CEDARS INTERNATIONAL

Critical Infrastructure Protection – Does AI Help or Hurt?

Branko Primetica

branko.primetica@cedars.rs

September 2024

CORPORATE OVERIVEW

MISSION	To enable secure and sustainable business optimization which increases productivity and improves citizen and/or customer services.
SERVICES	Cybersecurity; Management Consulting; Emerging Technology Planning/Insertion
MARKET FOCUS	Public Sector; Managed Service Provider for Private Sector Organizations.
EMPLOYEES	20 employees with access to more than 50 pre-screened Subject Matter Experts across the Western Balkans, Europe, and the United States
LOCATIONS	Cedars International d.o.o. is based in Belgrade, Serbia.

What is Critical Infrastructure?

Critical Infrastructure	Physical facilities, systems,, supply chains, IT, and communication networks which, if destroyed, degraded, compromised, would significantly impact the social or economic wellbeing of a nation, its citizens, or the ability to conduct national defense.	
Cited by the EU's NIS 2 Directive	• Energy • Transport • Banking • Financial Market Infrastructures	• Healthcare • Drinking water supply and distribution, • Digital infrastructures

The Growing Issue

Gartner expects that, by 2025, more than 30% of CI systems will experience security breaches

Development	Issue
Critical infrastructure (CI) systems are becoming more digitized, interconnected, and automated	Increased attack surface, including the possibility of affecting more than one CI system with a single attack
CI reliance on operational technology (OT) and information technology (IT)	Increased vulnerability to cyberattacks that could disrupt operations, compromise sensitive data, cause financial losses, or even threaten public safety
Increased use of emerging technologies such as IoT and cloud computing	Increased vulnerability and risk due to lack of proper security controls protecting data and decision-making systems.
Malicious actors, including nation states, are increasingly using AI-powered cyber attacks against "adversaries".	Most national critical infrastructure systems are not ready to withstand AI-powered attacks, which can overwhelm or sneak into operational systems.

Example AI Attacks on Critical Infrastructure

Attack	Definition
Deepfakes	• Uses existing video footage, photographs, and voice recordings to create AI-generated video and sound clips. • Can persuade employees to give up confidential information. Can spread propaganda causing reputational damage, misinformation, and financial losses
Malware AI Hacking	• Creates polymorphic malware that adapts and mutates its source code to avoid detection and security protocols
Brute Force	• Allow hackers to analyze user behavior to automatically rapidly exhaust all password combinations to crack a secured location.
Hack Phishing	• AI-automated phishing scams automatically create personalized emails which seem legitimate
Voice Cloning	• Duplicates audio fingerprints and mimics voice clips off sample vocals, meaning that voice-protected systems are vulnerable to hacking
Keystroke Listening	• Records different keys you type into your keyboard to steal passwords with almost 95% accuracy.

So does AI help or hurt CIP?

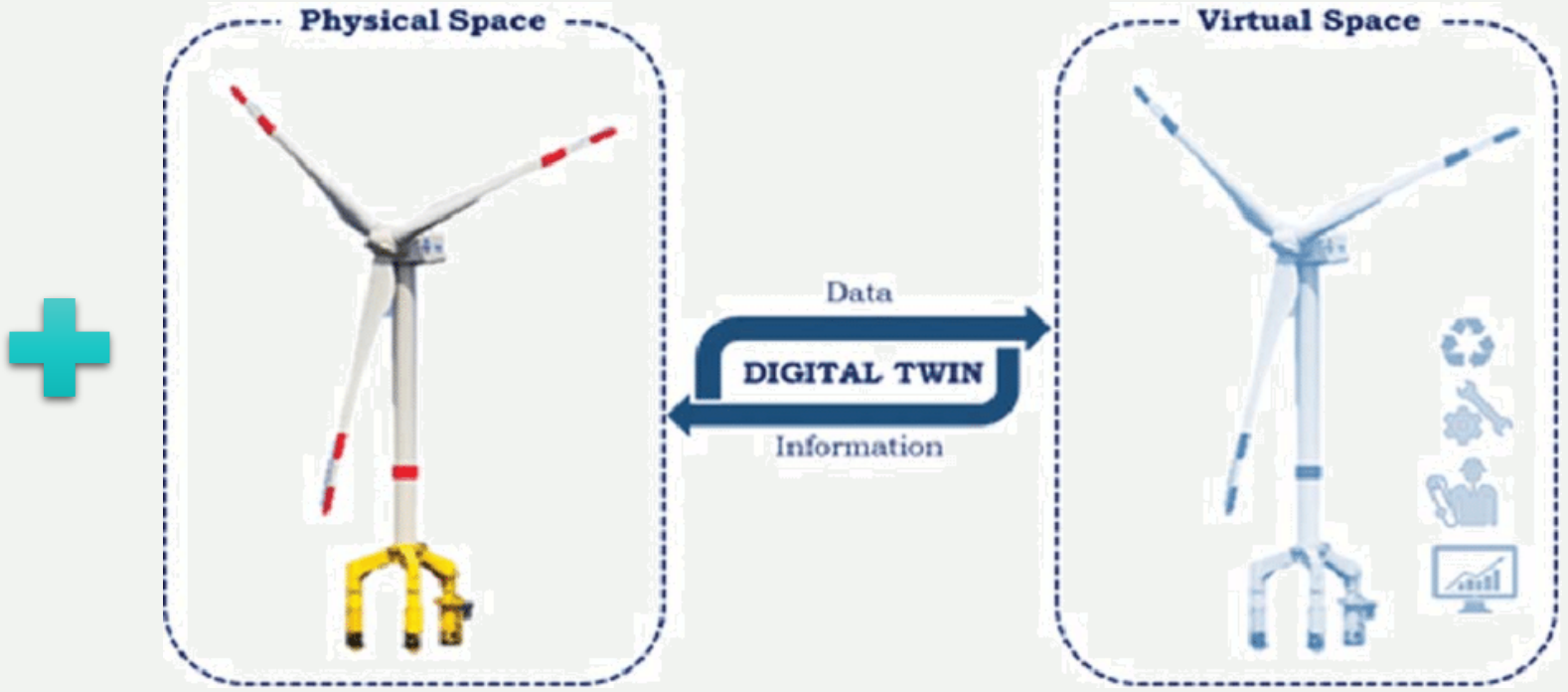
AI is the Only Way to Fight Back

AI-based cybersecurity solutions use machine learning, natural language processing (NLP), and advanced analytics to enhance detection, prevention, and response capabilities. Examples include:

AI Capability	Description
Anomaly Detection & Prevention	AI analyzes large volumes of data from multiple sources in real-time to detect anomalies and patterns indicative of cyber threats.
Behavioral Analytics	AI analyzes user, system, and device behavior in CI networks to detect abnormal user behavior (such as unauthorized access attempts, unusual data transfers) that indicate a cyberattacks
Threat Hunting	AI continuously analyzes data from threat intelligence feeds, logs, and network traffic, to proactively detect cyber threats in critical infrastructure systems
Incident Response	AI assesses security alerts in real time, prioritizes them based on severity, and automatically triggers appropriate incident response actions
Adaptive Security	AI learns from new data to dynamically adjust security measures based on changing threat landscapes and system conditions in critical infrastructure
Cyber Automation	AI can automate routine security tasks like patch management, security configuration management, and security event correlation

Generative AI (GAI) and Digital Twins

GAI enables the development of sophisticated threat scenarios to assess CI response to a number of potential cyber threats and/or attacks.



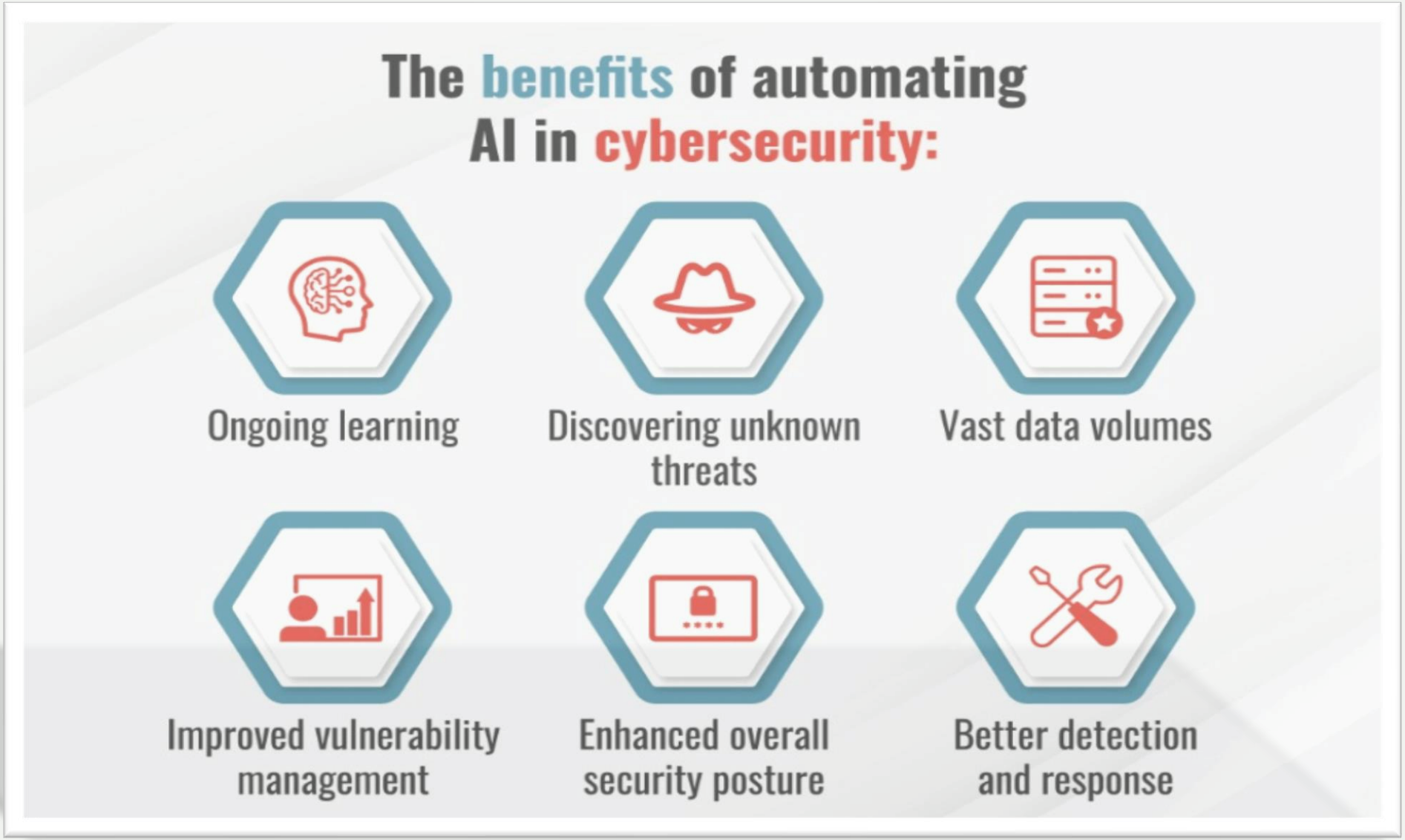
This combination enables:

- **Security Threat Modeling:** GAI simulates security threats while a Digital Twin simulate resulting cyberattacks to enable development of proactive mitigation strategies.
- **Emergency Response Planning:** GAI creates emergency scenarios while a Digital allows emergency responders to refine response strategies.
- **Cybersecurity Simulation:** GAI creates realistic attack scenarios, and a Digital Twin assess critical infrastructure vulnerabilities, enabling development of proactive cybersecurity measures.

Examples of Additional AI-powered Tools to Help

- **Extended Detection & Response (XDR):** Leverages advanced machine learning and AI to automate the detection and response process
- **AI Powered Threat Intelligence Platform:** Uses machine learning to identify emerging threats, predict attack patterns, and provide valuable information to security teams
- **AI Powered Endpoint Protection**: Utilize machine learning algorithms to detect and prevent advanced malware and ransomware attacks
- **AI-Based Intrusion Detection System (IDS):** Monitors network traffic to identify suspicious activities and anomalies that indicate possible intrusions.
- **Document Classification:** Categorizes digital files according to their level of confidentiality or sensitivity, allowing organizations to adequately protect the information

In Summary....


The benefits of automating AI in cybersecurity:
Ongoing learning
Discovering unknown threats
Vast data volumes
Improved vulnerability management
Enhanced overall security posture
Better detection and response

Questions?

branko.primetica@cedars.rs
+381 69 703 864