UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 1, e95736, p. 1-23, mar. 2026 • https://dx.doi.org/10.5902/2357797595736
Submissão: 13/03/2026 • Aprovação: 13/03/2026 • Publicação: 20/03/2026

Reflexões sobre Defesa e Segurança

Taking back the initiative: prospective intelligence and offensive capabilities enabling the proactive defense in the cyberspace

Retomando a iniciativa: inteligência prospectiva e capacidade ofensiva para a proatividade no ciberespaço

Jomar Barros de Andrade[I]

[I]Universidade Federal de Santa Maria, Santa Maria, RS, Brazil

Abstract

Considering the application of cyber power, the states are currently divided into three groups. The first one consists of the liberal democracies, characterized by doubt, division and caution. The second comprises the authoritarian states, whose actions in cyberspace combine strategic vision, concealment and boldness. The third encompasses most of the remaining countries which, due to lack of capability, have little to no effective influence. In this scenario, cyber threats operate at large, taking risks and harming states, companies and individuals. This work hypothesis is that the use of prospective Cyber Intelligence, combined to the development of offensive cyber capabilities, forms the backbone of a strategy capable of aligning state, academia and industry, aimed to democratically strengthen security, contribute to strategic warning and challenge the freedom of action enjoyed by the cyber threats. After reviewing the concepts of sovereignty and power in cyberspace, the advantages of the attacker over the defender and the risks of a reactive posture will be analyzed, in order to explain the success that authoritarian states are achieving in cyber deterrence. Next, the application of prospective scenario techniques in Cyber Intelligence will be presented, as an instrument of strategic warning against the cyber threats, highlighting that their actions, below the threshold of conflict, make the use of artificial intelligence solutions for incident prevention and response, by the states, worth the risk. Then, the synergy between defensive and offensive cyber operations will be examined, showing that the development of cyber weapons can drive proactive defense capability, while enabling better resilience of the critical infrastructures. Finally, it will be demonstrated that, in the face of threats willing to take increasingly greater risks, the combination of prospective intelligence and offensive capability is a practical and viable solution for the cyber defense of democratic states.

Keywords: Cyber sovereignty; Cyber power; Intelligence; Strategic prospective; Offensive cyber weapons

Resumo

A conjuntura atual apresenta uma divisão dos estados em três blocos. No primeiro estão as democracias liberais, caracterizados pela cautela no exercício do poder no espaço cibernético. No segundo estão estados autoritários, cuja atuação no ciberespaço combina visão estratégica, dissimulação e audácia. O terceiro é composto pela maioria dos demais países que, por falta de capacidade, não possuem efetiva influência. Nesse cenário, as ameaças cibernéticas atuam com desenvoltura, assumindo riscos e provocando prejuízos. A hipótese deste trabalho é que o emprego de Inteligência Cibernética Prospectiva e o desenvolvimento de capacidades cibernéticas ofensivas compõem a base de uma estratégia capaz de alinhar estado, academia e indústria para, democraticamente, fortalecer a segurança, contribuir para o alerta estratégico e desafiar a liberdade de ação explorada pelas ameaças cibernéticas. Após rever os conceitos de soberania e poder no ciberespaço, serão abordadas as vantagens do atacante sobre o defensor e os riscos de uma postura reativa, para explicar o sucesso que estados autoritários vêm obtendo na dissuasão cibernética.

Palavras-chave: Soberania cibernética; Poder cibernético; Inteligência; Prospectiva estratégica; Armas cibernéticas ofensivas

INTRODUCTION

For a concept that is so widely used, “power” is surprisingly elusive and difficult to measure, and becomes even more complex when analyzed in cyberspace. Although the notion of power based on information resources is not new, cyber power is, it depends on the resources that characterize cyberspace in its physical and virtual dimensions (Nye 2010, 2–5) and must necessarily consider a comprehensive approach to national capabilities (Flight; Hemani; Cassidy 2022, iv). Cyberspace is therefore another dimension in which the power of state and non-state actors is exercised, by the diffusion of values and ideas and the use (or possibility of use) of force, with or without kinetic effects.

Despite the significant growth in the literature on cyber deterrence, digital sovereignty, offensive operations, strategic foresight, and the application of artificial intelligence (AI) in cyberdefense, these fields remain, to a large extent, treated in a fragmented manner. Normative studies focus on the legal and ethical limits of state action; operational analyses address offensive and defensive capabilities isolated from each other; and works on strategic foresight rarely dialogue with the technical

and operational reality of cyber defense. As a result, there is a relevant analytical gap in understanding how democratic states can coherently and responsibly integrate prospective cyber intelligence and offensive cyber capabilities to regain strategic initiative in cyberspace, operating in a way consistent with international law and avoiding an unintended escalation to conflict.

Contemporary literature recognizes that cybernetic power is unevenly distributed. The academia has been making serious efforts in order to measure the cyber power of states and, although there are differences between the adopted methodologies and used data, there is a consensus that three countries possess a clearly superior cyber power: the United States of America (USA), China, and Russia (Voo; Hemani; Cassidy 2022, 9). The USA leads the group of countries that comprises most liberal democracies, including the European NATO members; while China and Russia, although different in their objectives and methods, are the main players among the states considered authoritarian.

In addition to the major powers, other countries are developing their capacity, with varying degrees of transparency. Nonetheless, the available data make it possible to identify at least 30 countries that are known to pursue in the building of their cyber power (Voo et al 2020). This does not mean that the remaining dozens of countries do not operate in cyberspace, nor that they are less exposed to be affected by the cyber threats.

Such threats target governments, businesses, non-governmental organizations, and individuals around the world and at all levels. Their operations are not limited to those of criminal organizations that seek only financial gain, but also include many that are sponsored by states, seeking economic, military, or other strategic advantages. The clash between these various actors creates intense strategic competition in cyberspace which, to date, has remained below the threshold of armed conflict (Sullivan 2023, 21).

The prevailing view in the West is that most cyberattacks target liberal democracies. Considering that many so-called attacks are routine probes, carried out

automatically (Gartzke 2015, 324), a particularly interesting survey by the Center for Strategic and International Studies (CSIS) has, since 2006, focused on state actions, espionage, and attacks that caused losses greater than one million dollars. According to the available data, as of October 2025, of the 1,138 most relevant records, 270 targeted the United States and 45 the United Kingdom, while China and Russia accounted for 31 incidents each (CSIS 2025). Although this survey reflects a Western perspective, it is a useful tool to indicate that, for various reasons, authoritarian regimes seems to be less exposed, or at least publicly protest less frequently against cyber threats, than liberal democracies.

In this geopolitical dispute, the posture of the main powers could hardly be more different. Relations between the great powers have become more conflictual, something that democracies are somewhat reluctant to acknowledge, an attitude that has favored China and Russia, which have been able to maintain the initiative for more than a decade, not only in cyberspace (Lewis 2022, 12). Meanwhile, many voices argue that confidence-building measures and norms, imposed by mechanisms of international bodies that do not yet exist, will succeed where deterrence and offensive capability would have failed (Taddeo 2017, 391).

There is no disagreement that traditional deterrence mechanisms, especially nuclear deterrence, do not properly apply to cyberspace. However, this article argues that an effective cyber strategy will have to address these issues in a flexible way, seeking to draw on the strengths of different strands of international relations theory.

Reality in cyberspace changes at high speed, so actors that merely adapt to circumstances will always be one step behind. In this context, although not all actors have the power to shape reality, seeing possible futures, in order to act from a position of advantage, is something feasible that should be a permanent objective of states. However, at present, no one is capable of achieving this goal relying solely on its own means. In addition to academia and industry, traditional allies in the search for progress in the Information Age, synergy with partners and allies strengthens advantages and mitigates individual weaknesses.

Thus, this article seeks to fill this gap by arguing that the combination of prospective cyber intelligence and the mastery of offensive capabilities constitutes the backbone of a viable strategy for democratic cyber defense. It is argued that strategic foresight allows anticipating trends, reducing surprises and supporting strategic alertness, while mastery of offensive techniques is a necessary condition for effective active defense, for concealment, for strengthening resilience and for limiting the freedom of action of cyber threats. To this end, the article adopts a qualitative and analytical approach, based on the review and critical synthesis of academic literature, institutional documents, and widely documented examples of state practice, with an emphasis on sources associated with NATO, the CCDCOE, and specialized security and defense journals.

To develop this argument, the article examines, initially, the concepts of power and sovereignty in cyberspace, as well as the structural advantages of the attacker and the limitations of exclusively defensive postures. It then analyzes the role of strategic foresight and cyber intelligence as instruments of anticipation and decision support, including the potential and limits of the use of artificial intelligence in this domain. Finally, it discusses the integration between offensive and defensive capabilities, exploring its legal, strategic, and operational implications for the cyber defense of democratic states.

It is recognized that the secretive nature of cyber operations, attribution challenges, and the limitation of public data impose empirical constraints; even so, the triangulation between theory, institutional practice, and known operational patterns provides a sufficient basis for discussing strategic and normative implications relevant to the cyber defense of democratic states.

DOES THE ATTACKER ALWAYS HAVE THE ADVANTAGE?

There is a broad academic debate about the utility of cyber capabilities in warfare. In the past, there was an expectation that cyber operations could have an independent impact on combat, enabling strategic cyberattacks and offering decisive advantages. In reality, such scenarios have not yet materialized. For several reasons, even with the escalation of cyber activities in recent years, the dispute in cyberspace has remained below the threshold of armed conflict (Maschmeyer 2021, 57).

Despite this, the value of offensive and defensive cyber operations for combat is not in dispute. The war in Ukraine has provided valuable lessons in this regard and, at the same time, has not demonstrated some unrealistic expectations. Consequently, although the growing trend of conflict in cyberspace indicates the need to develop new strategies (Lewis 2022, 12), full-scale cyberwar remains an unlikely scenario.

Thus, although democracies must always prepare for the worst, the very real and ongoing problem of low intensity competition in cyberspace requires the proper attention. The academic production on the matter already provides the decision-makers extensive advice on the legal gaps, uncertainties, and risks in the application of cyber power. It is time to further the discussion about what can be done and how, in order to answer the key question: within the limits of the international law, and with acceptable risks, how can democracies build and apply their cyber power against the many existing cyber threats?

In this context, the concept of cyber sovereignty has grown in importance, meaning the ability to create and enforce rules over cyberspace through state governance (Leiter 2020, 2). Thus, although it is now accepted that the general principle of sovereignty applies to cyberspace in its physical, logical, and social layers (Schmitt 2016, 11–12), its application to the characteristics of this domain will be determined by states, through their actions and/or the development of treaties and norms (Corn 2017, 210).

The limits on state action in cyberspace are directly related to their power. While there is no generally accepted definition of cyber power, it can be understood as a country's ability to achieve its goals using cyber means. So, the greatest global cyber power is the country that can establish clear national objectives in cyberspace, possesses the essential capabilities to pursue those objectives, and achieves multiple goals using cyber means (Voo et al. 2020). This approach is closely aligned with the concept of smart power, which combines coercion and retribution (hard power) with persuasion and attraction (soft power), a concept proposed by Joseph Nye Jr, after concluding that soft power is not the solution to all problems (2011, xiii) and cannot be the sole resource of an effective foreign policy (2011, 22).

Hard power in cyberspace means the development and application of offensive capabilities in this domain, a subject that often elicits notably negative reactions and opinions. The analogy with nuclear deterrence, the risk that cyber weapons may spill over beyond their intended targets, and especially the fear of escalation, all encourage a posture focused on cyber arms control, and on mitigating attacks between states, through confidence building measures (Borghard and Lonergan 2018).

However, it is now clear that equating cyber capabilities with nuclear weapons is exaggerated, as their effects are not comparably catastrophic and their attribution is more difficult (Nye 2010, 16). Moreover, while a sufficiently severe cyberattack could, in theory, escalate a crisis into armed conflict, there is no consensus on what that threshold would be and, thus far, nothing suggests that such a scenario is plausible (Libicki 2020, 202).

Even in such a case, escalation would depend on a credible attribution of responsibility. Although the scale and frequency of cyberattacks have led to an increasing number of indications of perpetrators, the public attribution of state-backed offensive operations remains complex (Derian Toth et al. 2021, 5–6). As a fundamental element for an acceptable response, attribution is an activity where political considerations are more relevant than technical ones and requires a solid intelligence foundation for decision-makers (Brock and Lewis 2025, 6).

Thus, even if evidence beyond any doubt is not required for the attribution of a cyberattack, the decision to attribute will always entail some degree of risk. Attributing with limited evidence may prompt questions about real authorship, while disclosing too much evidence may reveal excessive details about defensive capabilities. As a result, for any attacker minimally capable of anonymizing its actions, the chances of successfully concealing its identity are high.

Not everything is easy for the attacker, however. Offensive operations depend on significant prior investment in planning and preparation. They require intelligence support and exploitation operations to identify vulnerabilities, gain and maintain access, and develop the tools necessary for exploitation, often over extended periods of time, to achieve the desired effects (Lonergan and Montgomery 2022, 86). In addition to the expected difficulties, any security update or password change can get an operation back to square one. It is therefore natural that the highest priority is often given to what can be controlled: the defense of one's own networks.

But cyberspace is an environment of persistent attack. The defender must succeed all the time and everywhere, whereas attackers need to succeed only once to compromise their targets (Gartzke and Lindsay 2015, 322). Because strategic victory cannot be achieved through purely defensive measures, no matter how many short-term successes are obtained, state cyber defense has shifted from a purely reactive posture to more active strategies (Taddeo 2018, 4).

As is common with issues related to cyberspace, conceptual boundaries are often blurred. There is no clear dividing line between cyber operations conducted below and above the threshold of armed conflict, and many defensive actions exist in an ambiguous space between offense and defense (Lonergan and Montgomery 2022, 87). This ambiguity, which extends to several other aspects of the domain, creates both risks and opportunities. So, hence it can not be removed, it must be embraced.

Of course, no serious scholar can ignore the technical and policy issues that underpin more cautious positions and advocate a more limited role for offensive

actions in cyberspace (Jacobsen 2021, 720). However, believing that democracies and authoritarian states play by the same rules reflects an somewhat excessive degree of good faith, that is not justified by reality. Accusing adversaries of militarizing cyberspace, while simultaneously developing one's own capabilities, and conducting or sponsoring offensive actions against them, is simply part of the Grand Strategy old game. Consequently, although any announcement related to offensive cyber capabilities will be met with alarm, its practical effects on stability are likely to be more limited than feared (Lewis 2015, 6). Military personnel and diplomats play complementary roles in this dance, where the structural ambiguity must be considered, along with careful risk calculation, so that timely decisions can be made.

International law has evolved in its approach of cyber issues, although we are still far from a broad consensus. Tallinn Manual 2.0 (Schmitt 2016) is perhaps the best reference in this field, with particularly interesting positions on the right to self-defense, espionage, and intelligence in cyberspace. In summary, the manual establishes that states have the right to respond to cyber operations that reach the level of an armed attack, but it is clear when states that actions causing only minor interruptions of non-essential services do not qualify as such (Rule 71), and that peacetime espionage by states is illegal, per se (Rule 32). Cyber operations may thus be treated like intelligence operations, under international law (Corn 2017, 210).

Finally, much has been written about deterrence in cyberspace. Deepening the debate on the role of offensive operations, versus norms and confidence building measures, lies beyond the scope of this work. For its purposes, however, it is useful to offer a provocation. From the point of view of the cyber threats, whether state sponsored or not, the democracies place the individuals above the state, distrust their own governments, have a high aversion to conflict, and are willing to relinquish part of their capabilities, hoping to convince their adversaries of their good intentions. The democracies are, in short, easy targets.

As a result, even while suffering most of the attacks, still maintain a predominantly reactive posture and, although their patience has begun to show signs of exhaustion, still have great difficulty operating within the reality of competition bellow the threshold of conflict. Consequently, although authoritarian states are also important targets of cybercrime, the available data (CSIS 2025) indicate a much smaller number of attributed offensive actions against them.

There are many possible explanations for such: attackers are exceptionally capable and go undetected; authoritarian cyberspace controls and defenses are so strong that repel most attacks; or targets do not wish to reveal their weaknesses. However, a likely scenario is that, with the notable exceptions of the United States and Israel, democracies are indeed cautious in using their offensive capabilities, both due to a lack of appetite for risk and fear of potential public exposure, or unlikely conflict escalation. In other words, from the point of view of cyber threats, cyber deterrence works.

CAN ANYONE SEE THE FUTURE?

While it is not the objective of this work to delve deeply into prospective and foresight methodology, some contextualization is needed. Although there are several definitions, within the context of international best practice a scenario is a fictitious, yet plausible, sequence of events set in the real world, 3-to-20 years in the future (Neill, Hinkle, and Morgan 2016, 3). It is important to emphasize that scenarios are not predictions of what will happen, but foresights of possible paths. Their purpose is to support risk management and reduce surprises, so that they can be of maximum use to decision-makers.

The use of prospective scenarios is therefore a valuable tool, even though the application of this technique to cyber issues is complicated by the speed and instability of the environment. In this sense, the minimum time horizon of three years for scenarios may already be too distant for a domain in which disruptive innovations

occur regularly. So, a prospective approach to cyberspace must therefore necessarily have two distinct but complementary perspectives: a strategic one, which considers the influence of cyber power in the long term of internation competition, and a technical one, focused on the evolution of information technology systems, often affected by disruptive breakthroughs.

With respect to the strategic perspective, the inclusion of the cyber dimension in the scenarios produced by the Joint Warfare Centre (JWC) is a good indicator. It is natural that most of its products developed so far have prioritized the conventional spectrum of warfare, to support collective defense exercises under NATO's Article 5. However, the fundamentals of the strategic scenario design techniques, used in these works, are the same as those applicable to other situations. In this way, the Centre already contemplates the cyber domain and nonArticle 5 crisisresponse operations within the scope of its work (Baur 2024).

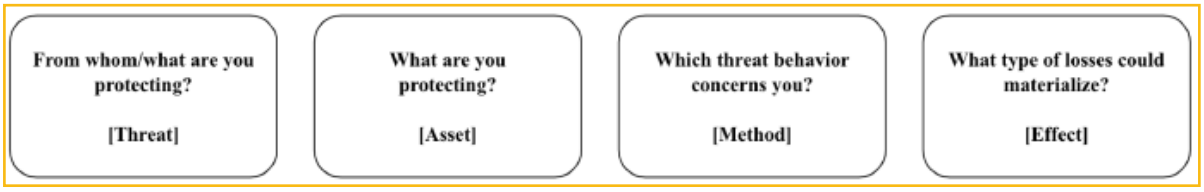
The next step would be to produce strategic scenarios focused specifically on the cyberspace dispute, below the threshold of armed conflict but characterized by frequent crises, arising from the permanent actions of intelligence services and cyber threats. Such products are not purely technical; they must also cover political and military factors and incorporate crisisescalation contingencies, thereby supporting realistic risk assessments. NATO has therefor already done the most difficult part: there is an established methodology and specialized personnel for producing scenarios.

To meet the needs of the more technical approach to cyber, a threatfocused perspective is a good starting point. Cybersecurity already encompasses the traditional areas of governance, risk, and compliance (GRC) and risk management, all related to the matter, and the Factor Analysis of Information Risk (FAIR) Institute has produced a taxonomy for cyber risk scenarios that presents a interesting and practical approach.

In brief, Goyal, Scott, and Tucker (2025. 3–4) define a cyber risk scenario through its key elements, summarized as: **[Threat] impacts [Asset] via [Method] causing [Effect(s)]**, where:

- **Threat**: any actor capable of acting against an asset in a way that could result in losses;
- **Asset**: something of value that may be affected in a way that causes losses;
- **Method**: a specific attack vector used to access or affect the asset; and
- **Effect**: how a loss is expected to materialize in a given asset.

Figure 1 – FAIR Cyber Risk Scenario Model

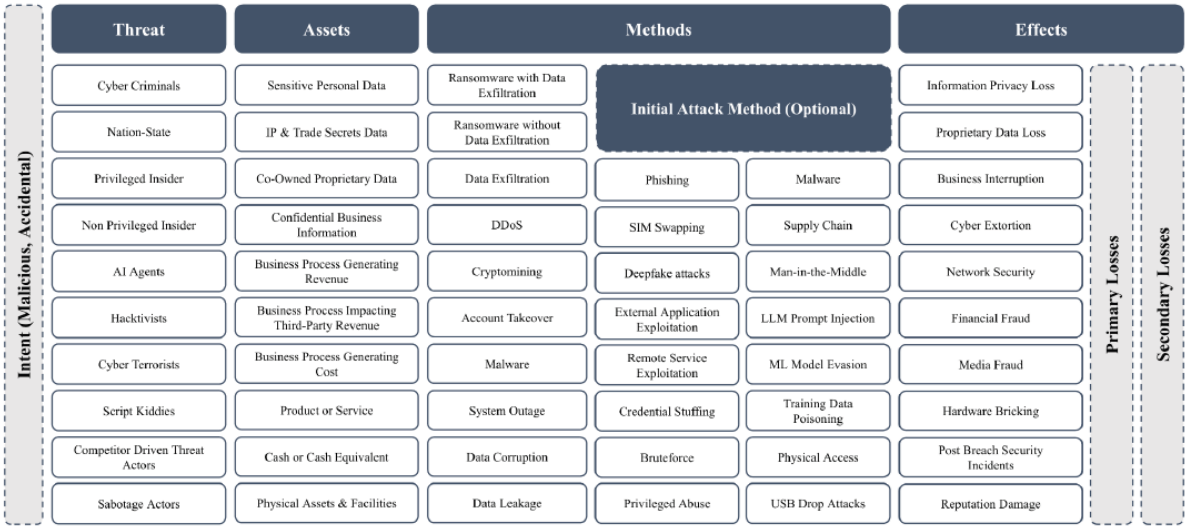


Source: Author (2026)

Although the development of a complete case study aligning a specific strategic scenario with its cyber developments, integrating the methodologies of the JWC and the FAIR Institute, is beyond the scope of this article, some aspects can already be highlighted. First, any scenario will only be useful if it limits its scope to what is most important. It is essential to resist the temptation to model and quantify all variables, so that the focus is not lost on the most relevant impacts on the organization and decisions can actually be made (ibid. 4).

At the same time, a cyber risk scenario requires its key elements to be well defined. Small distinctions can significantly improve clarity, facilitating understanding and mitigation actions. The key question is: how much precision is enough? There is no clear answer, and the issue must be addressed on a casebycase basis. Here again, however, the FAIR model provides a good starting point, summarized in a taxonomy that covers threats, assets, methods, and effects (ibid. 7).

Figure 2 – The FAIR Cyber Risk Scenario Taxonomy



Source: Adapted from Goyal, Scott and Tucker 2025

Evidently, this list is not exhaustive and, as the Institute itself warns, it should serve only as a starting point for each organization. Nonetheless, it can be said that threats, assets, and methods would be reasonably well covered for the purposes of strategic security and defense planning, leaving room for deeper elaboration of the effects. Even so, although there is a good basis from which to begin the analysis, crucial questions must still be answered (ibid. 20), such as:

- How many scenarios are needed?
- How can the most relevant scenarios be identified?
- How specific should scenarios be?
- Where can the appropriate data for analysis be found?
- How can we know whether the data and estimates are reliable?

The existence of the methodology itself does not solve all problems. For the purposes of this work, however, it is to be highlighted that there are already enough tools to address both the strategic and technical approaches mentioned above. It is therefore evident that the use of scenarios in support of strategic planning in the cyber domain is fundamental, by providing insights based on the variations of the

aforementioned key elements that can go far beyond the problems on the tactical level.

At this point, it is impossible not to address the promises of artificial intelligence, both for scenario supported planning and for the conduct of cyber actions. Vuuren (2025) argues that scenario planning is entering a "3.0 era," in which humans will set the intention, but AI will generate, test, refine, and recalculate futures at the speed of light. As with all promises arising from disruptive innovations, some caution is needed before embracing overly optimistic conclusions, but there is indeed reason for reflection.

A useful synthesis is presented in a briefing by the European Parliamentary Research Service (EPRS), which highlights trends and initiatives using Large Language Models (LLMs) to improve strategic planning and policymaking. Particularly interesting is its presentation of applications of generative AI in foresight, which introduces a step-by-step guide for horizon scanning and scenario generation (Vesnic Alujevic and d'Ambrosio 2025, 4). Although its details lie beyond the scope of this article, the guide points the way forward.

Important questions nonetheless remain. There is consensus that existing legal principles are insufficient for the use of AI systems in armed conflicts, which are marked by uncertainty and unpredictability. Such characteristics are particularly challenging for AI systems, which rely on large amounts of high-quality data, and lack the capacity to absorb qualitative and subjective content, such as commanders' intentions, which cannot be fully automated (Sullivan 2024. 216, 218).

However, as already seen, nearly all the intense activity of cyber threats is intentionally kept below the threshold of armed conflict and with a low likelihood of escalation, which creates an opportunity for the use of AI to confront such threats. A promising path for more immediate application lies in the use of AI for the production of cyber intelligence, intrusion detection, and incident response. In these fields, the most important issue is data quality, which paves the way for the development of better trained models (Halisdemir et al. 2022, 369).

In this regard, valuable lessons are being provided by the Exercise Locked Shields (ELS), organized by the CCDCOE since 2010. Dijk et al. (2025) conducted a broad analysis of earlier work, studying public data produced by the exercise, and proposed a vision for an automated Blue Team using AI technology and LLMs, in those use cases where these technologies use would be advantageous across the four phases of a cyber defense exercise (initial hardening, monitoring and response, reporting, and recovery), as shown bellow in Table 1.

Table 1 – Overview of use cases where LLMs provide a significant advantage compared to previous methods

Stage	Use Cases for LLMs
Initial hardening	• Identification and fixing of vulnerabilities and misconfigurations in software.
Monitoring and response	• Analyzing network traffic for malicious activities. • Analyzing event logs for malicious activities. • Parse support tickets, trigger corresponding actions, and generate responses. • Generate commands and configurations for remote management.
Reporting	• Link incidents to IoCs and generate human-readable reports. • Generate human-readable reports required for the exercise (e.g., post-incident summaries).
Recovery	• Identifying and documenting affected systems for recovery prioritization. • Reverting devices, misconfigurations, and patch failures using rollback mechanisms such as backups and snapshots. • Generating comprehensive post-recovery analysis and lessons learned documentation.

Source: Author (2026)

Despite the potential of technology, challenges persist. Developing models that accurately reproduce real world systems is a complex task and, considering that current algorithms have difficulty adapting to scenarios different from their training data. But even with such difficulties, in many situations the use of AI systems can

identify anomalies and pinpoint potential threats with greater accuracy than traditional methods (Dijk et al. 2025, 210) and, in order to improve even more the AI systems performance, the use of resources from multiple environments is likely to lead to far more efficient models (Gehri et al. 2023, 266).

Controversies surrounding AI, related to the lack of transparency of algorithms, potential discrimination in decision making processes, the legal status of AI, liability for damages caused, among other issues, have neither diminished nor been resolved (Wang 2024, 162). Yet, the initiative in this field cannot be left to threats because, as has been demonstrated, democratic states have sufficient room for maneuver to use existing models and references responsibly, with appropriate risk management, to exercise their power in cyberspace.

In summary, although predicting the future lies outside the scope of the work of intelligence and cyber defense analysts, initiative in cyberspace cannot be obtained and maintained through reactive postures. To this end, the use of prospective methods for the development of strategic scenarios, that include appropriate technical depth, is essential. AI should be employed in specific cases where technology offers genuine advantages, supporting decision-makers in planning and contingencies response. All of this is possible and already has basic foundations, but it will require hard work, tolerance for risk, and acceptance of the structural cyberspace ambiguity.

THE OFFENSIVE CAPABILITY AS THE BEST DEFENSE

For all of the reasons outlined so far, no state can hide behind a “Maginot Line” of firewalls without risking being overrun. Considering that cyber threats employ the same channels used by legitimate users, offensive techniques cannot simply be proscribed (Gartzke 2015, 316, 320), which once again demonstrates the inadequacy of comparisons with nuclear deterrence. In cyberspace, only those who master the techniques, tactics, and procedures, which ultimately define offensive capacity, will prevail in defense.

The exploitation of computer networks, a necessary condition for carrying out cyberattacks, is also employed in intelligence activity and lawful espionage in peacetime. Similarly, active defense and deception (such as threat hunting and the use of honeypots, among others) occupy this gray area, being also an important part of cyber defense (Lonergan and Montgomery 2022, 87).

While it is generally accepted that offensive operations seek to reduce the malicious activity of opponents and encourage them to come to the negotiating table, the development of offensive capability is not limited to these objectives. Likewise, the reluctance of threats to limit their actions does not suggest that the development of such capability should be abandoned, but rather that it should be combined with a broader diplomatic strategy involving allies, other states, and, ideally, opponents (Brock and Lewis 2025, 10).

Perhaps the best example of the importance of offensive capability for cyber defense is the use of Red Team Assessments (RTA) to proactively identify deficiencies in critical infrastructures. Usually carried out by request, RTAs simulate real malicious operations to assess an organization's ability to detect and respond to attacks, and later share their recommendations to improve cyber resilience (CISA 2024, 4). Especially promising is the integration of RTA with consolidated threat analysis methodologies, such as the MITRE ATT&CK framework, which promotes improvements in scenario design and reductions in response times, in addition to contributing to a shift from a reactive posture to a proactive approach (Yulianto et al. 2025, 11–12).

Such activities, which are fundamental for incident prevention, are only possible when there is proficiency in the most advanced offensive techniques, tactics, and procedures, as well as in depth knowledge of the modus operandi of threats, all achieved through strong integration with cyber intelligence.

Another fundamental but less discussed resource, about which there are even more doubts, is the use of cyber deception. Cyber threats rely on deception for virtually all offensive actions, but they do not have a monopoly on secrecy and

manipulation (Gartzke 2015, 318). The same factors that weaken deterrence and defense also make it possible to set traps for adversaries. Thus, offensive and defensive advantages in cyberspace results from the ability of organizations to employ deception and integrate it with broader strategic initiatives. However, the potential for deception on the Internet is still insufficiently addressed in discussions of the cyber domain (Gartzke 2015, 318, 326).

Deception is well-suited to the cyber domain, a global network of gullible minds and deterministic machines. In addition to its traditional applications in offensive intelligence operations, deception can be used defensively to delay the exploitation of valuable data by threats, to overload opponents with false leads and analysis costs, and even to compromise the attacker's infrastructure by releasing files containing exploits (Gartzke 2015. 333, 343).

Finally, as with many of the aspects discussed so far, there are doubts about the legality of and liability for damage caused by deception operations. The topic has not been widely debated, but the Geneva Conventions establish that, in general, the use of ruses of war is not prohibited. Thus, although the subject deserves broader discussion, it is difficult to identify international rules that deception operations in cyberspace would necessarily violate (Stejskal and Faix 2022, 210, 217), which makes their use in cyber defense highly worthwhile.

It should be noted, however, that there are still measures that can be taken, by targets of deception and active defense operations, without the complexity involved in the adoption of formal countermeasures. The most interesting and applicable of these, in the case of actions below the threshold of armed conflict, is retorsion. The literature cites several examples of it, such as exerting pressure through diplomatic relations, conducting operations within one's own networks (for example, using honeypots and sinkholes), influencing adversaries, establishing a presence in adversary networks, and delaying adversarial actions (ibid. 17–21). For not being limited to responding to acts that are illegal under international law, but being used in response to lawful

but unfriendly acts by another state, and not having a legal obligation to be notified (Kosseff 2020. 15–16), retorsion is a flexible and useful resource.

At this point, it is important to emphasize that the concept of retorsion is useful both from a defensive perspective, as a set of practical measures that can be part of the portfolio of cyber deterrence, and as a way of clarifying which actions a target can legally take in response to offensive operations, thus contributing to a better understanding of the risks involved. For all of these considerations, it is a valuable instrument to be in the democracies cyber law tool kit.

Finally, in the cyber domain, both action and inaction involve costs and risks. Pragmatically, however, it must be recognized that the difficulties of attribution are universal and that, in the absence of considerable material damage and loss of life, the risk of escalation is low and the adoption of countermeasures by targets is unlikely. Thus, given that intelligence activity, proactive posture, and deception have clear legal support and are fundamental for cyber defense, it can be safely stated that the development of offensive capability cannot be neglected by states that realistically defend the adoption of responsible behavior in cyberspace.

CONCLUSION

This article does not advocate a cyber arms race or the imposition of the law of the strongest but maintains that the taking back of the initiative in this domain will require strategic realism, calculated tolerance for risk and the overcoming of compartmentalized approaches, by the democratic states.

The value of transparency and confidence building measures is highly recognized as an important contributor for international stability and harmony in cyberspace. However, both theory and practice demonstrate that democracies cannot relinquish the exercise of their power, without the risk of conceding precious ground to threats that see their caution and responsibility as opportunities to be exploited.

So, in an environment marked by permanent competition below the threshold of conflict, the integration of foresight, intelligence, and offensive capability emerges as a pragmatic path to strengthen the security, resilience, and strategic credibility of democracies in cyberspace.

Ultimately, success in the cyber domain rests on the integration of strategic and tactical, operational and technical, legal and practical approaches, all within a comprehensive whole-of-state framework that employs national power to defend democratic values and interests.

As a closing remark, it is stressed that this work was intentionally broad, addressing strategic, legal, and technical aspects that are discussed in greater detail in the references. As the most important insights, I suggest that subsequent research could deepen case studies of cyber strategic scenarios; develop AI models and datasets for training attackers (Red Teams) and defenders (Blue Teams); refine deception strategies; and plan retorsion measures for cyber deterrence.

REFERENCES

Baur, Michel. 2024. **360-defree Scenario Design and Development**. Joint Warfare Centre. https://www.jwc.nato.int/our-work/scenario-development/

Borghard, Erica D.; Lonergan, Shawn W. 2018. **Confidence Building Measures for the Cyber Domain**. Strategic Studies Quarterly. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Borghard-Lonergan.pdf

Brock, Julia V.; Lewis, James A. 2025. **Mutual Defense in Cyberspace: Joint Action on Attribution**. Center for Strategic and International Studies. https://www.csis.org/analysis/mutual-defense-cyberspace-joint-action-attribution

Cybersecurity and Infrastructure Security Agency (CISA). 2024. **Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a U.S. Critical Infrastructure Sector Organization**. https://www.cisa.gov/sites/default/files/2024-11/aa24-326a-enhancing-cyber-resilience-insights-from-cisa-red-team-assessment_0.pdf

Corn, Gary P.; Taylor, Robert. **Sovereignty in the age of cyber**. Cambridge University Press. https://doi.org/10.1017/aju.2017.57

Derian-Toth, Garrett; Walsh, Ryan; Sergueeva, Alexandra; Kim, Edward; Coon, Relieves; Hada, Hilda; Stancombe, Jared. **Opportunities for Public and Private Atrribution of Cyber Operations**. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf

Dijk, Allard; Meier, Roland; Melella, Cosimo; Pihelgas, Mauno; Vaarandi, Risto; Lenders, Vincent. 2025. "Next Steps in Cyber Blue Tem Automation – Leveraging the Power of LLMs". **17th International Conference on Cyber Conflict: The Next Step**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/17th-international-conference-on-cyber-conflict-the-next-step/

Gartzke, Erik; Lindsay, Jon R. 2015. *W***eaving Tangled Webs: Offense, Defense, and Deception in Cyberspace**. Security Studies. Routledge. http://dx.doi.org/10.1080/09636412.2015.1038188

Gehri, Lina; Meier, Roland; Hulliger, Daniel; Lenders, Vincent. 2023. "Towards Generalizing Machine Learning Models to Detect Command and Control Attack Traffic". **15th International Conference on Cyber Conflict: Meeting Reality**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/15th-international-conference-on-cyber-conflict-meeting-reality/

Goyal, Pankaj; Scott, Cody; Tucker, Todd. 2025. **A FAIR Taxonomy for Cyber Risk Scenarios: An Analyst's Guide for Defining Risk Scenarios for Continuous Risk Management**. FAIR Institute. https://www.fairinstitute.org/resources/fair-cyber-risk-scenario-taxonomy

Halisdemir, Emre; Karacan, Hacer; Pihelgas, Mauno; Lepik, Toomas; Cho, Sungbaek. 2022. "Data Quality Problem in AI-Based Network Intrusion Detection Systems Studies and a Solution Proposal". **14th International Conference on Cyber Conflict: Keeping Moving**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/cycon-2022-book/

Jacobsen, Jeppe T. 2021. "Cyber offense in NATO: challenges and opportunities". **International Affairs 97**. https://www.researchgate.net/publication/350527052_Cyber_offense_in_NATO_challenges_and_opportunities

Kosseff, Jeff. 2020. "Retorsion as a Response to Ongoing Malign Cyber Operations". **12th International Conference on Cyber Conflict: 20/20 Vision – The Next Decade**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/12th-international-conference-on-cyber-conflict-20-20-vision-the-next-decade-proceedings-2020/

Leiter, Andrea. 2020. "Cyber Sovereignty: A Snapshot From A Field In Motion". **Harvard International Law Journal Frontiers**. https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/Leiter-PDF-format.pdf

Lewis, James A. 2022. "A Strategic Outlook for Cyberspace Operations". **Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/

Lewis, James A. 2015. "The role of offensive ciber operations in NATO's collective defence". *Tallinn Paper No. 8.* NATO CCDCOE Publications. https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf

Lonergan, Erica D.; Montgomery, Mark. 2022. "The Promise and Perils of Allied Offensive Cyber Operations". **14th International Conference on Cyber Conflict: Keeping Moving**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/cycon-2022-book/

Neill, Martin; Hinkle, Wade P.; Morgan, Gary. 2016. ***S*cenarios – International Best Practice: An Analysis of Their Use by the United States, United Kingdom and Republic of Korea**. Institute for Defense Analysis. https://www.ida.org/research-and-publications/publications/all/s/sc/scenarios-international-best-practice-analysis-of-their-use-by-the-united-states-united-kingdom-and

Nye, Joseph, Jr. 2010. **Cyber Power**. Belfer Center for Science and International Affairs". *Harvard Kennedy School*. https://www.belfercenter.org/publication/cyber-power

Schmitt, Michael N (editor). 2016. **Tallinn manual 2.0 on the international law applicable to cyber operations**. Cambridge University Press.

Stejskal, Petr; Faix, Martin. 2022. "Legal Aspects of Misattribution Caused by Cyber Deception". **14th International Conference on Cyber Conflict: Keeping Moving**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/cycon-2022-book/

Sullivan, Scott. 2023. "Unpacking Cyber Neutrality". **15th International Conference on Cyber Conflict: Meeting Reality**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/15th-international-conference-on-cyber-conflict-meeting-reality/

Sullivan, Scott; Ricket, Iben. 2024. "Targeting in the Black Box". **16th International Conference on Cyber Conflict: Over the Horizon**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/16th-international-conference-on-cyber-conflict-over-the-horizon/

Vesnic-Alujevic, Lucia; d'Ambrosio, Salvatore. 2025. "Augmented foresight: The transformative power of generative AI for anticipatory governance". **Policy Foresight Analysis**. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/774665/EPRS_BRI(2025)774665_EN.pdf

Voo, Julia; Hemani, Irfan; Jones, Simon; From Sombre, Winnona. 2020. **Reconceptualizing Cyber Power**. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/reconceptualizing-cyber-power

Voo, Julia; Hemani, Irfan; Cassidy, Daniel. 2022. **National Cyber Power Index 2022**. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/national-cyber-power-index-2022

Vuuren, Ian van. 2025. **The Dawn of Scenario Plannling 3.0)**. https://ianjvv2.substack.com/p/the-dawn-of-scenario-planning-30

Significant Cyber Incidents | Strategic Technologies Program | CSIS. 2025. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Taddeo, Mariarosaria. 2017. **Deterrence by Norms to Stop Interstate Cyber Attacks**. University of Oxford. https://ora.ox.ac.uk/objects/uuid:a58db80f-8661-4911-beb9-adf45f650c19.

Taddeo, Mariarosaria. 2018. “How to Deter in Cyberspace”. **Hybrid COE Strategic Analysis**. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-9-how-to-deter-in-cyberspace/

Wang, Wei-Che. 2024. “Legal, Policy and Compliance Issues in Using AI for Security: Using Taiwan’s Cybersecuriy Management Act ans Penetration Testing as Examples”. **16th International Conference on Cyber Conflict: Over the Horizon**. NATO CCDCOE Publications. https://ccdcoe.org/library/publications/16th-international-conference-on-cyber-conflict-over-the-horizon/

Yulianto, Semi; Soewito, Benfano; Gaol, Ford Lumban; Kurniawan, Aditya. 2025. “Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment”. **Cyber Security and Applications Volume 3**. https://doi.org/10.1016/j.csa.2024.100077

Autoria

1 Jomar Barros de Andrade

Mestre em Ciências Militares pela Escola de Comando e Estado-Maior do Exército; Oficial-General da Reserva do Exército Brasileiro; Pesquisador no Grupo de Análise Estratégica em Sistemas de Defesa

https://orcid.org/0009-0000-6136-1289 • jomar.barros@eb.mil.br

Como citar este artigo

ANDRADE, J. B. Taking back the initiative: prospective intelligence and offensive capabilities enabling the proactive defense in the cyberspace. **InterAção**, Santa Maria, v. 17, n. 1, e95736, p. 1-23, mar. 2026. DOI 10.5902/1980509895736. Disponível em: https://dx.doi.org/10.5902/2357797595736. Acesso em: dia mês abreviado. ano.