ресурсам, критично важливим структурам; для підриву політичної, економічної та соціальної системи; масованої психологічної обробки населення; для дестабілізації суспільства та держави, а також примушення держави до прийняття рішення на користь супротивника.
У книжці "The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests" наведено, що 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.

Центр протидії дезінформації https://cpd.gov.ua/reports/

Аналітичний звіт «Кампанія інформаційного впливу в африканському інформаційному просторі» (8 березня 2024)

Доповнення до модулю 1
Кібервійна та кібербезпека

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.

Кібервійська РФ

Структура кібервійських сил Російської Федерації включає кілька військових та спеціальних організацій, які відповідають за кібербезпеку, кібервійну діяльність та захист від кіберзагроз.
Основними складовими цієї структури є:
1. Міністерство оборони Російської Федерації (МО РФ): В МО РФ діє Головне управління забезпечення бойових дій (ГУСВБ), в межах якого існує служба кібервійських військ.
2. Федеральна служба безпеки Російської Федерації (ФСБ): ФСБ займається захистом національної безпеки, в тому числі в кіберпросторі. У ФСБ також існують підрозділи, що спеціалізуються на кібербезпеці та кібервійських операціях.
3. Міністерство внутрішніх справ Російської Федерації (МВС РФ): МВС має свої власні структури, які займаються боротьбою з кіберзлочинністю, в тому числі проведенням розслідувань кіберзлочинів та забезпеченням кібербезпеки.
4. Міністерство комунікацій та масових комунікацій Російської Федерації (Минкомсвязь Росії): Минкомсвязь займається регулюванням та контролем в сфері зв'язку та інформаційних технологій, включаючи питання кібербезпеки.
5. Російські розвідувальні агентства: Російські розвідувальні служби, такі як Головне розвідувальне управління Генерального штабу Збройних Сил РФ (ГРУ), Служба зовнішньої розвідки Росії (СВР РФ), також ведуть свою діяльність в кіберпросторі та можуть займатися кібервійськими операціями.
6. Приватний сектор та групи хакерів: Поза державними структурами, у Росії існує ряд приватних компаній та незалежних груп хакерів, які можуть бути втягнуті в кібервійську діяльність на різних рівнях.

Кібервійська

РФ

Війська інформаційних операцій
- Західний військовий округ, центр кіберзахисту
- Південний військовий округ, центр кіберзахисту
- Центральний військовий округ центр кіберзахисту
- Східний військовий округ центр кіберзахисту
- Об’єднане стратегічне командування “Північний флот” центр кіберзахисту
- Центр спеціальних розробок Міністерства оборони

Шосте Управління - Головне управління Генерального штабу
- 85-й головний центр спеціальної служби — Військова частина 26165
- Головний центр спеціальних технологій — Військова частина 74455

Кібервійська Китаю

Структура кібервійських сил Китаю є складною і включає кілька військових, розвідувальних та цивільних організацій, які відповідають за кібербезпеку, кібервійну діяльність та захист від кіберзагроз.

Основними складовими цієї структури є:
1. **Стратегічне кіберкомандування Народно-визвольної армії Китаю (PLA)**: Це військове командування в межах Народно-визвольної армії Китаю, яке відповідає за кібервійську діяльність та кіберзахист. Воно координує дії з кібербезпеки та ведення кібероперацій разом з іншими військовими структурами.
2. **Міністерство державної безпеки Китаю (MSS)**: MSS є головним розвідувальним агентством Китаю, яке також відповідає за контррозвідку та кібервійну діяльність. Воно займається захистом національної безпеки, в тому числі в кіберпросторі.
3. **Інформаційне міністерство Китаю (MIC)**: MIC відповідає за управління та регулювання інформаційних технологій, включаючи питання кібербезпеки та кібервійськості.
4. **Цивільні кібербезпечні органи**: Крім військових та розвідувальних структур, у Китаї також існують цивільні органи, які займаються кібербезпекою та кібервійною діяльністю. Наприклад, Центр кібербезпеки Китаю (China Cybersecurity Center) та інші.
5. **Приватний сектор та хакерські групи**: Поза державними структурами, у Китаї також існують приватні компанії та незалежні хакерські групи, які можуть бути втягнуті в кібервійну діяльність на різних рівнях.

Кібервійська

Кібервійська Китаю входять до складу Народної визвольної армії Китаю (НВАК).

People's Liberation Army Strategic Support Force (人民解放军战略支援部队)
People's Liberation Army Network System Department (人民解放军网络系统部)
Unit 61786 (61786 部队 - 61786 Bùduì)
57th Jiangan Computing Technologies Institute (第 56 江南计算技术研究所)
Cyberspace Security Academy (网络空间安全学院)

Розвиток китайських кібервійськ відповідає п’ятнадцатирічній стратегії інформатизації Китаю. Вона вміщує питання використання кіберзасобів для національної безпеки. Відповідно до документу «Enter the Cyber Dragon» структурно кібервійська Китаю зосереджені у Другому, Третьому та Четвертому департаментах НВАК. Вирішальну роль грає Третій департамент, який забезпечує кібершпіонаж та кіберконтррозвідку, а Четвертий департамент відповідає за атаки на комп’ютерні мережі.

Крім державних кібервійськ, відповідні підрозділи НВАК взаємодіють з Red Hacker Alliance. RHA є неформальною мережею хакерів, але із загальним керівництвом держави, включає десятки тисяч хакерів із самого Китаю та з інших держав, з китайської діаспори.

Основною місією Сил стратегічної підтримки НВАК є підтримка бойових дій, щоб НВАК могла отримати регіональні переваги в сферах космічної війни та кібервійни, а також забезпечити безперебійну роботу.

Функціонально та структурно Сили стратегічної підтримки діють як ракетні війська Народно-визвольної армії. Він формується з підрозділів, відповідальних за космос, кібер- та електронну війну в колишньому Департаменті Генерального штабу (включаючи можливості кібершпигунства колишнього Третього департаменту, заходи електронної підтримки колишнього Четвертого департаменту та космічну ISR систем та аерокосмічного розвідувального бюро та головного супутникового терміналу), загальнополітичного управління та департаменту загального озброєння (включаючи пускові установки, засоби телеметрії, спостереження та управління та науково-дослідні та дослідницькі організації). Вважається, що він має щонайменше 5 відділів, хоча в західних коментарях існували суперечки щодо існування можливого шостого відділу, присвяченого обладнанню.

Space Systems Department

Jiuquan Satellite Launch Center / 20th Testing and Training Base
Taiyuan Satellite Launch Center / 25th Testing and Training Base
Xichang Satellite Launch Center / 27th Testing and Training Base
Wenchang Aerospace Launch Site
Space Telemetry, Tracking, and Control
Beijing Aerospace Flight Control Center
Xi’an Satellite Control Center / 26th Testing and Training Base
Telemetry, Tracking, and Control Stations
China Satellite Maritime Tracking and Control Department
23rd Testing and Training Base
Aerospace Reconnaissance Bureau
Satellite Main Station
Aerospace Research and Development Center
Project Design Research Center
Astronaut Corps

Network Systems Department

Департамент мережевих систем PLASSF являє собою інтеграцію всіх можливостей щодо інформації про НВК та кібервійни, і, як вважають, він перебрав багато можливостей, які раніше мали Третій та Четвертий відділи НВАК. Станом на 2018 рік його очолював генерал-лейтенант Чжен Цзюньцзе, а генерал-лейтенант Чай Шаолінг був політичним комісаром, обидва з яких також є членами 13-го Національного народного конгресу. Під його контролем, поряд з численними військовими базами, розповсюдженими по всьому Китаю, знаходиться кафедра, що називається "Інженерно-технічний університет", який, у свою чергу, має під своїм контролем численні військові академії навколо Китаю.

Список військових баз за РНБ:

- Notional Base 31, Nanjing
- Notional Base 32, Guangzhou
- Notional Base 33, Chengdu
- Notional Base 34, Shenyang
- Notional Base 36, Beijing
- Notional Base 38, Kaifeng

Крім того, є військові академії та інші департаменти, які перебувають під контролем IEU

Науково-дослідний відділ S&T (科研 部)

Навчальний відділ (训练 部)
Академія командних інформаційних систем (指挥 信息 系统 学院)
Академія електронних технологій (电子 技术 学院)
Академія шифрувальної техніки (密码 工程 学院)
Лоянська академія іноземних мов (洛阳 外国语 学院)
Академія геопросторової інформації (地理 空间 信息 学院)
Академія безпеки кіберпростору (网络 空间 安全 学院)
Академія судноплавства та аерокосмічних цілей (导航 与 空 天 目标 工程 学院)
Академія базової освіти командира (指挥 军官 基础 教育 学院)
Академія блокчейнів (区块 链 研究院 ; розташована в Шеньчжені).

Китай розроблює кібер зброю для захоплення супутників

https://www.ft.com/content/881c941a-c46f-4a40-b8d8-9e5c8a6775ba

Китай розробляє кіберзброю, яка дозволить йому захоплювати під свій контроль супутники інших країн, позбавляючи їх спроможності передавати дані. Про це пише Financial Times з посиланням на “злиті” дані Пентагону. Документи Міноборони США свідчать про те, що китайські розробники, імітуючі сигнали, які супутники одержують від своїх операторів, змушують їх дати збій або повністю перехоплюють контроль над ними. У звіті наголошується, що завдяки цій технології КНР буде здатен “захоплювати контроль над супутниками, що зробить їх неефективним для підтримки систем зв’язку, зброї, спостереження та розвідки”.

У США вважають, що Китаю вдалось досягнути значного прогресу у розвитку військових космічних технологій, у тому числі в галузі супутникового зв’язку.

У березні 2023 року командувач Космічними силами США генерал-лейтенант Бредлі Чанс Зальцман американському Конгресу, що Пекін агресивно використовує свої можливості, намагаючись реалізувати свою “космічну мрію” стати передовою державою за межами земної атмосфери до 2045 року. “Китай продовжує агресивно інвестувати в технології, призначені для порушення, деградації та знищення наших космічних можливостей”, – сказав тоді він.

За його словами, КНР має загалом 347 супутників на орбіті, які може використовувати для “моніторингу, відстеження, націлювання та нападу на сили США у будь-якому майбутньому конфлікті”.

Кібервійська Ірану

Іран швидко вдосконалив свої кібернетичні можливості. Він все ще не входить до найвищого рангу кібердержав, але за стратегією та організацією для кібервійни випереджає більшість країн. Іран високо оцінює корисність кіберсистем як інструменту національної сили. Його великий досвід у прихованій діяльності допомагає керувати його стратегією та операціями, використовуючи кіберсистеми як інструмент примусу та сили, і він створив витончену організаційну структуру для управління кіберконфліктом. Це означає, що будь-який напад на США буде не випадковим, а частиною розширеної стратегії протистояння.

Іран розглядає кібератаки як частину асиметричного військового потенціалу, необхідного йому для протистояння США. Розвиток Іраном кібер-влади є реакцією на його вразливість. Іран є регулярною мішенню іноземного кібершпигунства. Іран та Ізраїль беруть участь у не завжди прихованому кіберконфлікті. Stuxnet, кібератака на об'єкти ядерної зброї в Ірані, прискорила власні зусилля Ірану в галузі кіберозброєння. Однак найбільше побоюються лідери Ірану - власного населення та ризику, що Інтернет розкриє щось на зразок Арабської весни. Іранські сили безпеки почали розвивати свої хакерські здібності під час «Зеленої революції» 2009 року для розширення внутрішнього нагляду та контролю. Ці внутрішні зусилля є корінням кібер-можливостей Ірану.

Кібервійська Ірану

Структура кібервійських сил Ірану складається з кількох військових та розвідувальних організацій, які відповідають за кібербезпеку, кібервійну діяльність та захист від кіберзагроз.

Основними складовими цієї структури є:

1. **Корпус стражів ісламської революції (IRGC)**: IRGC володіє власними кібервійськовими силами, які відомі як "Кібервійськові сили IRGC" (IRGC Cyber Forces). Вони відповідають за кібербезпеку, кібервійськову діяльність та кіберзахист у межах IRGC.
2. **Міністерство інформаційних технологій та зв'язку (ICT)**: ICT відповідає за управління та регулювання інформаційних технологій, включаючи питання кібербезпеки та кібервійськової діяльності, а також забезпечує координацію зусиль з кібербезпеки на рівні держави.
3. **Міністерство розвідки Ірану (VAJA)**: VAJA відповідає за розвідку та контррозвідку, включаючи діяльність у кіберпросторі. Ймовірно, VAJA має свої кібервійськові підрозділи для проведення кібероперацій.
4. **Іранські розвідувальні агентства**: Як і в інших країнах, в Ірані також існують розвідувальні служби, які можуть мати свої власні кібервійськові підрозділи або співпрацювати з іншими організаціями для проведення кібероперацій.
5. **Приватний сектор**: Багато компаній та організацій в Ірані також займаються кібербезпекою та можуть брати участь у захисті від кіберзагроз та кібервійськовій діяльності.

Приклад Ірану показує, як слабкіший противник може перерозподілити ресурси так, щоб побудувати кіберсилу. Три військові організації відіграють провідну роль у кіберопераціях: Іранський корпус революційної гвардії (IRGC), Басідж та іранська "Організація пасивної оборони (NPDO)". IRGC є виконавцем низки інцидентів, спрямованих на американські цілі, ізраїльську критичну інфраструктуру, Саудівську Аравію та інші держави Перської затоки. Басідж, цивільна воєнізована організація, підконтрольна IRGC, керує, як вважають лідери Басідж, 120 000 добровольців з кібервійни. Кількість, ймовірно, перебільшена, але Басідж використовує свої зв'язки з університетами та релігійними школами, щоб набрати довірену хакерську групу. NPDO відповідає за захист інфраструктури. Щоб забезпечити координацію між кіберзлочинністю та обороною, верховний лідер Алі Хаменеї створив «Вищу раду кіберпростору», до складу якої входять вищі військові та розвідники.

Взаємодія із Ізраїлем та Саудівською Аравією вплинули на покращення кіберпотужності Ірану, а досвід негласних дій дає Ірану можливість зрозуміти, як кібератаки вписуються у загальну військову картину. Інструменти, якими користується Іран, - це, як правило, модифікована шкідлива програма з кримінального ринку, яка не має руйнівного ефекту більш досконалої кібер-зброї. Як заявив ізраїльський генерал у 2017 році, "вони не є найсучаснішими, вони не є найсильнішою наддержавою в кібервимірі, але вони стають все кращими і кращими".

Іран розглядає кібератаки як частину конфлікту. Заступник командувача IRGC Хоссейн Саламі дав наступну характеристику стану в державі: "Ми знаходимося в атмосфері повномасштабної розвідувальної війни із США та фронтом ворогів Революції та ісламської системи ... Ця атмосфера є поєднанням психологічної війни та кібероперацій, військових провокацій, публічної дипломатії та тактика залякування".

Іран дослідив критичну інфраструктуру США в якості цілей, але успішність кібератаки не має певних гарантій. Так масові напади Ірану проти основних банків у 2011-2013 роках зараз будуть малоефективними, тому що їх захист постійно поліпшується. Найбільш складні види кібератак (такі як Stuxnet або російські дії в Україні) все ще виходять за межі іранських можливостей, але слабо захищені цілі в США є вразливими - менші банки або місцеві енергетичні компанії, які мають слабкий захист систем управління трубопроводами. Що зупиняє дії Ірану, це не брак цілей, а питання щодо корисності таких атак.

Наскільки ймовірний напад на США? Рішення щодо кібератаки на США буде залежати від іранських розрахунків ризику та зворотньої реакції США. Як правило іранці проникливі та розважливі в таємних діях і будуть розглядати способи покарання США, яке б не викликало зворотньої насильницької реакції. Кібернетичні дії Ірану проти американських цілей - дії проти великих банків або більш шкідливу атаку на казино Sands. Такі іранські атаки зроблено, щоб показати, що Сполучені Штати не є невразливими, але з бажанням уникнути ескалації конфлікту і недопустити збільшення присутності США в регіоні. Також на меті є демонстрація як власним громадянам, так і сусідам із Перської затоки, що США можуть бути оскаржені. Якщо Іран дійсно діє у Сполучених Штатах, відключаючі казино, це важливо, але не критично. Втручання у роботу електромережі або руйнування трубопроводу може привести до перетину червоної лінії.

Це простір для конфліктів, де правила незрозумілі, а ризики не виміряні.