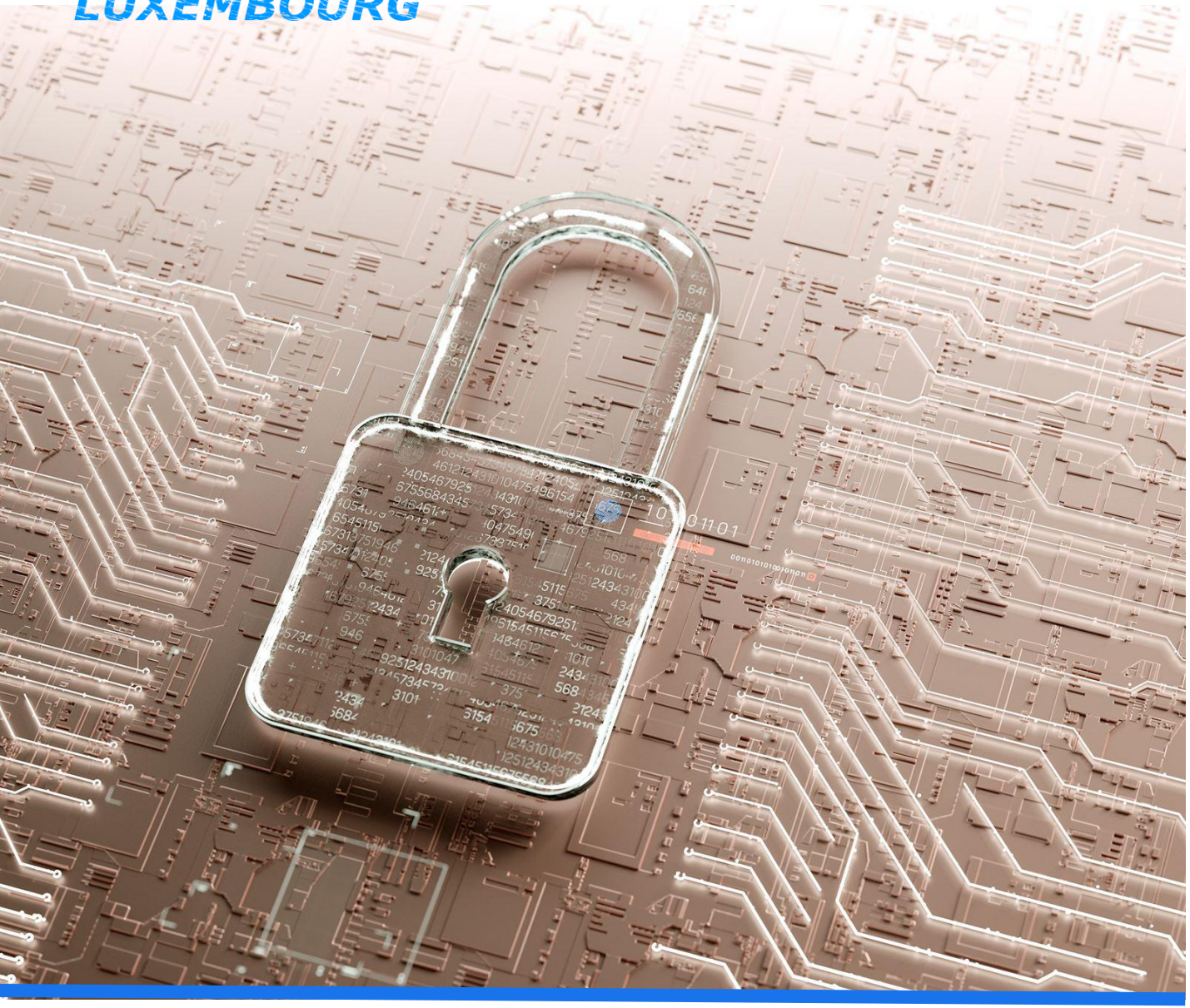
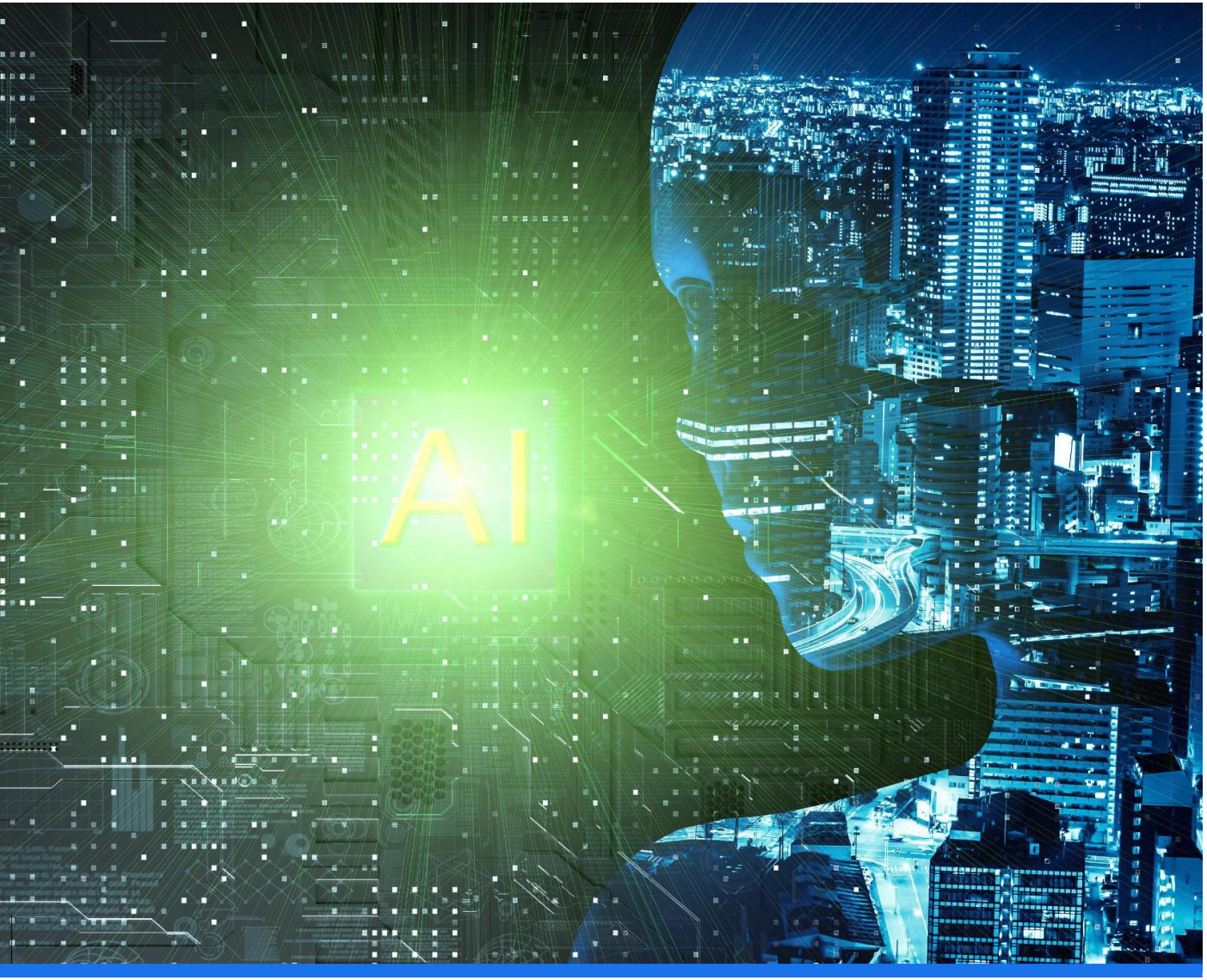
BSIDES LUXEMBOURG



The rise of generative AI: a major technological turning point

A DOUBLE-EDGED TOOL IN CYBERSPACE

- OFFENSIVE USE BY HACKERS
- DEFENSIVE USE BY CYBERSECURITY PROFESSIONALS



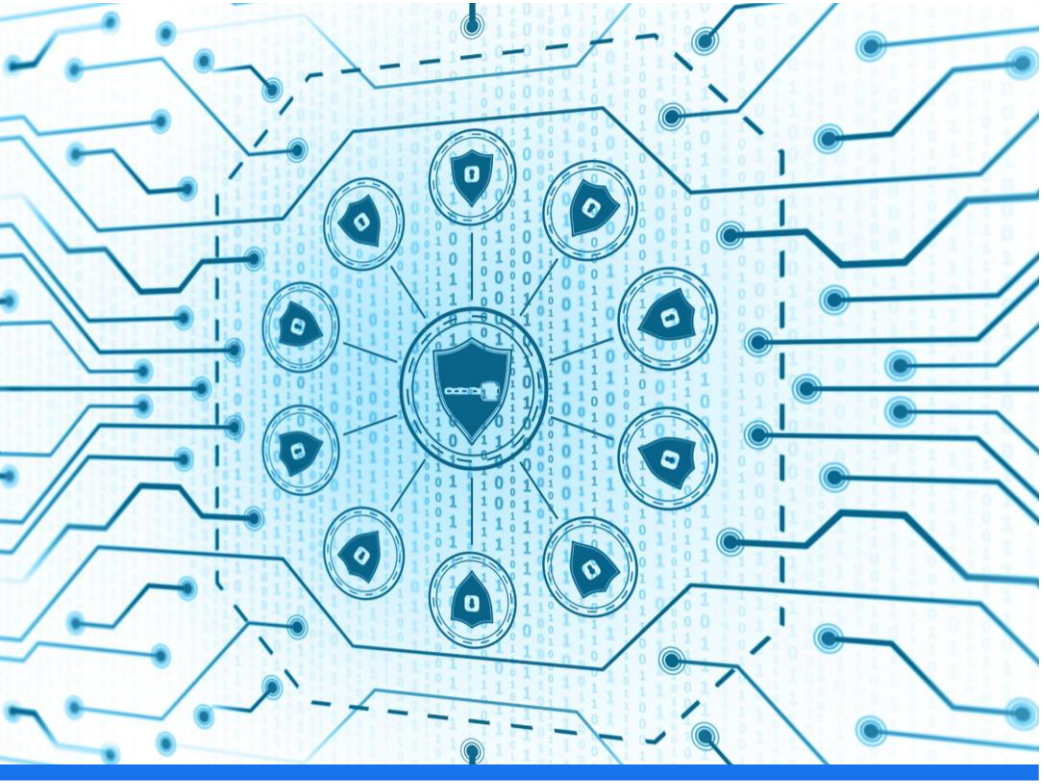
Agenda Items

- A double-edged tool in cyberspace
  - Offensive use by hackers
  - Defensive use by cybersecurity professionals
- A future where AI battles AI?
  - The scenario of AI versus AI seems inevitable
- Ethical challenges and bypassing safeguards
- Access to resources: a power issue
- Future Prospects and Recommendations
- Conclusion

BSIDES LUXEMBOURG

A double-edged tool in cyberspace

Intersection of AI and Cybersecurity



Enhancing Threat Detection

AI technologies significantly improve threat detection by analyzing patterns and identifying anomalies in data more efficiently.

Response Automation

AI can automate responses to security threats, enabling faster and more effective mitigation of potential attacks.

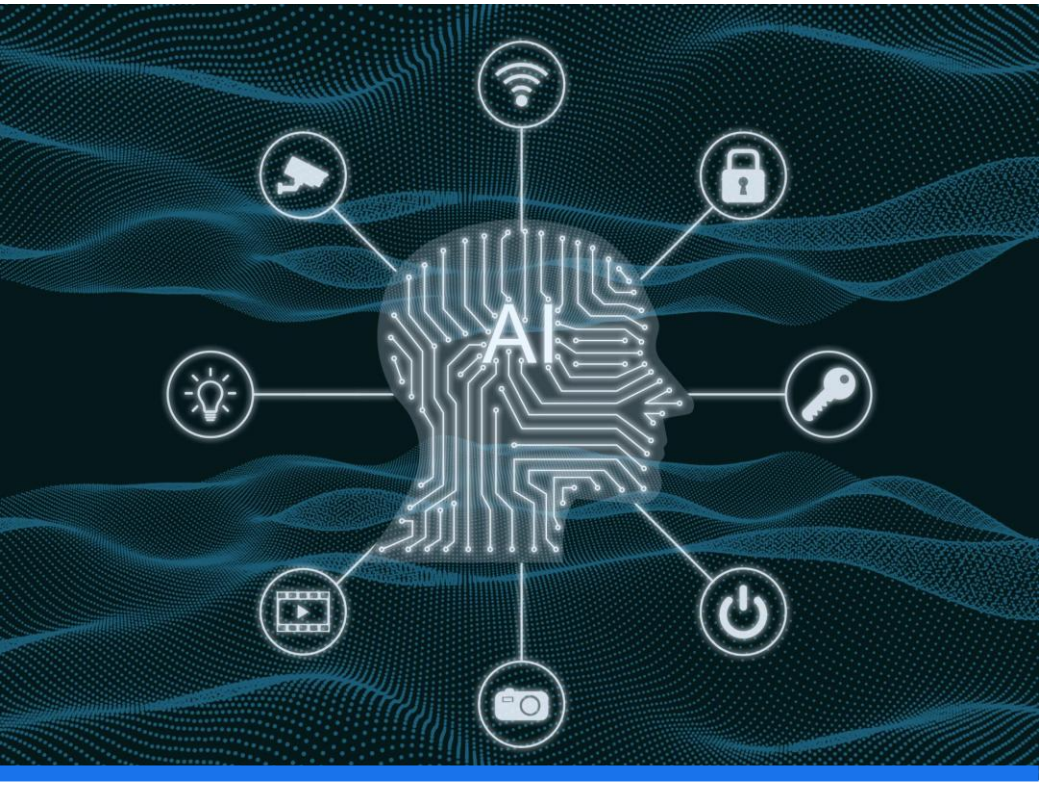
Exploitation by Cybercriminals

Cybercriminals also leverage AI to develop sophisticated attack methods, creating new challenges for cybersecurity systems.

Challenges and Opportunities

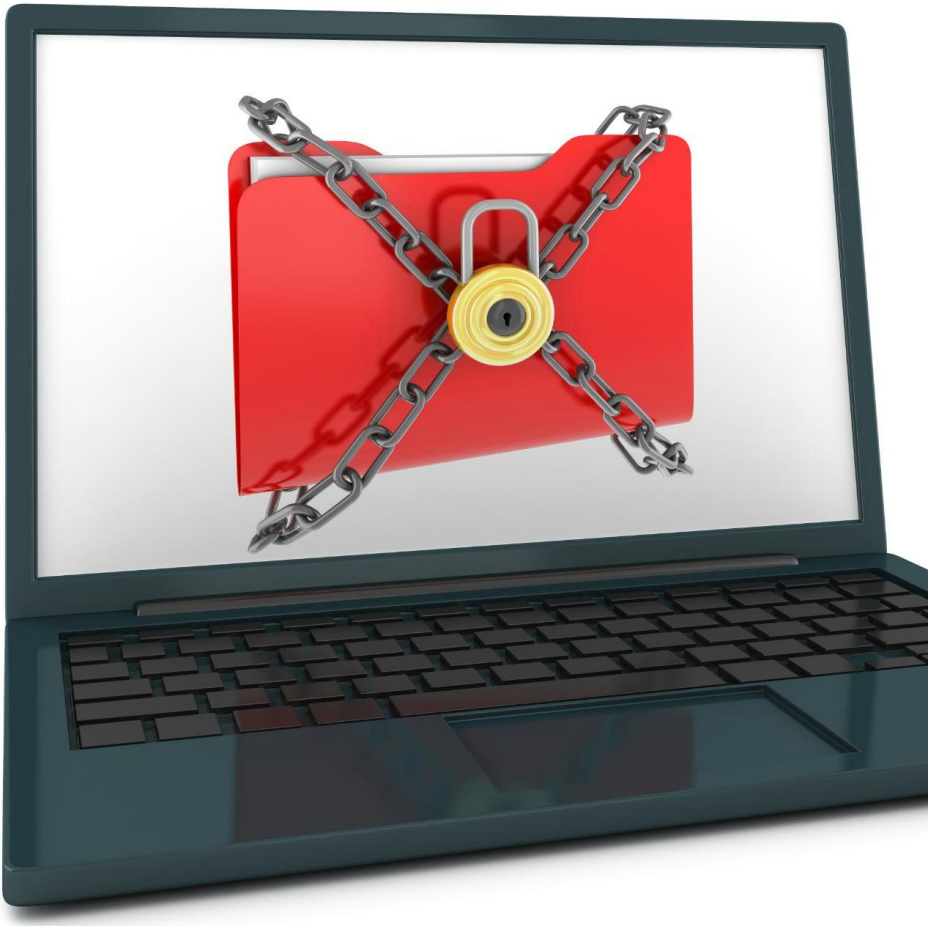
The intersection of AI and cybersecurity presents unique challenges but also opens new opportunities for innovation and improvement.

Offensive use by hackers



Hackers have not been left behind by this technological revolution. Generative AI can be exploited in many malicious ways:

- **Creation of voice or video deep fakes** tailored to the target's profile for social engineering.
- **Creation of highly realistic phishing e-mails,** tailored to the target's profile (thanks to generative templates fed by stolen data).
- **Automated development of malware** or polymorphic variants capable of evading conventional detection.
- **Leveraging AI to carry out automated attacks** such as *password spraying*, large-scale social engineering or *prompt injection*.
- **Use of specialized models trained locally or clandestinely**, without ethical restrictions, enabling hackers to lift the limits imposed on public AI.



AI-Generated Phishing and Social Engineering

AI in Cybercrime

Cybercriminals leverage AI technology to craft more convincing phishing emails that mimic legitimate communications.

Social Engineering Tactics

AI enhances social engineering tactics, making it difficult for individuals to identify malicious intent behind communications.

Increasing Threat Recognition Difficulty

The sophistication of AI-generated threats complicates recognition, leading to higher success rates for cybercriminals.

Automated and Sophisticated Attacks

Deep fakes

With GenAI, social engineering attacks can be more targeted, allowing cybercriminals to focus on specific people using deep fakes (audio and video).

Automated Cyber Attacks

AI facilitates the execution of automated cyber attacks that are faster and more efficient than traditional methods.

Sophisticated Malware Development

Cybercriminals use AI to create sophisticated malware that can learn and adapt to evade detection by security systems.

Defensive use by cybersecurity professionals

Defensive use by cybersecurity professionals

In the face of this threat, AI also serves as a technological shield:

- Real-time behavioral detection, by analyzing subtle discrepancies in network flows or user behavior.
- Automated threat hunting, capable of prioritizing alerts and identifying patterns invisible to the human eye.
- Simulated attacks (virtual red teaming) to test existing defenses with AIs playing the role of sophisticated attackers.
- Automated answer to incidents, isolating or neutralizing threats before human intervention.

Threat Detection and Response

Real-Time Threat Analysis

AI systems can quickly analyze large datasets to identify potential threats as they occur, enhancing security measures.

Faster Response Times

With AI, organizations can respond to threats more rapidly, minimizing damage and protecting assets effectively.

Effective Attack Mitigation

AI-driven responses allow for proactive threat mitigation strategies, reducing potential impact on systems and networks.

Anomaly Detection and Behavior Analysis

Machine Learning in Security

Machine learning is crucial for identifying unusual patterns in user behavior, enhancing security measures significantly.

Anomaly Detection Techniques

Various techniques are employed in anomaly detection to identify deviations in network traffic that may indicate security threats.

Preventing Security Breaches

Identifying anomalies early allows organizations to take proactive steps to mitigate potential security breaches before they escalate.

Automated Incident Response

Threat Identification

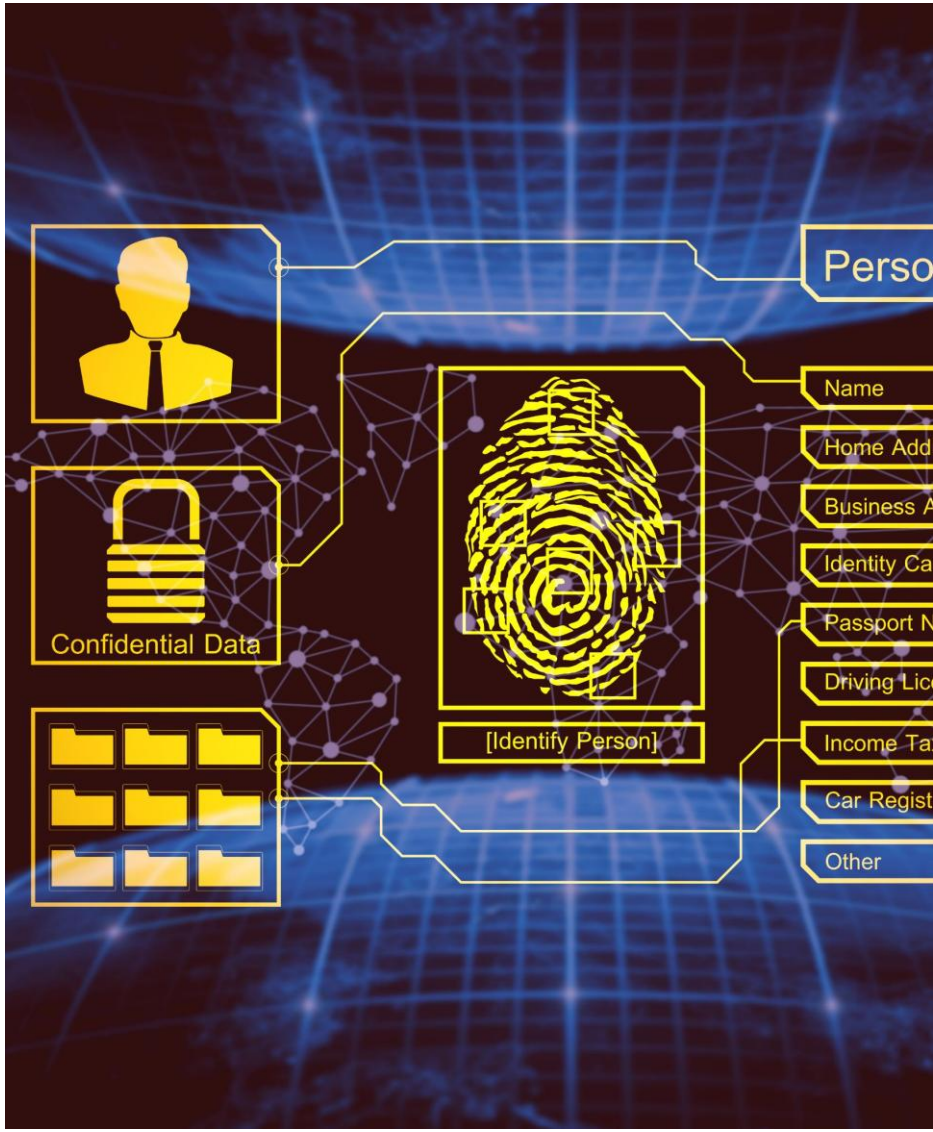
AI systems can efficiently identify potential security threats in real-time, enhancing the security posture of organizations.

Predefined Responses

Automated incident response includes the implementation of predefined responses, allowing for immediate action against identified threats.

Time Reduction

The use of AI in incident response significantly reduces the time taken to address security incidents, improving overall response efficacy.



BSIDES LUXEMBOURG

A future where AI battles AI?

The scenario of AI versus AI seems inevitable

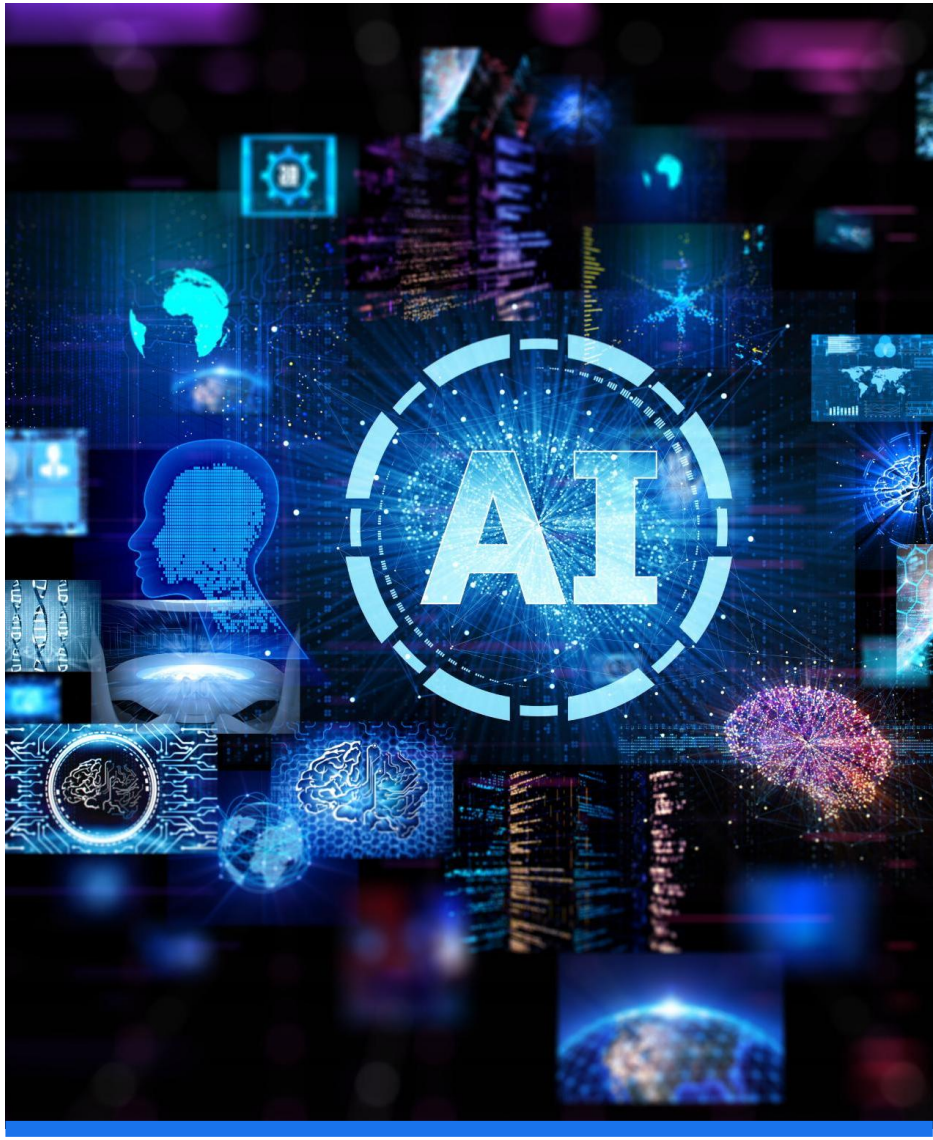
- AI-generated attacks vs. AI-driven defenses: this could become a standard in modern cyberconflicts.
- Emergence of an ecosystem of adversarial AIs where each AI must anticipate and neutralize the other, in a "cyber-evolution" logic.
- This technological escalation evokes an arms race, in which only those with sufficient resources will be able to develop more powerful AIs

BSIDES LUXEMBOURG

Ethical challenges and bypassing safeguards

Commercial AIs incorporate ethical filters to prevent malicious use, but :

- These filters can be bypassed by prompt engineering techniques, jailbreaking or the use of open-source models without constraints.
- It's difficult to define universal limits to what an AI should or shouldn't do, as the line between ethical use and misuse is often blurred.
- He also raises the question of the "moral responsibility" of AI: can a machine be responsible? Or is its designer? This becomes even more complex when AI is used by decentralized, anonymous groups.



Data Privacy and Ethical Concerns

AI in Cybersecurity

The integration of AI in cybersecurity introduces new challenges related to data privacy and the protection of sensitive information.

Ethical Concerns

Organizations face ethical dilemmas when implementing AI, particularly concerning user consent and data usage transparency.

Compliance with Regulations

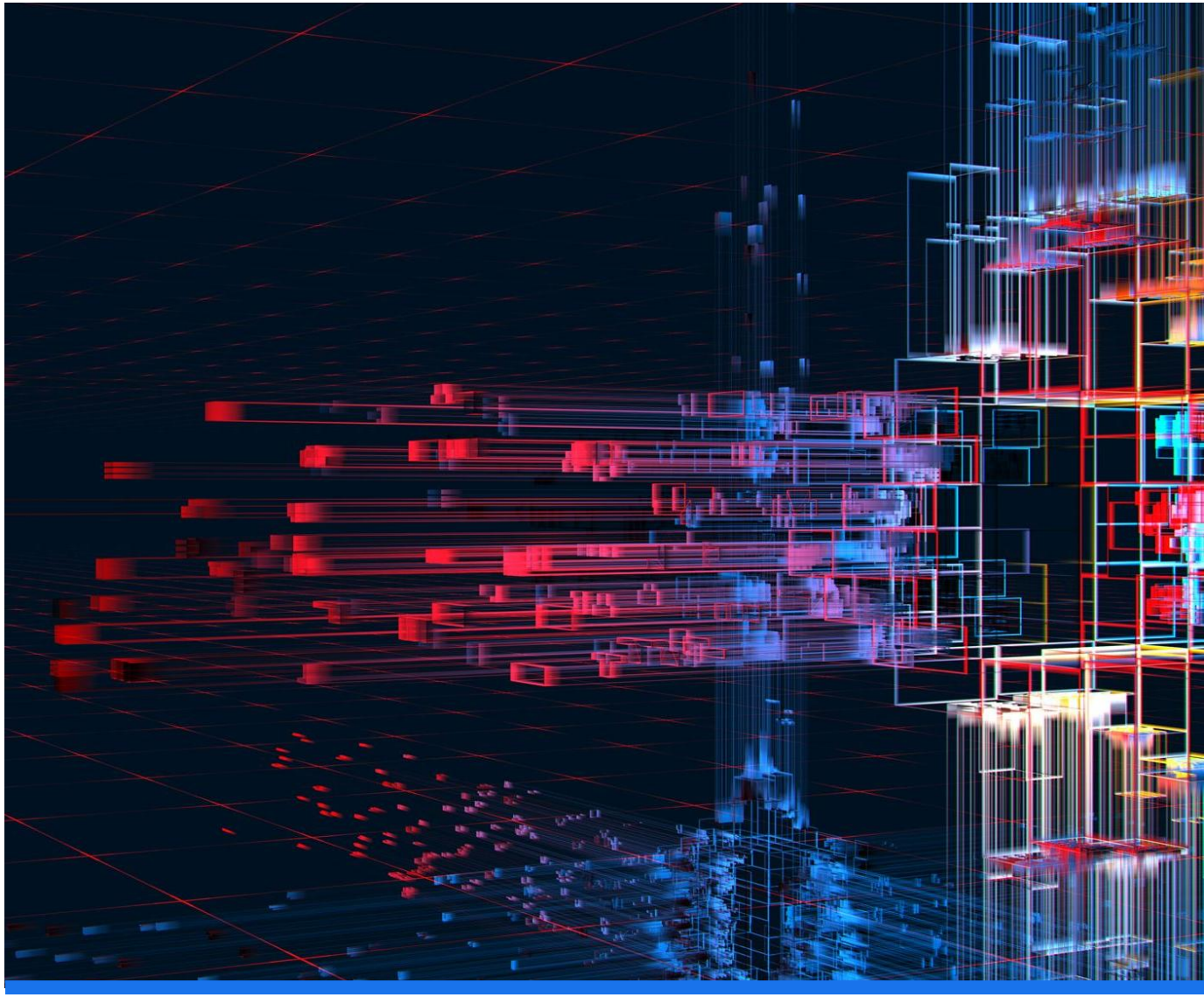
Compliance with regulations such as GDPR is crucial for organizations using AI in cybersecurity to protect user privacy.

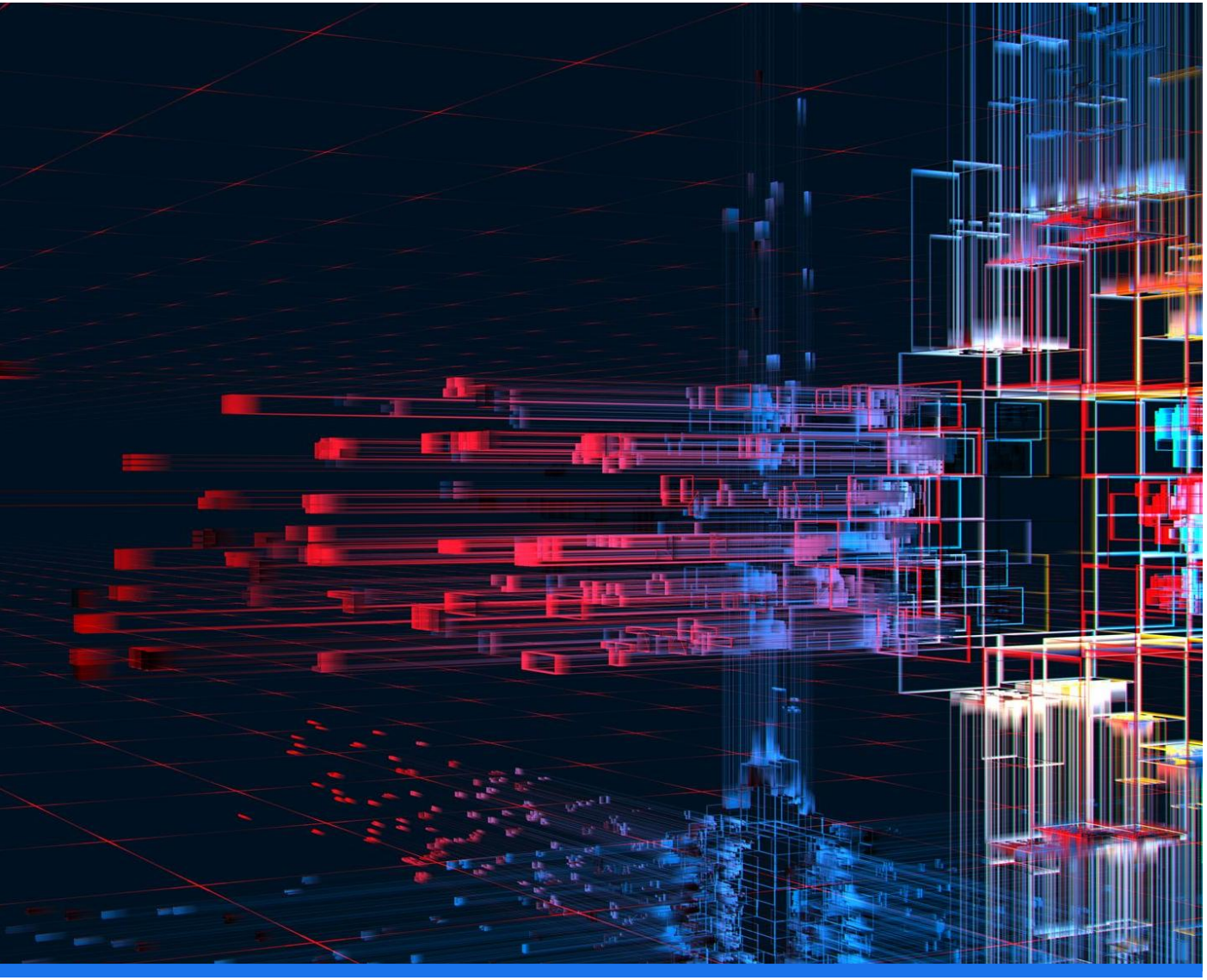
BSIDES LUXEMBOURG

Access to resources: a power issue

Powerful AIs require significant resources in terms of :

- Computing (GPU, TPU, cloud infrastructures) ;
- Storage and access to massive training data ;
- Huge energy consumption, which raises environmental and accessibility issues.





Will pirates still have access to these resources?

The best-organized groups can hack GPU servers or use cryptocurrencies to finance their cloud activities.

There are already parallel markets suggesting computing power on demand.

However, as infrastructure providers secure their platforms, access to powerful resources could become more limited for amateur cybercriminals, giving way to an elite of hackers with quasi-state resources.

BSIDES LUXEMBOURG

Future Prospects and Recommendations

Advancements in AI for Cybersecurity

Evolving AI Technology

AI technology is constantly evolving, enabling faster and more effective detection of cyber threats.

Sophisticated Detection Tools

With advancements in AI, tools for detecting cyber threats are becoming more sophisticated and reliable.

Importance of Staying Updated

Staying updated with the latest trends in AI and cybersecurity is crucial for effective threat management.

Balancing Innovation with Security

Need for Innovation

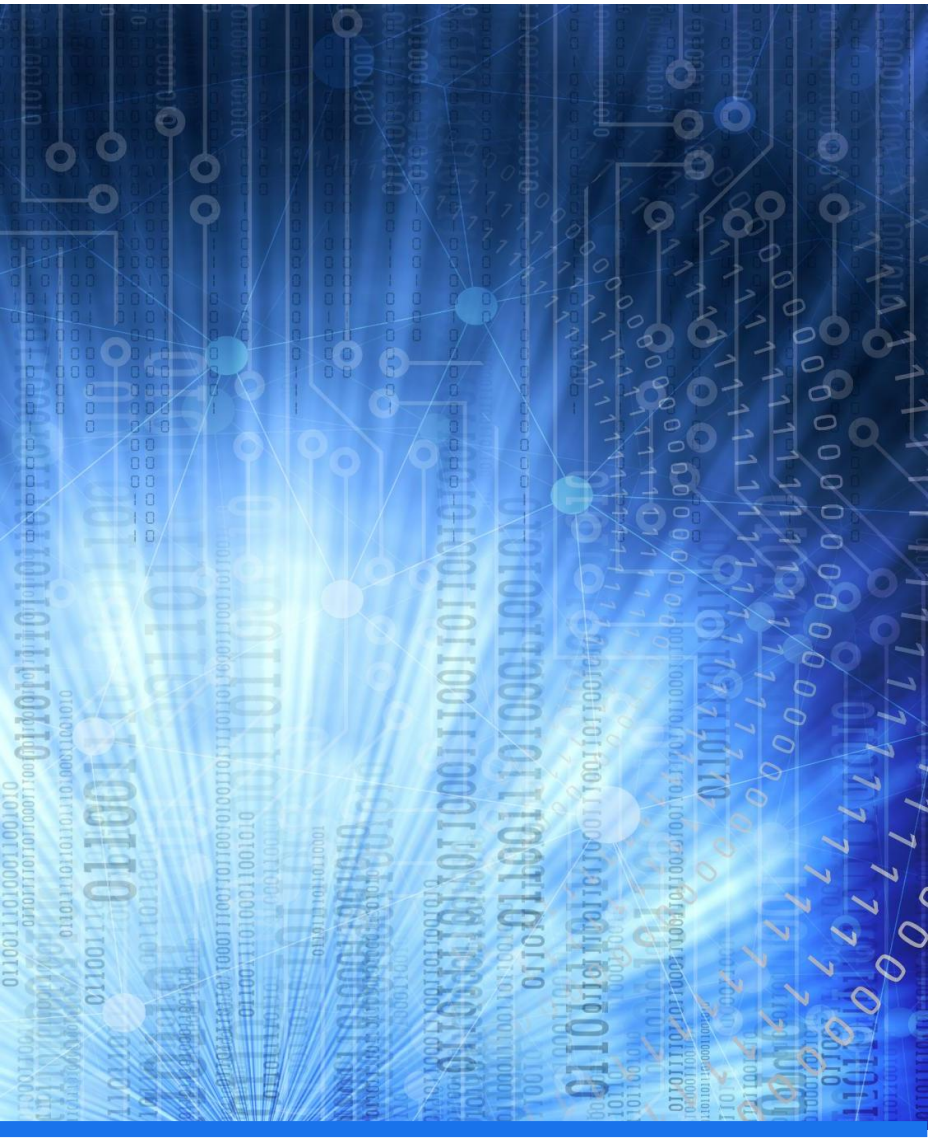
Innovation drives growth and efficiency within organizations, making it essential for competitive advantage in today's market.

Importance of Security

Robust security measures protect organizations from threats, ensuring the safety of data and maintaining customer trust.

Investment in Practices

Ongoing investment in both AI technology and cybersecurity is necessary to effectively balance innovation with security needs.



Strategic Recommendations for Organizations

Integrating AI in Cybersecurity

Organizations need to develop strategies that effectively integrate artificial intelligence into their cybersecurity frameworks for enhanced protection.

Addressing Ethical Challenges

It is crucial to address ethical challenges associated with AI use in cybersecurity to ensure responsible implementation.

Collaboration and Learning

Collaboration between teams and continuous learning are essential for effectively overcoming operational challenges in cybersecurity.

Conclusion:
towards an empowered and unstable cyberspace?

The rise of generative AI in cybersecurity points to an uncertain future:

The risk of **cyberspace being dominated by autonomous agents** is becoming tangible.

We'll need to rethink **AI governance** and **international collaboration**, and set up **new control and regulatory mechanisms**, without putting the brakes on innovation.

At the same time, **questions of ethics, energy, fair access and transparency** will become as critical as purely technical considerations.


BSIDES LUXEMBOURG
Thank you for your attention
Questions?
David HAGEN
david@hagenadvisory.lu
HAGEN ADVISORY