CHECK POINT

AI, kybernetická válka a budoucnost bojových konfliktů

Tomáš Vobruba, Lead Security Engineer

26.11.2025

YOU DESERVE THE BEST SECURITY

Cyberwars: AI Amplifies Disinformation and Influence Campaigns

In 2025, AI will be increasingly leveraged in cyber warfare, particularly in the context of disinformation and influence campaigns. Nation-state actors and cyber criminals alike are employing AI tools to amplify fake news, create deepfakes, and manipulate public opinion. As these technologies become more advanced and widely-used, the ability to manipulate media, elections, and public sentiment is growing, making it harder to differentiate between truth and fabricated content.

Another concerning trend is the rise of state-affiliated hacktivism. Hacktivists, often with the backing or encouragement of governments, are using cyber attacks to further geopolitical agendas, promoting disinformation and destabilizing their enemies. These activities could be a precursor to more severe cyber wars and a shift in strategy. We may soon experience a transition to larger, more sophisticated attacks with long-term consequences to their targets rather than the attacks that focus on immediate, high-impact damage we've seen in the past.

https://blog.checkpoint.com/research/5-key-cyber-security-trends-for-2025/
https://www.checkpoint.com/security-report/

Attackers will increasingly leverage advanced AI code generation tools, moving beyond code completion tools, like GitHub Copilot, to AI platforms capable of generating full code creation of malware from a single prompt. This shift will enable the rapid creation of sophisticated and highly targeted cyber threats, dramatically lowering the barrier to entry for malicious actors and making the world a far less safe place as these tools become more accessible, harder to detect, and capable of evolving faster than traditional security defenses can adapt.

Key Findings from the 2025 Report:

- **Evolving Cyber Wars**: Nation-states are shifting from acute attacks to chronic campaigns aimed at eroding trust and destabilizing systems. AI-powered disinformation and influence campaigns targeted **one-third of global elections between September 2023 and February 2024.**
- **Ransomware Evolution:** Data exfiltration and extortion overtook encryption-based attacks as the primary ransomware tactic, simplifying operations and maximizing payouts. Healthcare became the second most targeted industry, with a **47% increase in attacks year-over-year.**
- **Edge Device Exploitation**: Compromised routers, VPNs, and other edge devices served as key entry points for attackers. Over **200,000 devices** were controlled by advanced botnets like Raptor Train, operated by state-sponsored actors.
- **Prevalent Vulnerabilities: 96% of exploits in 2024** leveraged vulnerabilities disclosed prior to the year, underscoring the importance of proactive patch management.
- **Targeted Industries:** For the fifth consecutive year, education remained the most targeted industry, experiencing a **75% increase in attacks year-over-yea**r.

Autonomní a poloautonomní systémy v boji

Co se děje už dnes

- **Drony s prvky AI** dokážou samostatně navigovat, měnit trasu, reagovat na rušení, vyhledávat charakteristické tvary cílů či tepelné stopy
- Ve **válce na Ukrajině** vzniká "ekosystém dronů" – od FPV až po autonomní rojové koncepty. AI výrazně zrychluje OODA cyklus (Observe–Orient–Decide–Act)
- **Projekt Maven** využívá ML k analýze videa / satelitních dat → zrychluje identifikaci cílů – s minimem lidského dohledu

Dopad na taktiku

- Převaha ve vzduchu se přesouvá od stíhaček k levným dronům → *asymetrická výhoda i pro slabší stranu*
- Bojiště je neustále „viditelné". Utajení je téměř nemožné
- Velmi se snižuje hodnota tradiční „těžké techniky" bez anti-drone/anti-AI obrany

https://en.wikipedia.org/wiki/AIassisted_targeting_in_the_Gaza_Strip

https://arxiv.org/abs/1803.10664

Kybernetická válka a IT bezpečnost jako klíč boje

- Tady se odehrává *skrytá část války*, která je často významnější než kinetický boj
  - Zastarávání technologií
  - IT bezpečnost jako základní pilíř armády
  - Kybernetická dominance
  - Lethal Cyber Effects

- kdo nemá **zero-trust**,
- schopnost **rychlého patchování**,
- **AI-detekci anomálií**,

je *do týdne mimo hru.*

- Komunikace, drony, logistika, naváděcí systémy, nemocnice, elektrárny – vše běží na IT.
- Útoky typu **wiper**, **ransomware** nebo **supply-chain attack** (SolarWinds styl) dnes dělají:
  - výpadky komunikací,
  - ztrátu řízení jednotek,
  - logistický chaos,
  - kolaps zdravotní péče.

(3) Kybernetická dominance

- Rusko, Čína i západní státy používají AI pro:
  - generování phishingu,
  - automatizované exploitace,
  - detekci slabin v reálném čase,
  - deepfake operace.
- Útok může proběhnout *během sekund* – AI útočník/obránce dělá tisíce akcí za sekundu → člověk není schopen reagovat.

Dnes už kyberútok může přímo zabíjet:

- vypnutí světel ve městě → útok dronů
- manipulace GPS → havárie letadla/dronu
- vypnutí nemocnice → mrtví civilisté

Kybernetické bojiště **není nekinetické** — je jen tiché.

Informační a kognitivní válka

AI mění 3 klíčové oblasti

- **Propaganda & deepfake videa** – cílení na jednotlivé skupiny
- **Sociální analýza** – AI mapuje nálady obyvatel → předpovídá protesty či slabá místa
- **Psychologické operace (PSYOPS)** – mikro-cílení fake informací

Toto má často *větší dopad než zničit tank*.

Command & Control (C2) řízené AI

Velké armády přecházejí na síťové systémy řízení boje

Co to znamená

- AI propojuje satelity, drony, pozemní jednotky, radary → vytváří „jednu mozek armády“
- Rychlost rozhodování dramaticky roste
- Lidská role se posouvá z velitele → *supervizora rozhodnutí AI*

Dopad

- Strana s lepší AI vyhraje
- Armáda bez AI nebude schopná reagovat na dynamiku bojiště

Kybernetická obrana zbraňových systémů (velké téma!)

Moderní tank, letoun nebo raketa jsou **primárně software**.

Blokace, která rozhoduje o výsledku války:

- Anti-jamming
- Anti-spoofing
- Zero-trust armádních sítí
- AI-monitoring telemetrie
- Autonomní izolace infikovaných jednotek

Zranitelnost v firmware dronu může způsobit jeho převzetí → *zbraň se obrátí proti vlastní straně*.

Hlavní trendy, které nás čekají a závěr

- **AI roje dronů** s minimálním lidským dohledem.
- **Autonomní kyberobrana** (AI → AI boj).
- **Digitální dvojčata bojiště** pro predikci výsledků.
- **Plně automatizovaná logistika** → zásobování bez lidí.
- **Expresní zastarávání zbraňových systémů** kvůli rychlému vývoji útoků.

Moderní bojové konflikty se přesunuly ze světa „silnější vyhrává“ do světa **„rychlejší, chytřejší a lépe zabezpečený vyhrává“**.

Kdo kontroluje:
data,**AI**,**kyberprostor**,**informační tok**,
→ ten kontroluje celý konflikt.

CHECK POINT

Děkuji za pozornost

YOU DESERVE THE BEST SECURITY