# CYBERSECURITY – ORGANIZATION ON A EUROPEAN SCALE

**Ivan Velevski**
UNIBIT, Sofia, Bulgaria, ivovelevski@gmail.com

**Abstract:** Cyber attacks are becoming a recurring means of action to destabilize institutions or States. The evolution of technology and the connected world that results from it make these attacks increasingly damaging and dangerous for the economy but also the sovereignty of States. Especially since these attacks can be of considerable magnitude as shown by the NotPetya and Wannacry viruses of 2017 affecting hundreds of thousands of computers around the world. Until recently, the European Union relied on a defense policy specific to each State with an assurance of protection from NATO. It is beginning to realize the importance of direct action and is implementing initiatives to cooperate between States. However, it is not certain that this will be enough to have a real European cyber force. "Cyber crises know no borders," explains Mr. Juhan LEPASSAAR, Director of ENISA.The EU's great legacy of the free movement of people and goods is a significant acquis but also a weakness in terms of cybersecurity. Software and data are easily transferred from one EU country to another, so the virus from Spain could be transmitted and manifest in Sweden. Faced with the lack of security barriers, EU experts created the European Network and Information Security Agency in 2004. This agency has an advisory role on the use of defense instruments in cyber defense. In this matter, due to the known lack of consensus, each member state solves its problems at the national level. In the era of great tensions due to the war in Ukraine and the EU's support for Kiev, the dangers of cyber attacks have increased significantly. Today, cyber attacks have become an interdisciplinary and global activity whose victims can be all critical infrastructures in the world. Attacks often occur when elections, major events, or tensions are taking place in one of the countries. These attacks can paralyze life in a single society or in several countries. That is why cyber defense is of paramount importance for every country. Several questions of strategic importance arise: What is the situation with this matter in Europe? How will the EU cooperate in this area? What is the future of the EU in the domain of cybersecurity?.
**Keywords:** Cyberdefence, Cybersecurity, Cyber attacks, European Cyber Security Agency

## 1. INTRODUCTION

Cybersecurity issues in Europe and the world have become a central dimension of the context of the rivalry with Russia, China and North Korea. Sometimes there are simple paradoxes. The global threat of cyber attacks has forced developed countries to invest in the defense of the new digital space. However, this is not the case with countries with a lower rate of economic development. This has created a real mosaic in the field of cyber defense and cybersecurity in Europe and other continents. While the EU, especially the most developed countries such as France, Germany, Sweden, the Netherlands, Denmark, are recording impressive success in cybersecurity, the countries of Central Europe are significantly lagging behind. Most of these countries rely on the support of the NATO Alliance, and the Baltic states stand out among them.Western Europe first of all. Some countries such as France and Germany have become well aware of the importance of the phenomenon. France is already recognized for its cyberdefense policy, ANSSI and the French cyberdefense command won the LockedShields exercise in 2019, which consists of a competition between NATO allies to see who will best protect a fictitious country from a cyberattack. It was also recently ranked 2nd in cyber defense by a report from the Belfer Center, a research center associated with Harvard.2 Finally, France is also one of the few countries to have an offensive warfare doctrine, which was in fact unveiled in 2019 by Ms. Florence PARLY.3 Similarly, Germany quickly set up a cyber defense unit in 2017, forming a new branch of the army to specifically counter Russian attacks after a large-scale hack of the Bundestag in 2015. Last year, it announced that it was developing the offensive aspect of its cyber forces and would no longer focus solely on the defensive. Furthermore, it should make all of its forces available to NATO. We can also cite the Dutch and Spanish forces, which are doing significant work building a cyber force.-Regardless of certain successful moves, in the domain of cybersecurity in the countries that emerged from the Eastern Bloc, the domain of cyber attacks was assigned to internal security forces without involving the army. This is also an excuse why these countries do not use the term cyber defense but rather cybersecurity. In the Czech Republic, the National Security Agency is responsible for this phenomenon, which, depending on the issue, calls on the Ministry of Interior and its experts. On the other hand, when it comes to a massive attack, the Ministry of Defense is also involved, which deals with issues related to NATO. In Slovakia, due to the financial critical infrastructure, the Ministry of Finance is involved in cyber defense. One gets the impression that Hungary is not very engaged in cyber defense and its expectations are focused on cooperation with the NATO Alliance.(Taillat, S./Cattaruzza,A. Danet, D. (2018)

**2. EUROPEAN CYBER-COOPERATION**

During the 12th edition of the International Cybersecurity Forum (FIC) in January 2020, the French National Agency for the Security of Information Systems (ANSSI) called for strengthened European governance for the development of European sovereignty in cybersecurity and the promotion, at the international level, of European values for peace and stability in cyberspace. However, it recognizes solid foundations in digital security on the old continent. European and international crisis management mechanisms are all the more important in the event of a crisis of cybernetic origin since the latter does not respond to the geographical boundaries of our administrative divisions at whatever level they may be. The cross-border nature of cyberspace and the geographical transcendence1 of cyberattacks call for an articulation of national, European and international systems. Although the purpose of this article is not to describe all the bilateral agreements and international cooperations existing in the field of cybersecurity between countries, the resolution of cases such as the "Rex Mundi" case involving a joint investigation between the French (OCLCTIC), English (London Metropolitan Police), European (Europol) and Thai (Crime Suppression Division of Bangkok) authorities, testify to their existence and their necessity. The European Union Two clauses seem to be able to be invoked by a Member State in order to trigger European crisis management mechanisms: the mutual defence clause of Article 42 paragraph 7 of the Treaty on European Union (TEU) introduced in 2009 with the Treaty of Lisbon and the solidarity clause (Article 222 of the Treaty on the Functioning of the European Union (TFEU) which can be invoked in the event of a "particularly serious cyber incident or cyber attack". (Ibid.Taillat, S./Cattaruzza,A. Danet, D. (2018). Within the European Union, several institutions participate in the cyber protection and cyber defence of Europeans, including the European Commission, the Council of the EU, the EEAS, the EU Military Staff, ENISA, CERT-EU, Europol, Eurojust. In 2017, the European Commission adopted a recommendation: the Blueprint, defining the European cooperation and exchange procedures for the management of major cybersecurity incidents and crises that exceed the action capabilities of the Member State concerned alone or that affect several Member States. Three levels of crisis management are thus identified: political, operational and technical. While it is up to the Member States to respond to major cybersecurity incidents and crises that affect them, the Commission, the Council of the EU and the EEAS can play an important role in particular under EU law and "classic" crisis management mechanisms. Indeed, in the event of a major crisis, coordination may be carried out within the framework of the General Early Warning System "ARGUS" within the Commission, while the Council of the European Union will ensure political coordination via the Integrated Political Crisis Response (IPCR) mechanism. Finally, when the crisis has major implications related to foreign policy or the Common Security and Defence Policy (CSDP), the Crisis Response System (CRS) of the European External Action Service (EEAS) may be activated. Of course, the specialist bodies are at the heart of the response: ENISA, the European Network and Information Security Agency, plays an advisory role by providing recommendations and supporting the development and implementation of information security policies for the European Commission and the Member States. Its role is being strengthened, particularly in terms of certification and the organisation of exercises and in this respect Blue OLEx 2019 marked a turning point by testing the operational level of the European cyber crisis response framework by bringing together the heads of national cybersecurity authorities of the EU Member States, the European Commission and ENISA.

The "CERT-EU", the EU Computer Emergency Response Team, intervenes in the event of a computer emergency via a permanent team for the benefit of the European institutions. It cooperates in particular with the CERTs of the Member States and is part of the CSIRTs Network, the network of European CERTs established by the Network and Information Security (NIS) Directive and supported by ENISA, which provides its secretariat. General Didier Tisseyre, Commander of Cyber Defense at the Army Staff (COMCYBER), indicated during a hearing at the National Assembly for the National Defense and Armed Forces Committee that the European Union is more focused on cybersecurity issues than on military defense. However, he specified the presence of COMCYBER in the working groups dedicated to cybersecurity and cyberdefense and also in the operations and command structures of the European Union or the EU Military Staff (EUMS), a military structure integrated into the EU. Morgan JOU, Research Assistant at IRSEM in 2017, published an article in October 2019 in which he also shared this observation since he indicated that the EU does not have a specific operational response capacity for cyber alongside conventional capabilities. Although the EUMS is however well able to provide military and operational expertise via a policy and plans division (CON/CAP) and an information and command systems division (CIS), there is no single centre to manage planning and operational conduct in the cyber domain. The judicial component, i.e. investigation and investigation skills, falls under two agencies: Europol and Eurojust. The first, Europol, is the European agency specialising in the repression of international crime and terrorism and the fight against cybercrime, in particular via the European Cybercrime Centre (EC3) which operates at a strategic but also operational level, in particular via the Joint Cybercrime Action Taskforce (J-CAT). The second, the European Union Agency for Criminal Justice Cooperation (Eurojust), has as its main missions the coordination of investigations and prosecutions, and

cooperation between the authorities of the Member States. It seeks to make these investigations and prosecutions more effective, particularly in the fight against cybercrime. It supports who forms a network of prosecutors and cybercrime specialists. The latter aims to make investigations and prosecutions initiated in cybercrime more effective by improving cooperation between the judicial authorities of the Member States.

**3. THE NEED FOR COOPERATION AND COORDINATION**

The example put forward in the introduction to this development on the EU, clearly illustrates the need for cooperation and coordination of the judicial authorities and police services of the different countries in the fight against and investigation of cybercrime. These two issues are supported by Eurojust, and Europol. The intelligence services also provide their support. The European Union Intelligence Analysis Centre (INTCEN) and the European Union Military Staff Intelligence Directorate (EUMS INT) are both at the heart of the EEAS's Single Intelligence Analysis Capacity (SIAC). The latter also hosts the INTCEN Situation Room (SITROOM) and the European Union Hybrid Fusion Cell (within INTCEN) in the field of cybersecurity in particular. The European Union can also rely on the North Atlantic Treaty Organization (NATO), in particular since the signing in February 2016 of a technical arrangement on cyber defence - aimed at strengthening cooperation in the areas of information, training, research and exercises - between the EU Computer Emergency Response Team (CERT-EU) and the NATO Computer Incident Response Capability (NCIRC). Focus on the North Atlantic Treaty Organization The Alliance is an important support for cyber defence issues in Europe since its main function is collective defence, crisis management and cooperative security. While its priority remains the defence of its own networks, it is committed to strengthening the level of resilience of the Alliance member countries. Its actions aim to facilitate information sharing and mutual assistance in the event of a crisis, including - at the disposal of member countries, upon request and approval by the Alliance - NATO rapid reaction teams that can intervene 24 hours a day in the name of the mutual assistance clause of Article 5 of the North Atlantic Treaty (NAT). Within the NATO Computer Incident Response Capability (NCIRC) - which is part of the NATO Communications and Information Agency (NCIA) - some 200 experts ensure the protection of the Alliance's information systems in peacetime and in times of crisis. However, it was in 2018 that a turning point in incident response seemed to be emerging, since the members of the Alliance committed - at the Brussels Summit - to the creation of a Cyber Operations Centre (CyOC) integrated into the NATO command structure that could call on the cyber capabilities of the countries for its missions and operations. The latter should be operational by 2023. Nevertheless, General Didier Tisseyre also stressed the need for NATO to develop offensive cyber. The Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Tallinn, is NATO's centre specialising in research and education, in particular by developing rules of behaviour in cyberspace and in particular the question of the applicability of international law to cyberattacks used in armed conflicts via the "Tallinn Manual". NATO's European cyber defence exercises, Cyber Coalition and Locked Shields, are organised there.( Bockel,J-M.2012)

**4. AS GUERANTOR OF EU SECURITY**

NATO is still today the European Union's security guarantee against external state attacks. The organization is also a pioneer in the discipline, has substantial resources and an influential role. This omnipresence of NATO on cyber security issues has led the European Union to neglect any attempt at strategic autonomy in this area. However, we are seeing a gradual awareness of the Union of the importance of establishing its own cyber defense. A late but effective awareness Following the 2007 crisis in Estonia, ENISA did not have the skills to act on the ground, in direct support. Generally speaking, following this attack, the European Union has not really taken any tangible action to protect its members, and is relying on NATO's active and effective action in this area. An embryo of a common cyber defense policy nevertheless appeared in 2016 with the adoption of the NIS directive (Security of networks and information systems). This is the first legislative framework agreed across the entire EU. (Monahan C. 2023)This framework, transposed in 2018, sets up an audit obligation for companies, incident notifications and develops security measures for companies. The objective is less the cyber defense of the union than an initial protection of the entire territory against malicious viruses sent from foreign that can extract information or money from EU companies. This directive is the starting point for strengthened collaboration between countries, and voted unanimously, it shows the beginnings of awareness. But this awareness does not necessarily mean total agreement. The disagreements - outlined above - between the different countries prevented the implementation of an effective, binding policy, with a certain effect on European defense. Less than a year after the adoption - but before the transposition - of this directive, two computer worms affected the entire world: Wannacry and Notpetya. These worms are typical examples of what the NIS directive is supposed to prevent. In May and June 2017, they affected 8 hundreds of thousands of computers around the world. Presenting themselves as ransomware, they block access to computers and offer to give this access back in exchange for a ransom. These attacks caused several billion dollars

of damage and are considered the largest cyberattacks in history12. They are all the more dangerous because even today the international community has not found anyone responsible for any of the attacks. In addition, in 2016 and 2017, with suspicions of Russian interference in the American and French elections, the international community became aware of the urgent need to act more effectively and in a coordinated manner against external intrusions into a country's cyberspace. In response to these two phenomena, from 2017 onwards, the European Union began to act in a coordinated manner and on an ambitious scale. This was the objective of the European summit in Tallinn on 19 September 2017. Lawson,S.(2019) On the one hand, it proposed creating a new policy, more ambitious than the NIS directive, to protect against worms such as Wannacry. On the other hand, it created a new agency, in continuity with ENISA, to assist states directly against cyberattacks. In addition, a recommendation from the European Commission was made to allow Europol to act in partnership with all countries to help victims of cyberattacks to defend themselves and limit the damage. It set up secure communication networks, permanent points for exchanging information between countries. A new dynamic, awareness at European level, therefore emerged in 2017 and has developed since then. (Martelle, M.2018, 35,p.) Firstly, through the Permanent Structured Cooperation (PESCO). This structured cooperation is provided for by the Lisbon Treaty to deepen cooperation in the field of security and defence of Member States. It is therefore a military approach that is taken. Among the very first proposals for cooperation, Lithuania put forward the establishment of a joint cyber force to respond to cross-border crises: the cyber rapid response teams and mutual assistance in cyber security. This assistance brings together specialised units from each participating country. These units can be mobilized jointly to reinforce the defense. (Buchanan,B.2020,102,p.)

**5. EUROPEAN SOVEREIGNITY IN CYBER**

Among the very first proposals for cooperation, Lithuania put forward the establishment of a joint cyber force to respond to cross-border crises: the cyber rapid response teams and mutual assistance in cyber security. This assistance brings together specialised units from each participating country. These units can be mobilised jointly to strengthen the defence of a particular country in the event of an attack. It now brings together Lithuania, Estonia, Croatia, Romania, Spain and the Netherlands and is one of the most advanced projects within the framework of PESCO. Following the success of this project, 8 other proposals have been put in place. They were launched by different countries and each bring together some of the members. We can notably cite the French initiative for the development of common and secure military radio technologies (ESSOR), the Greek initiative for the development of common defence measures (for the moment these are mainly common firewalls), or the joint project between Spain and Portugal for the development of a cyber and innovation school to train experts in the field (EU CAIH). Finally, still in a spirit of cooperation, ENISA has been setting up the Blue Olex event since 2019 to strengthen the exchange of knowledge in the EU. (Lawson,S.2019) Organised in France in 2019 and then in the Netherlands this year, this event ultimately aims to prepare a political discussion on cyber defence by bringing together senior officials from the 27. To this end, this year's event enabled the establishment of CYCLONE with the idea of establishing an intermediate level between politics and technology in the management of cyber crises. 16 The objective is to enable a global and effective analysis in response to cyber crises between countries. This multiplication of initiatives shows Europe's interest in cooperating in this area to maintain its sovereignty in the face of external attacks. (Lawson,S.(2019)Towards European sovereignty in cyber? In the long term, it is possible to envisage an autonomous EU in cyberdefense. But there are many obstacles to such autonomy. A first obstacle to this autonomy lies in the reluctance of countries to share information and sovereignty prerogatives, particularly concerning defense. Without recounting the history of the EDC and the various failed European defense initiatives, the European Union is reluctant to pool its defense, including in the cyber domain. Some more advanced countries do not want to share too sensitive information for fear that it will then be transferred to less secure countries and ultimately stolen during an attack on this EU member country but with lower security standards. A second obstacle concerns the already strong cooperation with NATO. Some EU countries with underdeveloped cyber defense want to first develop their national defense, considering that NATO's current protection is sufficient. Even the most advanced countries are now relying on the organization, as we have seen with Germany, which will join the Netherlands in making its forces available to NATO and not to the European Union. NATO's cyber power and its rapid awareness, which have allowed in-depth work for more than a decade, make it a considerable force. For many, there is not much point in moving away from this protection to create another, autonomous, but less strong one. These few obstacles should not, however, make us forget the significant progress made by the European Union in cooperation. In this area, it is important to have leading countries that launch increasingly ambitious dynamics in the Union's cyber cooperation. We can cite Poland, which certainly remains under the NATO umbrella but strengthens its national forces and cooperates in many areas with the EU and France. (Fischerkeller, M./Goldman, E./Harknett, R.2022) The latter has not contributed its forces to NATO, preferring to launch many European defense projects, as

Emmanuel Macron specified in his 2018 Paris Call, calling for an autonomous European cyber power. These two leading countries are joined by the Baltic countries, with Estonia, which is a pioneer in this area, and Lithuania, which wishes to develop its capabilities in full cooperation with the European Union. Finally, the European Union is experiencing many dilemmas and fundamental disagreements on its joint management of cyber defense. Between countries that consider cyber to be a civil matter, those that rely on the NATO umbrella and those that are afraid to share information with countries that are too little advanced in terms of security, the EU has many challenges to overcome before achieving an autonomous and effective defense against the giants of cyber attacks such as China or the United States. (Taillat,S. 2024)However, progress is present, it is multiple and sometimes confusing but in a certain direction of strengthening European cyber power.

**6. CYBERDEFENCE MODE OF ACTION**

During a cyberattack, several criteria are analyzed: • Who attacks: single individual, group, cybercrime with a state-level actor behind it… • How they attack: break systems, espionage, use of a flaw… • What is the impact of the attack: systemic attack that brings down an entire part of an activity, limited attack… According to these criteria, a decision will be made on the organization in charge of responding. In the case of an attack on the systems of the Ministry of the Armed Forces, it will be the cyberdefense command. “Despite everything, in this cyberspace there are no borders, escalation can be rapid, so the principle is really to manage inter-ministerially,” specifies General Tisseyre. This is why the C4 (Cyber Crisis Coordination Center), made up of all state actors concerned by cyber, meets every week or depending on the attacks, in order to decide on possible responses (cyber, economic, diplomatic, etc.). These responses are governed by French law, and authorized to stop an attack. Within the armed forces, there is a report on the application of international law to operations in cyberspace. This defines the response framework and the use of cyber weapons in theaters of operations. Because even in cyberspace, "the law of armed conflict applies," explains General Tisseyre, "as does the principle of proportionality and justification for the use of cyber weapons in relation to other means." Particular attention is also paid to the discrimination between military targets and enemy targets: an armed terrorist group can be an enemy whose systems we want to block; (Taillat,S. 2024) However, when targeting a civilian target operating in the cloud, care must be taken not to bring down entire servers because this would impact the population. In theaters of operation, the cyber weapon is custom-designed to control its effect and avoid collateral damage. Care must also be taken not to encourage the proliferation of these cyber weapons. "In the past," explains a expert of NATO, "some have used cyber tools, which were recovered and allowed the person who had suffered the attack to upgrade, to be more efficient, and possibly to reuse these means." Unfortunately, in the dark web, a whole mechanism has already been put in place to support a very structured cybercrime: exchanges of information, identification of vulnerabilities, rentals of ransomware or other software... (Farrell, H./Nerwman,2023.98,p.)

**7. CYBER DEFENCE WEAPONS**

The details of the cyber weapons used by the armies are not known, for security reasons. General Tisseyre confides that the use of cyberspace is in the identification of vulnerabilities allowing entry into normally inaccessible areas. Each cyber attack is structured, with a detailed chain of actions. "Our process is to get as close as possible to the enemy's data to gather intelligence, and possibly hinder their own approach by bringing down their systems," confides the cyber defense commander. In the fight against Daesh, for example, cyber fighters have managed to infiltrate servers hosting propaganda and to know when and on which media it would be broadcast. They were thus able to stop this approach by blocking the broadcasts, and prevent the jihadist group from recruiting, particularly at that time (2015-2017) during which the objective was to encourage radicalized sympathizers to join the theaters of operations in Iraq and Syria. (Buchanan,B.2020)The cyber defense strategy is a "surgical strike, which will have a precise military effect within the framework of a global maneuver." These words illustrate those of the American Colonel Warden, which General Tisseyre explains: in a conflict, it is a question of identifying the different circles of decision, infrastructure, civilians, military, etc. and of correctly choosing the circle targeted by the attack, preferring a strategic strike towards the decision center rather than a confrontation between two military forces. Partnerships, exchanges and training Like intelligence on the "real" ground in theaters of operations, knowledge of the cyber-combatant enemy is important and must be anticipated: "we gather information, we study the modes of action, we create maps shared with ANSSI", specifies General Tisseyre. Partners are indeed essential in this fight against cybercrime. They can be civilians in France, but also foreigners within the framework of NATO or the EU. The example of SolarWinds (indirect cyberattack, in which software trapped by the attackers was acquired and developed in American administrations) demonstrated the need to include civilian industrial partners of defense in these exchanges. This is why in 2020, the Minister of the Armed Forces signed an agreement with eight major civilian defense contractors, suppliers of highly digitalized military equipment. It promotes sharing with

manufacturers and "enables us to ensure that they have the right level of security." Inter-ministerial exchange is also encouraged so that each entity of the Ministry of the Armed Forces or the State is protected and benefits from each other's knowledge in the field of cyber. Thus, the General Directorate of External Security or the Directorate of Military Intelligence provide additional information, a "more geopolitical, intelligence vision, analyzes Bockel,J-M.(2012)." Training is a central point of cyber defense, since it is constantly evolving. (Taillat,S. 2024) also specifies that within the Center for Analysis in Defensive Information Warfare, composed of experts (detection, analysis, reverse engineering of codes, etc.), 20% of the staff is still in training. Finally, NATO allied countries exchange training, make places available in schools (digital cyber defense by Portugal for example), in order to be more effective by speaking the same language and the same specific vocabulary.

**8. CONCLUSION**

Cyberspace, the theater of operations of the future? A NATO expert is convinced that the major engagements of the future will be preceded by an initial phase in cyberspace. A huge amount of information passes through this cyberspace that interconnects everything and everyone. In addition to allies, there may also be competitors, rivals or adversaries seeking to influence or hinder. However, the responses to this type of adversary are effective and inexpensive. "It is mainly human resources," experts note, "and behind it are software, computers, and it is not expensive when compared to the prices of fighter planes, armored vehicles, satellites or aircraft carriers." Several levels of risk exist today: • The strategic level at which the military prepares: elaborate attacks, high-intensity conflict. • Cybercrime that can affect everyone: more insidious, increasingly sophisticated. The latter requires common protection and awareness from each individual. Because the defense of all requires individual responsibility. "Every individual should have a minimum of notions of cybersecurity," says an EU expert, "that they feel concerned and are responsible: effective password, passage in a white station (editor's note: computer on which each USB key used in the military framework must be scanned in order to verify that it is safe and not infected), antivirus... Because if an individual is not safe, their entire network can be affected." To achieve a certain "collective maturity", specialists will therefore coordinate, structure, and write educational protocols. Cyberfighters are also sent on external operations, as well as digitalized weapons systems and operations command systems. Cyberdefense cannot be done constantly remotely. The many networks deployed represent an enormous mass of information, which would overload the satellites if this means were used. The teams on the ground can thus supervise, take charge of the equipment, and provide expertise in the event of a serious difficulty. However, if the attack or the problem encountered becomes too complex, a Cyber Intervention Group (GIC) is sent as reinforcements within a very short time. In a broader framework, Europe's cyber defense is being built; its civil and military skills are developing in order to understand the nature of the threats and how to counter them. The legal framework is also expanding, with the European Union's ability to prosecute any individual or group attacking in court. It is also important that Europe can defend itself against major powers (United States, Russia, etc.). Fighting cyber threats means establishing a common vision to prepare As the cybersecurity landscape continues to evolve, organizations are faced with increasingly volatile and unpredictable threats. The expanding attack surface (driven by increasing reliance on cloud, AI, connected devices, and third parties) requires an agile, enterprise-wide approach to ensure resilience. Aligning organizational priorities and readiness is critical to maintaining security and business continuity. Prepare for the threats that matter most. What worries organizations the most is what they are the least prepared for. The four most concerning cyber threats are: cloud-related threats (where France appears to be less prepared than the average of respondents 45% vs 34%), data breaches (which particularly concern France at 51%), third-party breaches, and attacks on connected products. This gap underscores the urgent need for better investments and stronger response capabilities.

**REFERENCES**

Bockel, J-M. (2012). *La Cyberdéfense : un enjeu mondial, une priorité nationale*, Sénat (France), 18 juillet 2012 (Rapport d'information du Sénat fait au nom de la commission des affaires étrangères, de la défense et des forces armées)

Buchanan, B. (2020).The Hacker and the State :Cyber attacks and the New Normal of Geopolitics, Cambridge, Harvard University Press,2020

Farrell, H., & Nerwman, A. (2023). The Undergraound Empire: How America Weaponized the World Economy, New York, Penguin Press

Fischerkeller, M., Goldman, E., & Harknett, R. (2022). Cyber Persistence Theory Redefining National Security in Cyberspace, New York, Oxford University Press,2022

Lawson, S. (2019). Cybersecurity Discourse in the United States:Cyber-Doom Rhetoric and Beyond,Abingdon, Routledge, 2019

Lindsay, J. (2020). Information Technology and Military Power, Ithaca, CornellTecnology University Press,2020
Martelle, M. (2018). Eligible Receiver 97:Seminal DOD Cyber Exercise Includede Moc Terror Strikes and Hostage Stimulations 1.08.2018
Monahan, C. (2023). Solar Sunrise After 25 Years: Are We 25 Years Wiser? 28.02.2023
Taillat, S. (2024). De la Cibersecurite en Amerique, (2024), PUF, Paris
Taillat, S., Cattaruzza, A., & Danet, D. (2018). *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 4 juillet 2018, https://www.armand-colin.com/la-cyberdefense-politique-de-lespace-numerique-9782200621292