

Ofenzivna sigurnost

Obavještajna priprema kibernetičkog prostora (engl. IPCE)

Vito Stanić, 12. siječnja 2026.

Pregled predavanja

- Motivacija i problem
- Što je IPCE?
- IPCE proces
- Prednosti i ograničenja
- Zaključak

Motivacija

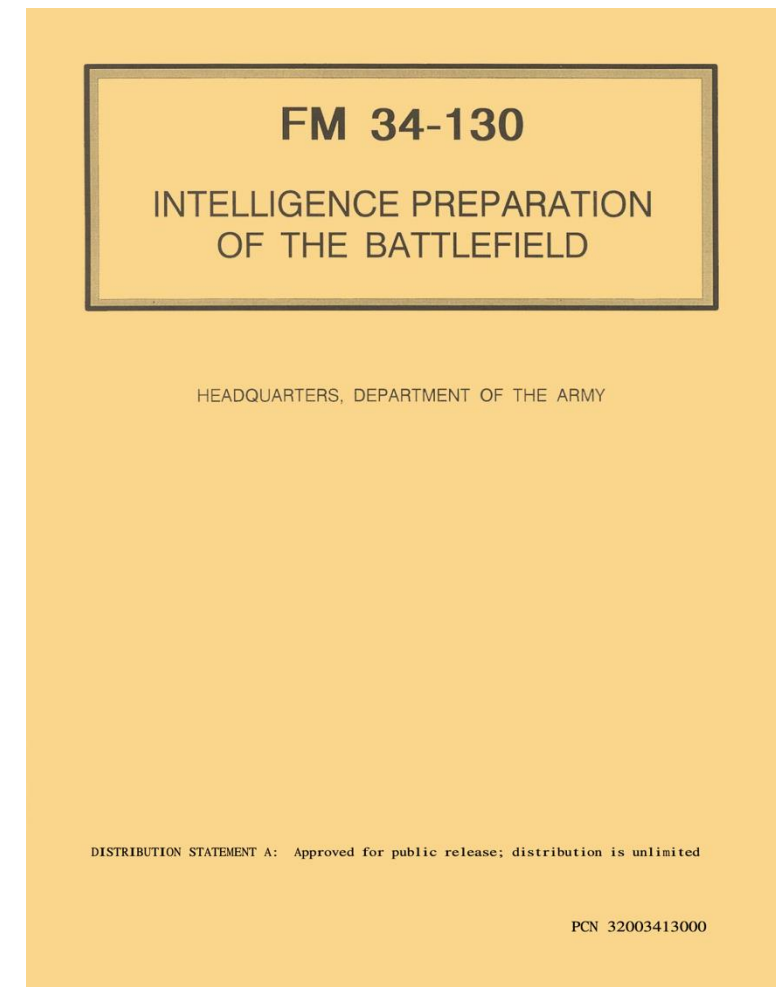
- Kibernetički prostor nije klasično bojište
- Koje prijetnje mogu djelovati na moj informacijski sustav i kako ih prepoznati?
- Kako umanjiti iznenađenje kompromitacije, pripremiti odgovor unaprijed, spriječiti incident, efikasno trošiti sredstva?

Pitanja za ispite

- Razumijevanje čega sve nam omogućuje obavještajna priprema kibernetičkog prostora? Nabrojite.
- Na kojem se konceptu temelji obavještajna priprema kibernetičkog prostora?
- Koja su 4 ključna koraka IPCE procesa?
- Zašto je ključna suradnja između crvenog i plavog tima među iteracijama IPCE procesa?
- Koje su glavne prednosti, a koja su glavna ograničenja IPCE-a?

IPB kao temelj planiranja

- **Obavještajna priprema bojišta (IPB)** je sustavni proces analize varijabli misije neprijatelja, terena, vremena i civilnih čimbenika u području interesa kako bi se utvrdio njihov utjecaj na operacije.
- Alat za donošenje odluka



Od IPB-a do IPCE-a

- Intelligence preparation of the cyber environment (IPCE)
- Kibernetičke operacije su nova domena ratovanja
- Potreba za prilagodbom, ne zamjenom
- IPCE kao evolucija IPB-a

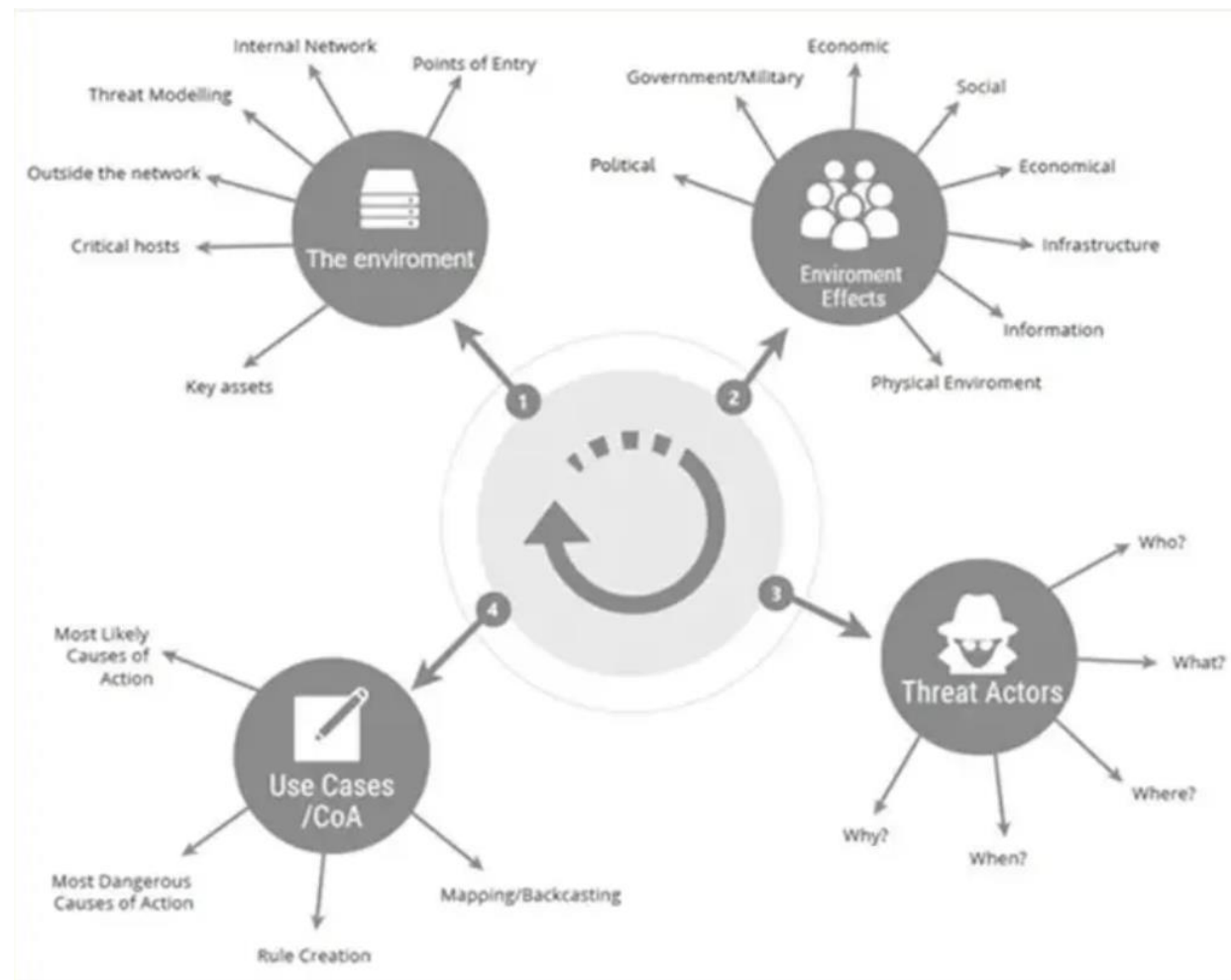
Što je IPCE?

- Sustavan i kontinuiran proces analize digitalnog okruženja i protivnika radi predviđanja prijetnji i jačanja otpornosti

IPCE proces

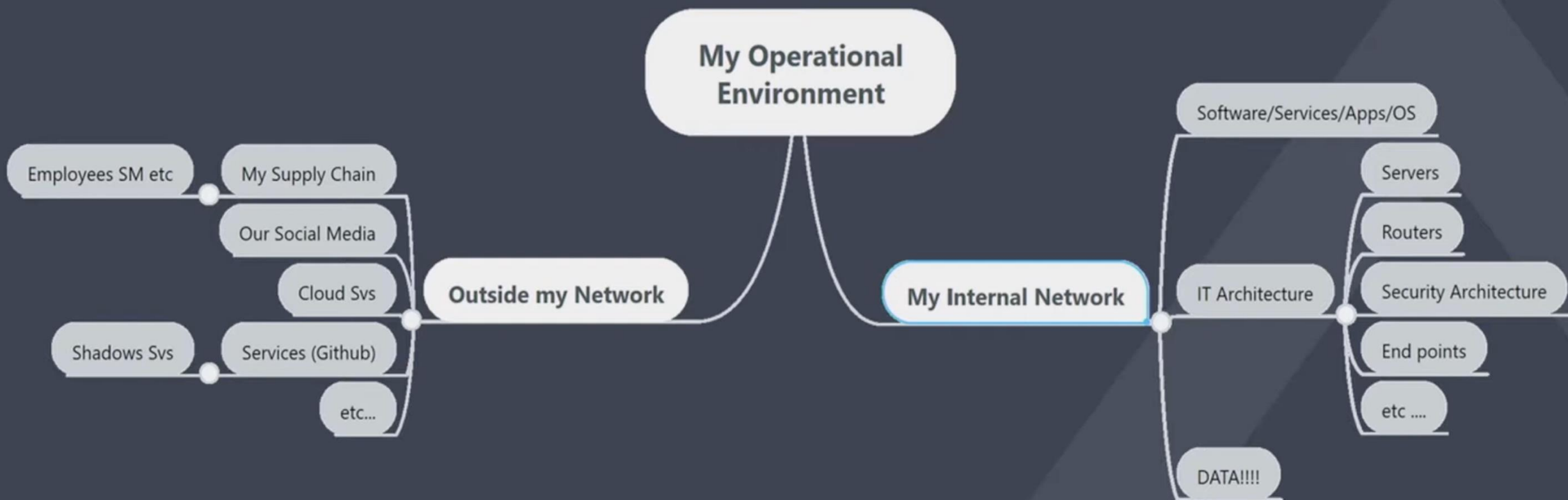
Odrediti:

1. operativno okruženje
2. utjecaje na okruženje
3. izvore prijetnji
4. scenarije prijetnji

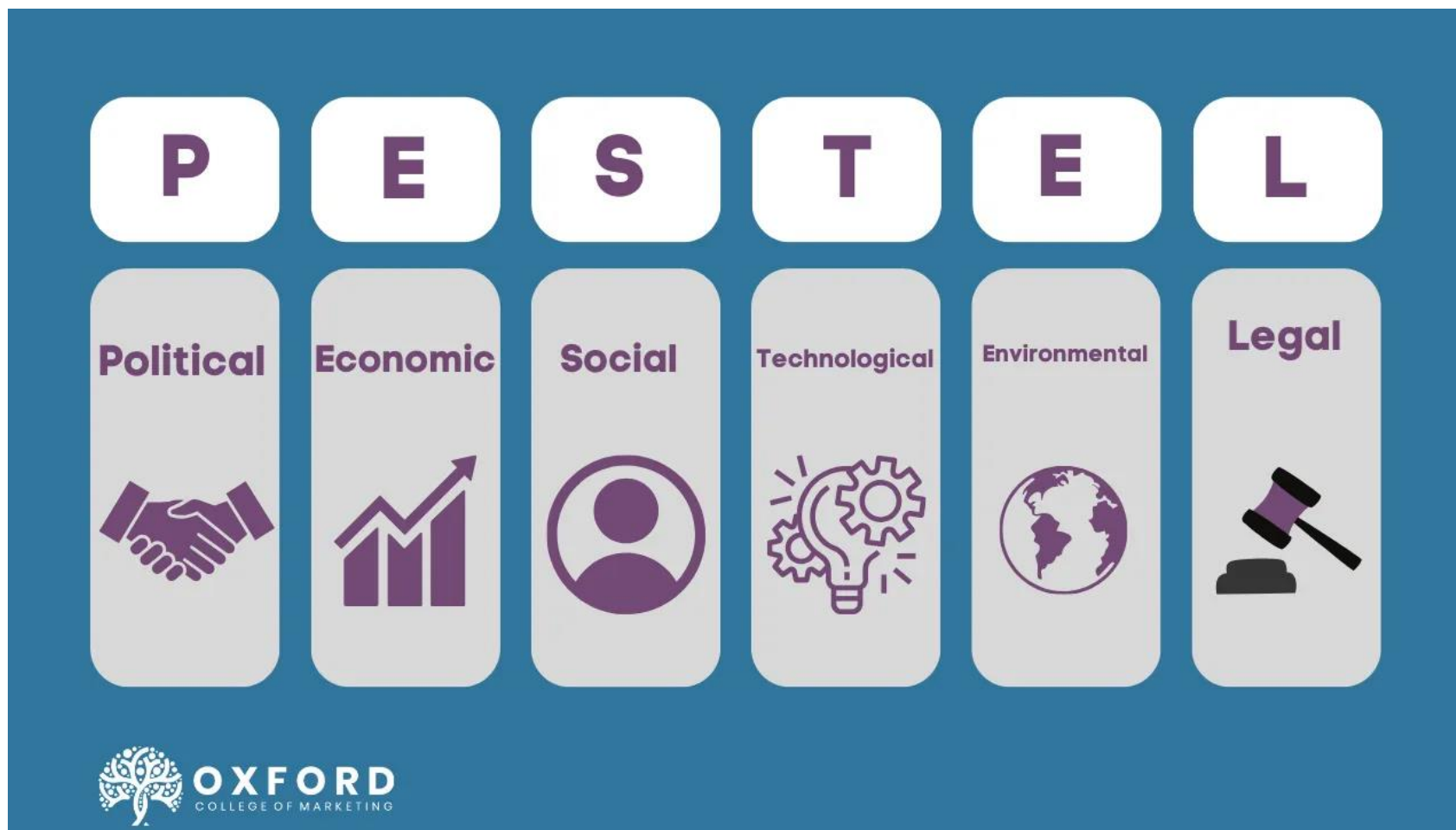


Izvor: [6]

1. Odrediti operativno okruženje



2. Odrediti utjecaje na okruženje



3. Odrediti izvore prijetnji

- Tko, što, gdje, kada, kako, zašto
- Podjela na kategorije
- Mogućnost i namjera napadača

4. Odrediti potencijalne akcije (CoA)

- Najčešći i oni najvećeg utjecaja
- Generički zadani

Kontinuirani proces

- IPCE **nije** jednokratni postupak
- Crveni tim testira scenarije
- Suradnja crvenog i plavog tima
- IPCE postaje alat učenja, a ne samo analize

Mogućnosti - senzori

- Konfiguracija IDS-a i ostalih senzora da prepoznaju protivničke CoA
- Automatizirani odgovori

Prednosti IPCE-a

- Strukturirano razumijevanje okruženja
- Fokus na protivnika, a ne samo na ranjivosti
- Poboljšana situacijska svijest
- Podrška u planiranju i automatizaciji

Ograničenja IPCE-a

- Složen i vremenski zahtjevan proces
- Ne uklanja neizvjesnost

Zaključak

- IPCE je kontinuirani proces učenja i uspješna adaptacija obavještajne pripreme bojišta
- IPCE ne obećava savršenu zaštitu, već informiranije, brže i konzistentnije donošenje odluka u kompleksnom kibernetičkom okruženju.

Literatura

- [1] A Lemay, S Knight, JM Fernandez, „Intelligence Preparation of the Cyber Environment (IPCE)”, 2014.,
<https://www.jstor.org/stable/26487107?read-now=1&seq=1>
- [2] SANS Cyber Threat Intelligence Summit 2018, “Intelligence Preparation of the Cyber Environment”,
<https://www.youtube.com/watch?v=3bXr-CF9NBI>
- [3] Prezentacije iz kolegija ”[SPNI] Sigurnosne prijetnje na Internetu”

Dodatna literatura

- [4] Vojska SAD-a, „Intelligence Preparation of the Battlefield”, 1994.,
<https://www.marines.mil/Portals/1/Publications/FM%2034-130.pdf>
- [5] Business To You, „PESTEL Analysis EXPLAINED”,
<https://www.youtube.com/watch?v=bYn4CyL3r5w>
- [6] Kraven Security, „IPCE + PESTLE Analysis”,
<https://kravensecurity.com/ipce-and-pestle-analysis/>
- [7] Oxford, „What is a PESTEL analysis?”,
<https://blog.oxfordcollegeofmarketing.com/2016/06/30/pestel-analysis/>

Hvala!