Ofenzivna sigurnost

Manevriranje

Eno Peršić 19.1.2026

Pregled predavanja

- Motivacija
- Povijest i definicija manevra
- Karakteristike kibernetičkog manevra
- Ofenzivni i defenzivni oblici
- Allenov model shema manevra
- Suverenitet i pravni izazov
- Zaključak

Motivacija

- Cyberspace kao peta domena ratovanja (uz kopno, more, zrak i svemir).
- Stanje stalnog sukoba (države, nedržavni akteri, privatni entiteti).
- Utjecaj na kritičnu infrastrukturu i nacionalnu sigurnost.

Pitanja za ispite

- Kako se definira kibernetički manevar u odnosu na kinetički?
- Nabrojite barem tri ključne karakteristike kibernetičkog manevra.
- Nabroji 3 vrste ofenzivnih manevara.
- U koliko kategorija je Dr.Allen podijelio kibernetičke manevre?
- Navedite jedan primjer sheme manevra.

Klasični manevar

- Manevar je vojna strategija koja podrazumijeva plansko kretanje snaga radi stjecanja povoljnog položaja u odnosu na neprijatelja.
- Izbjeći frontalni sukob i ostvariti prednost kroz iznenađenje, obuhvat, zaobilaženje ili napad na slabije točke protivnika

Definicija kibernetičkog manevra

- Primjena sile za zauzimanje, prekid ili manipulaciju resursima radi postizanja prednosti
- U cyberspaceu se ne kreću postrojbe, već se "točka napada" pomiče na virtualnu lokaciju.
- Cilj: Fizička, tehnička i kognitivna prednost nad protivnikom.

Karakteristike kibernetičkog manevra (1)

- Brzina i doseg
- **Brzina:** Akcije brzinom stroja, reakcije brzinom čovjeka (analiza).
- **Doseg:** Gotovo neograničen; geografska udaljenost je nebitna, ograničena samo sposobnošću prikrivanja.

Karakteristike kibernetičkog manevra (2)

- Pristup i evolucija:
- **Pristup:** Kontrola čvorova je ekvivalent izgradnji isturenih baza u ratu.
- **Dinamika:** Tehnologija se stalno mijenja; TTP (tehnike, taktike, procedure) koje rade danas, sutra su beskorisne.

Karakteristike kibernetičkog manevra (3)

- Prikrivanje i anonimnost
- Anonimnost je ključna značajka.
- Izuzetno teško otkriti tko stoji iza napada zbog "skakanja" (leapfrogging) kroz sustave trećih strana

Karakteristike kibernetičkog manevra (4)

- Masa i nelinearnost
- Brzo stvaranje mase putem botneta i "crowd-sourcinga„
- Paralelni napadi na više razina (taktička, operativna, strateška) istovremeno

Multi-domenske operacije

- Integracija svih domena radi prevladavanja slojevitih napada
- **Proaktivnost:** Umjesto čekanja na napad, stvaraju se ranjivosti kod protivnika
- "Persistent engagement" (stalni angažman) i "Defend forward" (obrana unaprijed)

Ofenzivni manevri

- **Eksploatacijski:** Krađa intelektualnog vlasništva i tajni (primjer: Kina)
- **Pozicijski:** Kompromitacija SCADA sustava ili C2 čvorova prije otvorenog sukoba
- **Utjecajni:** Manipulacija podacima radi narušavanja povjerenja zapovjednika.

Primjeri ofenzive: Izrael i Sirija

- **Operacija Dayr az-Zawr (2007):** Kibernetički napad onesposobio sirijske radare prije zračnog udara.
- Pozicijski manevar omogućio uspjeh kinetičke operacije.

Defenzivni manevri (1): Statična obrana

- **Perimeter Defense:** "Maginotova linija" cyberspacea (vatrozidi, IDS).
- **Defense in Depth:** Slojevita zaštita unutar mreže
- **Problem:** Statičnost omogućuje protivniku neometano ispitivanje ranjivosti.

Defenzivni manevri (2): Aktivna obrana

- **Moving Target Defense (MTD):** Stalna promjena parametara (IP adrese, MAC adrese) kako bi se zbunio napadač
- **Deceptive Defense (Decepcija):** Honeypots (zamke) za otkrivanje metodologije napadača

Allenova hijerarhija planiranja

- **Misija/Cilj:** Definira što se želi postići.
- **Shema manevra:** Slijed kategorija manevra (zapovjedna namjera)
- **Kategorije:** Trajni koncepti (npr. "odgodi", "skreni").
- Tehnička provedba koju bira osoblje.

Allenovih 21 kategorija manevra

- **Kinetički slični:** Zasjeda, herding (tjeranje), distrakcija, counterattack
- **Psihološki (MISO):** Privid nepobjedivosti, narušavanje povjerenja, lažni osjećaj sigurnosti.
- **Hakerski:** Osiguranje perzistentnosti, socijalni inženjering.

Allenovih 21 kategorija

Categories of Maneuver	Degrade	Disrupt	Destroy	Manipulate
Ambush: Attract to a "kill zone"				✓
Herd: Push to a "kill zone"				✓
Stimulate a Response				
Probe Adversary				
Distract				✓
Leverage Deception				✓
Delay Adversary				✓
Counter Asymmetric Advantage				✓
Launch Spoiling Attack	✓	✓	✓	✓
Launch Supporting Attack	✓	✓	✓	✓
Counterattack	✓	✓	✓	✓
Appear Invincible				✓
Undermine Adversary Confidence				✓
Create False Sense of Security				✓
Leverage Shifting Allegiances	✓	✓	✓	✓
Employ Influence Messaging				✓
Ensure Persistence				
Leverage Perishability				
Vary Launch Points				
Apply Social Engineering				✓
Change the Terrain	✓	✓	✓	✓

Primjeri shema manevra

- Probing i Zasjeda za pristup -> Narušavanje povjerenja -> Promjena terena -> Lažni osjećaj sigurnosti nakon postignutog cilja
- Promjena svih lozinki radi stimulacije reakcije protivnika -> Decepcija kroz decoy resurse -> Odgoda protivnika

Izazov suvereniteta

- Fizički hardver u državi vs. globalne logičke granice – „borderless” domene
- Prekršaji suvereniteta: Instalacija alata za daljinski pristup (RAT) u kritičnu infrastrukturu
- Problem neutralnih država kroz koje prolazi promet napada

Analiza – Prednosti i Mane

- **Prednosti:** Asimetrija (mali akteri nanose veliku štetu), anonimnost, brzina
- **Mane:** Rizik od eskalacije u kinetički rat, legalna siva zona, nemogućnost kontrole kolateralne štete

Zaključak

- Kibernetički manevar je primjena tradicionalnih principa na novu domenu
- Informacija je "valuta" modernog ratovanja
- Uspjeh ovisi o integraciji kognitivne agilnosti i multi-domenske suradnje

Literatura

- Applegate, S. D. (2012). *The Principle of Maneuver in Cyber Operations*. George Mason University.
- Allen, P. D. (2020). *Cyber Maneuver and Schemes of Maneuver*. The Cyber Defense Review.

Hvala!