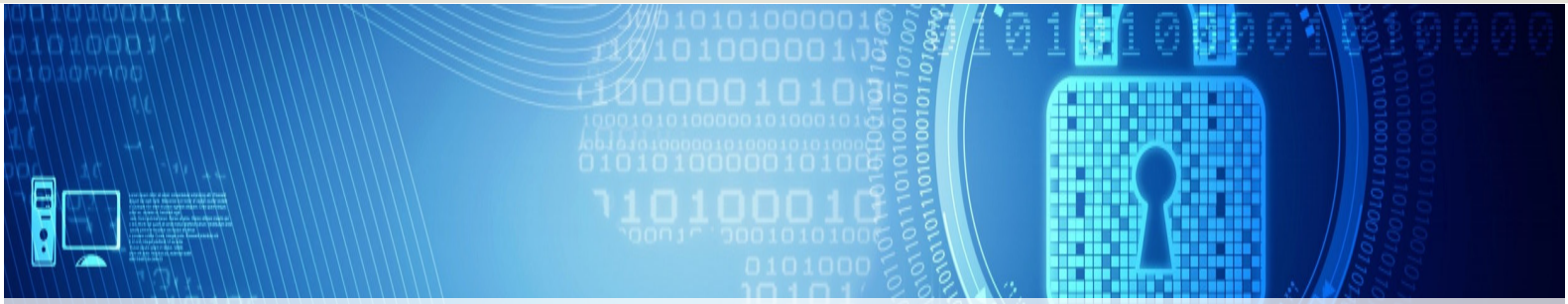

Information systems, artificial intelligence and cybersecurity

BRENNUS 4.0

Mesdames Claire Angelotti et Clarisse Naegels, rédactrices du pôle études et prospective du CDEC

Published on 02/04/2020

Sciences & technologies

Since the 2000s, the various official texts relating to national defence and security - White Paper, Strategic Review, Military Planning Law - have emphasised "knowledge and anticipation" as a strategic function of the Armed Forces. To ensure this strategic function, and with the aim of guaranteeing the operational superiority of French forces, information control and the optimisation of defence information systems have become major challenges for the Armed Forces. The development of Artificial Intelligence (AI) is today changing the use of information systems and data processing. Often described as a cyber vulnerability, AI is also an opportunity in the field of cybersecurity.

Information systems

The computerization of manual tasks and the digitization of the Armed Forces have resulted in the creation of multiple information systems used for command, intelligence, operational readiness and the conduct of operations. In a 2011 report, the Court of Auditors defines information and communication systems (CIS) as "organised sets of actors, procedures and technologies for capturing, grouping, storing, manipulating, protecting and disseminating information used in one or more operational processes". The aim of information systems is therefore to provide access to information at any time and in any place, to make operational use of it, to transmit orders and to ensure information sharing (at a joint, joint and combined arms level). The digitisation of operations has become a strategic imperative and has fostered the development of information flows within diverse and varied information systems. At the joint level, the Army Information System (AIS) programme was launched in 2010 to transform the operational and command information systems (OIS) of the three armies and ensure their convergence into a single system. The aim of the programme is to provide an operational response to the needs of the armies while drawing on advances from the civilian world. The proliferation of information systems (SICF for the Army, SIC21 for the Navy and SCCOA for the Air Force) has been a challenge for the interoperability of systems.

The French Army's Synergie du contact Renforcée par la Polyvalence et l'Infovalorisation (SCORPION) programme goes beyond capability renewal and aims to develop collaborative combat through the evolution of information and communication systems. At the tactical level, the SCORPION Combat Information System (SICS) must be able to replace all the information systems deployed to centralise data and communication, harmonise systems and make them easier to use. The SCORPION Combat Information System is designed as a "system of systems" for greater coherence. The objective is to ensure tactical information sharing and to promote interoperability between systems. SICS will be the single reference system for the deployed AIG. This will provide interconnectivity between the AIG, vehicle electronics (vetronics) and CONTACT radio communication systems.

The contribution of AI in information systems

Described as a "national defence priority" by Armed Forces Minister Florence Parly in her speech on AI on April 5, 2019, and as a "military power issue" by the 2017 Strategic Review and the 2019-2025 LMP, AI is at the heart of the department's transformation strategy. As a revolution for digitalized armament, but above all for data and information processing, it requires the full attention of the armed forces. Information systems have favoured the development of massive data flows that cannot be processed by human beings. There is no common definition of AI and the very notion of "artificial intelligence" is being debated. Nevertheless, the report of the AI Task Force, published in September 2019, refers to the Official Journal's definition of AI as an "interdisciplinary field of study".oric and practical field aimed at understanding mechanisms of cognition and reflection, and their imitation by a hardware and software device, for the purpose of assisting or substituting human activities". On the whole, AI would thus consist of reproducing cognitive means through the use of algorithms. It would be more accurate to speak of automation or "augmented intelligence", since the contributions of machine learning, inparticular the use of algorithms, can be used in the same way as the use of computer software.It would be more accurate to speak of automation or "augmented intelligence " , since the contributions of machine learning, in particular deep learning, clearly show that AI's capabilities exceed those of human beings in particular fields, such as the recognition of objects in images or videos.

As Michael C. Horowitz puts it, in the military field, AI is not a weapon but a facilitator that enables, among other things, better management of the operational environment and better operational preparation. It is a breakthrough in the field of threat detection and intelligence processing, from the reception of data to their analysis and representation (or visualisation). AI is being built in the continuity of the digital transformation and provides a response to the challenges of big data. It allows to go further than automatic data processing. Automatic learning and in-depth learning have made it possible to create multilayer networks that enable faster and more accurate data analysis. The machine learns from its mistakes and improves in three ways, either by reinforcement, supervised or autonomously. If the trajectory of the future military exploitation of AI is gradually taking shape, it is certain that politics will play a major role in its realization. All AI development framework nations have developed action plans. Faced with China, which launched its programme in 2017 and which wishes to obtain leadership in AI, France could join European and civil-military partnerships for the development of a sovereign and independent AI.

Cyber security and AI

Two logics clash around the notion of AI: the utopian vision of a world connected and optimized by AI is opposed to an apocalyptic vision of AI, a door open to all cyber dangers. The objective is not to fight against AI, but to find a balance between the improvement it brings and the inconveniences it brings.nents that it induces, to be able to define the framework rules to be created and make AI a reliable, stable and precise ally. The risks induced by AI, such as massive data theft, must be identified, but not stopped there. Technological developments can be used by the enemy as well as by our armed forces. Indeed, AIs are used both for attack (systems equipped with AIs capable of resisting the defensive system and therefore dedetect and circumvent its use for security purposes) and defence (systems with AIs capable of simultaneously detecting and processing viruses).

The question then arises as to the place of humans in the loop. In her speech on AI, the French Minister for the Armed Forces, Florence Parly, insisted on this point, stating that "whatever the degree of automation or even autonomy of our current and future weapons systems, they will remain subordinate to human command". Among the vulnerabilities induced by AI, machine learning exposes armies and manufacturers to decoys, hijackings or attacks during the learning phase, like the attack on Microsoft's TAY chatbot. AI can also be used in information warfare. Coupled with biometric, facial or voice recognition capabilities, it could mimic a person's voice or behaviour, thus contributing to misinformation.

However, AI is also an opportunity to combat cyber threats. It can indeed bring added value in the field of detection. According to a study by The Inde-dependent IT-Security Institute, 855 million viruses or malware would have been created in 2018. Thus, in the face of a varied and constant creation of malware, traditional methods of cyber protection seem to lack effectiveness. AI would make it possible to identify and detect a virus much more quickly thanks to automatic learning and the detection of weak signals. Until now, it was necessary to detect the virus in order to apprehend it. With AI, most viruses could be detected early and then processed. The British company Dark Trace has developed the world's most advanced machine learning tool. Inspired by the human immune system, this system automatically detects and fights the virus even if it has never been encountered before.

Finally, the AI provides a protection function. Man is the weakest link in computer security; the increased use of the cloud and connected objects (20 billion by 2020 according to a study by the Gartner agency) increases the vulnerabilities of cyberspace. For example, AI would make it possible to strengthen the security of authentication systems. Thanks to in-depth learning, AI would be able to record a fingerprint, a retina fingerprint or even a palm print. When added to the traditional authentication system, the use of biometrics would greatly improve the integrity of our data and prevent the loss of data.The use of biometrics, in addition to the traditional authentication system, would greatly improve the integrity of our data and ultimately prevent malicious software from penetrating a company, a vital operator or even a government department. The Defense Advanced Research Projects Agency (DARPA) is therefore developing an "active" authentication system whose purpose is to create a "cognitive signature" based on observation of the user's attitude when manipulating the computer tool. As a complement to France's cyber-defensive doctrine, last January the French Minister of the Armed Forces Florence Parly

announced the implementation of a cyber-offensive component. This measure demonstrates the growing importance of cyberspace and its bellicose aspect. Finally, the signing last November of a "cyber agreement" between the Ministry of the Armed Forces and representatives of 8 strategic industrial players in the defence sector, the French government and the European Union, was a major step forward in the fight against terrorism.Finally, the signing last November of a "cyber agreement" between the Ministry of the Armed Forces and the representatives of eight strategic defence manufacturers illustrates the progressive integration of cybersecurity issues from the development of weapons systems and information systems.

While AI can be a solution to cope with the increase in information flows, encouraged by the development of information systems, it is also an opportunity to combat cyber risks. More efficient than human detection, AI should be able to provide a network protection function. Through the SCORPION programme, the French Army wishes to integrate this technology into its weapon systems. Given its current low level of development, the integration of AI into weapon systems will nevertheless take time; time that is likely to be needed to better adapt equipment and forces to this technology.

Title : Mesdames Claire Angelotti et Clarisse Naegels, rédactrices du pôle études et pros-pective du CDEC

Author (s) : Mesdames Claire Angelotti et Clarisse Naegels, rédactrices du pôle études et pros-pective du CDEC

Release date 20/03/2020

FIND OUT MORE