New Advances in AI FOR DEFENSIVE CYBER OPERATIONS

(The French Case)

By: Professor Wael Saleh,
Expert at Trends Research & Advisory

In an era where cyberattacks increasingly target sensitive state information—particularly military operations—implementing effective cybersecurity measures has become a formidable challenge. Attackers often have access to more innovative tools than those used in defensive cyber operations, making cyber warfare one of the most critical battles of modern times.

One of the most effective strategies in this domain is leveraging artificial intelligence (AI) for defensive cyber operations. According to General Aymeric Bonnemaison, Commander of the French Cyber Defence Command (COMCYBER), the primary goal of AI integration in cybersecurity is intelligence gathering and disrupting enemy systems to enable military interventions under optimal conditions.

During the European Cyber Week (ECW) held at the end of 2024—where AI was incorporated for the first time—General Bonnemaison asserted, "There is no cyber defence without AI, and no AI without cyber defence." This statement underscores the growing global investment in AI-powered cybersecurity, as governments recognise that sustainable investment in this field is crucial for maintaining military operational advantages and achieving strategic goals in the digital age. This study aims to shed light on the latest advancements in AI for defensive cyber operations, with a specific focus on the French case. It is structured into two main sections: the first highlights the added value of AI in defensive cyber operations, while the second examines key AI-driven developments in France's cyber defence landscape.

» Aymeric Bonnemaison.

The Added Value of AI in Defensive Cyber Operations

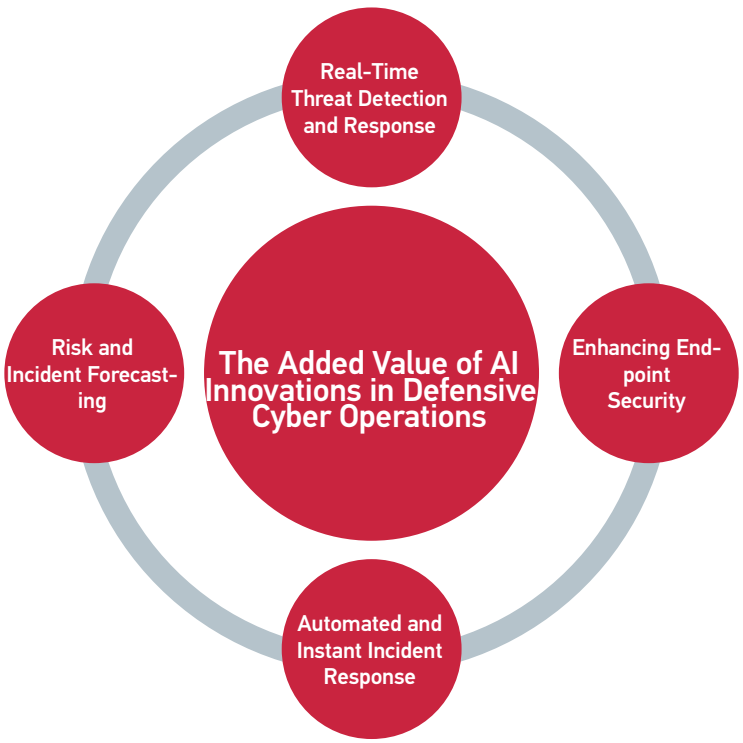
AI plays a pivotal role in cybersecurity, offering proactive solutions to counter increasingly sophisticated cyber threats. AI-driven cybersecurity enhances defence and security measures by providing advanced tools and methodologies to improve threat detection, response, and prevention. The primary areas where AI contributes to cyber defence include:

1. Real-Time Threat Detection and Mitigation

AI-powered systems continuously monitor network security to identify potential cyber threats against military institutions using machine learning algorithms that:

- Detect irregular behaviours that may indicate malware infiltration or phishing attempts.
- Identify vulnerabilities often overlooked by traditional security methods.

Strengthening Endpoint Security



Artificial intelligence is emerging as a decisive weapon in defensive cyber operations.

Artificial intelligence and cybersecurity are inseparable—one cannot exist effectively without the other.

- Provide real-time alerts, enabling rapid responses to security incidents.

2. Risk and Incident Prediction
By analysing historical data, AI can predict future cyber threats against defence and security institutions, allowing them to:
- Continuously plan and fortify defences against potential attacks.
- Detect and resolve critical vulnerabilities before they are exploited.
- Enhance risk management through data-driven, actionable insights.

3. Automated and Instantaneous Incident Response
AI enhances the speed and efficiency of incident response strategies by automating critical tasks to:
- Isolate compromised systems to prevent the spread of malware.
- Generate comprehensive forensic reports for post-incident analysis.
- Reduce the workload on human analysts by handling repetitive security operations.

4. Strengthening Endpoint Security
AI improves endpoint protection by:

- Continuously monitoring for unusual or suspicious activities.
- Detecting advanced persistent threats (APTs) that evade traditional antivirus tools.
- Using behavioural analytics to identify insider threats or compromised credentials.

Key Programs and Technologies Enhancing French Cyber Defence with AI include:
Mactan
Mactan is a technology that enables security and defence forces to maintain cyber protection for their operations anywhere in the world, without the need for specialists. Thanks to its modular design and guaranteed adaptability, Mactan seamlessly

» During Eurosatory 2024, Bertrand Rondpierre presented six examples of the use of artificial intelligence in the armed forces

The French Cyber Defence Academy is equipping elite experts with the skills to implement modern cyber warfare strategies.

With the rise of deepfake technology, manipulated videos, images, and voices pose a severe threat, especially if spread through social media or the internet.

» integrates with various security systems, such as the Endpoint Detection and Response (EDR) system, which detects threats and neutralises them before they spread across the network. In addition to its effectiveness in monitoring and protecting communication and information systems using AI, its ease of deployment, small size, and rapid installation make it particularly suitable for complex combat environments.

Reveal
Reveal is a program capable of thoroughly analysing and sanitising file content, extracting data from various file formats—including archives, emails, and attachments—or directly from virtual machines to neutralise malicious data.

DataSphere
DataSphere provides comprehensive document security throughout its lifecycle. This solution ensures compliance by combining data classification mechanisms, encryption, and continuous access control, making it an ideal cybersecurity tool for data centres.

Threat Watch
Threat Watch is designed specifically for threat monitoring and risk management related to security vulnerabilities affecting military information systems. The program provides real-time user alerts with personalised vulnerability analyses within their specific context, allowing for an accurate risk assessment. By consolidating all necessary security data into a single tool, it facilitates a smooth and efficient mitigation process.

SEDUCS
SEDUCS is a platform for developing AI-powered sovereign operating systems that can be deployed across all types of devices and systems to ensure optimum security. Its SEDUCS Unifyer solution enables the creation of a dual-band, dual-level workstation, allowing users to operate seamlessly in two separate cyber environments with distinct security requirements.

Advances in AI-Powered Cyber Defence: The French Case Study

A review of literature related to the latest developments in artificial intelligence for cyber defence operations in France highlights the following:

1. Expansion of Multidisciplinary Cyber Defence Recruitment
France's cyber defence sector is experiencing increased recruitment. General BonneMaison stated that 4,000 personnel currently work within Cyber Defence Command, with plans to hire over 1,000 additional professionals by 2025. He also emphasised the diverse

» France has created a cyber defense academy with the aim of training experienced cyber fighters capable of implementing modern combat doctrine in the fields of cyber warfare.

opportunities available in the field, encompassing roles in protection, cyberattack countermeasures, electronic espionage, and combating disinformation on social media. The variety of responsibilities necessitates a broad spectrum of professionals, including technicians, analysts, experts, as well as psychologists, linguists, and digital marketing specialists.

2. Institutionalising Cyber Defence Education and Training

As of January 1, 2025, the Cyber Operational Readiness Centre (C2PO) has been transformed into the Cyber Defence Academy. The aim is to train skilled cyber fighters capable of implementing modern cyber warfare doctrines. According to Lieutenant Colonel Yves-Marie, head of the Cyber Defence Academy, "This change is not just a rebranding; it marks a fundamental shift in the education and training model for cyber defence." The academy will not only focus on military cybersecurity specialists but also extend its reach to school and university students, private sector professionals, and civil society members.

3. Integrating Information Warfare and Narratives into AI-Enhanced Cyber Defence

France's AI-driven cyber defence strategy considers information warfare an integral part of any military strategy. Without the ability to influence narratives and counteract adversarial messaging, any military engagement risks failure. The rise of social media has reinforced this perspective, exponentially accelerating the spread of both accurate and false information, while increasing the frequency and scale of its dissemination. This enables adversaries to rapidly mobilise for violence and undermine the legitimacy of various stakeholders.

At the Eurosatory 2024 exhibition, Bertrand Rondpierre, Director of the French Ministry of Defence and AI Agency (Amiad), presented six examples of AI applications in the armed forces. Among them were AI-driven programs capable of detecting deepfake content and false information targeting the French military. As it is now easier than ever to manipulate videos, images, and audio, the spread of such deceptive content via social media or the internet could have severe consequences for French military units deployed both domestically and abroad.

4. Developing an AI-Enhanced Defence Cloud

The French strategy also believes that accelerating decision-making cycles, detecting changes and threats in real time, improving synchroni- »

» The most crucial investment in artificial intelligence is in developing skilled human resources.

» sation between services, ensuring the security of supply chains, and winning the battle of information and narratives must be achieved through AI-enhanced defence cloud technologies. These technologies can consolidate the digital and cyber sovereignty of military forces.

In this context, Sopra Steria has become a key partner of the French military and European security institutions due to its expertise and participation in core initiatives related to digital sovereignty and the next generation of AI-powered cloud solutions. This collaboration aims to establish a multi-domain, decentralised combat cloud—a global network protected from cyberattacks and capable of sustaining information exchange at strategic, operational, and tactical levels by 2035. Moreover, this cloud will provide advanced computing, storage, and information processing capabilities (on-site) with high-level security, thanks to AI.

5. Increasing Investment in AI-Enhanced Cyber Defence Innovation

In May 2024, the French Ministry of Armed Forces and Veterans Affairs established the Ministerial Agency for Defence and Artificial Intelligence (AMIAD) and appointed Bertrand Rondepierre as its director. The agency's goal is to ensure France's sovereign control over AI in defence, preventing reliance on foreign powers.

With a budget of €300 million, the new agency operates in two key sectors:

- A research sector based in Palaiseau (Essonne)
- A technical sector in Bruz, near Rennes

One of AMIAD's most important projects is developing language models—AI systems designed to translate natural language for machines, enabling them to understand, analyse, respond to requests, and eventually learn—tailored to the French military's operational framework.

Additionally, the agency has contracted the purchase of the most powerful AI-dedicated supercomputer in Europe, in partnership with HP and Orange.

Rondepierre has repeatedly stated that AI is the key weapon for winning future conflicts. To that end, AMIAD is working on new jamming systems capable of neutralising a specific drone from among others using highly targeted electromagnetic pulses—aided by AI detection algorithms.

» Emmanuel Macron.

THE FRENCH CASE STUDY

The French Ministry of Defence and Artificial Intelligence Agency is advancing electronic warfare capabilities with next-generation drone jamming technology.

Artificial intelligence continues to transform the landscape of cyber warfare, ensuring that battlefields of the future will never look the same.

Beyond these new jamming systems, AMIAD is actively developing a large number of AI projects, with about twenty set for delivery in 2025. According to Rondepierre, "the primary AI investment must be in human resources", which is why the agency plans to double its workforce by next year.

Conclusion

AI will undoubtedly continue to reshape the cyber battlefield, enhancing cyber defence while at the same time expanding the diverse capabilities of cyber adversaries.

Perhaps the most striking illustration of this came from French President Emmanuel Macron, who, in a speech to French ambassadors on January 6, 2025, remarked:

"Ten years ago if someone had told us the owner of one of the world's biggest social-media companies would support a new international reactionary movement and intervene directly in elections, who would have imagined that?"

Macron was referring to Elon Musk, the owner of X (formerly Twitter) and the AI-focused company XAI, as well as a co-founder of OpenAI in 2015.

Another example demonstrating the emergence of new players in AI-driven cyber operations, and the opportunities and risks associated with this trend, is Google's recent policy change. The company lifted its ban on using AI for weapon development and surveillance, as outlined in its updated AI usage policy.

This has raised concerns regarding Google's involvement in Project Nimbus—a joint cloud computing initiative between Google, Amazon, and Israel, which provides a full suite of AI and machine learning tools.■

Sources and references

- The Age of Techno-Fascism and the Shifts in Silicon Valley Policy, Thursday, Enterprise, February 6, 2025, https://enterprise.news/egypt/ar/news/story/pm/2025-02-06/3
- Conférence des Ambassadrices et Ambassadeurs 2025, https://il.ambafrance.org/Conference-des-ambassadrices-et-ambassadeurs-2025
- IA de défense : 6 cas d'usage concrets dans les armées, Ministère des Armées, 18 juin 2024, https://www.defense.gouv.fr/actualites/ia-defense-6-cas-dusage-concrets-armees
- Marc Jacob, Sopra Steria lance une version projetable de Mactan, novembre 2024, https://www.globalsecuritymag.fr/sopra-steria-lance-une-version-projetable-de-mactan.html
- Pas de cyberdéfense sans intelligence artificielle et pas d'IA sans cyberdéfense" (Général Bonnemaison) ، COMCYBER , 20 novembre 2024, https://www.defense.gouv.fr/comcyber/actualites/pas-cyberdefense-intelligence-artificielle-pas-dia-cyberdefense-general-bonnemaison-comcyber
- Naissance de l'Académie de la cyberdéfense : une offre de formation cyber pour l'ensemble des armées, COMCYBER, https://www.defense.gouv.fr/comcyber/actualites/naissance-lacademie-cyberdefense-offre-formation-cyber-lensemble-armees