The evolution of AI - Threats and Opportunities

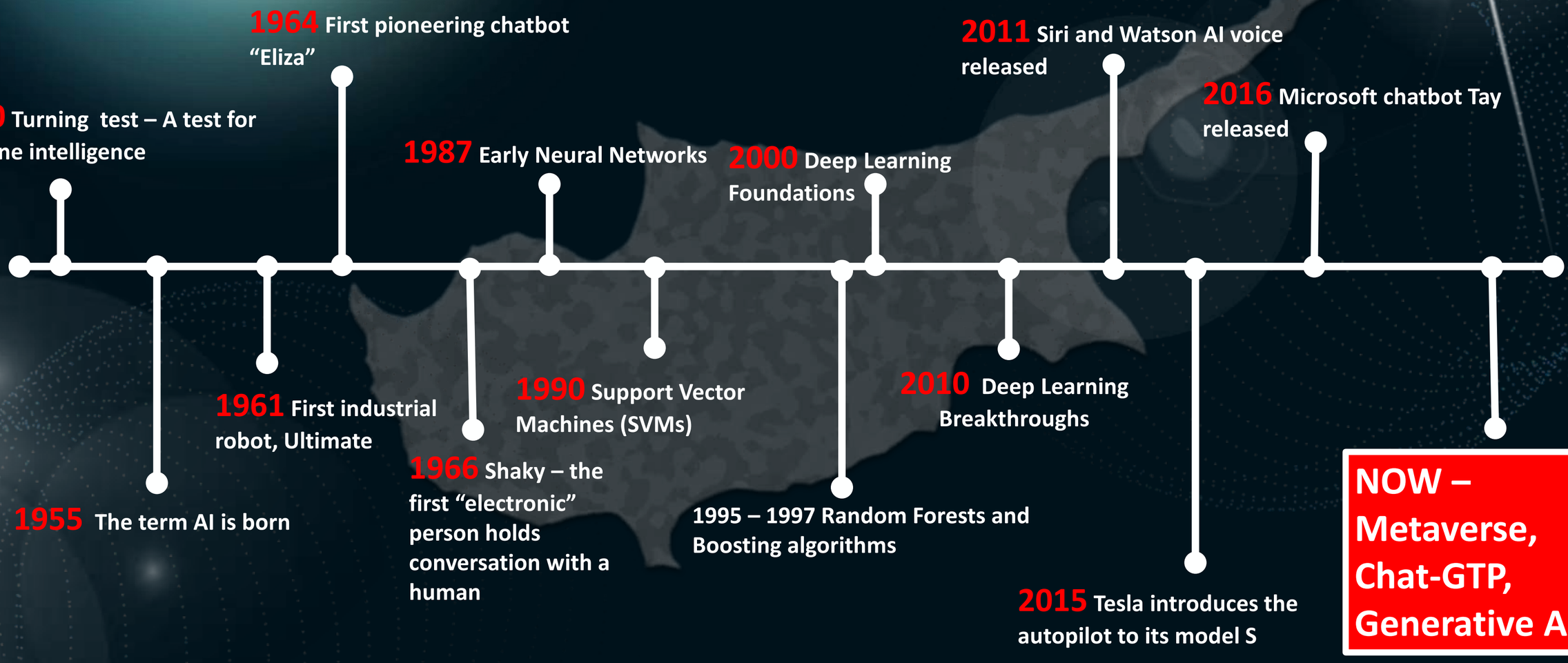
Demetris Skourides – Chief Scientist for Research, Innovation and Technology of the Republic of Cyprus

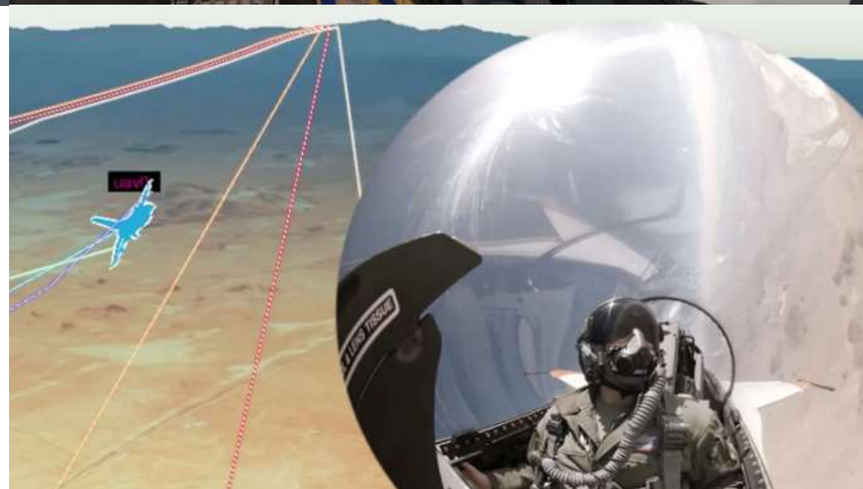
The Cyprus International Defence and Security Conference
13/12/2024

Chief Scientist for Research, Innovation and Technology

RESEARCH & INNOVATION FOUNDATION

The Evolution of AI





Next Generation AI Jets vs Co-Pilots

Advantages, Risks and Threats

Chief Scientist
for
Research, Innovation
and Technology

AI Applications in Defence

HEALTH CARE ON THE BATTLEFIELD

AUTONOMOUS WEAPONS AND TARGET RECOGNITION

CYBER SECURITY

LOGISTICS

SURVEILLANCE

C4ISR solutions (Northrop Grumman)

AI enhances situational awareness by helping to identify patterns in real-time, facilitating faster, more accurate decision-making

Iron Dome (Rafael)

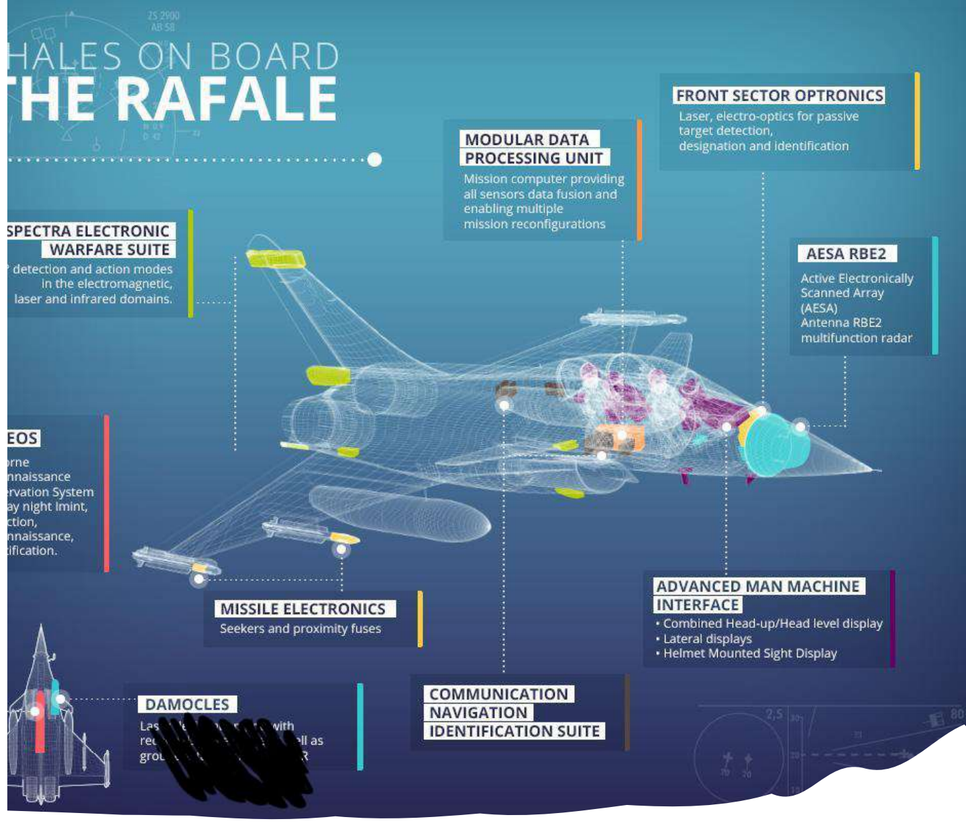
AI-powered algorithms analyze radar and other sensor data to track incoming missiles

SPEAR-EW Cruise Missiles (MBDA)

The AI-driven system, allows the missiles to collaborate with the aircraft controlling them.

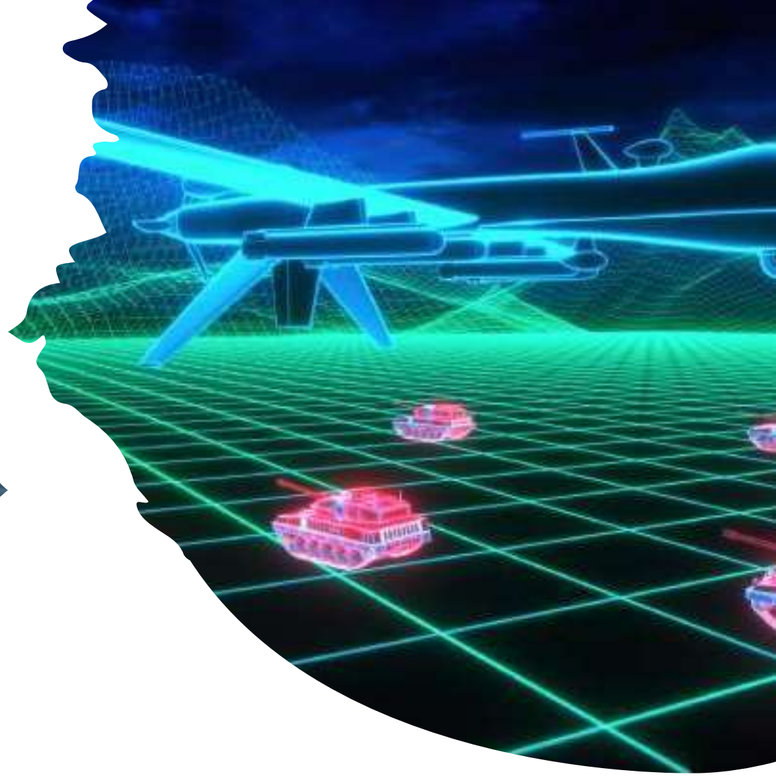
Lynx KF41 (Rheinmetall)

AI for target identification, autonomous navigation, and decision support in battle.



Redefining Modern Warfare

“AI enables humans and machines to SEE AROUND CORNERS enabling the communication of Operational insight across theatres possible in Real-time. This capability make the Art of the Impossible Possible” Demetris Skourides, Cyprus Chief Scientist for Research, Innovation and Technology



The Game Changer

“AI breaks across silos, disrupts use-cases, and when operational insight across all systems is combined, the cost of defending against is just too big. Defence analysts will have to rethink their playbook”
Demetris Skourides, Cyprus Chief Scientist for Research Innovation and Technology

Chief Scientist
for
Research, Innovation
and Technology

AI Applications in War – Deepfakes

- Deepfakes are increasingly being used in cyber warfare. They involve mixing real and fake content to create highly believable but false information

- Deepfakes pose a significant threat to national security by enabling the spread of misinformation and digital impersonation.

- Fake footage showing military atrocities or manipulative speeches can destabilize political situations, disrupt diplomatic negotiations, and incite violence.

Autonomous risk decisions and AI errors impacting warfare

- Autonomous systems rely on data-driven algorithms to process information and make decisions.
- These systems are prone to failures like incorrect pattern recognition, incomplete datasets, or adversarial manipulation.
- Such issues can lead to flawed decisions, including targeting errors or misinterpretations of battlefield conditions, potentially resulting in unintended escalation of conflict

AI ETHICS?

Texas Instrument Robot

Human Biotech Strength

Chief Scientist
for
Research, Innovation
and Technology

nccgroup

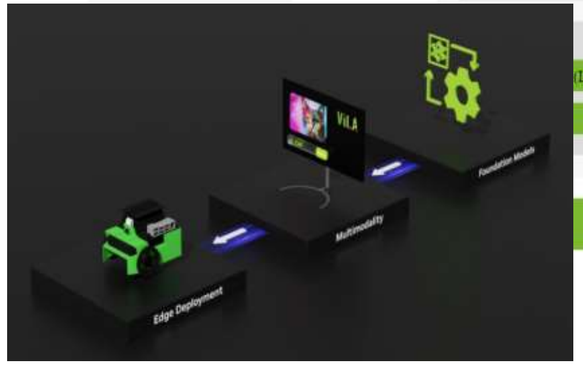
Security Risks of AI Hardware for Personal and Edge Computing Devices

Google
July 11, 2024

Key Findings

Some key concerns for threat modeling the use of specialized hardware in AI applications became apparent during the literature review:

- Based on recent vulnerability research explored in the AI Models Running Locally section, running AI models on dedicated hardware presents a complex attack surface in both edge computing and cloud computing environments. Vulnerabilities in components such as Graphics Processing Units (GPU) and Neural Processing Units (NPU) range from side-channel attacks that can leak data, to malware exploits of proprietary user space frameworks that interact with the GPUs where users can create custom GPU programs.
- Closed approaches to integrating AI capabilities in edge devices present different risks to taking a modular open approach. This includes risks around over-reliance on the vendors security practices, inflexibility when responding to security incidents and challenges around transparency and third party assurance. System owners should ensure they understand the security responsibilities they are implicitly delegating to vendors.
- Moving AI capabilities to the edge can result in performance and privacy improvements by performing at least some of the processing locally on user devices. However these privacy improvements become more nuanced when distributed deep learning is deployed as it becomes difficult to manage the privacy and integrity of data used in the distributed deep learning process.
- The context in which AI systems on edge devices are used affects their risk profile. Compliance requirements with regulations, such as the European Union (EU) AI act, will be driven by potential impacts which differ greatly in the context of an office or personal AI assistant versus capabilities deployed in safety or privacy critical industries.



Balancing Opportunities and Risks

- Robust Cybersecurity Measures
- Leverage Synthetic Data
- AI and Predictive Analytics
- Investment in AI Research
- Training and Development

THANK YOU

Chief Scientist
for
Research, Innovation
and Technology