CYBERDEFENCE - CONCEPTS, DOCTRINES AND ACTORS

Ivan Velevski
UNIBIT, Sofia, Bulgaria, ivoveervski@gmail.com

Abstract: A strategic issue and priority, cyber defense is a guarantor of national sovereignty. In cooperation with numerous actors, the Ministries of Defense in different countries actively participate in the protection and defense of information systems and the conduct of operations in cyberspace. Competition and conflict are no longer limited to traditional environments, land, sea, air and space. They have expanded to this new field as the use of digital data has grown. Cyber is now considered a weapon to be used in all operations. This consecration has found its articulation in the initiation of numerous expert debates on the topic of cyber defense, the expansion of legislation on this topic and the programming of military funds for the period 2019-2025. For this purpose, a significant increase in financial resources of 1.6 billion and the recruitment of several thousand cyber experts at EU level have been noted. In addition, the European Commission plans €6 billion in investments in the implementation of secure space connectivity by 2027. This effort was continued in the 2024-2030 military programming law with a budget of €4 billion over the programming period, an increase of 150%. This effort responds to a need that is becoming more urgent every day. The doctrinal work published in 2019 on defensive cyber warfare (LID) and offensive cyber warfare (LIO) in military operations complements the cyber defence strategy and contributes to preparing for the future of military operations by gradually integrating this new capability into the overall maneuver of armies.
Keywords: Cyberspace, Cyberwarfare, Cyberdefence, Cybersecurity, New capability

1. INTRODUCTION

Cyberspace: a space of vulnerability and opportunity While our adversaries have not fundamentally changed their objectives – espionage, sabotage or manipulation – the operating methods and techniques used to respond to them are constantly being renewed by the ongoing emergence of new practices and technologies related to digital technology, as well as the hyper-connectivity of our equipment and networks. Cyberspace has its own dynamics: instantaneous exchanges, network diffusion, massive data accessible to all, erasure of borders, etc. It is also an efficiency multiplier provided that we have the right data and information, which have become a critical resource at the heart of the political, economic and social functioning of modern societies. However, our adversaries have perfectly understood the political, economic or operational advantage that they could obtain from exploiting the vulnerabilities of this galloping digitalization, also affecting the battlefield. To reduce their vulnerability, military systems must offer the best possible level of "defendability". This involves, on the one hand, ensuring that the risk of a cyber attack and the potential consequences for the targeted organizations or individuals are properly taken into account and, on the other hand, being able to adapt our capacity for action and reaction to a cyber attack, depending on the operational context or the reality of the threat. Cyberspace is structured into three inseparable layers, from which all threats arise: 1/ a physical layer, consisting of equipment, computer systems and their networks with a material existence (therefore a territoriality that opens onto national, even international law); 2/ a logical layer, consisting of all digital data, software, processes and tools for processing, managing and administering this data, as well as their exchange flows, implemented in the hardware to enable them to provide the expected services; 3/ and a cognitive layer, also called an information layer, made up of information and social interactions of all kinds that are found in cyberspace and people who can declare several digital identities Beyond the notion of "defendability" of systems, cyberdefense within the Ministry of the Armed Forces is fully consistent with the six missions defined by the strategic review of cyberdefense published in February 2018: 1/ prevent: this involves making users aware of the risk represented by the digitalization of organizations or the equipment they serve. This mission is the responsibility of the Ministry's Senior Corresponding Official for Defense and Security (MSCODS); (RAVELLES,R.,2021, p.4.) 2/ anticipate: this involves constantly assessing the probabilities of cyberattacks and taking preventive measures when the threat appears sufficiently strong. This mission is the responsibility of the National Agency for the Security of Information Systems (ANSSI), in coordination with the intelligence services and the Cyber Defense Command (CYBERCOM) within the perimeter of the Ministry of the Armed Forces; 3/ protect: this involves reducing the vulnerability of our computer systems, both by complicating the task of potential attackers and by facilitating the detection of cyberattacks. Protection is necessary throughout the life cycle of the systems; 4/ detect: this involves looking for signs of a possible cyberattack in progress. This mission is the responsibility of CYBERCOM and the units subordinate to the Minister of the Armed Forces. To complete its information, it calls on its national and international partners; 5/ react: this involves resisting a cyberattack so that it does not prevent us from continuing our activity. In most cases, CYBERCOM then triggers a LID operation, in liaison with ANSSI. It

may lead to the use of means that are outside the domain of cyberdefense, or even the Ministry of the Armed Forces (referral to the courts, diplomatic action, economic retaliation, etc.);6/ attributing: this involves specifying the author of a cyberattack using evidence or a set of clues. The intelligence services are at the heart of this process of collecting attribution clues. The attribution decision is up to the highest political leaders. Prevention and protection actions concern the IT systems of the Ministry of the Armed Forces (friendly zone). Anticipation, detection and reaction missions focus on IT systems belonging to other categories of actors (neutral and enemy zones). (Tête,F./Vrignaud,L., 2019)

2. THREE DOCTRINES OF CYBER WARFARE: THE LID, THE LIO AND THE L2I

Operations in cyberspace are based on three doctrines: – the LID, which brings together all actions, technical or not, carried out to deal with a risk, a threat or a real cyberattack; – the LIO, which includes all actions undertaken in cyberspace, conducted autonomously or in combination with conventional military means, to produce effects against an enemy system in order to alter the availability or confidentiality of data; – and the L2I, which designates military operations conducted autonomously or in combination with other operations in the information layer of cyberspace in order to detect, characterize and counter attacks, support strategic communication, provide information or deception. (Chevillot-Miot E. et Le Guédard M. 2020)

a.The lid

The protection of computer networks and information systems is the first line of defense to prevent a computer attack. While this first line of defense is essential, the dynamics of digitization of the systems that support the ministry's activities, including for the benefit of its operational commitment via its command systems and weapons systems, offers new opportunities to attackers; it therefore requires us to develop new modes of defense, adapted to these new threats. It is on the basis of this observation that the Ministry of the Armed Forces wished to redefine its policy on LID. This ministerial LID policy, presented in the form of a ministerial instruction, develops principles for responding to these questions, by specifying the organization and missions that apply to all organizations placed under the authority of the Minister of the Armed Forces, as well as the expectations and constraints of those who contribute, through services or capabilities, to its commitment (industrialists, etc.). The LID brings together all actions, technical and non-technical, carried out to deal with a risk, a threat or a real cyberattack, with a view to preserving our freedom of action. The LID mainly covers three of these missions: anticipate, detect and react and completes the missions: prevent, protect and attribute. It thus contributes to the resilience of the armed forces and more generally to the development of response strategies at ministerial and interministerial levels. Within the Ministry of the Armed Forces, LID operations are planned and conducted by CYBERCOM, in coordination with ANSSI, the intelligence services, and possibly other partners (national or international).

-Military cyberdefense within the State The cyberdefense of the State is the responsibility of the Director General of ANSSI. For the Ministry of the Armed Forces, the conduct of the cyberdefense of its information systems is the responsibility of the Chief of Staff of the Armed Forces (CSAF). The CYBERCOM, subordinate to the CEMA, is responsible for the organization and operations of LID for the entire ministry. It coordinates very closely with ANSSI in the daily exercise of its cyberdefense missions. In the interests of consistency and efficiency, the chain of command for this cyberdefense is said to be unified, centralized and specialized for the entire ministry. That is to say, it is managed and coordinated by CYBERCOM and composed of experts and cyberdefense, it must also promote synergies between the different organizations responsible for LID while providing a global vision of the cyber situation. Within the ministry, each staff, directorate and department sets up LID resources within its area of responsibility in application of the principle of subsidiarity. Each cyberdefense manager within the ministry must be able to rely on an operational structure such as a Security Operating Center (SOC) responsible for supervising its systems. SOCs constitute the first level of detection of cyber attacks. At the ministry level, under the orders of CYBERCOM, the Defensive Computer Warfare Analysis Center (DCWAC) provides an overall technical "hypervision", which synthesizes and shares information on cyber situations produced by all SOCs or by its own means. At the top of the LID chain, CYBERCOM relies on the operations center to guide the work of CALID and SOCs. In particular, it shares the state of the cyber threat and new vulnerabilities discovered in order to optimize the effectiveness of the ministry's cyber defense and protection chain. The CO also supports CALID in managing a cyber incident. The digital transformation of the ministry is characterized both by the speed at which it is conducted and by an ever-increasing connectivity between systems, within the ministry, but also with our various partners including defense manufacturers. Thus, for greater effectiveness against the threat, these partners outside the ministry must be stakeholders in the ministry's LID. Indeed, the attacker is always looking for a weak or indirect point to penetrate military systems. (Ibid.Tête, F. Luc Vrignaud,L.2019)

-A permanent LID cyber posture for the defense of digital systems The Ministry's LID complies with rules of engagement and confidentiality issued by CYBERCOM. A LID operation may require degrading or interrupting a

service. This decision is generally made by the head of the unit using the system in question. However, if the seriousness or urgency of the situation requires it, the shutdown may be imposed by a higher level or COMCYBER. The tension generated by cyber attacks, cyclical or sudden, of varying severity, requires the adoption of constant vigilance, which is embodied in the permanent cyber defense posture (PPC) for the Ministry of the Armed Forces. The PPC consists of all the provisions adopted to ensure the permanent defense (24/7) of the Ministry's IT systems in the "competition-protest-confrontation" continuum. The Strategic Cyber Defense Review of February 2018 established a classification of computer attacks that takes into account the characterization of the impact (from negligible to extreme) and the possibility of legally characterizing this attack as an armed aggression. In line with this classification, the PPC identifies four levels of threat against the ministry's computer systems: yellow and orange, identifying more or less significant potential risks, red, hostile risks deemed plausible and scarlet, major and simultaneous risks. This risk scale, which combines threat level and system protection objectives, is supplemented by an alert stage, "vigilance", "reinforced", or "crisis", which specifies whether the attack is upcoming or ongoing, to adapt accordingly the measures to be taken within the ministry, which can thus occasionally vary from one area or particular domain to another. (Delerue,F.Desforges, Géry,A.- 2019)

b. The lio

LIO refers to all actions undertaken in cyberspace that produce effects against an enemy system, to alter its availability or confidentiality of data. The effects of LIO can be material (neutralization of a weapon system) or immaterial (temporary, reversible or definitive intelligence gathering). LIO can be used autonomously, but it is in combination with conventional military means that it takes on its full dimension as a potential multiplier of effects. In addition, LIO has its own temporality: if the effects can be dazzling, its integration into the overall operational maneuver is the result of long and very specific planning. The primary objective of LIO is to contribute to military superiority in cyberspace. It makes it possible to achieve three types of operational objectives in the conduct of operations: 1/ the assessment of enemy military capabilities by collecting or extracting information; 2/ the reduction, or even neutralization of adversary capabilities; 3/ and the modification of the adversary's analysis capacity. The targets targeted may be exposed on the Internet, isolated, or an integral part of a more global weapons system. The actions are not necessarily in physical contact with the adversary. Within the Ministry of the Armed Forces, the LIO is organized according to a unified chain of command under the responsibility of CYBERCOM. The use of the LIO requires control of political, legal and military risks. It is determined by the law, the cost/effectiveness ratio, the operational situation and the general political context. (Cabirol, M.,2022, p.1)

c. The l2i

L2I refers to military operations conducted in the information layer of cyberspace to detect, characterize and counter attacks, support strategic communication (StratCom) which makes it possible to frame the design and conduct of any military activity of the French armed forces as a coherent, credible and effective message to the main actors who are aware of it, provide information or deceive, independently or in combination with other operations. The place of action of L2I is the information layer of cyberspace. Due to the characteristics of this space, its control requires skills common to those of the LID and the LIO. The planning and conduct of L2I operations in this environment are ensured by CYBERCOM and integrated into joint actions. They consist, essentially, in detecting information attacks likely to harm the reputation of the armed forces or hinder their action, characterizing them, countering them and promoting the action of our forces. L2I can also offer, in our theaters of operations, opportunities for intelligence gathering and deception operations that must be fully exploited. Concretely, the actions carried out under L2I involve supporting StratCom, disrupting enemy propaganda, denouncing false information and mobilizing the adversary's opponents in order to amplify their actions. 3. Beyond the doctrines of cyber warfare Cyberspace is now a space for maneuver and confrontation in its own right, just like terrestrial, maritime, aerial and extra-atmospheric environments. It is a transverse environment without which almost no activity is possible in other environments. In particular, it has close links with the electromagnetic and information fields. Action in or from cyberspace can thus produce effects in all environments and fields. For example, a cyber attack can cause a satellite to deviate from its course. Conversely, an action in these environments and fields can produce effects in cyberspace. For example, a bomb launched against a data center can destroy its servers. In this context, cyberspace has acquired a strategic value that allows it to guarantee the freedom of action of forces in other environments and fields. However, the threat is multifaceted, permanent, non-territorialized and can impact all tactical levels, at the front as well as at the rear. (Filippone,D. 2019) This environment must therefore be taken into account in the maneuver to protect oneself and to seize opportunities to act. Above all, it must be taken into account from the competition phase of the "competition-protest-confrontation" continuum, in the neighborhood as well as on a mission. In fact, there are necessarily obvious specificities of the environment in the exploitation of the cyber component by the three armies. A submarine is not subject to the same cyber threat as a division PC installed in an industrial zone of a city or a military aircraft landed on a theater air base. Similarly, the adversary digital environment of a naval, land or air force

is closely linked to the environment. The three components of the Ministry of the Armed Forces' cyber defense policy (LID, LIO and L2I) allow the three armies to take these dimensions into account (protecting themselves, defending themselves and acting) in an appropriate and complementary manner thanks to an organization ensuring the overall coherence of the ministry's cyber model while respecting the specificities of the armies. But if the doctrines are a reference, they do not constitute a straitjacket. They define the principles and responsibilities and must adapt to employment. In a field as young as operations in cyberspace, it is relevant that they are reviewed regularly with the entire cyber community but also more broadly the military operations community because everything is changing very quickly. The appearance in the doctrinal field of the concept of multi-environment multi-field operations in the 2021 force employment concept reflects this state of affairs. (Filippone,D. 2019)

3. CYBERDEFENSE-ACTORS ET THE MINISTRY OF THE ARMED FORCES AND BEYOND

The three main cyberdefense actors at the Ministry of the Armed Forces: CYBERCOM, DGA and DGSE a. CYBERCOM Placed under the direct authority of the CEMA, the cyberdefense command (CYBERCOM) is an operational command that brings together all cyberdefense forces under a joint authority deployed on several sites in Paris and Rennes. CYBERCOM carries out its missions by delegation of the National Agency for the Security of Information Systems (NASIS-ANSSI), which is responsible for the cyberdefense and cybersecurity of public administrations, companies and, in particular, operators of vital importance (OVI-OIV). Created in May 2017, COMCYBER is responsible for: - designing, planning and conducting cyberdefense operations, as well as defending the information systems of the armed forces, departments and services (ADS) of the Ministry of the Armed Forces (with the exception of those of the DGSE and the DRSD); - the cyberdefense strategy by coordinating the contributions of the armed forces and joint organizations to the national and international cyberdefense policy and by ensuring the consistency of the cyberdefense model of the Ministry of the Armed Forces; - and the capability dimension of the cyberdefense policy by developing the cyberdefense human resources policy, by coordinating the definition of technical needs specific to cyberdefense and by managing the cyberdefense reserve. To fulfill its missions, CYBERCOM exercises operational command over more than 3,600 cyberfighters, divided between the cyberdefense headquarters and four entities: - the LID analysis center (CALID), in charge of monitoring and detecting cyberattacks, as well as anticipating threats and conducting defensive operations. As such, CALID is the Ministry of the Armed Forces' Computer Emergency Response Team (CERT) monitoring, alerting and response center for computer attacks, which constantly monitors the security of the ministry's ADS information systems 24 hours a day. Its personnel can be deployed both nationally and on external operations (NEOX-OPEX); - the information systems security audit center (CASSI), in charge of auditing the compliance and security of the ministry's information systems; – the cyber operational preparation center (C2PO), in charge of training EMDS for combat in cyberspace as part of national and international cyber defense exercises, including the annual joint exercise DEFNET and the international Locked Shields exercise of the cyber center of excellence in Tallinn, Estonia; – and the joint main approval center (CHPI), which conducts security studies leading to the approval of the ministry's new information systems before they are put into operational service. These four entities are intended to be fully grouped together by 2025 within the army cyber defense group (GCA), created on September 1, 2020 and located in the Stéphant district in the Rennes region. The GCA is in charge of identifying the needs of the Ministry of the Armed Forces' ADS in cyber defense reservists. In this capacity, it ensures their recruitment, selection and assignment across the national territory.(Billois, G. (2019,5p)

4. THE DGA

The DGA, along with the ANSSI and the DGSE, is the most important technical skills center within the State in the cyber domain. It is the technical expert of reference for the Ministry of the Armed Forces. Generally speaking, the DGA is responsible for the design and implementation of systems that guarantee the forces, over time, the cyber resilience of the capabilities they operate, and to acquire and maintain their freedom of assessment and action in cyberspace. This mission is divided into four areas: 1/ bring the cybersecurity of digital systems and weapons systems to a level adapted to the level of the threat in order to be resilient in the face of cyber attacks; 2/ equip our armed forces with systems that allow them to acquire and maintain their freedom of assessment and action in cyberspace, that is to say to conduct actions in the three areas of computer warfare; 3/ guide, maintain and develop the necessary technological and industrial capacities, in line with the national cyberdefense strategy; 4/ increase the cybersecurity of the BITD and contribute to the cyberdefense of the Nation within the C4 of which the DGA is a member alongside the DGSE, the DGSI, CYBERCOM and ANSSI. The DGSE In the field of cyberdefense, the DGSE participates in the protection of the fundamental interests of France through intelligence actions as well as in understanding and reducing the cyber threat (criminal or state). As part of this mission, the DGSE is a member of the C4 and shares its intelligence within this interministerial comitology. On national territory, with the

authorization of the Prime Minister after advice from the CNCTR, the DGSE implements all intelligence gathering techniques (TRR) authorized by the internal security code, according to the principle of proportionality. Abroad, the DGSE uses all types of TRR at its disposal. In anticipation of a hostile action that could affect France, cyber threat intelligence seeks to provide information on actors, whether state or criminal, known to be fueling aggressive projects in the digital space as well as on the tools and services marketed to implement these projects. In addition, in response to a hostile action that has affected France, threat intelligence will be tasked with identifying the perpetrator of the action and the person giving the order. 2. Other actors within the Ministry of the Armed Forces contribute, directly or indirectly, to the cyber defense policy (Manenti, B. 2013). The DIRISI Among the actors in charge of the LID, the Joint Directorate of Infrastructure Networks and Information Systems (DIRISI) plays a basic role. DIRISI's cybersecurity must meet both operational, regulatory and legal requirements, as well as the reality of operations. As such, it is integrated into all of DIRISI's management processes and tools and is subject to overall functional management provided by the DIRISI "cyber" sub-directorate. The DIRISI cyber organization's function is to integrate cybersecurity objectives into all of DIRISI's activities. DIRISI's chain of command simultaneously includes operational responsibilities for delivering SIC capabilities, controlling the cyber risk inherent in the capabilities delivered, and complying with regulations. To exercise these responsibilities, DIRISI has cybersecurity specialists in charge of advising and managing cyber actions. These specialists constitute the functional chain relating to cybersecurity within the directorate. The management of the cybersecurity function is provided by the "cyber" sub-directorate. Its purpose is to provide the central director with reliable information on the level of consideration of security objectives, on the level of exposure to the cyber threat, and to guarantee the consistency of the actions carried out across DIRISI.The "acquisition and logistics" department is responsible for implementing cyber policy and requirements in the drafting of contracts managed by DIRISI. The planning and management of cybersecurity actions relating to the IS operated by DIRISI are carried out within the "operations" division and are integrated into the underlying CIS operations. DIRISI therefore has a Security Operational Center (SOC).

5. THE DRSD

The DRSD is the intelligence service available to the Minister of the Armed Forces to assume his responsibilities in terms of the security of personnel, information, equipment and sensitive installations. Its mission is to detect, identify and neutralize any threat to the Defense sphere resulting from intelligence services, organizations, agents or individuals across the entire TESSCo spectrum (terrorism, espionage, sabotage, subversion, organized crime). The DRSD acts by crossing threats and vulnerabilities in the following areas: 1/ the identification and neutralization of threats are based on the national intelligence orientation plan (PNOR) which sets out the objectives assigned to the specialized intelligence services on the 4 major security and defense issues defined by the national intelligence strategy. The 2021 PNOR also includes a second section devoted to structuring issues for France and requiring a cross-cutting approach. It is regularly updated corresponding to new threats. 2/ the detection and reduction of vulnerabilities which are based, on the one hand, on a regulatory corpus and, on the other hand, on requests from the authorities, in particular with the assistance of the Directorate for the Protection of Defense Installations, Resources and Activities (DPID).(lemonde, The triple inspection role of the Service is defined in the Defense Code: protection of secrecy, protection of points of vital importance (PIV) and protection of the scientific and technical heritage of the Nation (PSTN), both for the armed forces and for defense companies. It is then broken down into the various interministerial and ministerial instructions. Action priorities result partly from planning based on regulatory timetables and imposed deadlines, but also from specific requests from the authorities. In terms of cyberdefense, the DRSD acts as for all the themes of the TESSCo spectrum, in two areas that make the DRSD a global player in intelligence and security: 1/ counter-interference of the forces (CIF): the Service supports CYBERCOM, particularly through the action of a liaison officer deployed by the DRSD within CYBERCOM; 2/ economic counter-interference (CIE) aimed at protecting the scientific and technical heritage of the Nation (PSTN) and the industrial and technological base of defense (BITD) against all forms of predation, in particular cybercrime and cyber espionage; (Tellier, M.(2018) In addition, the DRSD is continuing to develop its own cyber counter-interference capability in conjunction with ANSSI and COMCYBER. Its actions in this area focus across the board (CIF and CIE) on developing the intelligence needed to anticipate and attribute attacks, on investigations following the discovery of compromises, and on the cyber security of government control in the nuclear field. (Poupard, G.2018, 101-108,pp.)

6. The DPID

The DPID was created in 2015 and placed under the direct authority of the Minister for the exercise of its responsibilities in terms of protection of installations of interest to national defense, protection of deterrence means and activities, protection of persons and property of the Ministry, security of information systems of interest to

defense, protection of national defense secrets, protection of the scientific and technical potential of the nation, management of the continuity of ministerial activity. Beyond the Ministry of the Armed Forces and its public institutions, the responsibility of the DPID extends to defense companies and in particular to the Defense Industrial and Technological Base (BITD) and its operators of vital importance (OIV). The DPID is also the service available to the Senior Defense and Security Corresponding Official (HFCDS) of the Ministry. The HFCDS in office is the head of the military office of the Minister of the Armed Forces. The responsibilities of the DPID do not cover the operational use of the armed forces which fall under the responsibility of the CEMA. Both a synthesis level for the benefit of the minister and his office and a normative body, the DPID works to develop a defense and security spirit throughout the ministry. In order to "guarantee to the Minister that defense installations, resources and activities are protected against malicious or hostile acts, breaches of the protection of secrecy and cyber threats (Ventre, D. (2020) ", the DPID analyzes feedback from the field on the ministry's defense and security systems (incidents, inspections) and proposes the ministerial response (ministerial policies and instructions, orientation of the capacity response, approvals of installations or approval of "operator" security plans). The security of installations and means of deterrence - whether they come from public or private operators - is at the heart of the DPID's action. The DPID has around thirty people, civilians and military, including operational reservists, each with confirmed expertise. Digital security has recently been added to the DPID's missions. To improve the readability of digital governance and digital security, the information systems security officer (FSSI), previously attached to the DGNUM, was transferred to the DPID in 2019. This transfer made it possible to refocus the DGNUM on its mission as a "group IT department", responsible for ensuring that the guidelines and standards produced by the DPID are properly taken into account in projects led by the IT departments of the Ministry of the Armed Forces. This development made it possible to integrate digital security issues and "classic" defense and security issues into the DPID in a spirit of overall coherence. As part of this renewed governance, the DPID became the ministerial digital security authority (AMSN) by delegation of the HFCDS. Based on the FSSI, the AMSN pilots the ministerial governance of digital security and produces general documents that allow the interministerial documents to be broken down and the ministry's action to be framed. Based on the DRSD, the COMCYBER, the DGA, the SGA, the DGSE, the DGNUM and the DIRISI, the FSSI proposes the ministerial ambitions and strategic objectives of digital security. It also proposes the ministerial policy of digital security and monitors its application, based in particular on the DRSD whose inspections it mandates. It prepares the ministerial comitology of digital security. A monthly ministerial committee on digital security, chaired by the DPID, led by the FSSI, in the presence of the authorities qualified in information systems security (DGA, SGA, CEMA, DRSD and DGSE) and the aforementioned actors, allows for the regular discussion of topics necessary for the ministry's cybersecurity: human resources, finances, cryptography, threat updates, feedback, cybersecurity of defense companies, among others. This committee is overseen by a steering committee chaired by the HFCDS and by an executive committee chaired by the minister or his representative.Finally, a ministerial mapping of digital security risks and a dashboard, currently being stabilized, make it possible to prioritize the ministry's actions in a risk management logic.(Ventre, D. (2020)

7. CONCLUSION

The DGNUM's mission is to propose the ministerial digital policy and to manage its implementation. As part of the ministerial executive committees (EXCOM) of 2020 and 2021, a new organization of the governance of the conduct and monitoring of digital projects was decided. The DGNUM promoted the unification of the high governance of all IS, guaranteeing greater transversality, by associating the three subordinates under the aegis of the executive committee of the digital and CIS council (CECNum), with at the subordinate level governance by major domains. In this context, the DGNUM led the ministerial project "organization and governance" which made it possible to set up a new organization and to establish the digital governance of the ministry through renovated texts. This new organization, implemented since 2020, aims to simplify, modernize and improve processes, to pool and bring together complex and cross-functional functions and to strengthen the prerogatives of the authorities responsible for the use of digital and CIS products and services. The organizational model chosen to transform the “CIS and digital” function of the Ministry of the Armed Forces is based on that of the main large French groups, characterized in particular by the existence of IT departments with a strengthened role in the management of their portfolio and the operation of their IS. This organization is based on collegial governance of the ministerial digital policy led by the DGNUM. The implementation of the new organization was accompanied by work to renovate digital governance, focusing on clearly defining the roles and responsibilities of the players in this new ecosystem. The successful completion of this ministerial project to renovate digital governance required the updating of official texts. Thus, in the fall of 2022, the decree of September 9, 2022 establishing and organizing bodies relating to the defense CIS (role of the main players in the ministerial digital ecosystem) and the instruction of September 9, 2022 establishing ministerial governance of digital technology and CIS were officially published.

REFRENCES

Billois, G. (2019). Quand on l'attaque…" La doctrine cyber du ministère des Armées, https://www.institutmontaigne.org/expressions/quand-lattaque-la-doctrine-cyber-du-ministere-des-armees

Cabirol, M. (2022). Défense : comment la France veut se protéger au maximum de la menace cyber, https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/comment-la-france-veut-se-proteger-au-maximum-de-la-menace-cyber-939160.html

Delerue,F., & DesforgesGéryA., (2019). A Close Look at France's New Military Cyber Strategy, https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/

Filippone, D. (2019). Cyberdéfense : La France explicite sa vision du droit international, https://www.lemondeinformatique.fr/actualites/lire-cyberdefense-la-france-explicite-sa-vision-du-droit-international-76414.html

Le Monde avec AFP (2021). Cybersécurité : la défense française veut renforcer ses troupes de cybercombattants, https://www.lemonde.fr/pixels/article/2021/09/08/cybersecurite-la-defense-francaise-etoffe-ses-troupes-de-cybercombattants_6093949_4408996.html

Manenti, B. (2013). Cyberdéfense : les programmes secrets de la France, https://www.nouvelobs.com/high-tech/hacker-ouvert/20131030.OBS3274/cyberdefense-les-programmes-secrets-de-la-france.html

Poupard, G. (2018). Le modèle français de cybersécurité et de cyberdéfense, https://shs.cairn.info/revue-internationale-et-strategique-2018-2-page-101?lang=fr

Ravelles, R. (2021). LA CYBER-COOPÉRATION EUROPÉENNE- https://jeunes-ihedn.org/wp-content/uploads/2021/03/LJI_cyber-cooperation-europeenne_Remi-RAVEL_032021.pdf

Tellier, M. (2018). Cyberdéfense : qui nous défend en cas d'attaque ? https://www.radiofrance.fr/franceculture/cyberdefense-qui-nous-defend-en-cas-d-attaque-8657415

Tête, F., & Vrignaud, L. (2019). « Cyber-resilience vs Business resilience » in « Les risques et l'environnement numérique », LIREC, n°59, mai 2019

Ventre, D. (2020). *Intelligence artificielle, cybersécurité et cyberdéfense*, ISTE, Londres, juin 2020, 246 pages, (ISBN 9781784056797 et 9781784066796)