

OTPORNOST NA KIBERNETIČKE PRIJETNJE U EES-u



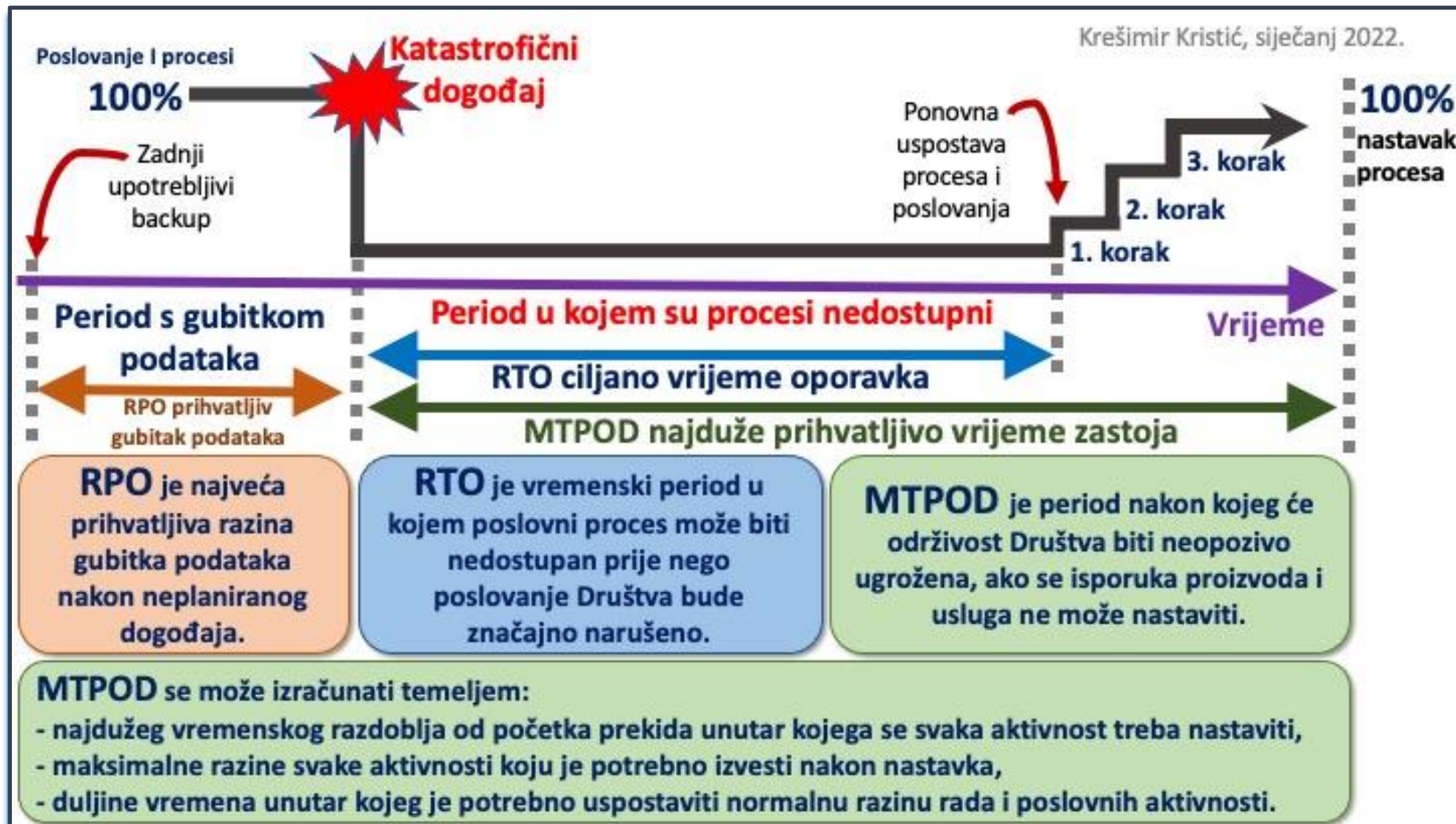
Preuvjeti otpornosti elektroenergetske kritične infrastrukture na kibernetičke prijetnje

Preduvjeti otpornosti elektroenergetske kritične infrastrukture na kibernetičke prijetnje

Sadržaj:

1. Uspješno provedeni napad 3 min
2. Što štitimo – BIA analiza i procjena rizika 2 min
3. Od čega i od koga štitimo – prijetnje i napadači 3 min
4. Otpornost – sigurnosna arhitektura i mjere 3 min
5. Legislativno organizacijski provedbeni okvir 3 min

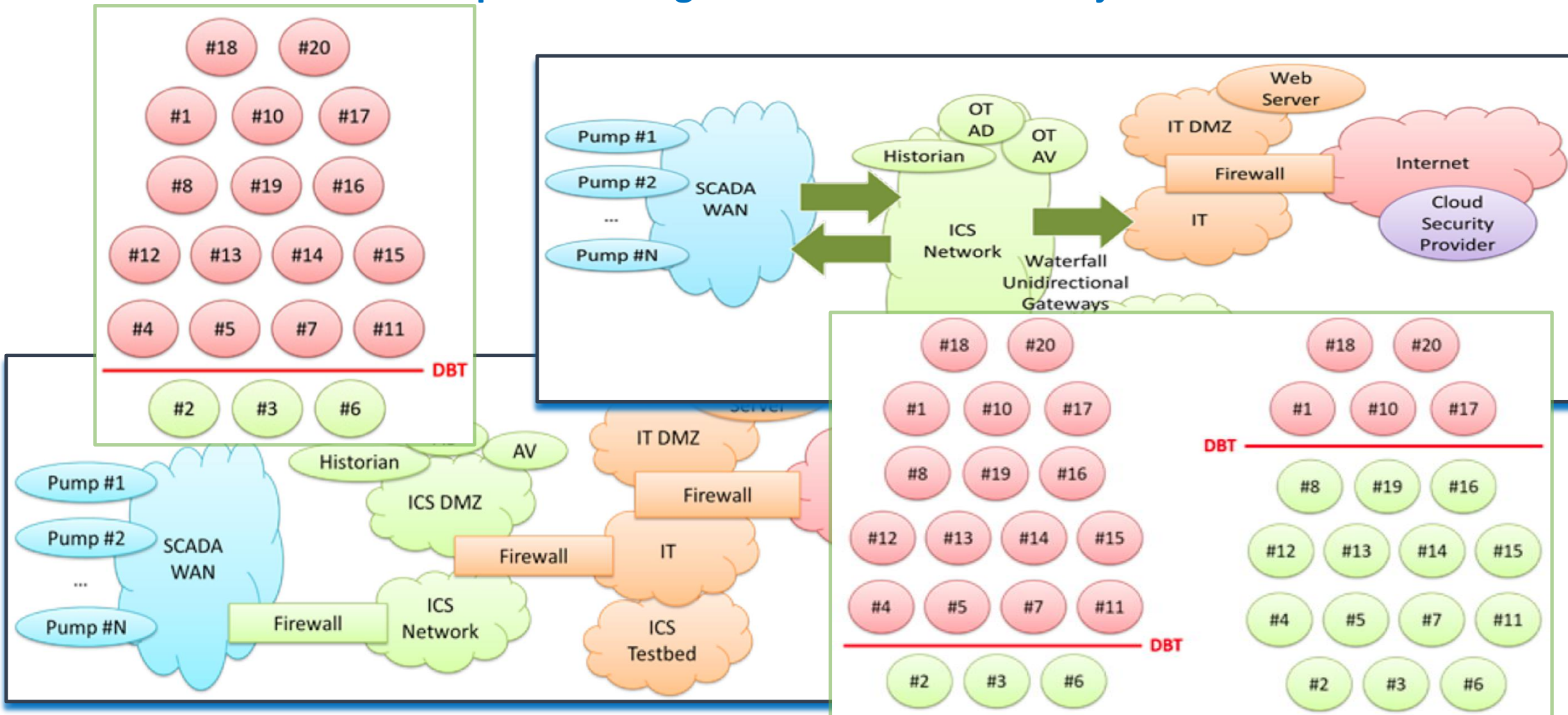
Što štitimo – BIA analiza i procjena rizika



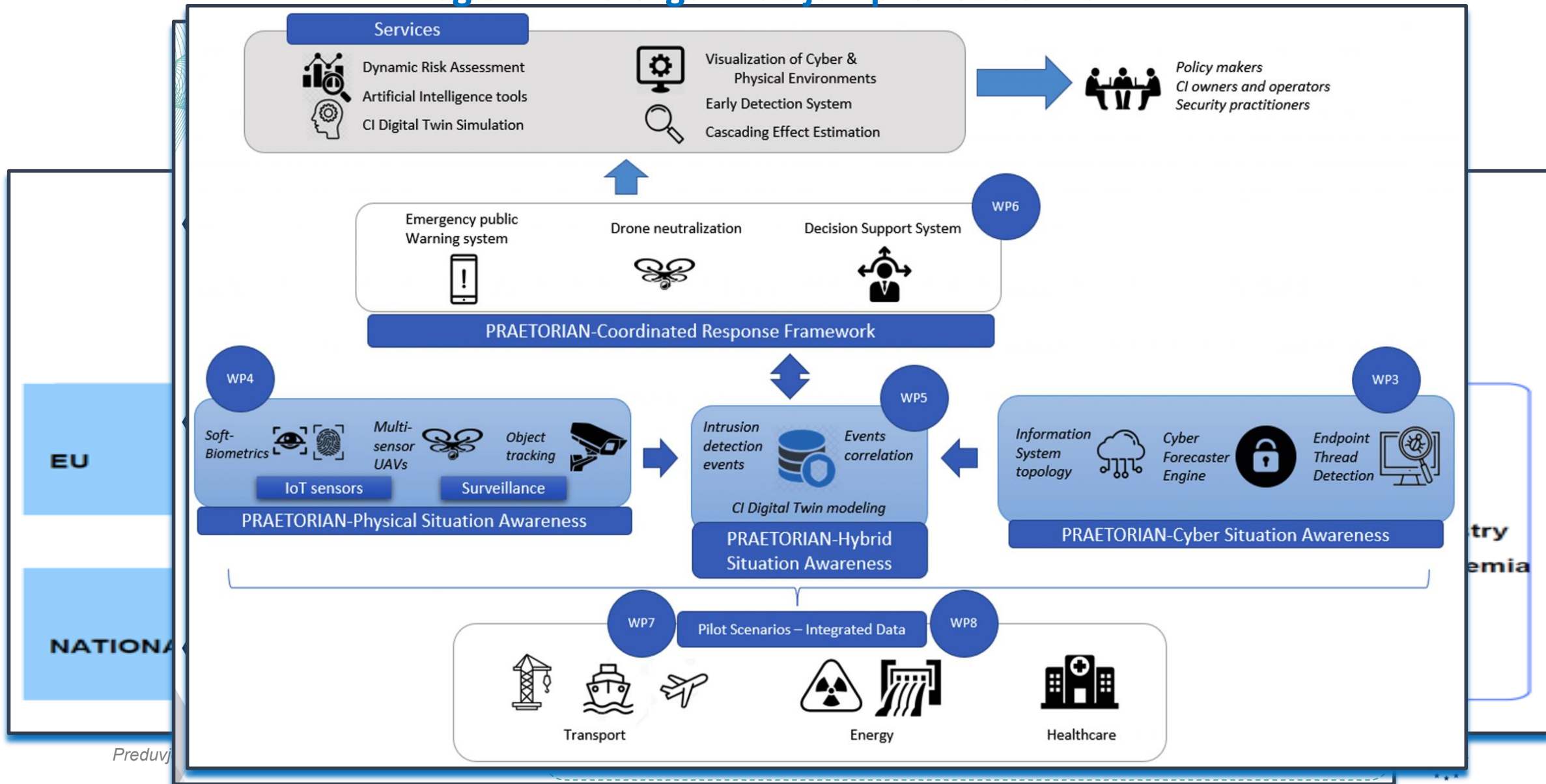
Od čega i od koga štitimo – prijetnje i napadači

1. ICS Insider	8. Market Manipulation	15. Compromised Remote Site
2. IT Insider	9. Sophisticated Market Manipulation	16. Vendor Back Door
3. Common Ransomware	10. Cell-phone WIFI	17. Stuxnet
4. Targeted Ransomware	11. Hijacked Two-Factor	18. Hardware Supply Chain
5. Zero-Day Ransomware	12. IIoT Pivot	19. Nation-State Crypto Compromise
6. Ukrainian Attack	13. Malicious Outsourcing	20. Sophisticated Credentialed ICS Insider
7. Sophisticated Ukrainian Attack	14. Compromised Vendor Website	

Otpornost – sigurnosna arhitektura i mjere



Legislativno organizacijski provedbeni okvir



Preduvjeti otpornosti elektroenergetske kritične infrastrukture na kibernetičke prijetnje

- Procjena i upravljanje rizicima, BIA
- Unaprijeđena sigurnosna arhitektura
- Nadzor i reakcija u stvarnom vremenu 24 x 7 x 365

Literatura:

Journal of energy, Vol 70, Nr 4, 2021, K. Kristić, *Cybersecurity of the Power Production and Distribution of Critical Infrastructure*

FER, 2022. Seminarski rad, K. Kristić, *Kibernetička sigurnost distribucijskih elektroenergetskih sustava*

FER, 2022. Seminarski rad, K. Kristić, *Kibernetička sigurnost pogona proizvodnog elektroenergetskog sustava*

Hvala Vam na pozornosti!



kresimir@cybertrackeu.hr

<https://www.cybertrackeu.hr>