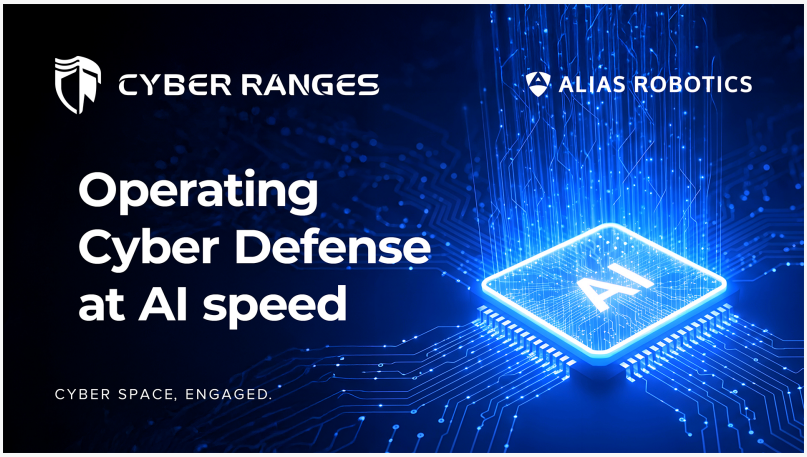
Operating cyber defense at AI speed: the defender’s 'unfair advantage'

Alias Robotics and CYBER RANGES validate a new operational model for national cyber defense capabilities



VITORIA-GASTEIZ, ALAVA, SPAIN, April 30, 2026 /EINPresswire.com/ -- For decades, cyber operations have been defined by an asymmetry: attackers move faster than defenders. Artificial intelligence is accelerating that imbalance—enabling threats to operate autonomously, at machine speed, and at scale.

Companies, public institutions and defense organizations are now facing a new class of threats: AI-powered attackers capable of executing automated operations in real time. In this context, traditional approaches —based on static testing and delayed response— are no longer sufficient to model or defend systems under real-world conditions.

New research from Alias Robotics demonstrates that cyber defense can now operate in real time against these threats.

Through dynamic cyber emulations carried out with CYBER RANGES, Alias Robotics has validated a new operational model: sovereign AI-driven defensive systems capable of monitoring, adapting, and responding to attacks as they unfold, deployed within fully controlled on-premise environments.

A shift in how cyber defense is built and operated

The findings point to three structural changes shaping the future of cybersecurity, supercharged by AI.

Static testing no longer reflects real-world threats

- AI-driven attackers can fully compromise environments without active resistance.

Defense must operate at machine speed

- Effective protection depends on systems that respond in real time, not after an incident.

Full control becomes essential: sovereignty as a requirement

- Cyber defense cannot rely on external cloud-based AI when operating in regulated or critical environments.

Validated in enterprise and defense environments

The research evaluated attacker and defender systems across multiple environments, from enterprise infrastructure to military-grade simulations.

Key findings include:

- Attacker success drop from 100% to 0% under active AI defense
- Full attack prevention is achieved in multiple configurations, including defense-grade scenarios
- Comparable results are achieved using specialized AI models deployed locally, maintaining full control over data and operations
- These results indicate that effective cyber defense is no longer defined by scale of compute but by the ability to operate continuously and under control.

Sovereign AI as national capability

The study challenges the assumption that advanced cyber defense depends on large, cloud-based AI models.

Instead, it demonstrates that sovereign, locally deployed systems can enable governments and critical operators to retain full control over infrastructure, data, and decision-making.

This approach aligns with increasing regulatory and strategic requirements, including frameworks such as GDPR and NIS2, and reflects growing demand for nationally controlled cybersecurity capabilities.

“The only way to combat attackers at machine speed is to deploy defenses at machine speed. And the only way to trust your defenses is by owning total control over them” says Endika Gil-Uriarte, CEO at Alias Robotics.

“The opportunity to test your defense abilities with hyper-realistic scenarios with AI-enabled

tools and sandbox warrants your cyber defense force remains ahead of the cyber game against increasingly complex threats" adds Al Graziano, CEO at CYBER RANGES.

Operational capability for real-world environments

Alias Robotics develops Cybersecurity AI (CAI), a platform designed to deliver cybersecurity automation capabilities in real-world environments.

Built for critical infrastructure and mission-critical systems, CAI enables:

- Continuous validation of security posture
- Automated detection, mitigation and response to threats
- Reproducible and auditable cyber operations
- Full control, full sovereignty
- The platform is designed for 100% on-premise deployment, ensuring that all operations and data remain within the organization's infrastructure.

About the research

The study was conducted by Alias Robotics in collaboration with the University of Naples Federico II and CYBER RANGES Group Ltd. It evaluates AI-driven attacker and defender systems across controlled and operational environments, including military-grade cyber exercises.

Alias Robotics and CYBER RANGES are available for strategic briefings with media, government stakeholders, and defense organizations.

Learn more and download research paper

https://cyberranges.com/operating-cyber-defense-at-ai-speed-the-defenders-unfair-advantage/

About Alias Robotics

Alias Robotics is a cybersecurity company focused on AI-driven defense for complex IT, OT, and critical infrastructure environments. The company develops technologies that enable organizations to operate cybersecurity continuously in real-world conditions, with a strong emphasis on data sovereignty, operational control and national capability.

About CYBER RANGES

Headquartered in Stafford, Virginia, with operations supporting global clients, CYBER RANGES is a pioneer in next-generation cyber range technology. Leveraging cloud-native architecture, the company delivers scalable, high-fidelity simulation environments for cybersecurity training, capability validation, and organizational resilience testing. Trusted by governments, militaries,

and enterprises worldwide—including as the official cyber range provider for the UN's International Telecommunication Union—CYBER RANGES empowers teams to build, test and refine cyber skills in realistic, mission-relevant scenarios.

Media Contacts

For further information or specific inquiries, please contact

Maite del Mundo
Chief Marketing Officer
maite@aliasrobotics.com

Marcello Hinxman-Allegri
Head of Marketing & Business Development
m.hinxman-allegri@cyberranges.com

Anthony Munns
CYBER RANGES
+1 800-959-0163
email us here
Visit us on social media:
LinkedIn
YouTube
