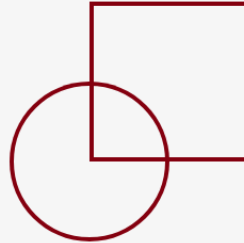
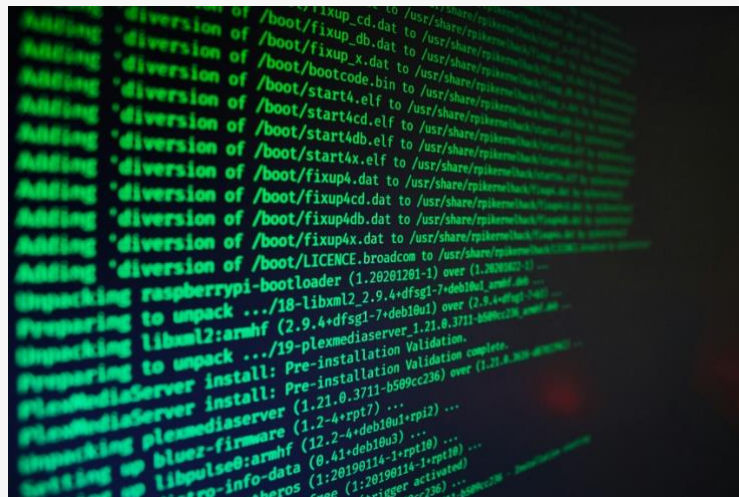


LA LIGNE FINE PAPERS N°10



LA LIGNE FINE

Institut



Strategic Cyber Warfare Series: Strategic Foundations

Authors: Alek UMONT
Published Date: April 9, 2026

Executive Summary

Cyberwarfare now occupies a permanent place in defence doctrines, national security strategies and competition between powers. However, this recognition does not mean that cyberspace has become a theatre of war comparable in its operation to the land, sea or air domains. Cyber operations have their own characteristics: they can be prepared long before they are used, be based on civilian infrastructures used daily by the whole of society, remain clandestine for several months or years, be difficult to attribute immediately and produce very different effects depending on the precise technical configuration of the target. The notion of "strategic cyberwarfare" must therefore be used with sufficient precision to distinguish between computer espionage, cybercrime, influence operations, sabotage and the use of digital capabilities directly integrated into a military confrontation.

The strategic importance of cyber does not come mainly from the theoretical possibility of remotely provoking the collapse of a state. Scenarios of general paralysis of national infrastructures have durably structured the imaginary associated with cyberwar, but they often lead to overestimating the autonomy of the cyber instrument and underestimating the conditions necessary to produce lasting effects. An attack on a complex infrastructure generally requires detailed knowledge of its architecture, dependencies and operating procedures. IT systems evolve, vulnerabilities are corrected, access is detected, configurations are modified and operators can restore services. An offensive capability is therefore not necessarily reproducible at will: it may depend on a specific vulnerability, access prepared well in advance or a set of technical conditions that disappear after its use.

The decisive transformation lies elsewhere. The digitization of administrations, critical infrastructure, economies and armed forces now allows states to constantly seek access to their competitors' systems. These accesses can be used to collect intelligence, map networks, prepare sabotage options or support subsequent military operations. The same clandestine presence in a network can thus perform several successive functions. An intrusion initially exploited for intelligence can be retained in order to allow for different action in times of crisis. The victim state does not necessarily have the elements to determine the attacker's real intention at the time it discovers this presence. This uncertainty makes prepositioning in networks a strategic issue in its own right.

The institutional recognition of cyberspace as a domain of operations reflects this evolution. NATO has formally recognised cyberspace as a domain of operations since the 2016 Warsaw Summit. Its current approach combines the protection of its own networks, support for Alliance operations, improving the national resilience of Allies and the possibility of consultation and collective action. The Alliance also specifies that a sufficiently serious cyberattack could, depending on the circumstances, lead to the application of Article 5, without defining an automatic threshold based on a particular technical category¹².

This approach is consistent with the nature of the domain. A cyber incident cannot be assessed solely on the basis of the tool used. The consequences, the target, the duration of the interruption, the likely intent and the political context determine its scope. An intrusion into an administrative server, the silent compromise of a software provider, an attack causing the temporary shutdown of a public service and an operation directly affecting a critical military system are of very different levels of severity. The policy response must therefore be based on effects and circumstances rather than on an automatic classification of the technique employed.

¹ Allied Command Transformation. (n.d.). *Cyber Defence*. NATO. <https://www.act.nato.int/activities/cyber/>

² North Atlantic Treaty Organization. (2024, July 30). *Cyber defence*. NATO. <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>

The digitalization of the economy is significantly expanding the scope of this competition. Much of the infrastructure on which a state depends is owned or operated by private companies: telecommunications, cloud services, software, energy networks, transportation, logistics platforms, data centers, payment systems, or industrial equipment. Administrations and armed forces themselves use commercial technologies and international supply chains. The distinction between military network and civilian environment remains legally important, but it is no longer sufficient to describe the actual structure of dependencies. An attack on a supplier can affect several administrations, companies, or infrastructures simultaneously; conversely, the defense of a military capability may depend on actions taken by a private actor outside the chain of command.

The threat landscape published by the European Union Agency for Cybersecurity illustrates the scale of this environment. The *ENISA Threat Landscape 2025* analyses 4,875 incidents that occurred between 1 July 2024 and 30 June 2025. The agency describes a landscape in which state-linked actors, criminal groups and hacktivists use sometimes converging techniques and exploit the same vulnerabilities or infrastructures. This diversity makes it difficult to distinguish between different forms of threat and forces authorities to analyse the purpose and context of operations rather than just how they operate³.

The porosity between state and non-state actors is another important element. States can conduct their operations directly through their intelligence services or armed forces, but they can also benefit from ecosystems that include companies, criminal groups or intermediary actors. The relationship between these groups and power can be close, opportunistic or deliberately difficult to establish. In July 2026, the North Atlantic Council condemned what it describes as persistent Russian cyber activities relying on a "cyber ecosystem" to target Allies and partners. This type of wording shows that threat analysis now goes beyond the search for an identified military unit or intelligence service and must take into account the more complex relationships between state actors and external networks⁴.

However, the difficulty of attribution does not mean that cyber operations are anonymous in nature. Governments, intelligence services, cybersecurity agencies and specialized companies have technical and non-technical means to link campaigns to specific actors. The analysis can take into account the infrastructure used, access methods, malware families, operational habits, chosen targets, hours of activity or information obtained from other sources. The central question becomes the level of trust needed to act. An internal assessment may be enough to take defensive measures before a government has the elements it considers necessary to proceed with a public attribution or coordinated with its partners.

This temporality limits simple models of deterrence. The threat of an immediate response loses credibility when it is first necessary to establish the origin of an operation or determine the level of responsibility of a state. Cyber deterrence is therefore based on several complementary mechanisms: making the attack more difficult, improving detection, limiting the movements of an attacker already present in the network, quickly restoring disrupted functions, assigning operations when there are sufficient elements, and having a range of responses that are not necessarily limited to cyberspace. Sanctions, diplomatic measures, legal proceedings, cyber operations and military instruments can be combined depending on the level of severity.

The European Union's policy places particular emphasis on resilience and crisis management. The *Cyber Solidarity Act*, which entered into force on 4 February 2025, aims to strengthen European capacities for the detection, preparedness and response to significant or large-scale

³ European Union Agency for Cybersecurity. (2025, October 1). *ENISA threat landscape 2025*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

⁴ North Atlantic Treaty Organization. (2026, July 13). *Statement of condemnation by the North Atlantic Council of Russia's malicious cyber activities*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities>

incidents. In particular, it provides for a European alert system based on national and cross-border cyber centres and a European emergency mechanism. A European cybersecurity pool composed of incident response service providers must be able to be mobilised in order to support Member States, institutions and other eligible entities facing major crises⁵⁶.

This policy reflects a useful evolution in the conception of cybersecurity. No sufficiently complex system can reasonably be considered inaccessible to any adversary. Performance must therefore be evaluated not only on the basis of prevention, but also on the basis of the speed of detection, the ability to contain the intrusion, the protection of priority functions and the time required to restore a service. Business continuity takes on strategic value when the targeted infrastructures are directly involved in the functioning of the State or its forces.

However, resilience should not be equated with a simple IT backup. Critical infrastructures often combine digital systems, physical equipment, human procedures and external dependencies. An attack on an industrial environment can change the functioning of a hardware process; its impact will then depend on security measures, the possibilities of manual intervention, available stocks, the ability of technicians to restore the installation and possible interdependencies with other sectors. A cyber operation capable of producing a significant physical effect often requires a much more precise understanding of the target than a data theft or denial of service campaign.

This relationship to materiality makes it possible to clarify the military role of cyber. Digital operations do not replace conventional means; they can, however, improve their effectiveness when coordinated with them. Disrupting a logistics network, delaying transmission, compromising certain data or temporarily limiting a communication capacity can have a significant operational effect if the action takes place at a time when a force is highly dependent on it. The military value of a cyber operation cannot therefore be deduced solely from the extent of the technical disruption. A limited but properly synchronised action may be more interesting than a spectacular campaign that has no direct link to the military objective pursued.

NATO's evolution confirms this integration. The Alliance continues to operationalise the cyber domain and has developed collective exercises, including *Cyber Coalition*, which bring together military personnel, national experts and partners to test coordination, information sharing and incident response. The 2025 edition brought together around 1,300 cyber defenders from 29 Allies and seven partner countries. The NATO Integrated Cyber Defence Centre is also expected to bring together civilian, military and industrial expertise to improve situational awareness and collective resilience⁷⁸.

The international dimension nevertheless remains marked by the absence of a control regime as precise as those historically developed for certain categories of armaments. The United Nations has gradually built a framework for discussion on threats, voluntary standards of responsible behaviour, confidence-building measures, capacity building and the application of international law. The Open-ended Working Group on Information and Communication Technology Security concluded its 2021-2025 cycle with the consensual adoption of a final

⁵ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

⁶ European Commission. (2025, August 26). *ENISA to operate the EU Cybersecurity Reserve*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/news/enisa-operate-eu-cybersecurity-reserve>

⁷ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

⁸ North Atlantic Treaty Organization. (2025, October 9). *NATO Secretary General at Cyber Defence Conference 2025: "No one stands alone in NATO"*. NATO. <https://www.nato.int/en/news-and-events/articles/news/2025/10/09/nato-secretary-general-at-cyber-defence-conference-2025-no-one-stands-alone-in-nato>

report in July 2025. A permanent global mechanism on information and communication technologies in the context of international security began its work in 2026⁹¹⁰.

These developments do not eliminate the divergences between States on the concrete interpretation of international law, the thresholds of seriousness or the modalities of response. They confirm, however, that cyberspace is now integrated into the debate on international stability and that the prevention of major incidents cannot be the sole responsibility of national technical measures.

Strategic cyber warfare must therefore be analyzed as a permanent component of the balance of power between powers, combining intelligence, preparedness, disruption and integration with military operations. It differs from autonomous warfare because its effects are generally dependent on specific infrastructures and often gain their reach when articulated with other instruments. It is also different from simple cybersecurity because states do not only seek to protect their own networks: they develop capabilities that allow them to understand, penetrate and, if necessary, affect those of their competitors. The main question then becomes that of the balance between two simultaneous requirements: to maintain options for action in adversary systems and to reduce national vulnerabilities sufficiently so that an adversary operation cannot cause a disproportionate political or military effect.

⁹ United Nations, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025, July 1). *Final report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025* [Draft] (A/AC.292/2025/L.1). United Nations. <https://digitallibrary.un.org/record/4084927>

¹⁰ United Nations. (2025, July 14). *Statement attributable to the Spokesperson for the Secretary-General – on the conclusion of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025*. <https://www.un.org/sg/en/content/sg/statements/2025-07-14/statement-attributable-the-spokesperson-for-the-secretary-general-the-conclusion-of-the-open-ended-working-group-security-of-and-the-use-of-information-and>

Problem

The development of cyber capabilities has profoundly expanded the means available to states to gather intelligence, disrupt infrastructure or prepare for a military operation. However, this evolution has not produced a stabilized definition of "cyber warfare". The term can be used to describe an espionage campaign, a ransomware attack on a hospital, an intrusion into a public administration, an operation targeting energy infrastructure or an action directly integrated into a military campaign. Such a broad category ends up bringing together operations whose purposes, perpetrators and consequences are too different to be analysed in the same way.

The distinction must first be made on the basis of the objective pursued. Espionage seeks to obtain information. It may target military secrets, diplomatic data, technology, commercial negotiations or personal information that could feed into other operations. Sabotage aims to alter or interrupt a capability. Cybercrime mainly seeks financial advantage. Influence acts on the information environment and on perceptions. Prepositioning consists of maintaining access that allows future action. The same tools or vulnerabilities may appear in several of these activities, but their strategic significance is not identical.

The ability to move from one function to another, however, makes the distinction less clear than it is in other areas. A clandestine presence in a computer system can be used for several months to collect intelligence and then, in times of crisis, become the starting point for an operation to modify or delete data. The victim state may discover the intrusion before the perpetrator has activated the second function. It must then decide how to deal with a capability whose exact intent remains unclear. This issue becomes particularly sensitive when access is to critical infrastructure or a military system.

The importance of prepositioning lies in the temporality of operations. A complex cyberattack cannot always be designed after the onset of a crisis. The attacker must have identified the target, understood its architecture, found or created an access route, maintained this access despite updates and verified that the desired effect remains possible. A cyber option may therefore require several months of preparation. The competition therefore takes place well before the political use of the capability is decided.

This situation transforms the relationship between intelligence and offensive operation. In many cases, the first step is identical: accessing the system without being detected. The difference is what the actor then does with this access. Intelligence services and cyber forces can therefore pursue closely related objectives, which explains the importance given to the coordination between technical intelligence and military planning.

The second problem concerns the strategic effect. Cyberattacks are regularly evaluated on the basis of their technical scope: the amount of data stolen, the number of computers affected, the duration of a denial of service or the estimated financial cost. These indicators are useful but not enough to determine the strategic scope of an operation. An attack affecting several thousand workstations can remain politically limited if the organization has backups and quickly restores its essential functions. A much smaller disruption can produce a significant military effect if it intervenes on a critical system at a specific time.

This difference requires us to place the cyber operation in its context. In a military confrontation, the interest of an attack on a railway network does not depend only on the number of delayed trains: it depends on the relationship between this network and the movements of forces or equipment at the time of the operation. A disruption of communications does not have the same value depending on whether it occurs during a period of low activity or during a decisive phase of a campaign. Cyber thus acts on functions whose value varies with the strategic situation.

The third challenge is related to the persistence of the effect. Infrastructure destroyed by a conventional strike typically requires physical repair. A digital system can sometimes be restored much faster if backups are available, hardware components are intact, and the organization has properly prepared for recovery. This feature reduces the ability of some cyber operations to produce prolonged effects. The attacker may need to maintain their action, have multiple accesses, or combine the digital operation with a physical action in order to prevent restoration.

Conversely, a discreet compromise can remain useful for a long time if it is not detected. Cyber therefore presents a notable difference between clandestine and destructive operations: access can have a long lifespan as long as it remains secret, while an offensive capability revealed by its use can quickly lose its value. An exploited vulnerability can be corrected as soon as the attack is analyzed. The use of a tool therefore involves an opportunity cost. A state may choose to retain access for a more serious crisis rather than reveal it to obtain a limited short-term advantage.

This calculation partly explains why espionage and prepositioning are much more common than destructive strategic cyberattacks. An espionage operation can continuously provide intelligence without requiring the actor to reveal all the technical possibilities at their disposal. A major attack often destroys part of the future value of the capacity used, since the victim then has information to fix vulnerabilities or modify its architecture.

The fourth difficulty relates to attribution. A cyber operation usually crosses several infrastructures and may use compromised systems belonging to third parties. The original technical address therefore does not directly identify the real perpetrator. The analysis must reconstruct the campaign from a set of clues and, where possible, combine them with non-public intelligence information.

Attribution must also distinguish between technical author and political responsibility. A group may be directly integrated into a state service, act on its behalf, cooperate with it on an ad hoc basis, or pursue its own objectives in an environment where the authorities choose not to intervene. This diversity allows states to benefit from a certain level of ambiguity, but it also complicates their own control over operations carried out from their territory or by groups close to them.

NATO's collective stance against cyber activities attributed to Russia shows that attribution is increasingly being used as a diplomatic tool. In July 2026, the Alliance publicly linked several malicious activities to a Russian cyber environment and labelled them as a threat to Allied security. Such a statement is not only a technical diagnosis; it also seeks to reduce the possibility for the alleged perpetrator to benefit from ambiguity in the long term and to show that Allies can coordinate their political assessment¹¹.

The fifth difficulty concerns the threshold between competition and conflict. States have long accepted the existence of espionage, even if they seek to prevent it. Massive theft of information by digital means can be considered hostile without being treated as an armed attack. Sabotage raises a more delicate issue when its consequences become comparable to those of military action. NATO deliberately maintains a margin of interpretation by stating that cyber activities can, in certain circumstances, lead to collective defence, but without establishing a fixed technical threshold. This approach allows for an assessment of the real effect of the operation rather than creating a rule that an adversary might seek to circumvent¹².

¹¹ North Atlantic Treaty Organization. (2026, July 13). *Statement of condemnation by the North Atlantic Council of Russia's malicious cyber activities*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities>

¹² North Atlantic Treaty Organization. (2024, July 30). *Cyber defence*. NATO. <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>

The central issue is therefore not to determine whether cyber can be used as a weapon, which is already established, but to understand how capabilities that are constantly prepared in adversary's networks can be integrated into a power strategy without daily competition mechanically leading to an escalation. This question requires us to analyze offensive and defense together: the value of a cyber option depends on the ability to gain access to the adversary, while national vulnerability depends on the time needed to detect, contain and restore after a similar intrusion.

Structural context

Strategic cyberwarfare is part of a digital environment that was not designed as a battlefield. The Internet, corporate networks, the cloud, professional software and much of the digital infrastructure were first developed to enable communication, automation, storage and exchange of data. Their gradual integration into almost all economic and administrative functions has then created a much wider surface of exposure. National security today depends on systems of which a significant proportion is privately owned, uses international components and evolves according to industrial cycles that do not necessarily correspond to the temporalities of defence.

Digitization of critical infrastructure

Energy infrastructure, transportation, telecommunications, financial services, healthcare, and government all rely on digital systems that vary in importance across functions. This dependency does not mean that all industries can be neutralized in the same way. Technical architectures are different, levels of segmentation vary, backup devices are not identical, and some processes can be maintained manually during an outage. A cyber defense strategy must therefore avoid a one-size-fits-all approach to "critical infrastructure" and precisely identify the functions whose shutdown would have chain consequences.

The European landscape described by ENISA shows the diversity of these threats. The 4,875 incidents analysed in its 2025 report cover very different modes of operation and actors, and the agency highlights the convergence of certain techniques employed by criminal groups, hacktivists and state-linked actors. The existence of numerous and heterogeneous threats requires organisations to maintain a permanent level of defence, even when no particular geopolitical crisis is underway¹³.

This situation has an important strategic consequence: the defensive capabilities mobilized against crime or ordinary incidents also participate in the preparation of a state against more serious operations. Good identity management, updates, backups, segmentation or logging does not distinguish between a criminal attacker and an intelligence service. The same practices can prevent or limit several categories of threat. National defense therefore directly benefits from a high general level of cybersecurity in the economy.

Digital supply chains

Network security depends on components, software, and vendors that the organization trusts at different levels. A company can properly protect its internal infrastructure while using a vulnerable product or compromised vendor. As a result, attackers may seek to penetrate a target through their supply chain rather than by attacking them directly.

¹³ European Union Agency for Cybersecurity. (2025, October 1). *ENISA threat landscape 2025*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

This approach can be particularly attractive when a vendor serves a large number of organizations. The compromise of a widely used product potentially allows multiple accesses to be obtained from a single initial transaction. The concentration of certain technology markets therefore increases the strategic importance of the security policies of a few companies.

The European Union is trying to reduce this risk through several regulatory instruments. The *Cyber Resilience Act* imposes cybersecurity requirements on products with digital elements and seeks in particular to strengthen security by design and during the life cycle. The Commission also proposed in January 2026 a revision of the *Cybersecurity Act* aiming, among other things, to strengthen the security of information and communication technology supply chains¹⁴¹⁵.

These policies do not eliminate risk. They seek to reduce the number of avoidable vulnerabilities and organize the accountability of actors. Their strategic interest lies in the cumulative effect: an ecosystem in which products are maintained longer, vulnerabilities are corrected more quickly, and obligations are better defined, increases the cost of running a sustainable campaign.

The civil-military interweaving

Armed forces have protected networks and specific systems, but their activities also use the general infrastructure of the economy. Personnel communicate, supply chains use commercial software, defense providers depend on cloud or telecommunications services, and industrial bases have many subcontractors. A strictly military architecture can therefore be secure while remaining dependent on more vulnerable external systems.

This situation makes it necessary to have a broader conception of cyber defence. Protecting only classified networks is not enough if mobilisation or the continuity of operations depend on easily disrupted civilian infrastructure. European crisis exercises are beginning to integrate precisely this type of problem, by testing scenarios in which several economic sectors are affected and must coordinate their response.

NATO is following a similar logic by seeking to bring together civilian, military and industrial actors within the NATO Integrated Cyber Defence Centre. The project aims to improve collective situational awareness and cooperation between organisations that each hold some of the information needed to understand a campaign¹⁶.

A competition without a clearly identifiable mobilization phase

A major cyber campaign can be prepared without visible movements of forces. The first steps often consist of identifying the technologies used, collecting information on employees, looking for vulnerabilities and building access. Some of these activities can resemble ordinary criminal operations or classic espionage. Strategic indicators are therefore less visible than in many military domains.

This lack of clearly identifiable mobilization does not mean that no warning signs can be detected. The services may observe an increase in scans, phishing, access attempts or other behaviors. But these phenomena are frequent enough in normal times that their interpretation

¹⁴ European Commission. (2026, September 7). *Cyber Resilience Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

¹⁵ European Commission. (2026, January 20). *Proposal for a Regulation for the EU Cybersecurity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>

¹⁶ North Atlantic Treaty Organization. (2025, October 9). *NATO Secretary General at Cyber Defence Conference 2025: "No one stands alone in NATO"*. NATO. <https://www.nato.int/en/news-and-events/articles/news/2025/10/09/nato-secretary-general-at-cyber-defence-conference-2025-no-one-stands-alone-in-nato>

remains difficult. The challenge becomes one of correlation: several weak signals can acquire meaning when compared with political, military or intelligence information.

Cyber defence must therefore operate at a constant pace. It is not realistic to maintain a low level of security in peacetime and then rapidly strengthen protection a few days before a crisis. If an adversary is already entrenched in the networks, late improvement of controls may not be enough. Audits, exercises and compromise search operations must therefore take place before the political need is clear.

The rapid evolution of technologies

The constant renewal of technologies is a particular constraint. Systems are updated, new cloud services are adopted, equipment becomes obsolete and new dependencies appear. This evolution can remove adverse access but also introduce unexpected vulnerabilities. Security therefore never reaches a stable state.

Artificial intelligence accentuates this dynamic. It can speed up certain offensive tasks such as data analysis, the preparation of social engineering messages or the search for vulnerable configurations. It can also strengthen defense by facilitating the detection of anomalies, the analysis of events or the prioritization of alerts. Its strategic impact will depend less on the simple availability of models than on their integration into operations and the quality of the data to which actors have access.

This should not be interpreted as saying that automation will remove the fundamental constraints of complex operations. Producing a precise physical effect on an industrial infrastructure always requires an understanding of the targeted environment. Maintaining surreptitious access continues to depend on operational discipline and knowledge of architecture. Artificial intelligence can reduce some costs, but it does not automatically make targets or campaigns interchangeable.

Power relations

Comparing cyber capabilities is much more difficult than comparing naval fleets or air forces. The most important capabilities are usually secret, precisely because their value depends on non-disclosure. A state does not publish a list of vulnerabilities that it can exploit, the networks to which its services have access or the tools it retains for a crisis situation. Public indicators must therefore be interpreted with caution.

Cyber power can nevertheless be analysed from several factors: the quality of intelligence services, the volume of qualified personnel, the depth of the technology sector, access to global infrastructure, relations with suppliers, the level of cybersecurity of the national economy, the ability to coordinate between agencies and the ability to integrate cyber operations into a broader strategy.

The United States: considerable capacities and a very large exhibition area

The United States has significant advantages in almost every one of these dimensions. Its technology sector is centrally positioned in software, cloud services, semiconductors, and many global digital infrastructures. Intelligence agencies and armed forces have significant resources, while the network of alliances allows for extensive information sharing.

However, this position is not equivalent to automatic superiority. The highly advanced digitalization of the US economy creates a considerable attack surface. Many essential

services rely on private operators whose level of security can vary. Offensive power and internal vulnerability can therefore advance simultaneously.

The integration of cyber capabilities into military operations is a particularly important advantage. An operation prepared by the competent services can be synchronised with other means, which increases its military value. However, this integration depends on maintaining access and the ability to transmit operational requirements to cyber units at an early stage. A target identified at the last moment cannot always be compromised with the necessary precision.

China: industrial depth and strategic intelligence

China has a large technological base, a considerable volume of skills and a security apparatus capable of integrating cyber operations into broader economic, political and military objectives. Technological and industrial intelligence is an important dimension of this activity, in addition to directly military objectives.

The balance of power with the United States holds a special place because of the interdependence between the two economies and their technological competition. The ability to understand adversarial networks, infrastructures and supply chains has a value that goes beyond the mere preparation for war. It also makes it possible to assess dependencies, collect information on priority technologies or follow up on political decisions.

China's rise in digital technologies is gradually reducing certain external dependencies while creating its own infrastructure to protect. As in the space sector, the expansion of national capacity therefore simultaneously increases the means available and the number of functions vulnerable to adverse action.

Russia: Exploiting Asymmetries and a Hybrid Ecosystem

Russia has recognized capabilities in intelligence, disruption and digital influence operations. Its overall economic and technological weight is lower than that of the United States or China, but cyberspace offers means of action that do not require replicating the conventional or industrial power of the adversary.

The activities publicly denounced by NATO in July 2026 also show the importance given to the environment of close or tolerated actors. The existence of an ecosystem comprising several types of groups complicates attribution and allows pressure to be exerted without each operation having to be directly conducted by an identifiable official structure¹⁷.

This model also has limitations. Criminal or semi-autonomous actors may pursue their own interests, cause unwanted incidents, or attract harmful international attention. Ambiguity increases flexibility but reduces complete control.

Europe: Collective Resilience and Operational Fragmentation

The European Union has a significant regulatory capacity and has gradually built a framework covering essential operators, digital products, crisis preparedness and response to major

¹⁷ North Atlantic Treaty Organization. (2026, July 13). *Statement of condemnation by the North Atlantic Council of Russia's malicious cyber activities*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities>

incidents. The *Cyber Solidarity Act* complements existing mechanisms by organising detection and a collective support capacity¹⁸.

This regulatory power does not correspond to a centralised European offensive capability. Cyber intelligence and action resources remain mainly national. This distribution reflects the Member States' competences in terms of defence and national security, but it requires significant coordination when a campaign affects several countries.

Europe therefore has a particular balance of power: it can raise the average level of security in its market through regulation and mobilise collective response mechanisms, while depending on national capacities for sensitive allocation and offensive operations. This architecture can work if information sharing procedures are fast and responsibilities have been defined before the crisis.

Non-state actors

Cyberspace allows non-state groups to produce effects that would be difficult to achieve in other areas. Criminal groups can temporarily shut down the activities of a large company or administration. Hacktivists can disrupt sites, publish data or conduct high-profile campaigns.

However, this capacity to cause harm must be distinguished from a strategic capacity comparable to that of a state with structured intelligence, long-term preparation and integration with other instruments of power. The most complex operations require a level of knowledge, patience and resources that considerably reduces the number of actors capable of carrying them out in the long term.

Interests at stake

States seek in cyberspace to protect their own infrastructures while retaining the ability to understand and affect those of their competitors. These two objectives cannot be separated. A power without an offensive capability loses part of its intelligence and action resources; a power unable to protect and restore its systems offers the adversary leverage capable of neutralizing the advantages obtained elsewhere.

Intelligence is usually the most constant interest. A presence in an adversary network can provide political, military, economic or technological information without immediately producing a visible incident. Espionage thus benefits from a particularly favourable cost-benefit ratio when access can be maintained for a long period of time.

Sabotage has a more restrictive logic. Its use often reveals the presence of the attacker and provokes a defensive reaction. It is therefore rational to reserve certain abilities for situations where the immediate effect justifies the possible loss of access.

Prepositioning falls between these two functions. It allows you to keep an option without using it immediately. Its value depends directly on the ability to remain clandestine and the stability of the target architecture.

The protection of critical infrastructure is the main defensive interest. However, the number of systems concerned requires prioritization. A State cannot protect all companies with the same level of requirements. It must identify the functions whose shutdown would have a systemic effect, the operators who provide them and the suppliers on whom they depend.

¹⁸ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

Companies pursue their own interests. They need to maintain their services, protect their reputation, meet regulatory obligations, and contain costs. These priorities do not always align exactly with those of the state. A strategically useful security measure may be costly in the short term for an operator; conversely, an economically optimal architecture can create a concentration of risk that is deemed problematic for national security.

The State must therefore organise this relationship through regulation, incentives and information sharing. The *Cyber Resilience Act* and other European policies seek to internalise part of these security costs in the design and maintenance of products¹⁹.

Alliances add an extra layer. A cyberattack against a member state can exploit infrastructure in another country, affect several Allies simultaneously, or rely on information held by multinational companies. The collective interest is therefore to reduce capability gaps between members and prevent an adversary from exploiting the least protected link in an integrated whole.

Dynamics of evolution

The most important development is expected to be the professionalization of pre-positioning. As infrastructure becomes better protected, achieving sustainable access requires more preparation, intelligence, and discipline. The most strategic campaigns may therefore be less visible than the opportunistic attacks that dominate public statistics. Their danger will lie precisely in their low operational noise.

The second dynamic is the increase in resilience requirements. European and allied policies show that mere prevention is no longer considered sufficient. The *Cyber Solidarity Act* organises a collective detection and response capability, while NATO is developing its own integrated defence mechanisms and exercises²⁰²¹.

A third dynamic is identity security and privilege limitation. Traditional models that rely on a relatively rigid distinction between inside and outside the network are increasingly unsuitable for environments using the cloud, remote work, many vendors and distributed services. NATO's Digital Strategy adopted in 2026 explicitly mentions the use of Zero Trust principles to strengthen the security of the Alliance's infrastructure²².

This approach is intended to prevent an initial compromise from automatically providing the attacker with broad access. Identity, context, and rights must be verified on an ongoing basis, which limits the possibilities for lateral movement in the network.

Artificial intelligence should then change the volumes of activity. Social engineering campaigns can be more automated and personalized; code, vulnerability, or log analysis can be accelerated. Defenders will benefit from the same tools to process a higher number of alerts or detect unusual behavior. It is therefore likely that AI will simultaneously increase the pace of attack and defense, without determining on its own which of the two gains a lasting advantage.

The fifth dynamic concerns the convergence between cyber and conventional operations. Military forces will seek to integrate cyber options more from the early planning phases. This

¹⁹ European Commission. (2026, September 7). *Cyber Resilience Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

²⁰ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

²¹ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

²² North Atlantic Treaty Organization. (2026, May 26). *NATO's Digital Transformation Implementation Strategy 2.0*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy>

evolution will require preparing access early enough and better informing cyber managers of the operational objectives likely to emerge in the event of a crisis. The usefulness of the tool will depend on this anticipation: a capability that does not exist at the time the campaign begins cannot be improvised.

Finally, the international framework is likely to continue to progress slowly. The consensus reached in 2025 at the UN provides a common basis but does not eliminate differences between powers. The global mechanism launched in 2026 institutionalizes dialogue, which can improve confidence-building measures and mutual understanding without impeding the development of offensive capabilities²³.

Prospective scenarios

The first and most likely scenario is that of permanent competition dominated by espionage, pre-positioning and limited disruption. States will continue to penetrate their competitors' networks in order to gather intelligence or prepare options, while generally avoiding the most destructive effects outside of a major crisis. At the same time, criminal and hacktivist groups will continue to produce a large volume of incidents, which will complicate the strategic reading of the environment.

This configuration is relatively stable but not guaranteed. Operations may remain below the threshold of open confrontation for a long time, but the discovery of access to critical infrastructure can provoke a significant political reaction if it occurs at the time of a crisis. The absence of a destructive effect does not therefore mean that there is no risk of escalation.

The second scenario corresponds to a systematic integration of cyber into a conventional conflict. Operations would begin before the first visible military actions in order to collect information, disrupt certain networks and prepare synchronized effects. Targets would be chosen according to their contribution to the campaign: logistics, communications, air defense, command, transport or industrial production. Cyber operations would not necessarily seek a general paralysis. A properly synchronized temporary interruption could provide a sufficient advantage.

The third scenario would be that of a major campaign against several critical civilian infrastructures. Such an operation would seek to create cumulative effects: disruption of energy, telecommunications, certain transport or financial services. However, its success would require maintaining several accesses simultaneously and reducing the capacity for restoration. The larger the campaign, the more likely it would also be to award and a significant international response.

The fourth scenario concerns an attack whose consequences go beyond the initial intentions. Digital infrastructures are highly interconnected and malware can spread beyond the intended target. An operation designed to produce a local effect can affect third companies or countries, which would widen the crisis and complicate the political decision of both the attacker and the victim.

The fifth scenario would be an increase in global digital fragmentation. Security considerations could lead governments to impose more restrictions on providers, data, cloud infrastructure or telecommunications equipment. Such a development would reduce some dependencies but increase costs, accelerate the development of distinct technology ecosystems and could reduce opportunities for cooperation on network security.

²³ United Nations, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025, July 1). *Final report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025* [Draft] (A/AC.292/2025/L.1). United Nations. <https://digitallibrary.un.org/record/4084927>

Recommendations

The first priority is to base cybersecurity policies on the functions to be maintained rather than on the uniform protection of all systems. Each administration or critical operator must identify the services whose interruption would have the most serious consequences, specify the technical dependencies necessary for their operation and determine the minimum level that must be able to be maintained during a crisis. This analysis makes it possible to allocate resources to systems whose compromise would have a truly strategic effect.

The second priority is detection. An organization can have significant protections and remain compromised for several months if it does not know how to identify anomalous behavior. Logging, monitoring, proactive threat hunting, and event analysis capabilities should therefore be considered critical functions. The time between initial access and detection provides a more useful metric than just the number of blocked incidents.

The third priority is segmentation and privilege control. A local compromise should not allow the attacker to automatically gain access to the entire system. Zero trust principles, rights limitation, strong authentication, and separation of critical environments should reduce the potential effect of initial access. The goal is not to make intrusion impossible, but to limit what an attacker can do when they manage to gain entry.

The fourth priority is restoration. Backups must be isolated from the primary environment, regularly tested, and accompanied by procedures to actually rebuild services. A backup that has never been restored under crisis conditions is not a sufficient guarantee. Operators need to know how long it will take to get their most important services back up and running.

The fifth priority is securing the supply chain. Suppliers should be ranked according to the access they have and the criticality of the services they provide. Contractual obligations should cover vulnerability management, incident notification, updates and audit rights. European policies on digital products provide a useful framework, but the ultimate responsibility for mapping dependencies lies with the organisations themselves²⁴.

The sixth priority is information sharing. State campaigns often reach several organisations before a complete picture can be built. Technical information must be able to be exchanged quickly between private operators, national authorities, European agencies and allies. Mechanisms must provide for the protection of sensitive information so that companies are not deterred from reporting incidents quickly.

The seventh priority is exercises. These should involve technical officials, business management, political authorities, security forces and, where the scenario warrants, the armed forces. A major cyber crisis does not only produce IT problems: it raises questions of public communication, accountability, economic continuity, attribution and international response. NATO exercises and European mechanisms are useful models for testing this coordination²⁵.

The eighth priority is the preparation of political attribution. States should define in advance the procedures for combining technical intelligence and other sources, the levels of trust needed for different types of response, and the mechanisms for coordination with allies. A public attribution should not be improvised under the pressure of a crisis.

²⁴ European Commission. (2026, July 27). *Cyber Resilience Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> *European Digital Agenda*

²⁵ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

The ninth priority concerns offensive capabilities. Their development must remain linked to specific political and military objectives. Maintaining access in a network has a cost and value that can be lost after use. The use must therefore be decided on the basis of the expected effect, the possibility of propagation, the risk of attribution and the interest in retaining the capability for a later situation. A credible offensive doctrine is not measured by the number of tools developed but by the ability to use them within a coherent strategic framework.

The tenth priority concerns European cooperation. The recently created instruments must be tested in truly complex situations. The *Cyber Solidarity Act* and the European reserve can provide additional capabilities, but their effectiveness will depend on the time frame for mobilisation and the articulation with the national authorities²⁶.

Finally, France must treat cyber defence as a common component of state continuity, economic security and military readiness. The administrative separation between these areas must not prevent the flow of necessary information. Civilian critical infrastructure, defence companies and public networks must be analysed as a set of dependencies whose disruption can affect different national functions.

Strategic implications

The first implication concerns the temporality of competition. Cyber allows states to prepare options long before the use of these capabilities is politically decided. This characteristic makes adversary networks comparable to a permanent intelligence space in which actors seek to understand architectures, identify dependencies and maintain access. The preparation of a future operation can therefore be difficult to distinguish from routine espionage until the moment access is activated.

This reduces the value of a solely reactive defence. When a crisis begins, it may be too late to look for all existing compromises or to completely rebuild the most vulnerable architectures. The level of security achieved before the crisis directly conditions the political room for manoeuvre available during the crisis. States must therefore accept that part of the cost of preparing for cyber warfare corresponds to permanent investments whose usefulness is difficult to see as long as no major incident occurs.

The second implication is the notion of offensive power. Cyber capabilities cannot be stored exactly like ammunition. A tool based on a vulnerability may lose its value when the flaw is patched. Clandestine access may disappear after an update or be discovered during an audit. Capabilities must be continually maintained and renewed. Their value depends as much on ongoing intelligence as on initial technical development.

This has several implications for military planning. Commands need to identify the types of systems that may be of interest in conflict early enough so that the necessary capabilities can be prepared. A request a few days before an operation does not guarantee that access will be available. Integrating cyber into planning cannot therefore be limited to adding a "cyber effect" to a plan that has already been completed.

The third implication concerns the limits of cyber autonomy. A digital campaign can produce significant effects, but its ability to impose a sustainable policy decision on its own remains uncertain. Institutions can restore services, operators can isolate networks, and companies can adapt to temporary disruptions. A cyber attack produces more value when it contributes to broader pressure or supports a military, economic, or diplomatic operation.

²⁶ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

This observation does not diminish its importance. On the contrary, it provides a better understanding of its function. Cyber can affect the pace of a campaign, complicate mobilization, provide intelligence, impose economic costs, and create uncertainty. These effects can be strategic when they are integrated into a coherent policy objective. They become much less useful when disruption is seen as an end in itself.

The fourth implication concerns national resilience. Civilian infrastructure is now important enough that its security directly affects the state's ability to sustain a protracted crisis. An army can have highly protected networks while depending on a society whose telecommunications, transport or production are vulnerable. Cyber defence must therefore be articulated with general resilience and not limited to military systems.

The European Union plays an important role in this dimension because its regulations can raise the level of security of many private actors. The *Cyber Solidarity Act*, the *Cyber Resilience Act* and the European certification policy address different elements of the same issue: reducing the number of vulnerabilities, better detecting campaigns and organising the response when a crisis exceeds the capacities of an operator or a State²⁷.

The fifth implication concerns alliances. Pooling makes it possible to improve allocation, share information and provide support to a member with less resources. But it also creates interdependence. An alliance with highly connected networks must take into account the differences in maturity between members and the risks introduced by common infrastructures. Improving the minimum level of protection therefore becomes a collective interest.

NATO is responding to this question through the development of common standards, exercises and structures. The 2025 edition of the *Cyber Coalition*, with around 1,300 participants from 29 Allies and seven partners, illustrates the importance of collective preparedness²⁸.

The sixth implication is deterrence. In cyberspace, deterrence cannot rely on a single threat of retaliation. The uncertainty of attribution, the frequency of incidents, and the wide variety of effects make an automatic response not credible. Deterrence must combine several mechanisms: preventing access where possible, limiting the effects of a compromise, restoring quickly, publicly exposing certain campaigns, imposing diplomatic or economic costs, and maintaining response options in multiple areas.

This approach also avoids artificial symmetry. A cyberattack does not necessarily have to be met with a cyber response. The instrument must be chosen according to the political objective. An economic sanction, an arrest, the expulsion of agents, an intelligence operation or military action may, depending on the circumstances, be more appropriate than a direct technical response.

The seventh implication concerns law and norms. The international consensus on the idea that international law applies to cyberspace does not resolve all issues. States retain different interpretations regarding thresholds, sovereignty, diligence and self-defence. Multilateral work nevertheless remains useful in building common expectations and confidence-building mechanisms.

²⁷ European Commission. (2026, July 7). *EU cybersecurity policies*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

²⁸ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

The conclusion of the 2021-2025 UN Working Group by consensus and the establishment of the Global Mechanism from 2026 provide a more permanent framework for these discussions²⁹.

This framework is unlikely to lead to a demilitarization of cyberspace. Major powers will continue to develop capabilities as long as they consider them to be valuable for intelligence and defense. The most realistic progress is in risk reduction, protection of critical civilian infrastructure, communication mechanisms, and the gradual clarification of behaviors considered particularly dangerous.

Conclusion

Strategic cyberwarfare cannot be reduced to the proliferation of cyberattacks or the prospect of a digital collapse of states. It is the sustained integration of digital capabilities into intelligence practices, enforcement policies, and military planning. States are constantly seeking to understand their competitors' infrastructures, identify their vulnerabilities, and maintain usable access if the political context requires more direct action.

This activity is made possible by the general digitalization of societies. Administrations, companies, critical infrastructure and armed forces use common technologies and depend on largely private supply chains. National security can therefore no longer be ensured only within a military perimeter. The general level of cybersecurity of an economy directly affects its ability to absorb a hostile campaign.

ENISA data reflect this European reality: several thousand incidents are observed in an environment where criminal groups, hacktivists and state-linked actors often use similar techniques³⁰.

This threat density complicates strategic analysis but also reinforces the value of basic security measures. Policies to limit privileges, patch vulnerabilities, segment networks, and test backups are useful against very different threats. The line between routine cybersecurity and preparation for a major confrontation is therefore less clear than it is for many military capabilities.

The main difference between a resilient and a vulnerable organization will become apparent after the breach. The time it takes to identify the attacker, isolate the affected systems, and restore services will often determine the strategic effect more than the initial technical success of the intrusion. An operation whose consequences are quickly contained produces little political benefit; a prolonged disruption can change a government's decisions or the conduct of a campaign.

Investments must therefore focus as much on recovery as on protection. This evolution is clearly reflected in European measures, in particular the *Cyber Solidarity Act* and the European Cybersecurity Pool, which are not only aimed at prevention but also at preparedness, response and recovery^{31,32}.

²⁹ United Nations, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025, July 1). *Final report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 [Draft]* (A/AC.292/2025/L.1). United Nations. <https://digitallibrary.un.org/record/4084927>

³⁰ European Union Agency for Cybersecurity. (2025, October 1). *ENISA threat landscape 2025*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

³¹ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

³² European Commission. (2025, August 26). *ENISA to operate the EU Cybersecurity Reserve*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/news/enisa-operate-eu-cybersecurity-reserve>

NATO is adopting the same logic in a different military setting. Cyberspace has been an area of operations since 2016, capabilities are integrated into collective defence, and the Alliance continues to develop organisations and exercises to improve coordination between states, armed forces, civilian experts and industry³³.

However, competition will remain largely national in its most sensitive functions. Intelligence services, offensive capabilities and political allocation decisions will continue to be primarily the responsibility of states. International organisations make it possible to coordinate, share and increase resilience; they do not replace the sovereign capabilities needed to understand a campaign or decide on a response.

For France and the other European powers, the challenge is therefore to articulate three levels. The national level must retain the intelligence, attribution and action capabilities necessary for essential interests. The European Union must strengthen the general security of the market and organise the collective response to incidents beyond the means of a single actor. NATO must ensure the integration of cyber into military operations and collective defence.

Finally, strategic cyberwarfare raises a question of analytical discipline. Not all malicious activity should be interpreted as a war operation. Most incidents are not strategic in scope, and many campaigns involve crime, espionage, or limited forms of pressure. Using the category of war for all of these phenomena makes it impossible to distinguish between actions that can actually change a balance of power.

The assessment should include the intended function, the duration of the effect, the political context, the restorative capacity, and whether the operation could be integrated into a broader strategy. A limited disruption can be militarily decisive if it occurs at a time when a force is precisely dependent on the system being affected. A technically spectacular attack may remain strategically secondary if services are quickly restored and no political decisions are affected.

The place of cyber in contemporary power lies in this difference. It does not offer a universal method to replace other instruments. It provides additional intelligence, preparedness and disruption capabilities that can be used long before a conflict begins and then combined with a broader campaign. The powers that are able to make the most of them will be those that prepare the necessary access early enough while reducing the possibility for their adversaries to do the same with their own infrastructure.

This competition will probably never be fully visible. Some of the most important capabilities will remain clandestine until they are used or discovered. The absence of major incidents will therefore not lead to the conclusion that there is no offensive preparation. Conversely, the existence of recurrent intrusions does not mean that a war is underway in the classic sense.

Strategic cyberwarfare is precisely located in this intermediate space, between permanent intelligence, crisis preparation and military employment. It is this continuity, more than the destructive power of digital tools alone, that explains its growing place in power strategies.

³³ Allied Command Transformation. (n.d.). *Cyber Defence*. NATO. <https://www.act.nato.int/activities/cyber/>