idn nação e defesa

NATO – UMA ALIANÇA RESILIENTE

SARAH DA MOTA THE TECHNOLOGICAL REVOLUTION IN 21ST-CENTURY NATO: THE NEW FRONTIERS OF SPACE AND MIND HELDER FIALHO JESUS O CIBERESPAÇO, A NATO E PORTUGAL – UMA TRILOGIA INTER-RELACIONADA ISABELLA NEUMANN COLLATERAL EFFECTS FOREVER: MILITARIZATION AND COMMERCIALIZATION IN NATO'S CYBERSPACE OPERATIONS INÊS AGUIAR BRANCO CABOS SUBMARINOS: NATUREZA CRÍTICA E VULNERABILIDADE ESTRATÉGICA NO CONTEXTO DA ALIANÇA DO ATLÂNTICO NORTE ANTÓNIO EUGÉNIO O YIN E O YANG DA NATO – DESARMONIAS NA DEFESA DA EUROPA

idn Instituto da Defesa Nacional

P.V.P. 8,50 €
Quadrimestral

Agosto 2024
n.º 168

idn nação e defesa

NATO – UMA ALIANÇA RESILIENTE

SARAH DA MOTA THE TECHNOLOGICAL REVOLUTION IN 21ST-CENTURY NATO: THE NEW FRONTIERS OF SPACE AND MIND HELDER FIALHO JESUS O CIBERESPAÇO, A NATO E PORTUGAL – UMA TRILOGIA INTER-RELACIONADA ISABELLA NEUMANN COLLATERAL EFFECTS FOREVER: MILITARIZATION AND COMMERCIALIZATION IN NATO'S CYBERSPACE OPERATIONS INÊS AGUIAR BRANCO CABOS SUBMARINOS: NATUREZA CRÍTICA E VULNERABILIDADE ESTRATÉGICA NO CONTEXTO DA ALIANÇA DO ATLÂNTICO NORTE ANTÓNIO EUGÉNIO O YIN E O YANG DA NATO – DESARMONIAS NA DEFESA DA EUROPA

idn Instituto da Defesa Nacional

P.V.P. 8,50 €
Quadrimestral

Agosto 2024
n.º 168

Capa
Nuno Fonseca/nfdesign

Normas de Colaboração
Consultar final da revista

Propriedade, Edição e Sede da Redação
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
NIPC: 600014002
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Paginação, Pré-Impressão, Impressão e Acabamento
Rainho & Neves, Lda.
R. Do Souto, 8 – São João de Ver – 4520-612
Tel: 256371470 E-mail: geral@rainhoeneves.pt Website: www.rainhoeneves.pt

ISSN 0870-757X Publicação Eletrónica ISSN 2183-9662
Depósito Legal 54 801/92
Tiragem 400 exemplares
ERC 127782 Registada na Latindex – Sistema Regional de Informação em Linha para Revistas Científicas da América Latina, Caraíbas, Espanha e Portugal; MIAR, RedAlyC e JSTOR. Disponível no RCAAP – Repositório Científico de Acesso Aberto de Portugal

Numa conjuntura em que a guerra grassa no espaço europeu, a relevância da NATO é ainda maior, enfrentando hoje um dos maiores desafios desde a sua fundação, há 75 anos. A NATO, através das disposições do Artigo 5.º do Tratado do Atlântico Norte, tem garantido, com os seus aliados, a robustez e coesão da segurança e defesa euro-atlântica. A NATO é também um ator significativo no quadro da política internacional, funcionando como uma plataforma para a inovação e para a livre iniciativa no quadro tecnológico, ligando o domínio dos assuntos militares ao das políticas de defesa nacionais, da investigação e da indústria.

Este número assinala o 75.º aniversário da Aliança refletindo sobre os desafios que a organização enfrenta, com uma guerra em curso no espaço europeu e as oportunidades decorrentes da adesão de novos membros.

No artigo "The Technological Revolution in 21st Century NATO: The New Frontiers of Space and Mind", Sarah da Mota aborda o espaço e a mente como dois domínios estratégicos e áreas de operação fundamentais que se desenvolveram no seio da NATO nos últimos 15 anos. De acordo com a autora, as dimensões do espaço e da mente sugerem um contraste acentuado entre uma dimensão material e uma dimensão imaterial, cuja interação está no centro do *smart power* da NATO.

Helder Fialho Jesus analisa a adaptação da NATO aos desafios do ciberespaço. O autor no artigo "Ciberespaço, a NATO e Portugal – Uma trilogia inter-relacionada" analisa os níveis político, militar e técnico da Aliança Atlântica, como domínios essenciais à compreensão da evolução da importância do ciberespaço.

Ainda no âmbito da mesma temática, o artigo "Collateral Effects Forever: Militarization and Commercialization in NATO's Cyberspace Operations" de Isabella Neumann explora as implicações das operações no domínio do ciberespaço na NATO e as mudanças ocorridas nas dinâmicas de poder e de funcionalidade no quadro da segurança entre os setores militar, civil e privado.

No campo das infraestruturas críticas, o artigo "Cabos Submarinos: Natureza Crítica e Vulnerabilidade Estratégica no contexto da Aliança do Atlântico Norte" de Inês Aguiar Branco examina os riscos associados à vulnerabilidade dos cabos submarinos com implicações para a segurança e interesses dos Estados aliados.

Finalmente e encerrando o dossiê temático dedicado à NATO, António Eugénio, no artigo "O Yin e o Yang da NATO – Desarmonias na Defesa da Europa", reflete sobre a necessidade de uma maior integração, modernização e digitalização da base tecnológica europeia, de modo a poder concorrer com as suas congéneres norte-americanas e examina a desejável divisão de encargos entre países aliados, de modo a esta passar a incluir o valor comercial dos dados dos cidadãos, empresas e organizações europeias, aos quais as gigantes tecnológicas norte-americanas têm acesso sem reciprocidade.

Destaque ainda para o artigo Extra Dossiê, assinado por Teresa Rodrigues e Félix Ribeiro "África no Tabuleiro de Xadrez Mundial: Estruturas, Desafios e Oportunidades" que analisa vários indicadores que podem desempenhar um papel significativo na análise do posicionamento do continente africano no sistema internacional.

Isabel Ferreira Nunes

NATO – Uma Aliança Resiliente

The Technological Revolution in 21st-Century NATO: The New Frontiers of Space and Mind

Sarah da Mota
University of Coimbra, School of Economics.

Abstract

In the context of the current technological revolution, this article approaches specifically Space and Mind as two realms that are key strategic domains and areas of operation that have developed within NATO in the last 15 years mostly. While maintaining a scientific and technological edge has always been part of NATO's strategy to remain relevant and successful, we argue that the dimensions of Space and Mind are suggestive of a sharp contrast between a material and an immaterial dimension, whose interplay is at the centre of NATO's smart power, which is emblematic of 21st-century development and practice of power. As a result, relations with peer competitors are renewed in a way that is essentially dematerialized and discursively confrontational, making the use of conventional physical force increasingly obsolete, while at the same time reminding us of what the subjectivity of the North Atlantic is or should be.

Keywords: NATO; Technological Revolution; Space Policy; Cognitive Warfare; Disinformation; Smart Power.

Resumo

A Revolução Tecnológica na NATO do Século XXI: as Novas Fronteiras do Espaço e da Mente

No contexto da atual revolução tecnológica, este artigo aborda especificamente o Espaço e a Mente como dois domínios estratégicos e áreas de operação fundamentais que se desenvolveram no seio da NATO, sobretudo, nos últimos 15 anos. Embora a manutenção de uma vantagem científica e tecnológica tenha sempre feito parte da estratégia da NATO para se manter relevante e bem-sucedida, defendemos neste artigo que as dimensões do Espaço e da Mente sugerem um contraste acentuado entre uma dimensão material e uma dimensão imaterial, cuja interação está no centro do smart power *da NATO, que é emblemático do desenvolvimento e da prática do poder do século XXI. Assim, as relações com os seus concorrentes são renovadas de uma forma essencialmente desmaterializada e discursivamente conflituosa, tornando cada vez mais obsoleto o uso da força física convencional, ao mesmo tempo que nos recorda o que é ou deve ser a subjetividade do Atlântico Norte.*

***Palavras-chave**: NATO; Revolução Tecnológica; Política Espacial; Guerra Cognitiva; Desinformação; Smart Power.*

Artigo recebido: 18.01.2024
Aprovado: 18.03.2024
https://doi.org/10.47906/ND2024.168.01

Introduction

NATO's evolution in the 21st century has been somewhat tumultuous. After striving to consolidate its new post-bipolar *raison d'être* throughout the 1990s (cf. Bosnia-Herzegovina and Kosovo), the 2000s have brought multidimensional strategic and political challenges: out-of-area mandates; the accession of new members who have extended the sphere of influence eastwards, though precariously; internal disagreements that continually test the unity of the Allies (cf. Afghanistan and Libya); new Strategic Concepts (2010 and 2022); the creation and extinction of the NATO-Russia Council (2002-2022); progressively strengthened cooperation with the EU; among others.

One prominent aspect of NATO's contemporary evolution, which has gained increasing importance over the last decade in particular, and that this article wishes to address, is the technological dimension of the Alliance's strategic adaptation. Technologies like artificial intelligence, quantum technologies, space technologies, biotechnology and human enhancement, among others, are the protagonists of the current seventh-generation military revolution and have been occupying an ever-increasing significance in this adaptation (NATO, 2020b; NATO STO, 2020). In fact, over the last 75 years, NATO has maintained a "strategy of technology" that is at the core of the Alliance's successful durability. This strategy of technology has notably enabled the organisation's military and political framework to carry out its core activities of consultation, cooperation, coordination, interoperability, deterrence and united action, which critically depend on leveraging decision-making and a scientific and technological edge (NATO STO, 2020: pp. 1-2).

This should not be surprising, for over the centuries science and technology have decisively influenced not only the way wars are fought, but also determined strategic advantage and superiority (McNeill, 1982), so much so that individual scientists such as Archimedes, Leonardo da Vinci, Galileo, Newton or Descartes dedicated themselves to solving military problems (Smit, 2006: pp. 723-724). In fact, contemporary political theory has been dominated by a paradigm of technological determinism, which tends to favour a positive image of technology, essential for solving various problems, and whose most negative effects come mainly from harmful use (Bijker, 2006: p. 683). In the system of modern democracy, it is even assumed that technology produces a visible and unsuspected concept of power, insofar as it is used responsibly in the eyes of the general public (idem: p. 690).

Classic IR theories such as Realism and Neorealism see technology as one component among others in defining the material power of states, as well as a channel for developing strategies for their survival. Nevertheless, there is a reflection on the rationality of nuclear war, for example, arising from a sensitivity to mutual destruction and the systemic transformations driven by technology (Morgenthau, 1961; Waltz, 1979; Fritsch, 2014: p. 121). In Liberalism, technology is identified as

the main driver of globalisation and its complex interdependence, thus assuming a central role in debates about the current state of the global system, the search for global governance solutions and democratic control over them (Risse-Kappen, 1995; Keohane & Nye, 1998; Fritsch, 2014: p. 122). It is also possible to find a concern from the English School with how international society shapes technology, to show how a civilisational dimension was attributed to the role of high technology that differentiated the "society of civilised states" from non-European societies in the 19th century, with a special focus on China and India (Stroikos, 2020: p. 2). One may definitely infer from this broad yet brief theoretical spectrum that technology plays a decisive material and strategic role in international relations, with the power to transform relationships, whether by exerting domination, solving global problems, bringing nations closer together, or creating new dynamics of competition between them.

In this regard, to the Alliance, one important development regarding technology has to do with how the democratization of technology has diversified the range of players involved – peer competitors, terrorists, and irregular forces. By investing in science and technology, these players have reduced the advantages that exist for NATO, with many strategic, economic, social and technical challenges having arisen from such reduction. That is why concerns about losing the technological edge have been so critical to the Alliance (NATO STO, 2020: p. 2, 38). Indeed, the very literature on NATO has been dominated by aspects related to its strategic and operational adaptation to the evolution of threats, in particular hybrid threats, from which cybersecurity has emerged as the Alliance's most prominent area of specialisation (Aaronson *et al.*, 2011; Ducaru, 2016; Fidler *et al.*, 2013; Mälksoo, 2018; Oren, 2016).

In that context of technological revolution, this article draws on the need to further explore the implications of two important and rather novel areas of technological action by NATO, namely Space and Mind. In the light of the above-mentioned technological and intellectual edge that is considered to have sustained NATO's success and longevity so far (NATO STO, 2020: p. 1), the choice of this binomial is intended to emphasise the distinction between a dimension that is essentially material and one that is immaterial, for their interplay, it is argued, lies at the centre of NATO's smart power that is emblematic of 21st-century development and practice of power. As a consequence, the conceptualisations, perceptions and representations of where and how defence is to be carried out have come to dematerialise into new frontiers, where interrelations with peer competitors suffer new dynamics that are mostly discursively confrontational. Security is thus dematerialised, making the use of conventional physical force increasingly obsolete, while at the same time reminding us of what the subjectivity of the North Atlantic should be for both the Alliance and its security subjects.

The notion of smart power is hereby understood as a combination of hard and soft power that relevant military organisations may pursue in the context of interventions

and operations other than war, so that military force is only to be employed under extreme circumstances (Chong, 2015: pp. 233-234). Smart power is thus multifunctional, as it entails the right combination of ideational and material tools and is fairly interwoven with society as to the need to win hearts and minds, achieve a "common vision, or at best, an ideological solidarity akin to an alliance relationship" (idem: p. 234). Of course, Space and Mind do not represent the sole innovations occurring within NATO in this century that can be related to smart power. But in a defence and security environment driven by "chaos, complexity and competition" (NATO STO, 2020: p. 37), and a threat environment that is increasingly and irremediably hybrid, Space and Mind fundamentally highlight how strategic requirements of this era have demanded an extended, widespread, and comprehensive adaptation by the Alliance to contemporary technological revolutions both at the material and ideational levels. To understand this, this article first focuses on the main steps, developments and features that characterize the NATO Space Policy. We will see how space has become critical for the Allies' strategic superiority, with a multidimensional impact both on their daily routine operations and on the more decisive and tactical ones to respond to imminent challenges on the ground. Furthermore, it will be interesting to note how, although NATO does not possess its own autonomous space capabilities and assets, it still manages to pool the Allies' resources through the creation of various operational centres that optimise the collective action of the security community. For clarification purposes, it should be noted from this point on that when referring to "space technologies" it is assumed that space begins around 90 to 100km above sea level, which makes them rely on a unique operational environment that is defined by features such as freedom of action and access, speed, near-vacuum, micro-gravity, isolation and extreme conditions in terms of temperature, vibration, sound and pressure (NATO STO, 2020: p. 75).

Afterwards, the second section will approach the role of Mind as a theatre of operations of its own, by looking into how the notion of "Cognitive Warfare" has developed within the Organisation. Here, it will be revealed how the Mind occupies a prominent place in the Alliance's mission and in contemporary international relations. Behaviours, knowledge, perceptions and beliefs thus play a central role in the way NATO relates to peer competitors, positions itself geopolitically and defends its own existence. Hence, the importance of information, disinformation and propaganda and of technological intervention in their control and management.

1. NATO Space Policy

When compared to the EU, ESA or EDA, the development of space policy within NATO had a rather late take-off. Space was first referred to in NATO's Strategic Concept of

2010 as a realm whose access can be impeded by technological factors such as laser weapons and electronic warfare, which was ultimately seen as having major impacts on the Alliance's military planning and operations (NATO 2010: par. 14). Prior to that, not even the term "space" was present in any previous strategic concept. However brief, that first reference established, for the first time, the importance of space as a yet sensitive strategic and operational area, vulnerable to technological attacks.

Despite this, it is possible to find considerations for a NATO space policy prior to 2010, which recommended the development of a space strategy and doctrine. USAF Major Thomas Single (2008: p. 1), for instance, identified space as a critical enabler for security and defence, by elaborating on how it could contribute to NATO's identity and cohesiveness, and how, militarily, its strategic importance was justified given that NATO forces had become "expeditionary", relying increasingly on space systems for their ongoing operations. Single (2008: pp. 2-5) thus suggested concepts and guiding principles to be included in the development of said space policy, such as the peaceful uses of space, the development of space power and an industrial base, and the need for assured access to space, among others.

After the 2010 Strategic Concept, the framework for a NATO space policy was gradually advanced. Within the organisation, some reports progressively worked on identifying existing capabilities – and comparing them with those of the EU or the US -, challenges, and future tasks. At the time, there was a clear asymmetry of power between the US and European nations. In a long-standing disparity, the US had a more pronounced perception of the risk of conflict in space than the EU, and invested three times as much as the next 11 nations combined in the area of Space, possessing a robust, assertive and mature space policy, which is understandable as it has been developed since the 1950s (NATO, 2012: p. 10). Therefore, retrospectively, each security and defence goal present in the 2010 Strategic Concept could be connected to some specific space-related requirement or capability. For example, regarding the core task of safeguarding "the freedom and security of all its members by political and military means" (NATO, 2010: par. 1), the implied space requirement was to "provide strategic intelligence, missile warning, satellite navigation, satellite communication" (NATO, 2012: p. 8).

Only in November 2019 was space formally recognized as a new operational domain, alongside air, land, sea and cyber, in preparation for the meeting of the North Atlantic Council (NAC) taking place the following month in London (NATO, 2019a; 2019b). The London Declaration issued from that meeting officially initiated NATO's Space Policy. The Allies thereby justified space's importance in tackling security challenges in connection with the need to maintain their technological edge, and increase the resilience of societies, energy security and critical infrastructure (NATO, 2019b: par. 6). This acknowledgement was enshrined in the 2022 Strategic Concept, in which space is now part of the current "strategic environment", namely as a stage for the conduct of

malicious activities by authoritarian actors in particular, with the potential to disrupt the openness, interconnectedness and digitalization of Allied nations (NATO, 2022b: par 7). In it, the People's Republic of China is specifically referred to as one of the strategic competitors that seeks to control key technological and industrial sectors and critical infrastructure, and attempts to subvert the rules-based international order, including in the space domain, among others (idem: par. 13). In this sense, space appears as a high-stakes domain, where such strategic competitors and potential adversaries may degrade Allied capabilities, but also restrict their "access and freedom to operate in space" and target civilian and military infrastructure (idem: par. 16). Regarding NATO's core tasks of deterrence and defence, space capabilities surge as complementary to other capabilities such as nuclear, conventional, missile defence, and cyber, all to be employed in a proportionate, coherent, and integrated manner (idem: par. 20). It is also specified that malicious cyber activities, for instance, or hostile operations to, from or within space could reach the level of armed attack and lead the NAC to invoke Article 5 (idem: par. 25).

Although neither the Policy nor the 2022 Strategic Concept explicitly define or elaborate on what NATO's space capabilities are, the Joint Air Power Competence Centre has previously indicated that they consist of "orbital and non-orbital capabilities whose primary function is to deliver products and applications supporting NATO operations in the doctrinal mission areas of: space force enhancement; space control; space support; and space force application" (NATO, 2012: p. 15). This definition includes, for example, crafts or vehicles that operate at altitude in the absence of any aerodynamic control; electromagnetic links used to monitor, command, control and communicate with crafts or vehicles; and the personnel trained to do everything mentioned so far (ibid.).

Now, NATO's Space Policy offers a very comprehensive appraisal of that complex strategic domain, referring to space's multiple benefits, opportunities, risks and vulnerabilities, such as crisis management, threat anticipation, its dual-use nature, counter-space threats by potential adversaries, and even challenges to the "Allies' traditional perceptions of time, distance and geography" (NATO, 2022a: par. 2). In fact, the uses of space technologies include both civilian and military activities, ranging from weather monitoring, environment and agriculture, to transport, science, and communication (idem: par. 1). Actually, the key roles of space systems identified by the Policy refer to the Alliance's core tasks in collective defence, deterrence and crisis management, which concretely implies "informing the Alliance's situational awareness, decision-making, readiness and posture management across the spectrum of conflict" (idem: par. 6). Indeed, space-based tasks such as weather monitoring, satellite communications, positioning and navigation are transversal to the reading of the operational environment, tactical assessment, as well as to activities of intelligence, surveillance, reconnaissance, planning and execution (idem: par. 7) – basically any

kind of typical NATO operation. In practice, the addition of a strategic space domain essentially allows NATO planners to request space capabilities and services from the Allies, such as hours of satellite communication (NATO, 2019a). Figure 1 below summarises the operational use and effects of different space capabilities.

Figure 1
NATO Space Capabilities and Usage

Space Capability	NATO Use and Effects
Position, Navigation Time (PTN) & Velocity	Precision Strike Force Navigation Support to Personnel Recovery (PR)/ Combat Search and Rescue (CSAR) Network Timing
Integrated Tactical Warning and Threat Assessment	Force Protection Attribution Missile Warning
Enviromental Monitoring	Mission Planning Munitions Selection Weather Forecasting
Communications	Command and Control Unmanned Aerial Vehicle Ops Beyond-the-Horizon communications
Intelligence, Surveillance and Reconnaissance	Coverage of Operation Execution (in the operations centre) Battle Damage Assessment (BDA) Intelligence Targeting

Source: NATO STO (2020) *Science and Technology Trends 2020-2040. Exploring the S&T edge.* Brussels: NATO Science & Technology Organization, p. 76.

Besides the adoption of the Space Policy, a NATO Space Centre was established in 2020 at Allied Air Command in Ramstein, Germany. Acting as NATO's central coordinating entity in the space domain, this centre helps the Allies share information about potential threats, supporting their activities and operations, and works closely with the Allies' national space agencies to fuse data, products and services, such as imagery, navigation and early-warning.[1] In February 2023, the Alliance Persistent Surveillance from Space (APSS) was launched as the first global Intelligence Surveillance and Reconnaissance (ISR) space initiative. The APSS allows optimizing

1 Information on NATO Space Centre consulted and available at: https://ac.nato.int/missions/we-coordinate-nato-space-matters

space data collection for improved intelligence and surveillance activities, in close support of military missions and operations. Thus, it enhances NATO's situational awareness and decision-making, through the establishment of a virtual constellation called "Aquila". Aquila is a data-centric initiative that connects both national and commercial space assets, such as satellites, so the APSS actually draws on existing and future space assets in Allied countries (NATO 2023a). As a step further, NATO's Space Centre of Excellence was also officially accredited in July 2023 and established in Toulouse, France, aimed at providing knowledge, analysis and support on space-related matters.[2]

Furthermore, it is important to stress that the idea of the weaponisation of space – so criticised in the literature on space policy in general – has been explicitly referred to as not being an objective nor an intention of the Alliance (NATO, 2019a; 2023b). A significant distinction is made when referring, for example, that the use of satellite navigation to aid weapons delivery is not to be considered as "weaponisation", because it is an accepted legitimate use of space capabilities (NATO, 2012: p. 12). Since the war in Ukraine started, the distinction has been made increasingly difficult. NATO's support of Ukraine has implicated the use of space-based data and assets that are made available by the Allies, along with the international private industry's contribution to create a Ukrainian space coalition (Maurin, 2023: p. 33). As a reaction, the Russian head of the non-proliferation and arms control department of the Ministry of Foreign Affairs, Konstantin Vorontsov, stated in October 2022 that the space infrastructure, even civilian and commercial, that was used by the US and its allies for military purposes might become a legitimate target for retaliation (cit. in Maurin, 2023: p. 30). Prior to that, the Alliance had considered Russia's anti-satellite missile test of 15 November 2021 to cause orbital debris that could threaten the peaceful access to space for all, which directly contradicted Russia's claims to oppose the weaponisation of space (NATO, 2023b).

Between 2010 and 2023, the evolution of space policy within NATO has been remarkable, as space went from being a sensitive and vulnerable area to an omnipresent and omniscient dimension, a multifunctional operational domain with links to any of the Alliance's tasks and objectives. Of course, technological development is as remarkable as the acceleration of time it brings about, so it is fairly understandable that this trajectory has undergone such appreciable changes. In general, the trend towards a gradual hardening of the security environment in space seems clear and raises the question of whether the peaceful use of space is truly feasible and for how long.

2 Information on NATO Space Centre of Excellence consulted and available at: https://www.space-coe.org/

2. NATO's "Cognitive Warfare"

The notion of "Cognitive Warfare" has been developed as part of NATO's research and concept development activities and has been made public since 2021. In 2013, a collaboration began between General Denis Mercier, NATO's Supreme Allied Command Transformation (ACT), and Professor Bernard Claverie, director of the National School of Cognitive Science (ENSC), about cyberpsychology and the weaponisation of neurosciences. This cooperation gave rise in 2017 to a collaboration agreement between ENSC and ACT, under which the NATO-ACT Innovation Centre began to develop the topic of "Cognitive Warfare". Given the recent outburst of psychological manipulation processes for fraudulent purposes, knowledge of human behaviour and the ability to influence it have become the focus of a "battle of perceptions" that affects all sectors of society and, in particular, the security and defence sectors, constituting a major new strategic issue (Claverie *et al.*, 2021: p. xii).
In the main and only public document that addresses, explores and explains Cognitive Warfare, it is possible to find the following definition:

> [c]onvergence of "Cyber-Psychology," "Weaponization of Neurosciences," and "Cyber-Influence" for a provoked alteration of the perception of the world and its rational analysis in the military, politicians, and other actors and decision makers, for the purpose of altering their decision or action, for a strategic superiority at all levels of tactical intervention concerning individual or collective natural intelligence, as well as artificial or augmented intelligence in hybrid systems (Claverie *et al.*, 2021: p. xiv).

In a cognitive war, the battlefield lies in the mind itself. Its aim is to manipulate the psychological, social and informational environment, to shape what people think individually and as a group, and to influence how they act and interact collectively. At its peak, cognitive war is said to have the potential to destabilise societies and military organisations and fracture alliances (idem: p. 1). Through cyber, psychological, informational and social engineering capabilities, Cognitive Warfare seeks to create confusion, doubt, false narratives and false representations through an overabundance of information and disinformation, which saturates the mind, causes distraction, and can radicalise individuals and amplify social polarisation (ibid.).
Although attempts to manipulate the enemy and citizens in order to weaken, influence, subjugate or destroy them are dated elements of warfare, Cognitive Warfare refers to a new discipline that combines new communication tools, new methods and objectives, and generally involves a biased presentation of reality that is digitally altered. It is a combination of two operational fields that used to be managed separately: on the one hand, PSYOPS and influence operations (soft power), and on the other, cyber operations (cyberdefence) aimed at degrading or destroying physical information

assets (idem: pp. 22-23). Cognitive Warfare thus constitutes an interdisciplinary field in which the means, targets and objectives converge in the mental field. It is a war against what the enemy thinks, values or believes; it is a war waged by altering the enemy's representation of reality in order to affect their certainties, assumptions, beliefs and competitiveness; it is a war whose declared aim is "to attack, exploit, degrade or even destroy how someone constructs their own reality, their mental self-confidence, their trust in processes and approaches necessary for the efficient functioning of groups, societies or even nations" (idem: 23).

On a more practical level, NATO has indeed shown great concern about hybrid threats, and the need to prevent and guard against such attacks. But the main protagonist in this field is disinformation, which ends up being the most empirical and daily manifestation of Cognitive Warfare. NATO (2020a) defines disinformation as "the deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead […] to deepen divisions within and between Allied nations, and to undermine people's confidence in elected governments". It is interesting to note that, while NATO (2020a) has identified the annexation of Crimea by Russia in 2014 as a turning point in the increase and intensification of disinformation and propaganda, the actual beginning of an "incessant process of distorting the historical record" by Vladimir Putin may be traced back to the 2007 Munich Security Conference (Schuette, 2023: p. 51). In any case, the phenomena of disinformation, propaganda and misinformation really intensified during the COVID-19 pandemic, and especially during the lockdown period between March and June 2020. By then, the most notorious cases involved, for example, a fake letter supposedly from NATO Secretary General Jens Stoltenberg to Lithuanian Defence Minister Raimundas Karoblis stating NATO's intention to withdraw troops from the country; a forged letter in which a Polish military leader criticizes US troops; and a fake interview accusing Canadian troops in Latvia to have brought the virus to the country (NATO, 2020a).

Even more decisively, since the invasion of Ukraine by Russia in early 2022, a cognitive war has been ongoing. Here, the Alliance is faced with one of Russia's most prominent disinformation narratives, that is, that NATO broke a pledge made at the end of the Cold War not to expand eastwards, used to justify its invasion of Ukraine (Schuette, 2023: p. 34).The notion of "cognitive weapon" has in fact been discussed in Russia to designate the introduction of false theories and concepts into an enemy's intellectual environment as a way of influencing its state administration and decision-making, but also mass consciousness, in order to deflect loyalties and weaken national defence (Thomas, 2015: p. 18). To Ioana Leucea (2022: p. 83), the kind of politics of identity that is being practiced in wars, such as in Ukraine, can be seen as a warfare strategy that uses culture, theories and philosophies that ultimately shape or change people's perceptions about what is just action and what is not.

In this sense, the Cognitive Warfare hereby discussed has a critical impact on the very rules and structures that sustain international society. This form of hybrid war is one that "destabilises the traditional cognitive security environment of states and international organisations, and consequently, renders their identity insecure" (Mälksoo, 2018: p. 379). That is why NATO cares about disinformation; it cares because disinformation "tears at the fabric that holds our societies together"; because it undermines people's trust in governments, feeds their fears and prejudices, inflames extremism, and degrades the feelings of belonging to a community, all in order to divide and conquer (NATO, 2023c). NATO cares because, for 75 years, its success as a collective defence alliance has relied on the strength and assertiveness of its discourse about Atlantic unity and democracy, a discourse that feeds on the civilised habitus and on NATO's ability to defend and maintain it over time, regardless of the systemic changes that may arise (da Mota, 2018). That is why it does not hesitate to point to China and Russia as the "malicious actors" who seek to diminish public trust and undermine the Alliance's solidarity (NATO, 2023c).

In that context, although the response to countering Russian disinformation has been led by the US and the EU, through their respective official websites and entities that raise public awareness regarding the Kremlin's disinformation operations (Schuette, 2023: p. 49), NATO has adopted an "Understand and Engage approach". Accordingly, *understanding* means continuously analysing the information environment to keep track of what people are saying, hearing and reading about NATO, to then *engage* with the public audiences through various channels, providing accurate information in its public communications (NATO, 2023c). Since the war in Ukraine has started, it is possible to find on the Alliance's website a section dedicated to "Setting the record straight" and "de-bunking Russian disinformation on NATO" that is frequently updated with the latest myths that are then fact-checked (NATO, 2024). Some examples of these debunked myths include for example "NATO is encircling Russia", "Ukraine will not join NATO", and "NATO is aggressive".

As both a means and an objective of war, cognitive warfare raises rather deep questions about the meaning of war, its deeper implications, motivations, and possible paths. What is at stake in a cognitive war, the power to define the prevailing episteme, or the power to think freely? Can a cognitive war be regulated? And how can a cognitive war be won? Trying to answer these questions opens the way not only to new conceptions of war but also to new theorisations of International Relations, in which the role of neuroscience is critical.

Conclusion

The point of this article was to give particular prominence to Space and Mind, as two emblematic components of the technological revolution that NATO has both led and responded to in this century. By exploring how these two elements have evolved conceptually, strategically and institutionally, it was possible to portray a smart form of power, in which the material dimension of the technologies that sustain the functioning of the Alliance has become increasingly intertwined with the immaterial dimension of the ideas and values it stands for. In this symbiotic relationship, what is rather new are the objects and what they allow to do and achieve, namely in a faster, more effective and cleaner way.

With regard to the immaterial dimension, it proves to be timeless; disinformation and propaganda are not new issues. In fact, they are reminiscent of the Cold War and take us back to the classic operations that pitted the US against the USSR. What was at stake in the past has not changed – neither or very little have the players; democratic values in democratic societies are what is to be defended against authoritarian regimes. The novelty here probably lies in the acknowledgement that the fight for unsuspected knowledge, and the validity of its claims, is worth fighting for in a Cognitive Warfare that has unprecedented technological and scientific means at its disposal. A curious aspect of Cognitive Warfare is that it still does not allow us to say that NATO is formally at war with Russia, for instance, in a conventional and classic sense of international law.

So far, the literature has approached different aspects of the technological revolution with a mainly strategic concern, because the dynamics of competition are clear, as are the objectives of strategic advantage and superiority over Russia and China. However, it is worth taking on the idea that a technological and scientific edge is now compulsory for the Alliance's permanence, to reflect on what the implications of this requirement are for societies of NATO countries at large. Technological developments are not independent or dissociated from societal developments; on the contrary, they are closely linked, relating to each other in a process of "co-evolution" or "co-production", bringing together material and immaterial elements, that is, material infrastructures, cultures and political coalitions, social values, worldviews and paradigms (Smit, 2006: pp. 733-734). In this sense, the impact of these technologies on so-called psychological and social realities requires in-depth questioning. So, what is required from NATO populations in order to accompany, legitimise, and empower the political and military framework of an Alliance willing to maintain a technological edge and win the hearts and minds in a cognitive battlespace? What are the concrete effects and consequences of practicing smart power in this century? In a world increasingly dominated by technology, in which the material and immaterial dimensions are increasingly blurred, the role played by military organisations such as

NATO is critical. By adopting strategic concepts and policies, NATO defines security concepts and practices, identifies adversaries and potential enemies, as well as states the needs for defence and battlefields. Moreover, by doing that, NATO defines and conveys meanings about what is valid knowledge, controlling thought structures, perceptions and understandings of the world – and all this based on non-human means, henceforth. Nevertheless, what one cannot overlook is that the technological revolution cannot happen at the expense of the ethics of security.

Bibliography

Aaronson, M.; Diessen, S.; de Kermabon, Y.; Long, M. B.; Miklaucic, M. (2011). NATO countering the hybrid threat. *Prism,* 2(4): 111-124.

Bijker, W. (2006). Why and how technology matters, in Goodin, R.; Tilly, C. (eds.), *The Oxford Handbook of Contextual Political Analysis.* Oxford: Oxford University Press: 681-706.

Chong, A. (2015). Smart power and military force: an introduction, *Journal of Strategic Studies*, 38(3), 233-244.

Claverie, B.; Prébot, B.; Buchler, N. and Du Cluzel, F. (2021). *Cognitive Warfare*. First NATO scientific meeting on Cognitive Warfare. Bordeaux (France), 21 june 2021.

Da Mota, S. (2018). *NATO, Civilisation and Individuals. The unconscious dimension of international security.* New Security Challenges Series (ed. G. Christou). London: Palgrave Macmillan.

Ducaru, S. D. (2016). The cyber dimension of modern hybrid warfare and its relevance for NATO. *Europolity*, 10(1): 7-23.

Fidler, D.; Pregent, R.; Vandurme, A. (2013). NATO, cyber defense, and international law. *Journal of International and Comparative Law*, 4(1): 1-25.

Fritsch, S. (2014). Conceptualizing the ambivalent role of technology in IR: between systemic change and continuity, in Mayer, M.; Carpes, M.; Knoblich, R. (eds.), *The Global Politics of science and technology* (vol. 1). *Concepts from IR and other disciplines.* Heidelberg: Springer, 115-138.

Keohane, R.; Nye, J. (1998). Power and interdependence in the information age. *Foreign Affairs*, 77, 81-94.

Leucea, I. (2022). The cognitive warfare in designing the international society (and the security environment). *RCIC International Conference*, Brasov, 5-7 May.

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *European Security*, 27(3): 374-392.

Maurin, A. (2023). The war in Ukraine and space theatre. *Les Cahiers de la Revue Défense Nationale.* (French Air and Space Force – Paris Air Show 2023 – Aerospace Power & High Intensity Warfare), 30-36.

McNeill, W. H. (1982). *The Pursuit of Power: Technology, Armed Forces, and Society since A.D. 1000*. Chicago: Chicago University Press.

Morgenthau, H. (1961). Western values and total war. *Commentary*, 32, 277-304.

NATO (2010). *Active engagement, modern defence. Strategic Concept for the Defence and Security of the Members of NATO*. Adopted by the heads of state and government at the NATO Summit in Lisbon, 19-20 November 2010. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO (2012). *Filing the Vaccum – a framework for a NATO Space policy*. Kalkar, DE: Joint Air Power Competence Centre.

NATO (2019a). Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain, 20 November 2019. Available at: https://www.nato.int/cps/en/natohq/news_171028.htm?selectedLocale=en

NATO (2019b). London Declaration issued by the Heads of State and Government. Meeting of North Atlantic Council in London, press release nº 115 (4 December 2019). Available at: https://www.nato.int/cps/en/natohq/official_texts_171584.htm

NATO (2020a). NATO's approach to countering disinformation: a focus on COVID-19" 17 July 2020. Available at: https://www.nato.int/cps/en/natohq/177273.htm

NATO (2020b). Speech by NATO Deputy SG Mircea Geoana on NATO and innovation at HumanAIze, an online forum on AI and public-private sector collaboration. 28 September 2020. Disponível em: https://www.nato.int/cps/en/natohq/opinions_178354.htm?selectedLocale=en [15 October 2020].

NATO (2022a). "NATO's overarching space policy". 17 January 2022. Available at: https://www.nato.int/cps/en/natohq/official_texts_190862.htm

NATO (2022b). *NATO 2022 Strategic Concept*. Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2023a). Alliance Persistent Surveillance from Space (APSS). Factsheet, February 2023. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230215-factsheet-apss.pdf

NATO (2023b). NATO's approach to space. 12 April 2023. Available at: https://www.nato.int/cps/en/natohq/topics_175419.htm

NATO (2023c). NATO's approach to countering disinformation. 8 November 2023. Available at: https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

NATO (2024). Setting the record straight. De-bunking Russian disinformation on NATO. Available at: https://www.nato.int/cps/en/natohq/115204.htm

NATO Science and Technology Organization (2020). *Science & Technology Trends 2020-2040. Exploring the S&T Edge*. Brussels: NATO Science and Technology Organization.

Oren, E. (2016). A dilemma of principles: the challenges of hybrid warfare from a NATO perspective. *Special Operations Journal*, 2(1): 58-69.

Risse-Kappen, T. (1995). *Bringing transnational relations back in: Non-state actors, domestic structures and international institutions.* Cambridge, MA: Cambridge University Press.

Schuette, C. (2023). Russian disinformation on NATO expansion and the War in Ukraine. *Journal of Strategic Security*, 16(4): 34-56.

Single, T. (2008). Considerations for a NATO Space policy. *ESPI Perspectives*, nº 12, September.

Smit, W. (2006). Military Technologies and politics, in Goodin, R.; Tilly, C. (eds.), *The Oxford Handbook of Contextual Political Analysis.* Oxford: Oxford University Press, 722-744.

Stroikos, D. (2020). China, India, and the social construction of technology in international society: the English School meets Science and Technology Studies. *Review of International Studies*, 46, 1-19.

Thomas, T. (2015). Russia's 21st century information war: working to undermine and destabilize populations. *Defence Strategic Communications*, 1(1): 11-26.

Waltz, K. (1979). *Theory of international politics*. New York: McGraw-Hill.

O Ciberespaço, a NATO e Portugal – uma Trilogia Inter-relacionada[1]

Helder Fialho Jesus
Capitão-de-mar-e-guerra.

Resumo

Este artigo tem por objetivo analisar a adaptação da NATO aos desafios do ciberespaço, no século XXI, bem como a forma como Portugal o encarou na área da segurança e defesa, no mesmo período. Assim, incidiu-se a investigação nos níveis político, militar e técnico da Aliança Atlântica, de modo a perceber-se a importância do ciberespaço e quais as alterações preconizadas, situação posteriormente estendida a Portugal, tendo em vista conhecer o contributo nacional para a NATO nesta área. Na componente militar foi adotada a metodologia DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability), para efeitos de sistematização e coerência, para ambas as partes. No final apresenta-se de forma sumarizada uma análise e conclusões, mostrando quais as áreas onde Portugal se evidenciou. Efetuou-se, complementarmente, uma análise ao conceito estratégico da NATO, aprovado na Cimeira de Madrid, em 2022, no que ao ciberespaço diz respeito, tendo em vista verificar o alinhamento entre o ciberespaço e as três tarefas estratégicas.

Palavras-chave: NATO; Ciberdefesa; Cibersegurança; Operações no Ciberespaço; Conceito Estratégico.

Artigo recebido: 25.01.2024
Aprovado: 08.04.2024
https://doi.org/10.47906/ND2024.168.02

1 Ao longo do presente artigo, serão empregues as designações originais, em inglês, dos diversos organismos, projetos, iniciativas ou outros, conforme conhecidos na NATO, no sentido de garantir a coerência com o assunto, evitando-se traduções diferenciadas.

Abstract
Cyberspace, NATO and Portugal – an Interrelated Trilogy

This article aims to analyze the adaptation of NATO to the challenges of cyberspace, in the 21st century, as well as the way in which Portugal approached cyberspace in security and defense, in the same period, then making a connection between the two parties. Thus, we focused on the political, military, and technical levels, to understand the importance of cyberspace and the changes adopted, what is the current status in NATO and in Portugal, and what was the national contribution to the Alliance. In the military component, the DOTMLPFI methodology was considered for systematization purposes, for both parties. At the end, analysis and conclusions are briefly presented, pointing out the areas where Portugal stood out. An analysis was also carried out on NATO's Strategic Concept, approved at the Madrid Summit in 2022, regarding cyberspace, with the aim of verifying the coherence between cyberspace and the three strategic tasks.

Keywords: *NATO; Cyber Defence; Cybersecurity; Cyberspace Operations; Strategic Concept.*

1. Introdução

No 75.º aniversário da NATO[2], a sociedade atravessa a sua quarta revolução industrial, conforme Klaus Schwab (2016), presidente do World Economic Forum (WEF), descreve no seu livro com o mesmo título, e que se carateriza por uma Internet omnipresente, com sensores de dimensões cada vez mais diminutas, contudo de maiores capacidades, e pela Inteligência Artificial (IA), permitindo assim a interconexão do mundo físico e virtual. Neste sentido, três elementos são fundamentais, nomeadamente os dados, a informação e a comunicação.

Por sua vez, o ambiente de segurança que se vive está a tornar-se mais imprevisível (Burton e Lain, 2020, p. 3), cujas ameaças podem provir de intervenientes estatais e não estatais, com características assimétricas, onde se incluem os ciberataques e a guerra híbrida, confundindo os limites entre as formas convencionais e não convencionais de conflito, cujos ataques estão a aumentar em velocidade, sofisticação e diversidade (NATO, 2023a).

A relevância do ciberespaço[3], que é um produto do ser humano, começou a ser sentida em finais do século passado, com as oportunidades de desenvolvimento na sociedade, mas também pelos riscos associados. Os assuntos ligados à segurança estão, consequentemente, em evolução contínua e a atual era digital acelerou este processo, à medida que as ameaças se desenvolvem rapidamente e a manutenção das capacidades se torna mais complexa (EDA, 2023, p. 23), aumentando a fragmentação e incerteza.

Complementarmente, o sistema internacional também está em transformação contínua, consequência da evolução tecnológica que se está a verificar no mundo. Esta transformação assenta em três grandes categorias: (1) atores – com o surgimento de atores não estatais; (2) meios – com o surgimento do ciberespaço e de tecnologias disruptivas, onde se insere a IA; e (3) contexto – a perceção de uma crise internacional (Carcelli e Gartzke, 2017), que a COVID-19 e a invasão da Crimeia em 2014, reforçada com a guerra na Ucrânia em 2022, representaram para a sociedade ocidental.

A complexidade e a incerteza que caraterizam as sociedades atuais (UNDP, 2021), obrigam a uma preparação para enfrentar as crises, as quais têm três componentes: ameaça, urgência e incerteza (Boin *et al.*, 2016, p. 5), onde os exercícios são fundamentais para garantir a resiliência. A componente do ciberespaço vai tendo um papel cada vez

2 NATO – North Atlantic Treaty Organization

3 Não existe uma definição consensual a nível internacional para Ciberespaço. Em Portugal está definido como: "Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação" (ENSC – disponível em https://www.cncs.gov.pt/pt/estrategia-nacional/, a qual é diferente da NATO, apresentada mais à frente.

mais primordial, com o reconhecimento dos níveis de topo de diversas organizações internacionais, como sendo a União Europeia (CYBRID)[4], o G7 (Cyber exercise)[5], o World Bank (CSE)[6] ou a própria NATO (CMX)[7]. Esta última tem-se esforçado para se adaptar e transformar ao mesmo ritmo que a sociedade, tendo apresentado a iniciativa NATO 2030 (NATO, 2021a), que se pretende constituir como uma agenda ambiciosa visando garantir que esta Aliança permanece pronta, forte e unida para uma nova era de aumento de competição global. Nesta está incluída a Transformação Digital da NATO (ACT, 2023), onde para além das alterações tecnológicas está implícita uma mudança cultural e mental, a qual pretende facilitar as Multi-Domain Operations (MDO), visando garantir a interoperabilidade, um maior conhecimento situacional e uma tomada de decisões baseada em dados.

As restruturações organizacionais levadas a cabo pela Aliança aos níveis político, militar e técnico, o desenvolvimento de novas capacidades, as novas necessidades de treino, onde o contexto do ciberespaço[8] é cada vez mais relevante, levam a uma maior cooperação e colaboração intra-NATO, com os Aliados, com a União Europeia (UE) e outros países parceiros, bem como com a indústria e o meio académico. O novo conceito estratégico da NATO (NATO, 2022), aprovado na Cimeira de Madrid de 2022, reforça precisamente a importância do ciberespaço e apresenta um regresso à tradição dos conceitos anteriores a 2010, onde é reafirmado que o objetivo fundamental da NATO é garantir a defesa coletiva das nações aliadas, conforme os princípios fundadores da NATO, consagrados no Tratado de Washington de 1949. Como complemento a este objetivo e ao de garantir a segurança das nações aliadas, são apresentadas as três tarefas principais, sendo elas a dissuasão e defesa, a prevenção e gestão de crises e a segurança cooperativa, e que se podem considerar como o elemento vital da estratégia da NATO.

4 https://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf

5 https://www.ecb.europa.eu/paym/pol/shared/pdf/November_2020-G7-fundamental-elements-of-cyber-exercise-programmes.el.pdf

6 https://documents1.worldbank.org/curated/en/099125002162330340/pdf/P1776920e37f660f70b6640fe108468feb5.pdf

7 https://www.nato.int/cps/en/natohq/news_212527.htm

8 De acordo com o *NATO Glossary of Terms and Definitions*, AAP-06 Edition 2021, têm-se as seguintes definições para alguns dos termos associados ao tema do presente artigo:
Cyber Defence – "The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems".
Cyberspace – "The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data".
Cybersecurity – Não existe.

A natureza do ciberespaço exige uma abordagem holística através da unidade de esforços em três níveis: político, militar e técnico. A política de ciberdefesa da NATO de 2021 e o seu plano de ação correspondente, reforçam as atividades nestes níveis e em novembro de 2023, em Berlim, decorreu a primeira NATO Cyber Defence Conference, com a presença de decisores destes três níveis (NATO, 2023a). Assim, também será neste sentido que se desenvolve o presente artigo, na parte respeitante à NATO, a que se juntam outros elementos complementares, relativamente à ciência e à cooperação. Seguidamente, apresenta-se uma forma de olhar para a adaptação de Portugal ao ciberespaço, com ênfase para as áreas da Segurança e Defesa e com elementos do contributo de Portugal junto da NATO, no que ao ciberespaço diz respeito, com ênfase a partir de 2015, data da primeira estrutura nacional de ciberdefesa – o Centro de Ciberdefesa (CCD). Termina com uma breve análise, conclusões e considerações de futuro.

2. NATO

Um elemento que é transversal aos três níveis acima referidos é a arquitetura digital da NATO, sendo esta de uma enorme complexidade, na medida em que tem de responder aos seguintes fatores[9]: (1) ambientes estático e projetável; (2) três níveis de comando (estratégico, operacional e tático); (3) diversos requisitos dos espectros das operações militares, sejam específicos dos domínios de operações (ar, mar, terra, ciberespaço e espaço) ou para o *Command, Control, Communications, Computers, Intelligence, Surveillance, Targeting and Reconnaissance* (C4ISTAR); (4) requisitos diferentes das várias comunidades de utilizadores; (5) a visão e serviços, onde se incluem as camadas de dados, serviços e aplicativos com as respetivas funcionalidades necessárias; (6) redes com diferentes classificações de segurança; e (7) sinergias com outros projetos a fim de evitar "reinventar a roda".

a. Nível Político

A Cimeira de Praga (NATO, 2023a), em 2002, constitui-se como um marco de referência no reconhecimento da importância do ciberespaço ao nível político, tendo o termo *cyber* sido utilizado com uma alusão aos *cyber attacks* na declaração final da cimeira. Ainda neste contexto, o termo *cyberspace* foi utilizado pela primeira vez na Cimeira de 2010, em Lisboa (NATO, 2010a), e só mais tarde, na Cimeira de

9 https://www.ndia.org/-/media/sites/ndia/divisions/international/niag/niag-n_2021_0002_calling_notice_geospatial-data-infrastructure_sdi.ashx

Varsóvia (NATO, 2016), em 2016, passou a ser considerado como um domínio para as operações militares, à semelhança da terra, do ar e do mar. A partir desta, o termo *cyberspace* esteve sempre presente nas declarações formais até à Cimeira de Vilnius (NATO, 2023b) em 2023, com exceção da Cimeira de Madrid (NATO, 2022a), na qual foi aprovado o atual conceito estratégico (NATO, 2022b), mas onde a palavra "ciberespaço" não consta, apesar das alusões às ciberameaças, às ciberdefesas e às atividades neste domínio. A resiliência também recebe um papel proeminente no novo conceito, sustentando a ênfase abrangente na defesa coletiva e nas três tarefas principais.

Relativamente ao ciberespaço, este novo conceito reconhece que é um lugar onde existe uma grande competição, com atores maliciosos que tentam degradar as infraestruturas críticas, interferir com os serviços governamentais, roubar informação e propriedade intelectual, bem como impedir as atividades militares. De notar que são feitas referências à Federação Russa e à China na utilização deste domínio, numa alusão às atividades híbridas. Sobre as três tarefas principais, no contexto da ciberdefesa é estabelecido que: (1) a dissuasão e defesa da NATO é uma postura que se baseia numa combinação adequada das capacidades de defesa nuclear, convencional e antimísseis, sendo complementadas por capacidades nos domínios espaciais e no ciberespaço; que o artigo 5.º do Tratado de Washington pode ser invocado pelo *North Atlantic Council* (NAC), decorrente de um conjunto único ou cumulativo de atividades maliciosas no ciberespaço caso atinjam o nível de um ataque armado. Esta é a tarefa onde se centram a maioria das atividades no ciberespaço, seja no reforço de capacidades, seja para reforço da ciberdefesa, das redes e das infraestruturas; (2) a Segurança Cooperativa releva a parceria estratégica com a União Europeia (UE), que já teve três grandes momentos, sendo eles o da assinatura inicial em 2016, na Cimeira de Varsóvia, de uma declaração conjunta (EP, 2016), pelo Secretário-geral da NATO e pelos presidentes do Conselho Europeu e da Comissão Europeia, em 2018 e mais recentemente em 2023, onde a cooperação e partilha de informação no ciberespaço são elementos preponderantes, assim como o combate às ameaças híbridas e a defesa contra ciberataques; (3) A tarefa de prevenção e gestão de crises não tem qualquer alusão ao ciberespaço nem aos ciberataques.

Importa ainda relevar, ao nível político, mais alguns elementos que mostram a preocupação da NATO com o ciberespaço.

Como primeiros passos organizacionais pode relevar-se, em 2002, a aprovação de um *Cyber Defence Programme*, que contemplava a criação da *NATO Computer Incident Response Capability* (NCIRC). Mais tarde, em 2008, o estabelecimento de uma política de ciberdefesa, aplicada às autoridades políticas, militares e técnicas da NATO, que se estendia às nações Aliadas, bem como a criação da *Cyber Defence Management Authority* (CDMA) para coordenar a ciberdefesa em toda a Aliança, sendo esta posteriormente gerida pelo *Cyber Defence Management Board* (CDMB) (Healey e Jordan, 2014, p. 2).

Em 2010, com a aprovação do anterior conceito estratégico (NATO, 2010b) na Cimeira de Lisboa, o ciberespaço ganhou relevância, pois foi a primeira vez que surgiu a este nível. Mas ainda com um objetivo de desenvolvimento de capacidades para efeitos de prevenir, detetar, defender e recuperar de ciberataques. No fundo para garantir a cibersegurança das redes da NATO e dos países aliados.

Em 2012, a ciberdefesa foi introduzida no *NATO Defence Planning Process* (NDPP) (JAPCC, 2017, p. 3), através de uma identificação e prioritização dos requisitos para o processo de planeamento de defesa.

Na Cimeira de Gales (NATO, 2014), em 2014, foi assumido que o direito internacional é aplicável ao ciberespaço, assim como a decisão de invocar o Artigo 5.º no caso de um ciberataque a ser tomada pelo NAC, caso a caso. Criou-se a *NATO Industry Cyber Partnership* (NCIP), destinada à partilha atempada de informações sobre ciberameaças, permitindo aos participantes melhorar o seu conhecimento situacional, aprovou-se uma *enhanced Cyber Defence Policy*, atualizando a versão então existente de 2011 (CCDCOE, 2018a), onde foi considerado que a ciberdefesa era parte integrante na defesa coletiva da Aliança.

Na cimeira seguinte (NATO, 2016), na cidade de Varsóvia, para além do ciberespaço ter sido considerado como um domínio das operações, os Aliados concordaram em implementar o *Cyber Defense Pledge*, que constitui um compromisso para reforçar e melhorar a segurança das redes e infraestruturas nacionais contra ciberataques. No fundo, visava a cibersegurança destes elementos e a sua resiliência, reafirmando que as obrigações previstas no Artigo 3 do Tratado de Washington também se aplicam às capacidades no ciberespaço. Esta situação foi reforçada na última cimeira, em 2023, em Vilnius, de modo a ser uma questão prioritária. Posteriormente, em fevereiro de 2017, os ministros da defesa aprovaram um *Cyber Defence Action Plan* e um roteiro para implementar o ciberespaço como domínio das operações, visando o aumento da capacidade dos Aliados de trabalharem em conjunto, desenvolverem capacidades e partilharem informação.

Da Cimeira de 2018 (NATO, 2018a), em Bruxelas, verificou-se uma alteração na postura da Aliança face às ameaças no ciberespaço, com a criação de um *Cyberspace Operations Centre* (CYOC) e foi ainda acordada a integração dos efeitos no ciberespaço, fornecidos voluntariamente pelos Aliados, nas operações e missões da Aliança, naquilo que é conhecido como *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA). Ainda em Bruxelas, mas na Cimeira de 2021 (NATO, 2021b), releva-se a nova *Comprehensive Cyber Defence Policy*, o reconhecimento que o CYOC atingiu a sua *Initial Operational Capability* (IOC) e a criação do cargo de *NATO Chief Information Officer* (CIO), no contexto de uma restruturação levada a cabo na sede NATO. Este CIO tem a responsabilidade do desenvolvimento de uma abordagem empresarial para a transformação digital e o fornecimento de capacidades da NATO. Na Cimeira de Vilnius (NATO, 2023b), foi lançada a nova *Virtual Cyber Incident Support Capability*

(VCISC), tendo os Aliados concordado com a *Digital Transformation Implementation Strategy*, a qual visa reforçar a capacidade da Aliança de conduzir Operações Multi-Domínio, promover a interoperabilidade e melhorar o conhecimento situacional.
Ainda no nível político, importa relevar dois pontos: (1) de governação – com o *Cyber Defence Committee* (CDC) (NATO, 2023a), criado em 2014, sendo um órgão subordinado ao NAC com a responsabilidade pela governação e pela política de ciberdefesa. Desempenha um papel fundamental na ligação da política, tal como definida pelo NAC, com os níveis operacional e técnico na NATO. Até 2021, o órgão com responsabilidade pelo planeamento estratégico, direção executiva sobre o tema das redes da NATO e da segurança do ciberespaço na Aliança era o *Cyber Defense Management Board* (CDMB), onde havia uma grande ligação civil-militar e representação nacional (CCDCOE, 2018a). Nesse ano, fruto de uma restruturação na sede da NATO, o CDMB foi extinto, sendo substituído pelo *Senior Executive Group* (SEG); (2) de assessoria – com o *Assistant Secretary General – Innovation, Hybrid and Cyber* (IHC) (NATO, 2024) – o principal conselheiro do Secretário-Geral sobre os desafios emergentes de segurança e as suas implicações para a segurança da Aliança.
De destacar ainda o *Crisis Management Exercise* (CMX) (Got, 2020), exercício que serve para testar os procedimentos de consulta e tomada de decisão da Aliança no nível político-militar estratégico, num cenário civil-militar complexo, em ambiente híbrido, onde se incluem os ciberataques.
Releva-se ainda as palavras do Secretário-geral da NATO quando afirma que: "As we have seen in Ukraine, private companies, such as Microsoft, Amazon and Starlink, have become critical actors in their own right. (…) It is not possible to keep our nations safe without the private sector" (NATO SECGEN, 2023), mostrando a relevância de atores não estatais com poderes únicos e dos quais as sociedades estão cada vez mais dependentes, naquilo a que Joseph Nye (2010) refere como a difusão do poder.
A terminar este ponto apresenta-se o foco (NATO, 2023a) da Aliança para a ciber-defesa, que é a de proteger as suas redes próprias, operar no ciberespaço (missões e operações da NATO), ajudar os Aliados a aumentar a sua resiliência nacional e fornecer uma plataforma para consulta política e ação coletiva.

b. Nível Militar

A principal resposta da NATO na vertente militar, relativamente ao Ciberespaço, ocorreu em 2016, na Cimeira de Varsóvia, quando este foi considerado como um domínio das operações (e não domínio operacional, como às vezes é apresentado): "Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea".

Esta situação revela uma alteração significativa na abordagem deste tema, deixando de ter uma postura meramente "técnica", assente numa dissuasão pela negação (Burton, 2015, p. 13) e orientada para a segurança das suas redes e dos países aliados, para passar a ter também uma postura de "missão" (Bigelow, 2017, p. 6). Assim, esta determinação obrigou a alterações em diversas áreas, desde a política, à estratégia, aos conceitos, às doutrinas e aos procedimentos, bem como ao desenvolvimento de capacidades e capital humano face aos novos desafios.

Após esta decisão, foram elaborados dois documentos fundamentais (JAPCC, 2017), sendo eles o *Roadmap to Implement Cyberspace as a Domain of Operations* e a *Military Vision and Strategy on Cyberspace as a Domain of Operations*, tendo em vista a consecução da orientação política, nomeadamente na integração dos efeitos e da doutrina, assim como na revisão das *NATO Rules of Engagement* (ROE) (Goździewicz, 2019). Naturalmente, surgiu posteriormente o CYOC, no *Supreme Headquarters Allied Powers Europe* (SHAPE)[10], para efeitos de acompanhamento e coordenação da atividade operacional da NATO no ciberespaço, planeamento centralizado, bem como para efeitos de conhecimento situacional (NATO, 2018a). Tendo em conta que a NATO se considera como uma organização defensiva, conforme estabelecido logo no primeiro parágrafo do seu conceito estratégico, ter a iniciativa de criação de efeitos no ciberespaço seria incoerente. Assim, estabeleceu-se o conceito de SCEPVA, para efeitos da integração da criação de efeitos no ciberespaço nas operações e missões da NATO, que são fornecidos voluntariamente pelos Aliados. Aqui importa realçar uma grande diferença relativamente aos outros três domínios (terra, mar e ar) e que tem a ver com a transferência de responsabilidade dos meios/plataformas/unidades das nações para a NATO, aquando da integração destas em missões e/ou operações. Ao contrário do que acontece nos três domínios naturais referidos, no ciberespaço as nações garantem a criação dos efeitos pretendidos pelo Comandante da missão/operação, aquando do planeamento e da execução, mas sem qualquer transferência de autoridade sobre os meios que os criam, mantendo-se estes na alçada das nações. A integração dos diversos domínios de operações militares, onde o espaço também é considerado, conflui para o conceito de MDO, aumentando a complexidade no planeamento, assim como as probabilidades de uma execução mais eficaz e eficiente para se atingirem os objetivos estabelecidos.

As nações têm feito um esforço no sentido de terem uma capacidade no ciberespaço, para fins próprios de soberania, mas também para apoiar a NATO. Assim, e tendo em consideração que o desenvolvimento de uma capacidade assenta em oito vetores *Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Intero-*

10 Quartel General do *Allied Command Operations* (ACO), em Mons (https://shape.nato.int/military_command_structure)

perability (DOTMLPFI) (JALLC, 2016) segue-se esta lógica para apresentar os seus desenvolvimentos na Aliança Atlântica, na componente militar relativa ao ciberespaço:

- ***Doctrine*** – A publicação *Allied Joint Doctrine for Cyberspace Operations* (AJP 3-20) (UKGOV, 2020) constitui-se como a doutrina Aliada para efeitos de planeamento, execução e avaliação das operações no ciberespaço, no contexto das operações Aliadas conjuntas. Aqui, de forma clara, estabelece-se que as atividades no ciberespaço são de dois tipos: (1) Cibersegurança[11], tendo em vista a aplicação de medidas de segurança para a proteção da comunicação, da informação e de outros sistemas eletrónicos, e da informação que é armazenada, processada ou transmitida nesses sistemas no que diz respeito à confidencialidade, integridade, disponibilidade, autenticação e não repúdio; e (2) Operações no Ciberespaço definidas como ações no ciberespaço ou através dele tendo em vista preservar a liberdade de ação amiga neste domínio e/ou a criar efeitos para alcançar os objetivos definidos pelos comandantes. Estes tipos de operações podem ser defensivas, para efeitos de garantir um ciberespaço livre, ou ofensivas de modo a projetar poder para criar efeitos que alcancem objetivos militares. De notar que o termo *Cyber Defence* não faz parte do corpo deste documento, surgindo apenas nas referências e nos acrónimos e abreviaturas. Esta situação pode configurar uma maior dificuldade na taxonomia utilizada pelos diferentes níveis na Aliança, bem como no entendimento e interpretação por parte das nações.
- ***Organization*** – O principal realce vai para o CYOC, o qual tem os seguintes objetivos (Brent, 2019): fornecer conhecimento situacional; planear de forma centralizada as operações e missões da Aliança e proceder ao seu acompanhamento e coordenação. Assim, desempenha um papel central neste domínio, colaborando com diversas entidades, que para efeitos de conhecimento situacional recorrem aos países Aliados, bem como a agências da NATO, nomeadamente aos *NATO Intelligence Fusion Centre* (NIFC), *Allied Command Counter-Intelligence* (ACCI) e *Cyber Threat Assessment Cell* (CTAC). De acordo com o coronel Don Lewis (2019), CYOC *deputy director*, este centro serve como componente de teatro para o ciberespaço, com um paralelismo com os comandos geográficos na cobertura dos seus domínios físicos específicos. Por sua vez fornece aos comandantes aconselhamento neste domínio, apoio ao planeamento e integração de capacidades. De notar uma maior integração de capacidades, agregando o ciberespaço com os *Communication Information Services* (CIS) e a de *Electronic Warfare* (EW).

11 Cyber security: The application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

De notar que a *Allied Command Operations (ACO) Comprehensive Operations Planning Directive (COPD) Version 3.0* (2021) que articula o *Operations Planning Process* (OPP) para os níveis estratégico e operacional da NATO, em apoio ao *NATO Crisis Response Process* (NCRP), estabelece, para o CYOC, o seguinte: ao contrário das forças aéreas, terrestres, navais e de operações especiais, que normalmente executam as suas missões e tarefas ao nível operacional e tático dentro de um teatro de operações, os efeitos do ciberespaço, incluindo os CIS, são muitas vezes planeados e executados a um nível estratégico através de uma função centralizada de *Command and Control* (C2).

- ***Training*** – O exercício *Cyber Coalition* (ACT, 2023b) constitui-se como principal exercício da Aliança tendo por base o ciberespaço, realizando-se numa base anual desde 2008, e reúne organismos NATO, Países Aliados e Parceiros e a União Europeia com um total de cerca de 1000 participantes. É planeado e conduzido pelo *Allied Command Transformation* (ACT) sob os auspícios do *Military Committee* (MC) e tem em vista o reforço da capacidade da Aliança de dissuadir, defender-se e combater ameaças no e através do ciberespaço. A sua realização tem três grandes objetivos: (1) Exercitar os mecanismos existentes de interação entre os participantes para melhorar a colaboração no domínio do ciberespaço; (2) Melhorar a capacidade da Aliança para conduzir operações no ciberespaço, exercitando-se o conhecimento situacional e a partilha de informação sobre o ciberespaço e (3) Identificar lacunas de capacidades, requisitos de formação e validar procedimentos em desenvolvimento, a fim de apoiar o desenvolvimento das operações no ciberespaço e melhorar a educação e formação neste domínio. Importa ainda relevar o exercício *Trident Juncture* (Friedl, 2018), que é um exercício destinado a testar a capacidade da NATO para planear e conduzir uma grande operação de defesa coletiva – desde o treino de tropas ao nível tático, até ao comando de grandes elementos de uma força da NATO. No exercício de 2018 (Wright, 2019, p. 30), a integração do ciberespaço como parte ativa deste tipo de exercícios, em complemento aos outros três domínios, foi um marco assinalável, e que tem continuado nos exercícios seguintes:

  > "The impact of Space and Cyber on JISR continues to drive pace into innovation in the Joint Force Commands and SHAPE."

- ***Material*** – A este nível pretende-se responder à seguinte questão: a NATO tem a tecnologia e os equipamentos necessários para equipar as forças de modo a usar a capacidade de forma eficaz (Kamel e Gallup, 2022, p. 5)? O fator interoperabilidade é aqui preponderante, perante a miríade de companhias que desenvolvem as suas soluções, sejam de *hardware* ou de *software*. Neste sentido, o *NATO Standardization Office* (NSO) (NATO, 2017) tem promulgado *Standard Agreements* (STANAGs) e publicações tendo em vista o desenvolvimento de capacidade de agir em conjunto

de forma coerente, eficaz e eficiente para alcançar os objetivos táticos, operacionais e estratégicos dos Aliados, sendo o *NATO Interoperability Standards and Profiles* (NISP)[12] (ADatP-34) um exemplo, entre muitos. A criação do já referido NCIP vem ao encontro desta necessidade, tornando a ligação entre as empresas e os utilizadores mais facilitada.

- ***Leadership*** – A adoção do ciberespaço enquanto domínio das operações, com o estabelecimento de uma política para a Ciberdefesa, com o desenvolvimento subsequente de doutrina, estratégia, conceitos, procedimentos específicos para o ciberespaço e de forma integrada com os outros domínios, mostra a existência de uma liderança efetiva. Pode ainda referir-se, em específico, o cargo de *Deputy Chief of Staff for Cyberspace* (Blessing, 2021, p. 268), para efeitos de orientação estratégica ao *Supreme Allied Commander Europe* (SACEUR).
- ***Personnel*** – As questões relacionadas com as pessoas constituem um dos elementos mais complexos de resolver, porque exige profissionais com conhecimentos específicos, os quais requerem constante atualização, no contexto de um mercado que é muito concorrente. A necessidade de profissionais ligados ao ciberespaço é uma situação que é transversal a todos os países aliados e à própria NATO e que tem a ver com a existência de pessoas qualificadas em tempo de paz e em tempo de guerra, que os acontecimentos mais recentes no leste da Europa a isto obrigam responder. E foi precisamente sobre este tema que o General Curtis. M. Scaparrotti (SACEUR) fez a sua primeira pergunta na visita ao CCD, em outubro de 2017.
- ***Facilities*** – Para além do NATO HQ e dos dois comandos estratégicos, ACT e *Allied Command Operations* (ACO), que se complementam na definição do ambiente operacional atual e futuro[13], onde as questões do ciberespaço estão englobadas, existem três organismos que têm responsabilidades diretas no que ao ciberespaço diz respeito: (1) O CYOC, anteriormente referido, e (2) dois organismos que resultaram de uma grande transformação levada a cabo na NATO em 2012: (a) a *NATO Communications and Information Agency* (NCIA) (NATO, 2022c), que é o principal fornecedor de serviços de comunicações e informação da NATO, onde a cibersegurança das redes da NATO é uma das suas principais responsabilidades. Neste sentido, faz a gestão de incidentes de cibersegurança de rotina, com uma perspetiva técnica e responde ao CYOC quando existe impacto operacional; (b) o *NATO Communications and Information Support Group* (NCISG) (sd), que tem um trabalho complementar ao da NCI Agency, estendendo as redes estáticas por esta gerida até onde são necessárias operacionalmente para as forças destacadas.
- ***Interoperability*** – releva-se o *NATO Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (*CWIX) (ACT, sd), que é o maior evento de

12 ADatP-34 (https://live.nisp.nw3.dk/pdf/NISP-Vol1-v15.pdf)
13 https://www.act.nato.int/about/the-command/

interoperabilidade na NATO, na área técnica. Destina-se a desenvolver a capacidade de agir em conjunto, de forma coerente, eficaz e eficiente para alcançar os objetivos dos Aliados e cumpre um amplo espectro de requisitos de validação e verificação de interoperabilidade. Neste evento, que tem lugar anualmente no *Joint Force Training Centre* (JFTC), em Bydgoszcz, na Polónia (JFCT, 2022), a NATO, as nações Aliadas e as nações parceiras testam as suas capacidades de comando e controlo visando a eliminação dos riscos de interoperabilidade como um primeiro passo essencial para missões da NATO. Ao mesmo tempo, o CWIX é um banco de testes para especificações de interoperabilidade que são integradas em capacidades experimentais e de campo, prontas para futuras missões da NATO, onde a ciberdefesa é uma das 19 áreas contempladas.

c. Nível Técnico

A preocupação da NATO relativamente ao ciberespaço surgiu inicialmente na componente técnica. Isto porque eram os técnicos quem tinha de lidar com o assunto, nomeadamente na resolução dos incidentes que surgiam na rede da NATO, quer fossem falhas de operação, avarias ou ciberataques. Como exemplo, a partir de 1998, com as operações da NATO nos Balcãs, os ataques de *Distributed Denial of Service* (DDoS) passaram a ser regularmente sentidos nas redes da Aliança, nomeadamente por *hackers* sérvios, tendo em vista criar disrupção nos sítios e nos servidores de e-mail da NATO (NATO PA, 2009).

A Cimeira de Praga, em 2002, preparou o caminho para se criar o *NATO Computer Incident Response Capability (NCIRC)* em 2002. Decorrente da determinação da Cimeira de 2010 em Lisboa, em 2012 foi então criada a NCIA (NATO, 2023a), como o resultado da integração de vários organismos da *NATO Consultation, Command and Control Organization* (NC3O). A NCIA constituiu-se, assim, como o principal fornecedor destes serviços na Aliança, que incorporou o *NATO Computer Incident Response Capability Technical Centre* (NCIRC-TC), sendo este o órgão responsável pela proteção técnica centralizada no que aos ciberataques dizia respeito e atingindo a sua *Final Operational Capability* (FOC) em 2014. Em 2018, o *NATO Cyber Security Centre* (NCSC) substituiu NCIRC-TC, sendo responsável por todo o ciclo de vida das atividades de cibersegurança da NATO, ao nível da aquisição, manutenção e sustentação, bem como na condução de operações e resposta a Incidentes no ciberespaço. A NCIA (NCIA, sd) conta com uma equipa de 3.000 funcionários civis e militares, distribuídos por 29 localizações, na Europa e na América do Norte. A agência está na linha da frente contra as ciberameaças, protegendo as redes da NATO 24 horas por dia, sete dias por semana. Fornecem também capacidades e serviços que são críticos para a capacidade da NATO de cumprir as suas tarefas principais e trabalha igualmente

em parceria com a indústria, a academia e organizações sem fins lucrativos. Existem ainda as *NATO Cyber Rapid Reaction Teams* (RRT) para ajudar os Aliados em caso de ciberataques, que têm uma prontidão de 24 horas, que atuam quando solicitado e aprovado pelo NAC.

A *Alliance C3 Strategy*[14] constitui-se como mais um marco na adaptação da NATO para dar resposta às necessidades, introduzindo o conceito de *NATO Enterprise*, o qual viria a ser posteriormente definido no *The NATO Enterprise Approach for the Delivery of C3*, e com o desenvolvimento posterior da *NATO Enterprise C&I Vision*, tendo em vista a coerência das capacidades C3 com os serviços de Tecnologia de Informação e Comunicação (TIC).

Em termos de projetos em curso, pode referir-se que, em 2019, foram dados passos muito importantes para a modernização das redes da Aliança (NCIA, 2020), através do programa Polaris, que se constitui como um dos primordiais focos da NCIA, sendo o apoio às operações o principal. Este programa destina-se a consolidar a infraestrutura de TIC da NATO, implementando padrões técnicos modernos, de modo a poder ser gerida centralmente, bem como na adoção de novas formas de trabalhar. Este programa inclui esforços para melhorar a cibersegurança e reduzir os custos de manutenção.

A assinatura de acordos bilaterais é um exemplo das parcerias criadas entre a NATO e a Indústria, no âmbito da NCIP (NCIA, 2018), e que são estabelecidos pela NCIA. Estas parcerias visam a partilha atempada de informações sobre ciberameaças (informação técnica não classificada relacionada com ameaças e vulnerabilidades no contexto do ciberespaço) permitindo melhorar o conhecimento situacional e a proteção das redes. Na prática, facilitará o intercâmbio bilateral rápido e atempado de informações. Como exemplos de entidades têm-se a Microsoft, Fortinet, CISCO, Thales, a Vodafone, a AT&T e a CY4GATE.

No âmbito dos projetos de Smart Defence, no que ao ciberespaço diz respeito, são três os que se apresentam (Cordey e Dewar, 2019, p. 123): (1) O *Multinational Cyber Defence Capability Development* (MNCD2) (NCIA, 2014) e que se destina a facilitar a troca de informações relacionadas a ciberincidentes entre equipas nacionais de *Computer Security Incident Response Teams* (CSIRT), tendo em vista a criação de um "*Cyber Information and Incident Coordination System*"; o (2) *Malware Information Sharing Platform* (MISP) (NATO, 2013), liderado pela Bélgica, e concebido para ajudar na defesa contra ciberataques. Esta plataforma visa facilitar a partilha de informação sobre as características técnicas de *malware*, numa comunidade confiável; e o *MultiNational Smart Defence Project on Cyber Defence Education & Training* (MNCDE&T) (MNCDET, sd), liderado por Portugal (Monteiro, 2017), que se destinava a criar uma Plataforma de Coordenação de Educação e Treino (E&T) de Ciberdefesa e apresentar

14 C-M(2014)0016 – 07April2017.

novas iniciativas visando colmatar as deficiências de E&T de Ciberdefesa das nações aliadas e da NATO. Este projeto terminou em 2019 (DELNATO, 2019), apresentando uma estrutura curricular para a formação de peritos em cibersegurança. Os novos cursos passaram, posteriormente, a ser lecionados nos diferentes países Aliados e Parceiros, bem como na NCI Academy, em Oeiras[15].

A *NCI Academy*, que se estabeleceu formalmente em Oeiras em maio de 2019 (MDN, 2019), encontra-se na dependência da NCIA. A sua localização em Portugal decorreu das alterações aprovadas no seio da NATO quanto à nova orgânica dos seus Comandos, decorrente da Cimeira de Lisboa em 2010, e que determinaram a desativação do *Allied Joint Force Command Lisbon* (JFC Lisbon). No mesmo espaço encontra-se agora a *NCI Academy*, que até então estava sediada em Latina, Itália, com a designação de *NATO CIS School* (NCISS). Incorporou ainda outras entidades independentes de educação e formação individual, como o *NATO Programming Centre*, localizado em Glons e a *NATO Consultation, Command and Control Agency* (NC3A), localizada em Haia. Assim, a *NCI Academy* mantém uma longa tradição de oferta de educação e formação na área de *Consultation, Command, Control, Communications and Intelligence, Surveillance and Reconnaissance* (C4ISR) e do ciberespaço (NCIA, 2022).

Ao nível da governação importa referir pelo menos dois pontos: (1) o *Digital Policy Committee* (NATO, 2023c) – responsável perante o NAC pela assessoria política e técnica em diversas áreas, entre elas a ciberdefesa. Em dezembro de 2023, por decisão do NAC, substituiu o *NATO Consultation, Control and Command Board (NC3B)*, para melhor refletir o seu âmbito e visão, na era digital. Com esta alteração, a NATO considera que vai permanecer na vanguarda dos novos desenvolvimentos tecnológicos, mantendo ao mesmo tempo a interoperabilidade para uma interface perfeita entre os domínios militares e as forças armadas Aliadas; (2) o *Chief of Information Officer* (CIO) (NATO, 2023a) – responsável por garantir a integração, o alinhamento e a coesão dos sistemas e serviços de TIC em toda a NATO e supervisiona o desenvolvimento e a operação das capacidades de TIC. O CIO é também a autoridade para as questões de cibersegurança em toda a NATO, onde se inclui a liderança da gestão de incidentes, a orientação de investimentos específicos nesta área, a melhoria da postura de cibersegurança da Aliança, bem como o aumento da sensibilização em cibersegurança.

15 https://otan.missaoportugal.mne.gov.pt/pt/noticias/ultima-reuniao-do-projeto-multinational-cyber-defence-education-and-training-na-sede-da-nato

d. Complementar

Em complemento aos três níveis acima referidos, identificam-se ainda outras iniciativas que concorrem para a forma como a NATO aborda o ciberespaço. Neste sentido destacam-se:

(1) *NATO Science and Technology Organization* (STO) (STO, sd) – Órgão criado para satisfazer as necessidades coletivas de Ciência e Tecnologia da NATO e dos Aliados, através da partilha e disseminação de conhecimento científico, desenvolvimentos tecnológicos e inovação resultantes de inúmeras atividades suas. Este foi criado em 2012, como resultado da reforma que a NATO levou a cabo nesse ano, o qual reúne a maior rede mundial de investigação em defesa e segurança, reunindo cientistas, engenheiros e analistas nacionais, a indústria e o meio académico para colaborarem no âmbito de um quadro confiável da NATO.
(2) *Science for Peace and Security* (SPS) (NATO, 2023e) – Programa que promove o diálogo e a cooperação prática entre os Estados-membros da NATO e os países parceiros com base na investigação científica, na inovação tecnológica e no intercâmbio de conhecimento. No âmbito deste artigo, as atividades SPS na área da ciberdefesa visam melhorar a sensibilização, o reforço de capacidades, bem como a investigação e o desenvolvimento, sendo exemplos mais recentes o Azerbaijão, a Jordânia, a Tunísia, a Macedónia do Norte, a Mongólia e a República da Moldávia. Com estes dois últimos, a NCIA (NCIA, 2021a.b.) forneceu equipamento, formação e aconselhamento técnico para o estabelecimento de *Cyber Incident Response Capabilities* (CIRC) para as respetivas forças armadas.
(3) *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) – Com a integração da Estónia na NATO, em 2004, este país apresentou o conceito de um centro de excelência internacional para a Ciberdefesa (CCDCOE, sd), o qual foi aprovado pelo *Supreme Allied Commander Transformation* (SACT) em 2006. O CCDCOE foi criado em 2008, com a respetiva acreditação e estatuto de *International Military Organizaton* atribuídos pelo NAC. Atualmente conta com 39 nações (CCDCOE, 2023), sendo 9 delas nações parceiras e tem como missão apoiar os países Aliados e a NATO com conhecimentos interdisciplinares únicos no domínio da investigação, formação e exercícios de ciberdefesa, abrangendo quatro áreas de foco: tecnologia, estratégia, operações e Direito. O *Steering Committee* é o principal órgão de orientação, supervisão e decisão sobre todos os assuntos relativos à administração, políticas e funcionamento do CCDCOE, onde as nações Aliadas integrantes estão representadas. Este centro desenvolveu três grandes produtos: (1) a *International Conference on Cyber Conflict* (CyCon)[16], que teve a sua primeira

16 https://ccdcoe.org/cycon/

edição em 2009, e que tem uma periocidade anual tendo-se tornado um evento de referência na comunidade de profissionais de cibersegurança e ciberdefesa, aderindo aos mais altos padrões de pesquisa académica. Durante três dias, contando com cerca de 600 presenças onde se incluem decisores políticos, líderes de opinião, especialistas em Direito e tecnologia, militares, meio académico e indústria de quase 50 países, são discutidos os atuais desafios de segurança no ciberespaço, de uma forma interdisciplinar; (2) O exercício *Locked Shields*[17], cuja primeira realização ocorreu em 2010, sendo o maior e mais complexo exercício internacional de ciberdefesa. Este exercício técnico expandiu-se consideravelmente ao longo dos anos, simulando toda a complexidade de um incidente massivo no ciberespaço – além da defesa de sistemas informáticos e militares regulares, juntamente com infraestruturas críticas, os especialistas em cibersegurança e ciberdefesa podem praticar a tomada de decisões estratégicas e a comunicação jurídica e mediática, tendo uma periodicidade anual; (3) o *Tallinn Manual*, cujo processo foi lançado em 2009, e que se constitui como uma das realizações de investigação mais conhecidas e reconhecidas internacionalmente para o CCDCOE. A edição original, publicada em 2013, abordava as operações no ciberespaço mais notórias – que têm a ver com o uso da força e o exercício do direito de autodefesa pelos Estados. Em 2017 foi publicado o *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[18], que ampliou a anterior edição, com uma análise jurídica dos incidentes no ciberespaço que ficam abaixo dos limiares do uso da força ou do conflito armado. Apesar deste manual ser uma análise muito abrangente sobre como o Direito Internacional existente se aplica ao ciberespaço, há também quem considere que apresenta uma visão ocidental de abordar esta realidade[19]. Em 2021 foi lançado o projeto para o *Tallinn Manual* 3.0, que envolverá a revisão de capítulos existentes e a exploração de novos temas de importância para os Estados, face às alterações entretanto surgidas desde 2017. Importa ainda relevar duas outras iniciativas do CCDCOE, concretamente o (1) *Cyber Commanders' Handbook* (CCDCOE, 2020) que apresenta linhas de orientação para apoiar o planeamento, coordenação, execução e avaliação das operações no ciberespaço e (2) o exercício *Crossed Swords*[20], que teve a sua primeira edição em 2016, onde são testadas as capacidades e habilidades práticas necessárias ao planeamento e execução de operações ofensivas no ciberespaço.

17 https://ccdcoe.org/exercises/locked-shields/

18 https://ccdcoe.org/research/tallinn-manual/

19 A este respeito é interessante ver "De" colonizando o direito internacional do ciberespaço: a desconsideração da visão latino-americana, publicado pelo *Brazilian Journal of Development*, em 2022, no sítio https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/45756

20 https://ccdcoe.org/crossed-swords/

3. Portugal

Para a salvaguarda do Ciberespaço em Portugal, no contexto da sua proteção, segurança e defesa (conceito PSD) são vários os momentos e os atores que intervêm. Nesta parte, pretende apresentar-se, de forma sintetizada, aqueles que se consideram de maior relevância, com um destaque posterior para a componente militar, pela sua ligação prática e mensurável à NATO.

Assim, em 2013, o *Conceito Estratégico de Defesa Nacional* (CEDN) (RCM, 2013a) e a Reforma "Defesa 2020" (RCM, 2013b) definiram as orientações políticas para a implementação da reforma estrutural na defesa nacional e nas Forças Armadas em 2014/2015. O primeiro ao caraterizar a tipologia das ameaças transnacionais refere que, para responder às ameaças e riscos seria necessário definir, no contexto do ciberespaço, uma estratégia e uma estrutura nacional, a criação de órgãos técnicos necessários; a sensibilização dos operadores públicos e privados para a natureza crítica da segurança informática, assim como levantar a capacidade de ciberdefesa nacional. A segunda reforça este último ponto, estabelecendo a necessidade de se proceder ao levantamento da capacidade de ciberdefesa nacional, como uma das orientações específicas no ciclo de planeamento estratégico. No âmbito desta reforma, e no seguimento da aprovação à primeira alteração à Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA) (AR, 2014) foi aprovada uma nova orgânica do Estado-Maior-General das Forças Armadas (EMGFA) (MDN, 2014), determinando que a estrutura interna do EMGFA seria aprovada por decreto regulamentar. Assim, através do Decreto Regulamentar n.º 13/2015 (MDN, 2015), é criado o Centro de Ciberdefesa. Em 2023, este passou a designar-se por Comando de Operações de Ciberdefesa, através do Decreto Regulamentar n.º 2/2023 (MDN, 2023), que aprova a nova estrutura orgânica do EMGFA, concluindo desta forma a nova reforma da estrutura superior das Forças Armadas iniciada em 2021, com a revisão da Lei de Defesa Nacional e com a aprovação da nova LOBOFA (AR, 2021).

Em 2014 surgiu o Centro Nacional de Cibersegurança (CNCS) (PCM, 2014), na alçada do Gabinete Nacional de Segurança, num trabalho que já vinha desde 2012, e que vem dar robustez à resposta nacional para os incidentes no ciberespaço. Com a publicação do Regime Jurídico da Segurança do Ciberespaço (AR, 2018) é atribuída ao CNCS a competência de Autoridade Nacional de Cibersegurança e ao CERT.PT a de ponto de contacto único internacional para reação a ciberincidentes.

Em 2016 é criada a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) (MJ, 2016), na Polícia Judiciária, sendo a unidade operacional especializada para resposta estrutural, preventiva e repressiva ao fenómeno do cibercrime e do ciberterrorismo[21]. Ainda na área da cibercriminalidade existe, na

21 https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=20161118-mj-pj

Procuradoria-Geral da República, desde 2011, o Gabinete Cibercrime[22] que tem caráter de estrutura de coordenação da atividade do Ministério Público nesta área. Os Serviços de Informações de Segurança (SIS) têm um órgão que trata os assuntos do ciberespaço, onde se integram também as tarefas de combate à ciberespionagem. Em 2016 foi criado o cargo de embaixador para a Ciberdiplomacia[23] e em 2020, em acumulação, o cargo de embaixador para a Diplomacia Digital.

Em Portugal existe uma forma holística de encarar a PSD do ciberespaço, tendo-se constituído em 2018 o G4, que é um grupo informal de caráter operacional, integrando o CNCS, CCD, UNC3T e SIS para efeitos de partilha de informação, conhecimento situacional e coordenação de ações. Naturalmente que em certas circunstâncias existem ligações com outras entidades, fruto das necessidades de resposta.

No início dos anos 2000, as Forças Armadas procuraram criar capacidades próprias para dar uma resposta à segurança das suas redes, situação igualmente ocorrida no meio académico. Em 2002 foi criado o CERT.PT, no âmbito da Rede Ciência, Tecnologia e Sociedade (RCTS) gerida pela Fundação para a Computação Científica Nacional (FCCN), sendo a única equipa de resposta a incidentes de segurança informática em Portugal, e acreditada internacionalmente. Em 2014, o CERT.PT transitou para o CNCS com a criação deste centro que assumiu formalmente a coordenação da resposta nacional a incidentes de segurança informática[24]. Na alçada da FCCN surgiu a Rede Nacional CSIRT[25], em 2008, e que pretende criar em Portugal uma cultura de cibersegurança, de partilha de informação e apoio entre os organismos intervenientes na resposta a incidentes, contando atualmente com cerca de 60 entidades registadas.

Ao nível estratégico, e nas áreas da segurança e defesa[26], releva-se a Estratégia Nacional de Segurança no Ciberespaço (ENSC) (RCM, 2019), que apresenta uma visão integrada do ciberespaço, sendo o documento agregador e enquadrador das restantes áreas específicas, as quais deveriam posteriormente elaborar estratégias setoriais. A ESNC define ciberespaço como um "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação". Nota-se que é mais abrangente do que a apresentada pela NATO, agregando as três camadas do ciberespaço (física, virtual e das pessoas) também assumidas pela NATO, mas não vertidas por esta na sua definição. Também na ENSC está a definição de ciberdefesa, que "consiste na atividade

22 https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_da_actividade_de_2012.pdf

23 https://www.c-days.cncs.gov.pt/luis-barreira-de-sousa/

24 https://www.fccn.pt/seguranca/rcts-cert/

25 https://www.redecsirt.pt/

26 Em Portugal foram promulgadas várias estratégias no contexto da sociedade onde a digitalização e o ciberespaço são elementos de base, tais como a Estratégia para a Transformação Digital na Administração Pública, mas que não são objeto de análise neste artigo.

que visa assegurar a defesa nacional no, ou através do, ciberespaço", entre outras. Em 2022 surgiu a Estratégia Nacional de Ciberdefesa (ENCD) (RCM, 2022), clarificando que compete às Forças Armadas a execução de operações no ciberespaço ou através dele, quer sejam de natureza ofensiva ou defensiva, como forma de salvaguardar a defesa dos interesses e valores fundamentais, da ordem constitucional, a soberania e independência nacionais, bem como a integridade do território. No entanto, sendo a ciberdefesa uma área setorial contemplada na ENSC, ao ganhar um estatuto nacional, coloca algumas dúvidas nas linhas orientadoras para uma estratégia nacional de segurança global e de hierarquização dos assuntos a nível nacional.

Na parte militar, destaca-se a Diretiva Estratégica do EMGFA 2018-2021 (EMGFA, 2018), onde a Ciberdefesa é considerada como um dos nove objetivos estratégicos, visando a edificação de uma capacidade de ciberdefesa. Nesta decorrência foi criado um grupo de trabalho, liderado pelo EMGFA e com a participação dos três ramos, para a elaboração de um Plano de Ação, o qual está na base da atual estrutura orgânica do Comando de Operações de Ciberdefesa. A Diretiva Estratégica do EMGFA 2021-2023 (EMGFA, 2021) contempla a criação de uma Escola de Ciberdefesa visando capacitar a área dos recursos humanos.

Como nota final, a terminar esta abordagem macro, salienta-se a criação do *Cyber Academia and Innovation Hub* (CAIH) (PCM, 2023), um projeto de Cooperação Estruturada Permanente (PESCO) da UE que tem a liderança de Portugal, cuja visão é de estabelecer uma ligação entre a dimensão militar e civil da segurança do ciberespaço.

Os factos acima apresentados permitem ver que Portugal tem acompanhado as alterações que se têm verificado a nível internacional, adaptando-se ao quadro estratégico para fazer face às ameaças e riscos à segurança, neste caso, no ciberespaço.

A ligação à NATO ao nível político é efetuada através do Ministério dos Negócios Estrangeiros (MNE), que articula com as restantes entidades nacionais a resposta de Portugal. No caso do tema da Ciberdefesa, Portugal tem respondido ao *Cyber Defence Pledge*, de forma articulada envolvendo o EMGFA, o Ministério da Defesa Nacional (MDN) e o Ministério dos Negócios Estrangeiros (MNE), assim como teve participação em reuniões do CDC e do então CDMB. A participação nacional também se tem feito ao nível do exercício CMX, onde a parte do ciberespaço tem presença cada vez mais assídua, no qual as entidades antes referidas, entre outras, participam nas suas áreas de responsabilidade.

Na ligação ao nível militar, os exemplos a seguir apresentados, seguem igualmente a lógica do DOTMLPFI, para efeitos de coerência e sistematização. Assim:

- **Doutrina** – O Estado-Maior-General das Forças Armadas promulgou o PDMC 3.20 – Doutrina Militar Conjunta para Operações no Ciberespaço, alinhado com o AJP-3.20 e outros documentos doutrinários. Portugal participou ainda ativamente na elaboração do *Cyber Commanders' Handbook*.

- **Organização** – A criação do Centro de Ciberdefesa em 2015 e posteriormente, em 2023, do Comando de Operações de Ciberdefesa, ilustram a adaptação e maturação da resposta nacional às operações militares no ciberespaço. O espírito conjunto está presente desde a primeira hora, inicialmente, com o CCD tendo uma lotação de 10 militares, dos três ramos, numa vertente de proteção das redes da Defesa Nacional. Com o decorrer do tempo, constatou-se que não havia capacidade de resposta para o que seria pretendido para uma componente militar neste domínio, nomeadamente para a realização de operações no ciberespaço. Isto, pela sua complexidade e exigência, em várias áreas, entre elas as de planeamento, de C2, *targetting*, de sincronização, de avaliação, entre outras. A realidade atual já é diferente, com uma estrutura alinhada com as boas práticas das nações Aliadas, e com um incremento em recursos humanos para dar resposta às diversas solicitações, processo este ainda em curso e particularmente exigente, no que aos recursos humanos diz respeito.
- **Treino** – O treino é um elemento fundamental para o adestramento tendo em vista o desenvolvimento de conhecimentos, habilidades e atitudes para um desempenho mais eficiente. Os primeiros exercícios de cibersegurança e ciberdefesa realizados em Portugal foram organizados pelo Exército, através da série CiberPerseu, iniciada em 2012[27] e depois pelo EMGFA, conduzidos pelo Centro de Ciberdefesa, em 2018, através do exercício CyberDEx[28], numa vertente militar. Por sua vez, o CNCS passou a ter, também a partir de 2018, o Exercício Nacional de Cibersegurança[29]. Estes exercícios contribuem igualmente para o desempenho nos Exercícios Cyber Coalition, em que Portugal participa desde 2014, como observador, e desde 2016 de forma permanente. Também no âmbito internacional, Portugal passou a participar no exercício *Locked Shields* em 2018 e no exercício *Crossed Swords* em 2020, ambos da responsabilidade do CCDCOE. Nestes dois exercícios internacionais é criada uma equipa nacional, contando com elementos do EMGFA, que lidera, dos três ramos, do MDN, do CNCS e de outras entidades que tenham interesse e/ou necessidade em participar, num conceito de geometria variável, face aos cenários a jogar. Portugal participa ainda no CWIX, sendo a presença nacional assegurada pelo EMGFA, os três ramos, MDN e empresas nacionais, em função do que se pretende testar, sendo uma ocasião de excelência para se procederem a testes de experimentação, pela diversidade de sistemas presentes. Há a registar a presença nacional nas seguintes *Focus Areas* (FA): *Federated Mission Networking* (FMN), *Cyber Defence* (CD) e *Friendly Force Tracking* (FFT), Communications, GeoMetoc num total de 19 FA em 2023. Em 2024 está prevista a participação nacional em mais duas FA, concretamente *Space* e *LandOps*.

27 https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/exercicios/ciberperseu
28 https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/exercicios/cyberdex
29 https://www.cncs.gov.pt/pt/exercicio-nacional-ciberseguranca/

- **Material** – A ligação à indústria é um fator relevante nesta área onde a aquisição de equipamentos, plataformas e *software* é exigente e em constante atualização. Assim tem sido, através de empresas nacionais e internacionais, tendo em vista a obtenção das melhores condições para se garantir a segurança das redes, dos ambientes técnicos de treino, através do Cyber Range, e de formação, através da Escola de Ciberdefesa. De relevar também a forma como se procedeu ao alinhamento entre o EMGFA, os três ramos e o MDN nesta área, centralizando-se as aquisições de modo a serem criadas sinergias e um ambiente de trabalho idêntico para todos, facilitando assim o processo administrativo de aquisições, bem como de interoperabilidade e entreajuda.
- **Liderança** – A liderança nacional em atividades NATO, no contexto do ciberespaço, tem pelo menos duas situações de menção: (1) o projeto de *Smart Defence MNCD&ET*, que terminou em 2019 (DELNATO, 2019) e (2) o exercício CWIX, com a liderança da *FA Cyber Defence*, que ocorreu entre 2018 e 2021[30]. Neste período foram realizados testes de interoperabilidade, e exploradas e experimentadas diversas soluções em ciberdefesa, muitas vezes consideradas vanguardistas e inovadoras. Deste trabalho resultou um aumento da confiança por parte do ACT e pelos pares no trabalho desenvolvido, cujo reconhecimento foi várias vezes realçado. O abandono desta liderança foi uma decisão própria.
- **Pessoal** – A colocação de elementos nacionais nas estruturas da NATO, no contexto do presente artigo, cinge-se ao SHAPE, na divisão *J6 Cyberspace* e do NCISG. Fora da estrutura da NATO, mas a esta ligados, os assuntos relacionados com o ciberespaço são acompanhados na sede da NATO, em Bruxelas, tanto na Delegação Portuguesa junto da Organização do Tratado do Atlântico Norte (DELNATO), como na Representação Militar de Portugal junto do Comité Militar da NATO (MILREP).
- **Instalações** – A Estação NATO *Satellite Ground Terminal* (SGT) F12 (AR, 2019), que se encontra na Fonte da Telha e através da qual os serviços de CIS são disponibilizados aos navios da Marinha portuguesa em missões na NATO e a *CIS Support Unit* (CSU) Lisboa, que apoia a SGT-F12 e igualmente a *NCI Academy*.
- **Interoperabilidade** – Em termos técnicos, releva-se a participação no exercício CWIX, bem como a integração no projeto *Smart Defence* MISP.

Na lógica do capítulo anterior, dedicado à NATO, na parte complementar podem referir-se duas situações: (1) STO – Portugal participa em diversos projetos, podendo indicar-se, neste contexto, o *Multi-Domain Quantum Key Distribution (QKD) for Military Usage*, por proposta do Instituto de Telecomunicações. A gestão destas atividades está a cargo da Direção-Geral de Recursos da Defesa Nacional (DGRDN), cuja sensibilização da Base Tecnológica e Industrial de Defesa (BTID) é efetuada pela idD Portugal

30 https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/exercicios/cwix

Defence[31]. (2) CCDCOE – A adesão de Portugal ao CCDCOE (CCDCOE, 2018b), em 2018, constitui-se como um momento de afirmação e demonstração de que existe uma preocupação nacional com este domínio. Este centro conta com a presença de um oficial português em permanência, inicialmente no ramo das operações, passando posteriormente para o ramo da estratégia.
Ao nível técnico, na relação entre as duas partes releva-se todo o apoio e disponibilidade para a criação da NCI Academy, em Oeiras, a qual se encontra na dependência da NCIA.
Uma palavra final sobre a temática do ciberespaço, da ciberdefesa e das operações no ciberespaço para três trabalhos académicos no Instituto Universitário Militar (IUM), designadamente nos cursos de promoção a oficial general (CPOG), onde foi concluído que o ciberespaço deveria passar a ser entendido como plataforma para o desenvolvimento de operações, onde as Forças Armadas portuguesas deveriam atuar, conforme os parâmetros, requisitos e procedimentos da NATO (Honorato *et al*., 2017); a importância da articulação entre a cibersegurança e a ciberdefesa, no contexto da defesa coletiva e na gestão de crises (Coelho, 2018); e a necessidade de criar e operacionalizar, com a maior brevidade possível, uma estratégia militar para o ciberespaço, tendo em vista o desenvolvimento da capacidade de ciberdefesa nacional (Nunes, 2020).

4. Análise e Conclusões

A primeira parte deste artigo explora a evolução do ciberespaço na NATO, incidindo essencialmente nos níveis político, militar e técnico. Em termos globais, a aprovação de um conceito estratégico tem subjacente o surgimento de alterações organizacionais, as quais são significativas, como foram os exemplos decorrentes das Cimeiras de Lisboa (2010) e Madrid (2022). Atualmente encontra-se ainda em fase de implementação um conjunto de mudanças, onde a Transformação Digital é um elemento de referência. Assim, pode considerar-se que a NATO é uma organização aprendente (*learning organization*) à luz do estabelecido por Garvin (1993).
Analisando a estratégia da NATO na vertente do ciberespaço, à luz dos três paradigmas estratégicos, referidos por Couto (2020, pp. 249-250) e Ribeiro (2010b, p. 32), pode dizer-se que: na componente genética, de geração e criação de novos meios, são exemplos as novidades introduzidas com a Transformação Digital em curso ou a criação do CIO; na componente estrutural, de organizar e articular os meios, as alterações efetuadas nas diversas estruturas, sendo exemplos o CDC e o DPC (político), CYOC (militar) e o NCSC (técnico). Na componente operacional, de utilização dos

31 https://www.iddportugal.pt/nato-sto/

meios, tal apenas se aplica na componente de cibersegurança, de defesa das suas redes, visto que as operações no ciberespaço, sejam defensivas ou ofensivas, estão a cargo das nações, através do mecanismo SCEPVA, sendo estas que utilizam os meios.
A postura da NATO perante as ameaças no ciberespaço também se alterou, passando de uma posição de proteção de defesa das suas redes, conforme estabelecido no conceito estratégico de 2010 para uma atitude mais musculada, na versão de 2022. Isto porque o ciberespaço é contemplado na postura de dissuasão e defesa da NATO, a qual se baseia numa combinação de capacidades de defesa nuclear, convencional e antimíssil, complementada por capacidades do espaço e do ciberespaço, sendo considerado um domínio das operações militares. O reforço das capacidades no ciberespaço para aumento da resiliência e a sua ligação à segurança e defesa coletiva, elevam a sua relevância, assim como a alusão a invocar-se o artigo 5.º tendo por base um ciberataque. Relativamente à dissuasão no ciberespaço, este tema tem sido discutido na comunidade académica, não se vendo muito essa abordagem ao nível da NATO, podendo inferir-se que é um assunto classificado. Mas a dissuasão funciona com várias dimensões, sendo uma delas a comunicação, no sentido de chegar aos vários destinatários, para efeitos de balizagem de comportamentos.
Nas três tarefas indicadas no novo conceito estratégico, e já referidas anteriormente, estranha-se a ausência do ciberespaço no que à "prevenção e gestão de crises" diz respeito, podendo até afigurar-se uma contradição. Isto porque as atividades maliciosas no ciberespaço têm um impacto cada vez mais significativo na sociedade, podendo originar crises, onde os países mais desenvolvidos acabam por ser os mais vulneráveis, como os ciberataques à Estónia ocorridos em 2007 constituem um excelente exemplo (Joubert, 2012). Por sua vez, Jamie Shea (2017), anterior *Deputy Assistant Secretary General for Emerging Security Challenges*, refere que o Secretário-geral da NATO considera que um ciberataque pode ser tão devastador quanto um ataque convencional. Por sua vez, na Conferência de Segurança de Munique, em 2018, a *NATO Deputy Secretary General Rose Gottemoeller*, relevou a importância de uma maior cooperação entre a NATO e a UE, onde a componente da gestão de crises e do ciberespaço, foi várias vezes realçada (NATO, 2018b).
E o exemplo que se tem hoje na guerra entre a Federação Russa e a Ucrânia mostra bem isso. Assim, uma alusão ao ciberespaço neste contexto permitiria um entendimento mais global deste tipo de ameaças à sociedade, a qual está cada vez mais digitalizada e dependente desta componente. Até porque a NATO criou as *Rapid Reaction Teams* (RRT), que têm por objetivo prestar assistência às nações ou instalações da NATO em caso de ciberataques[32], o que a acontecer será no contexto de uma crise, que a nação, só por si, não consiga resolver.

32 https://www.nato.int/cps/en/natohq/news_118855.htm

No nível militar, um aspeto que é importante para a ação de comando é a compreensão da gestão do risco (Hutson, 2022), a qual é inerente a esta função, e que no caso do ciberespaço pode apresentar algumas dificuldades, uma vez que este é um novo domínio das operações, sendo transversal e apoiante dos restantes, em relação aos quais já existe um nível de maturidade superior.

Por sua vez, as tensões geopolíticas crescentes que se verificam a nível mundial, obrigam a garantir que os ativos e a infraestruturas de TIC sejam mantidos adequadamente, com as respetivas atualizações regulares, a fim de se garantir a proteção e a segurança contra as ciberameaças, cada vez mais complexas e disruptivas. No entanto, sendo a propriedade destas TIC em grande parte de companhias privadas, aumenta a dependência da NATO e dos Estados destes novos atores cada vez mais poderosos, como o atual conflito na Ucrânia o bem demonstra. Por outro lado, este desenvolvimento tecnológico, onde as MDO são um bom exemplo, assentando em grande parte na utilização e exploração do ciberespaço, pelos meios plataformas e equipamentos, obrigando a uma necessidade de maior interoperabilidade. No campo da taxonomia, pode salientar-se que a expressão "operações militares no ciberespaço" é utilizada pela comunidade operacional, que planeia e executa este tipo de operações, encontrando-se o termo "ciberdefesa" em desuso, o qual é muito utilizado ao nível político. Tal pode verificar-se na publicação doutrinária da NATO, o AJP-3.20, em que o termo *Cyber Defence* não surge no seu corpo. Por outro lado, considerando que esta mesma publicação refere a cibersegurança, e a define de forma consensual com aquilo que é comummente aceite, a ausência do termo *Cybersecurity* do AAP-6 é de estranhar, visto que reflete efetivamente o que a NATO faz para a proteção das suas redes. Esta breve descrição mostra que existe a necessidade de uma clarificação dos conceitos e da sua aplicação.

A análise na parte militar, à luz da metodologia DOTMLPFI, permite uma sistematização dos resultados, onde se releva a doutrina através do AJP-3.20, o exercício *Cyber Coalition* para treino e adestramento, o NCISG para apoio às forças destacadas e na parte da interoperabilidade o exercício CWIX. Na parte técnica destaca-se a criação da NCIA, pela importância que esta tem na proteção das redes da NATO e no apoio às operações, sendo um elemento estrutural para a parte política e militar.

Na segunda parte deste artigo, procurou-se apresentar o que foram os desenvolvimentos ocorridos em Portugal no ciberespaço, nas componentes de segurança e defesa. A promulgação do CEDN, em 2013, foi o primeiro momento que caraterizou a preocupação nacional com o ciberespaço, tendo sido depois promulgada documentação diversa. Portugal acompanhou e foi-se adaptando às alterações que foram surgindo no panorama internacional, tendo ocorrido duas modificações substanciais na área da defesa, concretamente em 2014/15 e 2021/22. A primeira com o surgimento do Centro de Ciberdefesa e depois com a passagem deste para Comando de Operações de Ciberdefesa. De relevar ainda a inclusão da ciberdefesa

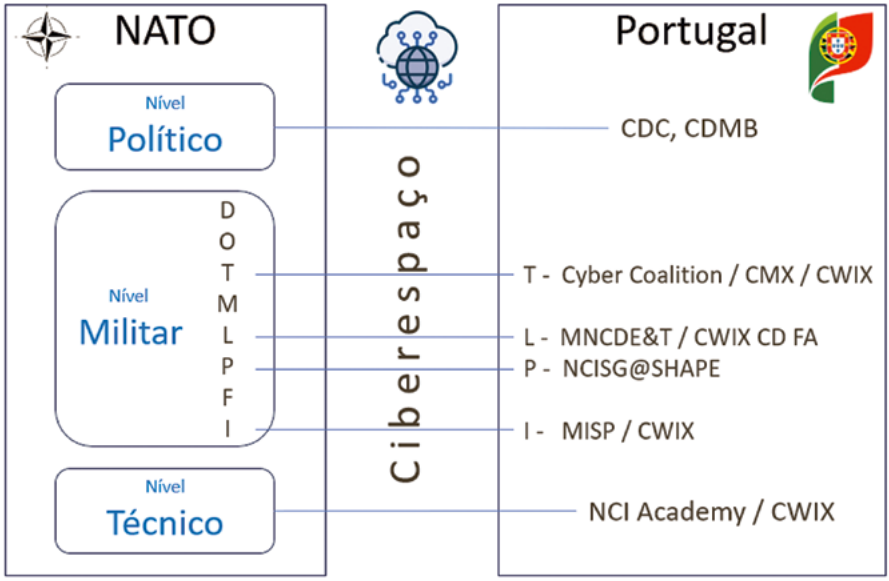
como um dos nove objetivos estratégicos na DEEMGFA 2018-21, que permitiu o foco no desenvolvimento desta capacidade.

Em 2022 foi promulgada a ENCD, alinhada com a ENSC, de 2019, tendo ambas o ciberespaço na sua base. Uma mais geral (ENSC), que engloba a cibersegurança, a ciberdefesa, o combate ao cibercrime, numa postura holística, de orientação e de alinhamento, aguardando-se a posterior promulgação de estratégias setoriais. A outra de caráter setorial (ENCD), para o caso específico da ciberdefesa, a qual pode originar alguns conflitos de análise, no caso de se tentar perceber uma hierarquia estrutural na organização do Estado nesta temática. Por outro lado, tendo em conta a terminologia de Ciberdefesa e Operações no Ciberespaço, seria interessante uma reflexão sobre estes dois termos em dois patamares diferentes, visando uma maior clarificação. Apresenta-se como proposta que o termo Ciberdefesa fique ao nível do MDN, numa vertente política, e as Operações no Ciberespaço ao nível do EMGFA, para a condução deste tipo de operações, à semelhança de outros países, trazendo desta forma maior coerência ao assunto, a que se deveria juntar uma Política para a Ciberdefesa.

Na ligação de Portugal à NATO, no nível político, podem referir-se as participações nas reuniões dos diversos comités e grupos. No nível militar, procurou igualmente seguir-se a metodologia DOTMLPFI, garantindo a coerência de análise. Assim, pode destacar-se, para além das alterações anteriormente referidas ao nível organizacional da ciberdefesa, que seguiram, no geral, as boas práticas internacionais e a elaboração do PDMC 3.20, tendo por referência a doutrina da NATO. Releva-se a participação nos exercícios *Cyber Coalition*, *Locked Shields* e *Crossed Swords*, estes dois últimos da responsabilidade do CCDCOE e, na área da liderança, o projeto de *Smart Defence MNCD&ET*, já concluído e cujo trabalho foi devidamente reconhecido, assim como a liderança portuguesa da *Cyber Defence FA*, do exercício CWIX, entre 2018 e 2021, que também teve o seu reconhecimento, e que poderia ser uma bandeira nacional presente neste 75.º aniversário da NATO. Relativamente à área do pessoal, destaca-se a colocação de um militar no NCISG e a nível da interoperabilidade a participação no MISP. O exercício CWIX, pelas suas características, âmbito e dimensão é transversal a mais de uma área. A NCI Academy, na dependência da NCIA, foi considerada como um contributo nacional no nível técnico.

Em termos finais, pode afirmar-se que a NATO e o ciberespaço, na sua exploração, têm uma relação de um quarto de século, a qual será cada vez mais profunda e dependente, como na maior parte das organizações, e onde Portugal também manterá a sua presença. A NATO continuará a enfatizar a proteção das suas redes e continuará a adaptar as suas políticas, estratégias, conceitos e capacidades no ciberespaço para enfrentar a crescente complexidade das diversas ameaças e desafios. Nestes incluem-se as *Multi Domains Operations*, pela exigência na interoperabilidade, estando o ciberespaço cada vez mais presente na cenarização dos exercícios, bem

Figura 1 – Relação de atividades/áreas de atuação em que Portugal participou de forma efetiva junto da NATO, no contexto do ciberespaço, nos níveis político, militar e técnico



DOTMLPFI – *Doctrine, Organization, Training, Material, Leadership, Personel, Facilities, Interoperability*

como nas questões ligadas à gestão de crises, através dos exercícios da série CMX. As novas tecnologias disruptivas, onde se insere a IA, também se constituem como desafios internos visando o melhor aproveitamento das suas funcionalidades, ou podem constituir-se como ameaças, no caso da sua utilização por parte de atores opositores, num contexto cada vez mais híbrido. Para além do elemento pessoas, o ciberespaço é virtual e físico e não se limita às redes da NATO, pelo que vai exigir novas formas de pensar, de trabalhar e de interagir seja vertical e horizontalmente, bem como interna e externamente, onde a gestão do risco é fundamental para um comandante, face à incerteza predominante. Assim, será reforçada a resiliência desta Aliança e dos países integrantes, através de uma postura robusta, tecnologicamente avançada e cooperativa.

Bibliografia

ACT (2023a). Empowering NATO's Multi-Domain Operations Through Digital Transformation. Disponível em https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/, consultado em 08Jan2024.

ACT (2023b). NATO Exercises to Enhance its Cyber Resilience & Exercise Cyber Coalition. Disponíveis em https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/; e https://www.act.nato.int/activities/cyber-coalition/, consultados em 09Jan2024.

ACT (2023b). NATO Exercises to Enhance its Cyber Resilience & Exercise Cyber Coalition. Disponíveis em https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/; e https://www.act.nato.int/activities/cyber-coalition/, consultados em 09Jan2024.

ACT (sd). Coalition Warrior Interoperability Exercise-CWIX. Disponível em https://www.act.nato.int/our-work/exercises/coalition-warrior-interoperability-exercise/, consultado em 10Jan2024.

AR (2014). Lei Orgânica n.º 6/2014 – Lei Orgânica de Bases da Organização das Forças Armadas, Assembleia da República (AR). Disponível em https://diariodarepublica.pt/dr/detalhe/lei-organica/6-2014-56384929, consultado em 12Jan2024.

AR (2018). Lei n.º 46/2018 – Estabelece o regime jurídico da segurança do ciberespaço, Assembleia da República (AR). Disponível em https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384, consultado em 12Jan2024.

AR (2019). Resolução da Assembleia da República n.º 221/2019 – Estatuto da NCIA em Portugal, Assembleia da República (AR). Disponível em https://files.diariodarepublica.pt/1s/2019/11/21400/0000700038.pdf, consultado em 13Jan2024.

AR (2021). Lei Orgânica n.º 2/2021 – Lei Orgânica de Bases da Organização das Forças Armadas, Assembleia da República (AR). Disponível em https://diariodarepublica.pt/dr/detalhe/lei-organica/2-2021-169256653, consultado em 12Jan2024.

Bigelow, B. (2017). Mission Assurance: Shifting the Focus of Cyber Defence. 9th International Conference on Cyber Conflict – Defending the Core. NATO CCD COE Publications, Tallinn. Disponível em https://ccdcoe.org/uploads/2018/10/Art-03-Mission-Assurance-Shifting-the-Focus-of-Cyber-Defence.pdf, consultado em 10Jan2024.

Blessing, J. (2021). Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain. Project MUSE. Brookings Institution Press, pp. 261-288. Disponível em https://muse.jhu.edu/pub/11/oa_edited_volume/chapter/3103404, consultado em 10Jan2024.

Boin, A., Hart, P., Stern, E., Sundelius, B. (2016). *The Politics of Crisis Management*, 2nd Edition. Cambridge University Press. https://doi.org/10.1017/9781316339756

Brent, L. (2019). NATO's Role in Cyberspace. Disponível em https://www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/NATOCyberspace.pdf, consultado em 06Jan2024.

Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, *Defence Studies*, 15:4, 297-319, DOI: 10.1080/14702436.2015.1108108.

Burton, J. e Lain., C (2020). Desecuritising cybersecurity-Towards a societal Approach. Tailor and Francis Group. https://doi.org/10.1080/23738871.2020.1856903. Disponível em https://www.tandfonline.com/doi/abs/10.1080/23738871.2020.1856903, consultado em 10Jan2024.

Carcelli, S. e Gartzke, E. (2017). The Diversification of Deterrence: New Data and Novel Realities. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.745. Disponível em https://oxfordre.com/politics/display/10.1093/acrefore/9780190228637.001.0001/

acrefore-9780190228637-e-745?d=%2F10.1093%2Facrefore%2F9780190228637.001.0001%-2Facrefore-9780190228637-e-745&p=emailAofSHchKzpCMs, consultado em 09Jan2024.

CCDCOE (2018a). The North Atlantic Treaty Organization (NATO). Disponível em https://ccdcoe.org/organisations/nato/, consultado em 06Jan2024.

CCDCOE (2018b). Portugal to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. Disponível em https://ccdcoe.org/news/2018/portugal-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-tallinn/, consultado em 13Jan2024.

CCDCOE (2020). Cyber Commanders' handbook. NATO CCDCOE publications. Tallinn.

CCDCOE (2023). The NATO CCDCOE welcomes new members Iceland, Ireland, Japan, and Ukraine. Disponível em https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/, consultado em 12Jan2024.

CCDCOE (sd). About us. Disponível em https://ccdcoe.org/about-us/, consultado em 12Jan2024

Coelho, J. (2018). O Ciberespaço na Defesa Coletiva e na Gestão de Crises: Articulação entre a Cibersegurança e a Ciberdefesa. Lisboa: Instituto Universitário Militar (IUM). Disponível em https://comum.rcaap.pt/bitstream/10400.26/24522/1/TII_CMG_SCoelho.pdf, consultado em 12Jan2024.

Cordey, S e Dewar, R. (2019). National Cybersecurity and Cyberdefense Policy Snapshots. Disponível em https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_2.pdf, consultado em 11Jan2024.

Couto, A. (2020). *Elementos de Estratégia – Apontamentos para um curso* – Vol I. Fundação Casa Carvalho Cerqueira. Leya.

DELNATO (2019). Última reunião do Projeto "Multinational Cyber Defence Education and Training" na sede da NATO. Disponível em https://otan.missaoportugal.mne.gov.pt/pt/noticias/ultima-reuniao-do-projeto-multinational-cyber-defence-education-and-training-na-sede-da-nato, consultado em 11Jan2024.

EDA (2023). Enhancing EU Military Capabilities Beyond 2040. Disponível em https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities--beyond-2040.pdf, consultado em 09Jan2024.

EMGFA (2018). Diretiva Estratégica do EMGFA 2018-2021. Disponível em https://www.emgfa.pt/Documents/2019/DiretivaEstrategicaEMGFA-2018-2021_Ver.2.pdf, consultado em 12Jan2024.

EMGFA (2021). Diretiva Estratégica do EMGFA 2021-2023. Disponível em https://www.emgfa.pt/Documents/2022/DIRETIVA%20ESTRAT%C3%89GICA%20EMGFA_2021-2023%20-%20Copy.pdf, consultado em 12Jan2024.

EP (2010). NATO Defending against cyber attacks. European Parliament. Disponível em https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf, consultado em 08Jan2024.

EP (2016). EU-NATO Joint Declaration, 8 July 2016, Warsaw. European Parliament. Disponível em https://www.europarl.europa.eu/delegations/en/dnat/documents/eu-texts, consultado em 08Jan2024.

Friedl, M. (2018). U.S. Joins NATO's Trident Juncture Exercise. US DoD. Disponível em https://www.defense.gov/News/News-Stories/Article/Article/1666272/us-joins-natos-trident-juncture-exercise/, consultado em 09Jan2024.

Got, A. (2020). NATO crisis management exercises: preparing for the unknown. Disponível em https://www.nato.int/docu/review/articles/2020/02/07/nato-crisis-management-exercises-preparing-for-the-unknown/index.html, consultado em 09Jan2024.

Goździewicz, W. (2019). Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA). *Cyber Defense Magazine*. Disponível em https://www.cyberdefensemagazine.com/sovereign-cyber/, consultado em 13Jan2024.

Grossman, T. (2023). Cyber Rapid Response Teams Structure, Organization, and Use Cases. Center for Security Studies (CSS), ETH Zürich, disponível em https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2023-11-Cyber-Rapid-Response-Teams.pdf, consultado em 12Jan2024.

Healey, J., Jordan, K. (2014). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. Atlantic Council – Brent Scowcroft Center On International Security, Washington. Disponível em https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf, consultado em 19an2024.

Honorato, M., Santos, L., Mateus, R. (2017). O ciberespaço como 5.º domínio operacional – Impacto estratégico na Política de Defesa Nacional. Lisboa: Instituto Universitário Militar (IUM). Disponível em https://comum.rcaap.pt/bitstream/10400.26/21956/1/07_TIG%20AEE%20-%20Ciberespa%C3%A7o%205%C2%BA%20Dominio%20de%20Opera%C3%A7%C3%B5es.pdf, consultado em 11Jan2024.

Hudson, P. (2022). Managing Cyber Risk to Mission at the Operational Level. The Three Swords 38/2022, pp 68-71. Joint Warfare Centre (JWC). Disponível em https://www.jwc.nato.int/application/files/1416/7092/6318/CyberRisktoMission_2022.pdf, consultado em 14Jan2024.

JALLC (2016). Joint Analysis Handbook 4th Edition. Disponível em https://www.jallc.nato.int/application/files/9416/0261/6056/Joint_Analysis_Handbook_4th_edition.pdf, consultado em 05Jan2024.

JAPCC (2017). NATO Joint Air Power and Offensive Cyber Operations. Joint Air Power Joint Air Competence Centre. Kalkar-Germany. Disponível em https://www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf, consultado em 10Jan2024.

JFCT (2022). CWIX 2022 poised to deliver a more interoperable, innovative Alliance. Disponível em https://www.jftc.nato.int/articles/cwix-2022, consultado em 10Jan2024.

Joubert, V. (2012). Five years after Estonia's cyber attacks: Lessons learned for NATO? NDC. Disponível em https://www.files.ethz.ch/isn/143191/rp_76.pdf

Kamel, M. e Gallup, S. (2022) Quantifying, Visualizing, and Tracking Capability Gaps. Naval Postgraduate School, Naval Research Program. Disponível em https://apps.dtic.mil/sti/pdfs/AD1184027.pdf, consultado em 09Jan2024.

Lewis, D. (2019). What is NATO really doing in Cyberspace? Texas National Security Review, Disponível em https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/, consultado em 08Jan2024.

MDN (2014). Decreto-Lei n.º 184/2014 – Lei Orgânica do Estado-Maior General das Forças Armadas, Ministério da Defesa Nacional. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/184-2014-65983261, consultado em 12Jan2024.

MDN (2015). Decreto Regulamentar n.º 13/2015 – Estrutura Orgânica do Estado-Maior General das Forças Armadas, Ministério da Defesa Nacional. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-regulamentar/13-2015-69920325, consultado em 12Jan2024.

MDN (2019). Portugal entrega formalmente escola da NATO que pretende responder aos desafios da Ciberdefesa e Cibersegurança. Disponível em https://www.defesa.gov.pt/pt/comunicacao/noticias/Paginas/Portugal-entrega-formalmente-escola-da-NATO-que-pretende-responder-aos-desafios-da-Ciberdefesa-e-Ciberseguran%C3%A7a.aspx, consultado em 11Jan2024.

MDN (2023). Decreto Regulamentar n.º 2/2023 – Estrutura Orgânica do Estado-Maior General das Forças Armadas, Ministério da Defesa Nacional. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-regulamentar/2-2023-214042394, consultado em 12Jan2024.

MJ (2016). Decreto-Lei n.º 81/2016 – Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/81-2016-105263934, consultado em 12Jan2024.

MNCDET (sd). Multinational Cyber Defence Education and Training Project (MN CD E&T). Disponível em https://mncdet.wixsite.com/mncdet-nato, consultado em 11Jan2024.

Monteiro, A. (2017) Portugal at Forefront of Global Cyber Initiatives. AFCEA – Signal – Cyber Edge. Disponível em https://www.afcea.org/signal-media/cyber-edge/portugal-forefront-global-cyber-initiatives, consultado em 11Jan2024.

NATO (2010a). Lisbon Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_68828.htm, consultado em 04Jan2024.

NATO (2010b). Strategic Concept 2010. Disponível em https://www.nato.int/cps/en/natohq/topics_82705.htm, consultado em 04Jan2024.

NATO (2013). Sharing malware information to defeat cyber attacks. Disponível em https://www.nato.int/cps/en/natolive/news_105485.htm, consultado em 11Jan2024.

NATO (2014). Wales Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_112964.htm, consultado em 04Jan2024.

NATO (2016). Warsaw Summit Communiqué. Disponível em https://www.nato.int/cps/en/natohq/official_texts_133169.htm, consultado em 04Jan2024.

NATO (2017). NATO Standardization Office (NSO). Disponível em https://www.nato.int/cps/en/natohq/topics_124879.htm, consultado em 08Jan2024.

NATO (2018a). Brussels Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_156624.htm, consultado em 05Jan2024.

NATO (2018b). Panel Discussion – ''Defence Cooperation in the EU and NATO: More European, More Connected, More Capable?'' Disponível em https://www.nato.int/cps/en/natohq/opinions_152237.htm?selectedLocale=en, consultado em 14Jan2024.

NATO (2021a). NATO 2030-Making A Strong Alliance Even Stronger. Disponível em https://www.nato.int/nato2030/, consultado em 06Jan2024.

NATO (2021b). Brussels Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/news_185000.htm, consultado em 05Jan2024.

NATO (2022a). Madrid Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_196951.htm, consultado em 04Jan2024.

NATO (2022b). Strategic Concept. Disponível em https://www.nato.int/cps/en/natohq/topics_210907.htm, consultado em 04Jan2024.

NATO (2022c). NATO Communications and Information Agency (NCI Agency). Disponível em https://www.nato.int/cps/en/natohq/topics_69332.htm, consultado em 07Jan2024.

NATO (2023a). Cyber defence. Disponível em https://www.nato.int/cps/en/natohq/topics_78170.htm, consultado em 04Jan2024.

NATO (2023b). Vilnius Summit Communiqué. Disponível em https://www.nato.int/cps/en/natohq/official_texts_217320.htm, consultado em 04Jan2024.

NATO (2023c). Digital Policy Committee (DPC). Disponível em https://www.nato.int/cps/en/natohq/topics_69279.htm, consultado em 11Jan2024.

NATO (2023d). Science for Peace and Security Programme. Disponível em https://www.nato.int/cps/en/natohq/topics_85373.htm, consultado em 11Jan2024.

NATO (2024). Principal officials. Disponível em https://www.nato.int/cps/en/natohq/who_is_who_51639.htm, consultado em 09Jan2024.

NATO PA (2009). NATO and Cyber Defence. NATO Parliamentary Assembly. Disponível em 2009 – 173 DSCFC 09 E BIS – CYBERDEFENCE – MYRLI REPORT.doc (live.com), consultado em 11Jan2024.

NATO SECGEN (2023). Speech by NATO Secretary General Jens Stoltenberg at the first annual NATO Cyber Defence Conference. Disponível em https://www.nato.int/cps/en/natohq/opinions_219806.htm, consultado em 9Jan2024.

NCIA (2014). MN CD2 Nations release tool to share cyber incident information. Disponível em https://www.ncia.nato.int/about-us/newsroom/mn-cd2-nations-release-tool-to-share-cyber-incident-information.html, consultado em 11Jan2024.

NCIA (2018). New NATO-Industry cyber partnerships signed at NITEC18. Disponível em https://www.ncia.nato.int/about-us/newsroom/new-natoindustry-cyber-partnerships-signed-at-nitec18.html, consultado em 11Jan2024.

NCIA (2020). NATO Platform to lay the foundations for services, apps and agility. Disponível em https://www.ncia.nato.int/about-us/newsroom/nato-platform-to-lay-the-foundations-for-services--apps-and-agility.html, consultado em 11Jan2024.

NCIA (2021a). NATO assists Mongolia in bolstering its cyber security posture. Disponível em https://www.ncia.nato.int/about-us/newsroom/nato-assists-mongolia-in-bolstering-its-cyber-security-posture.html, consultado em 11Jan2024.

NCIA (2021b). NATO assists Moldova in improving its cyber security capabilities. Disponível em https://www.ncia.nato.int/about-us/newsroom/nato-assists-moldova-in-improving-its-cyber-security-capabilities.html, consultado em 11Jan2024.

NCIA (2022). Introducing the NATO Communications and Information Academy. Disponível em https://www.ncia.nato.int/resources/site1/general/what%20we%20do/nci%20academy/nci_academy_brochure_web_2022_sep.pdf, consultado em 11Jan2024.

NCIA (sd). Who we are. Disponível em https://www.ncia.nato.int/about-us/who-we-are.html, consultado em 11Jan2024.

NCISG (sd). About us – NATO Communications and Information Support Group. Disponível em https://ncisg.nato.int/about-us, consultado em 10Jan2024.

Nunes, P. (2020). A Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Definição de uma Estratégia Militar para o Ciberespaço. Coleção "ARES", 36. Lisboa: Instituto Universitário Militar (IUM). Disponível em https://www.ium.pt/pub/65, consultado em 11Jan2024.

Nye, Joseph (2010). *Cyber Power*. Belfer Center for Science and International Affairs | Harvard Kennedy School.

PCM (2014). Orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança (CNCS). Disponível em https://files.diariodarepublica.pt/1s/2014/05/08900/0271202719.pdf, consultado em 11Jan2024.

PCM (2023). Decreto-Lei n.º 34/2023 – Cyber Academia and Innovation Hub (CAIH). Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/34-2023-213345452, consultado em 12Jan2024.

RCM (2013a). Conceito Estratégico de Defesa Nacional (CEDN). Resolução do Conselho de Ministros n.º 19/2013. Disponível em https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Conceito-Estrategico-de-Defesa-Nacional.pdf, consultado em 12Jan2024.

RCM (2013b). Reforma "Defesa 2020". Resolução do Conselho de Ministros n.º 26/2013. Disponível em https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Defesa-2020.pdf, consultado em 12Jan2024.

RCM (2019). Estratégia Nacional de Segurança no Ciberespaço (ENSC). Resolução do Conselho de Ministros n.º 92/2019. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962, consultado em 12Jan2024.

RCM (2022). Estratégia Nacional de Ciberdefesa (ENCD). Resolução do Conselho de Ministros n.º 92/2019. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924, consultado em 12Jan2024.

Ribeiro, A. (2010). *Teoria Geral da Estratégia – O essencial ao processo estratégico*. Coimbra: Almedina,

Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.

Shea, J. (2017). Cyberspace as a Domain of Operations. What Is NATO's Vision and Strategy? Disponível em https://apps.dtic.mil/sti/pdfs/AD1068701.pdf, consultado em 10Jan2024.

STO (sd). About the NATO Science and Technology Organization (STO). Disponível em https://www.sto.nato.int/Pages/default.aspx, consultado em 11Jan2024.

UK Gov (2020). Allied Joint Doctrine for Cyberspace Operations (AJP-3.20). Disponível em https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320, consultado em 05Jan2024.

UNDP (2021). UNDP's Strategic Plan 2022-2025: Designing for Complexity and Uncertainty. Disponível em https://www.undp.org/future-development/blog/undps-strategic-plan-2022-2025-designing-complexity-and-uncertainty, consultado em 09Jan2024.

Wright, N. (2019). Some Lessons From Command Post Exercise Trident Juncture 2018. Joint Warfare Centre (JWC)- The Three Swords Magazine, Stavanger Disponível em https://www.jwc.nato.int/application/files/4116/4680/4222/issue34.pdf, consultado em 09Jan2024.

Collateral Effects Forever: Militarization and Commercialization in NATO's Cyberspace Operations

Isabella Neumann
Universidade de Coimbra.

Abstract

This article explores the implications of cyberspace operations within NATO, shedding light on shifts in power dynamics, functions, and sectoral boundaries spanning military, civil, and private domains. These transformations reveal two pivotal potential dynamics: militarization and commercialization. As the significance of cyberspace operations continues to rise, the study ties together the pressing necessity for adaptive governance and strategic approaches to navigate evolving security landscapes within the Alliance and address the potential challenges.

Keywords: Cyberspace; NATO; Civil-Military Relations.

Resumo
Efeitos Colaterais Para Sempre: Militarização e Comercialização nas Operações do Ciberespaço da NATO

Este artigo explora as implicações das operações no ciberespaço dentro da NATO, elucidando sobre as mudanças nas dinâmicas de poder, funções e fronteiras setoriais que abrangem os domínios militar, civil e privado. Essas transformações revelam duas potenciais dinâmicas: militarização e comercialização. À medida que a importância das operações no ciberespaço continua a crescer, este estudo vincula a necessidade urgente de uma governança adaptativa e abordagens estratégicas para navegar pelas paisagens de segurança em evolução dentro da Aliança e enfrentar os potenciais desafios.

Palavras-chave: *Ciberespaço; NATO; Relações Civil-Militares.*

Artigo recebido: 26.03.2024
Aprovado: 13.04.2024
https://doi.org/10.47906/ND2024.168.03

1. Introduction

NATO began to pay close attention to cyber threats in earnest at the Prague Summit 2002. There, the alliance resolved to "strengthen [...] capabilities to defend against cyber-attacks"[1] (NATO, 2002, p. 53), heavily swayed by events that catalyzed a profound reorientation in its security agenda, such as the Y2K bug, the onset of cyberattacks during the Kosovo conflict, and the ensuing apprehensions surrounding terrorist exploitation of the internet and cyberterrorism in the aftermath of 9/11 (Burton & Lain, 2020).

The incidents in Estonia in 2007 and Putin's speech at the Munich Conference further underscored the necessity of a robust cyber defense strategy (Shuya, 2018), leading to the Bucharest Summit Declaration in 2008, where NATO acknowledged the need to "protect key information systems by their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber-attack" (NATO, 2008).

In 2011, the NATO Policy on Cyberdefense became effective, establishing clear priorities and strategies to address cyber threats (NATO, 2011). Later, following the Russian invasion of Crimea in 2014, a normative leap in NATO's cyber defense[2] posture took place. The Wales Summit Declaration of that year declared that cyber-attacks could reach a threshold threatening "national and Euro-Atlantic prosperity, security, and stability" (NATO, 2014), a sentiment echoed by Tosbotn and Cusumano (2020). This change in perception was further reinforced in subsequent summits, such as the one in Warsaw (2016), where cyberspace was referred to as a domain of operations alongside land, sea, and air (rather than merely an operational domain), and during the Brussels summit in 2018, when NATO set up a Cyberspace Operations Centre in Belgium to enhance situational awareness and coordinate operational activities within cyberspace.

1 Cyber attacks are characterized "by the use of instruments or technologies with the purpose of disturbing, sabotaging, intercepting, destroying or even modifying digital data or electronic systems or materials present in cyberspace" (Ragot, 2015, p. 57).

2 According to some authors, cyberdefense "[...] combines information assurance, computer network defense (to include response actions), and critical infrastructure protection with enabling capabilities (such as electronic protection, critical infrastructure support, and others) to prevent, detect, and ultimately respond to adversaries' ability to deny or manipulate information and/or infrastructure" (Bogatinov, Bogdanoski & Angelevski, 2016). According to the NATO Glossary of Terms and Definitions (2021), cyberdefense is "The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information, or other electronic systems, or the information that is stored, processed, or transmitted in these systems" (NATO, 2021).

Therefore, it soon became evident that cyberspace operations extend far beyond mere network protection, evolving into a matter concerning "the integrity of democratic institutions in NATO countries" (Shea, 2017, p. 166).

Last year, the Vilnius Summit Communiqué (2023) made it clear that NATO's cyber effort relies heavily on significant technology companies, demonstrating its dependence on these private enterprises. As mentioned, NATO "Agreed to continue our work on multi-domain operations, enabled by NATO's Digital Transformation, which further drives our military and technological advantage, strengthening the Alliance's ability to operate decisively across the land, air, maritime, cyberspace and space domains" (Ibid., 2023).

The involvement of diverse actors in NATO's cyberspace operations – including the military forces, civil bureaucracies, and private companies – presents a multifaceted defense landscape that extends beyond traditional boundaries (Buzan *et al*., 1998) and that has become a central concern for the alliance (NATO, 2014). Offering unique insights into broader international relations and security dynamics across various levels (Buzan *et al*., 1998; Kikuchi & Okubo, 2019), it is undeniable that cyberspace operations influence the restructuring of functions, borders, and responsibilities of the military, civil, and private authority, as well as the harmonization of norms and practices across diverse sectors (Heeren-Bogers *et al*., 2020; Pačka & Mareš, 2021). All these points deserve attention and should be analyzed.

Here, however, the goal is simple and specific: this article seeks to delve into the repercussions arising from the possible dynamics of militarization and commercialization, catalyzed by the reorganization of civil, military, and private sectors in reaction to cyberspace operations within NATO's framework. Incorporating existing studies such as those by Shea (2017), Aggarwal and Reddie (2018), and Pion-Berlin *et al*. (2020), this research endeavors to build upon their findings and insights.

These two dynamics have been selected for examination primarily due to their profound impact on shaping the contemporary cyberspace landscape, as well as influencing critical aspects of security, governance, and international relations. Furthermore, they play a pivotal role in shaping strategic decision-making, driving technological advancements, and molding the evolving nature of conflicts in the digital age. Given their significant influence on policy and strategy formulation, delving into their complexities and implications to foster a more comprehensive understanding and facilitate informed decision-making is an aim that is always welcomed.

This study examines NATO's cyber approach, drawing from both NATO publications and existing literature. It then proceeds to analyze the potential impacts of militarization from a constructive perspective and the effects of commercialization from a civil-military perspective. Ultimately, it concludes by showing how the prospective implications of militarization and commercialization from NATO's cyberspace

operations have the potential to reshape and impact NATO's foundational principles of democracy and governance.

2. Cyber in NATO

The joint transnational responsibility for cohesion among actors across various NATO sectors indicates a fluidity in delineating borders during defense activities (Feaver, 2009; Pačka & Mareš, 2021; Ellison, 2022). This phenomenon is comprehensively explained due to the multidimensional nature of threats, which blurs the boundaries between the public and private sectors and between civil and military domains (Efthymiopoulos, 2019), sustaining a grey zone[3] (Cusumano & Corbe, 2018; Jacobsen, 2021) that significantly impacts the interaction among the key stakeholders.

This underscores why cyberspace operations remain a compelling subject for in-depth analysis. Different from traditional warfare, the effects of cyberspace operations unfold with less visibility (Gomez, 2016), making it challenging to discern both the providers and recipients of security. Furthermore, the potential for militarization and commercialization of security is an imminent concern (Ehrhart, 2017; Ahmad, 2020), emphasizing the necessity for thoroughly comprehending their implications.

For NATO, the treatment of cyber materializes through several security interconnected branches since its structure is rooted in the perception that "everything associated with the global cyberspace domain (…) could impact the security, safety, missions and/or the environment where NATO operates" (Domingo *et al.*, 2021, p. 509). In other words, cyber operations cross broadly along the conflict spectrum (Cavelty & Egloff, 2019).

As cyberspace operations expanded politically and technologically, the classification of cyberspace as a security concern introduced complexities that necessitated distinct approaches from civil, military, and private sector perspectives (Ehrhart, 2017; Ahmad, 2020).

The point is that the contribution of the military, civil, and private sectors is essential for NATO to achieve its principles of prevention, resilience, and non-duplication in the cyber defense realm (Hristov, 2018). Regarding prevention, which is to strengthen the capacity so that attacks do not occur, and resilience, which is to know how to remain resistant to attacks that have already happened (NATO, 2011), NATO has been updating new training programs to adapt its forces to the latest threats of the system that go beyond the traditional and classic ones. The Alliance already

3 We understand "grey zone" as a "zone conflicts are characterized by the opacity of the parties involved and relative uncertainty about the relevant policy and legal frameworks that apply to them" (Kapusta, 2015).

understands that only military measures are not enough when fighting and that coordination with the private and civil actors is necessary (Hristov, 2018), essentially because the threats "target all aspects of states and their societies, which must be able to collectively prevent, resist and recover from aggressive action when and if required" (Zekulić *et al*., 2017, p. 32).

On the principle of non-duplication, it touches directly on the civil and military exercises issue because it demonstrates that the "joint employment of military forces and civil resources for protection can help make it much 'smarter' and more efficient" (Štitilis; Pakutinskas & Malinauskaitė, 2017, p. 5). In other words, cyber security brings outcomes that must be dealt with extensively because such outcomes are not limited to only specific sectors. It is worth noting here that NATO is aware of these challenges, as civil-miliary coordination is one of the Alliance's most excellent intentions for its members (Robinson, 2021), but defining the military role in cyber defense is arduous. Some authors claim that the military cannot help in a cyber defense context because its primary focus, protecting borders, simply does not exist (Cavelty & Egloff, 2019). Others consider the investment in the military legitimate because they see that cyber attacks mainly occur between national states and, therefore, active military forces can contribute to other strategic steps (Kallberg & Cook, 2017; Lewis, 2018).

Determining the roles within NATO's cyberspace operations is thus a multifaceted issue that hinges on questioning the role of the military forces, mainly as operations fluctuate between 'hot' and 'cold' circumstances[4] (Soeters, 2018). The transformation and modernization of the military forces to adapt to cyberspace operations involve adjusting to a context that demands multitasking and assuming different responsibilities[5] (Cornish, 2021).

As a result, "the community of like-minded democracies gathered under the NATO umbrella is challenged as never before by diverse and dynamic cyber threats" (Stevens *et al*., 2021, p. 4). Despite the roadmaps already presented on cyber defense (Romansky *et al.*, 2019) and the advances within CIMIC (Anwar & Yamin, 2021; Lutsenko *et al.*, 2021), we note that the lack of guidance from political leaders persists in accommodating the cited effects during the NATO cyber defense exercise (Pačka & Mareš, 2021). Cusumano & Corbe (2018) report that since the Cold War, the relationship between the military, civil, and private sectors was marginalized or treated only as

4 "'Cold' peacetime and routine conditions resemble conventional organizations. The other operates in 'hot' conditions, during crisis and peace operations or outright war" (Soeters, 2018, p. 1).

5 Multitasking and playing different roles is a quality that Heeren-Bogers *et al.,* (2020) call "ambidexterity" and it is based on the ability not to lose its identity and the ability to carry out primary activities while updating to new demands such as natural disasters, humanitarian and migratory crises, and anti-terrorism activities. In terms of Soeters (2018), "to bond and bridge" or in terms of Zhaohong (2022), "Top-Down Innovation and Bottom-Up Adaptation".

guides for other domains, such as intelligence, which, while significant in terms of expertise and formulations of NATO centers of excellence, may be insufficient to provide viable responses to an unbalanced linkage among the actors.

The study of civil, military, and private relationships along with cyber operations seems limited mainly by the perspective of activities, cooperation, and civil-military interaction (Heeren-Bogers *et al.*, 2020), which aims to improve their strength and intelligence in tasks. So, although a study on military missions and civil-military relations was carried out by Wilén and Strömbom (2022) and Harig, Jenne, and Ruffa (2022) – the latter being very useful in indicating the "variables that have been shown to influence important aspects of the military, notably behavior, restraint, and force posture" (Harig *et al*., 2022, p. 9) –, we still do not have considerable researches about the implications of the civil, military and private reorganization as result of NATO's cyberspace operations.

More discussion needs to be held about how the reorganization of sectors influences and potentially yields outcomes for the Alliance. The consequences of reorganizing civil, military, and private sectors are often perceived as unchanging and stable, with minimal consideration for how power distribution, responsibilities, and functions shape new dynamics. Studies predominantly concentrate on enhancing coordination from a technical perspective, disregarding potential conflicts and repercussions. Therefore, delving into the influences of cyberspace operations, particularly those that might exacerbate the dynamics of militarization and commercialization, is a good start.

3. Militarization Processes

Militarization may arise as a plausible consequence of reorganizing boundaries between civil, military, and private sectors driven by cyber operations, which increasingly allocate security-focused roles and responsibilities among these domains. Let us explore how this process unfolds, beginning with examining the Theory of Securitization.

Nicholas Onuf introduced the concept of securitization in 1989 through his constructivist approach to International Relations, which underscores world politics' ideational and intersubjective nature. Constructivism suggests that social realities and facts are shaped by human actions rather than existing as independent entities. This perspective, recognizing the role of human interactions and perceptions in forming the international system, gained traction, particularly after the unexpected end of the Cold War, a phenomenon not anticipated by neorealist and neoliberal theories (Onuf, 1989; Adler, 2004).

Expanding on constructivist principles, the Copenhagen School, led by thinkers like Williams (2003) and Buzan *et al.* (1998), introduced the Theory of Securitization. This

theory frames security as an inherently political and social process, emphasizing the role of language and speech acts in constructing threats. The School's empirical approach to security processes examines how issues become labeled threats, justifying extraordinary responses such as military action contingent upon societal acceptance (Buzan *et al*., 1998; Betz & Stevens, 2013).

In this framework, issues range from being non-politicized to politicized and ultimately securitized, involving different actors like referent objects (those demanding protection), agents (who initiate securitization), and functional actors (who influence security dynamics). This approach significantly broadened the range of perceived threats and referent objects, particularly in the context of identity and societal security (Buzan & Hansen, 2012, p. 71).

Although some scholars critique the politicization of defense and the widespread use of war rhetoric, these dynamics are evident in cyberspace operations (Libicki, 2012; Lawson, 2013). Cyber threats, which were previously not considered, have now been placed within the security category.

Militarization is a broad phenomenon in which military procedures and models become present in civil activities (Zaverucha, 2010), entering spheres beyond the traditional function of protecting the territory from external enemies. In Bonacker's (2018, p. 2) definition, militarization is "the transformation of security as increasingly thought to be something provided by the military or military means and thereby marginalizing other civilian approaches to security" (Bonacker, 2018, p. 2). For the purpose at hand, it is essential to explore two primary pathways through which militarization occurs: the first is through politicization, and the second is through transformations in the organizational practices of security (Bonacker, 2018).

First, militarization comes from politicization when agents bring the way of dealing with social problems closer to military practices, making them part of the military security sector (Henry & Natanel, 2016). As stated earlier, referent objects require protection because they come to be considered significant for state or organization sovereignty. Such developments require new adoptions of specific military doctrines and strategies that are not fully clear or explicit for other state and non-state actors in the international and domestic arena, promoting ambiguity of purposes capable of generating political tension (Poirier, 2021). In doing so, militarization changes the way threats are faced (Mabee & Vucetic, 2018), with military action increasingly being perceived as appropriate and necessary to protect referent objects (Bonacker, 2018) – this concept aligns more closely with the notion of securitization.

For instance, while an organization's network may be the primary target, individuals could experience repercussions at home, such as compromised email systems. Suppose a securitizing agent convinces an audience that this risk to personal emails constitutes the organization's security. In that case, the issue transcends normal bureaucratic processes and becomes a security threat, potentially warranting a

military response. In other words, when "there is no public or private violence. There is only violence that becomes 'public' and violence that becomes 'private'" (Owen, 2008, p. 979).

This dimension likely has implications for democracy issues because, although it operates through the democratic course that helps stability and accountability (Rosenberger, 2020), the politicization of the problem leads to militarization because military means *par excellence* become more present in tasks and approaches in both planning and strategy areas as they have more significant contact with the civilian population (Olszewski, 2016) – even in organizations that are already based on the military, there will be "new" areas to be militarized. Cyber operations blur the traditional boundaries between the civil, military, and private sectors. This often leads to the military occupying roles and spaces previously not within its domain, redistributing responsibilities, functions, and powers (Bruneau, 2020; Pion-Berlin *et al*., 2020).

The second way of looking at militarization is through restructuring security practices that occur when an organization intends to achieve security but intends to avoid following through with political debate. Since "organizations are often not allowed to participate in politics but have to stick to their operational task" (Bonacker, 2018, p. 10), militarization can arise from established security practices that are not even presented for public debate because they are typically routinized, as the use of technologies for border surveillance, for instance (Bonacker, 2018). For that, what counts for the organization is a specific combination of necessary conditions for this desire to fight to be put into practice, such as resource feasibility and risk perception (which changes depending on the state regime) (Aggarwal & Reddie, 2018, p. 8) and pre-existing rivals (Maness & Valeriano, 2015). The version of security turns theirs, and the instruments to achieve it can be created through a technical production of security that comes from the routines of bureaucratic decisions, something that is processed outside the political arena and that can encourage the military to broaden its jurisdiction to act on its logic and expertise (Elbe & Richter, 2012).

Moreover, militarization is also perpetuated by politically driven actors who shape and broaden security practices without democratic oversight (Szenes *et al*., 2021). This escalation of militarization bears significant consequences for an organization's democratic fabric, blurring the lines between civil, military, and private security realms by introducing new actors, threats, tasks, technologies, and targets into play, thereby linking these dynamics (Owens, 2008; McCarthy, 2018; Nøkleberg, 2020) that potentially affect their member states.

However, the imperative of maintaining an organization that, at the very least, the military remains subordinate to civilian control for strictly military purposes is a fundamental pillar of democracy (Bove *et al*., 2020). Suppose the organization faces challenges from crescent militarization, there will be a potential underminer of dem-

ocratic values due to its intrusive security practices, impacting NATO's objectives (Bonacker, 2018; Hanağası, 2022)

Another notable characteristic that comes along with militarization is the blurred distinction between defensive and offensive cyber capabilities. While the primary objective of cyber defense is the protection of an organization's critical infrastructure and sensitive data, many organizations have concurrently developed offensive cyber capabilities. These capabilities serve not only as a deterrent against potential adversaries but also as a means of retaliatory action in response to cyber threats. This dual-purpose nature of cyber capabilities has raised complex ethical and legal quandaries, particularly concerning using force within the cyber domain (Gomez, 2016; Olszewski, 2016; Poirier, 2021).

As the stakes in cyberspace continue to rise, the militarization of cyberspace operations has engendered international tensions and rivalries (Ooijen, 2020; Salminen & Kerttunen, 2020). Accusations of cyberattacks between different actors have become increasingly commonplace, and attributing such attacks poses significant challenges. This state of affairs has engendered diplomatic disputes, the imposition of sanctions, and the consideration of cyberattacks as acts of war under certain circumstances.

Anyhow, an outcome of this transformation is a substantial increase in budgets and investments allocated to cyberspace operations (Jacobsen, 2021). NATO has committed significant financial resources to bolster its cyber defense capabilities, responding to the evolving landscape of modern warfare where cyber threats pose significant challenges. This encompasses funding for technology development, cybersecurity training programs, and recruiting skilled personnel, reflecting a broader trend towards militarization in non-traditional domains of warfare.

Lastly, the militarization of cyberspace operations, as highlighted by Jacobsen (2021) and Poirier (2021), raises concerns about unintended consequences for civilian infrastructure. Cyberattacks targeting critical systems like power grids, healthcare facilities, and financial networks can lead to widespread societal disruption. This dynamic requires organizations to balance safeguarding national security interests and minimizing collateral damage to civilian assets. As reliance on digital infrastructure grows, so does the imperative to enhance cybersecurity measures while mitigating the broader impact on civilian populations and essential services.

Given these escalating dynamics, there is an emergent need to establish international norms and agreements to govern cyberspace. Endeavors such as the Tallinn Manual and the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) seek to delineate rules and norms for responsible state conduct in cyberspace.

4. Commercialization Process

The increasing demand for cyber defense arose from the realization that cyberspace could cause significant damage to states and their infrastructures, highlighted by events such as the 2008 conflict between Georgia and Russia (Chivvis & Dion-Schwarz, 2017; Carvalho, 2018). This has underscored to NATO that cyber-attacks can be just as destructive as conventional military threats (Iftimie, 2020).

As a result, organizations have had to integrate the cyber domain into their defense frameworks, adopting new doctrines, weapons, institutional models, strategies, specialists, private actors, and even concepts such as cyber power and cyber warfare. It is worth noting that cyber power encompasses all power exercised entirely or partially through cyberspace, while cyber warfare refers to conflicts conducted within this digital realm (Clarke & Knake, 2015; Betz, 2017).

Introducing the Civil-Military theory is pertinent in this context. Civil-military relations are founded on the principle that civilians, who are accountable and prudent, should govern state affairs, and the military should obey them (Owens, 2008; Anwar & Yamin, 2021). The Civil-Military relations theory grapples with the central dilemma of "Who guards the guardians?". This question underscores the challenge of maintaining control over a military force capable of defending yet potentially dominating the state (Bruneau & Matei, 2008, p. 915; McMahon & Slantchev, 2015). While this issue is already significant— as mentioned earlier, determining the military's placement is already a question— the complexity magnifies when the private sector enters the equation, promoting the commercialization of security.

Cyber defense processes signify a dynamic evolution in how security is conceptualized, warfare is conducted, and the traditional state monopoly on violence is questioned. Historically, the state maintained this monopoly, but its exclusivity has waned with the long-standing trend of "privatization of security." Additionally, supranational defense organizations like NATO are pivotal in shaping modern security paradigms influencing how cyber threats are addressed globally.

Therefore, the national Armed Forces are no longer solely responsible for security. They are increasingly supported by private companies and supranational organizations, which provide flexibility and specialized expertise to the security landscape (Singer, 2008).

Hiring employees or companies to carry out security tasks has become prevalent once more[6] since the end of the Cold War. For some authors, it happened because

6 The "traditional" definition of public/private strongly appeared during the Napoleonic wars, in which the need for a loyal and honored national army that shared the same objectives as the state made the model of national security forces a tonic element of the modern state (Brancoli, 2010). During the modern period, the Armed Forces were considered a national force that aspired to the collective good of promoting the state and its citizens since, in this way, greater state control

the number of actors participating in the conflict grew, and the technical competence to deal with them demanded training and speed that was not satisfactorily found in the state military force (Paoliello, 2016). Others argue that political expediency for the state, including simplifying bureaucracy, reducing accountability and transparency in operations, minimizing external effects, and exploiting gaps in the judiciary system, constitutes significant reasons for outsourcing security (Hillebrand, 2014; Kruck, 2014; Lindahl, 2015).

Outsourcing is a prevalent practice in the domain of free enterprise, particularly within the cyber domain, which has its roots and development closely intertwined with private firms. This close association suggests that questioning security privatization in the cyber realm may not even be pertinent, as cybersecurity was fundamentally born within the private sector (Pattison, 2020).

Faced with the extreme technique, know-how, and expertise about potential vulnerabilities involved in the processes, cyber defense calls for outsourcing given the constant speed and updates necessary to conduct its activities- being it "to a large extent a privately traded commodity" (Broeders, 2021, p. 4). Besides that, the private sector is fundamental for the agility of the crisis management of states or member states organizations (Pačka, 2019; Lehto & Limnéll, 2021), mainly because these actors do not seem to evolve at the same speed in terms of innovation and response time (Boeke *et al*., 2015; Collier, 2018; Romanosky *et al.,* 2019; Marrone & Sabatino, 2021). Cusumano and Kinsey (2022) reinforce that the advancement of technological innovation and outsourcing go hand in hand since the gap between policymakers or strategists and IT specialists makes states highly dependent on the private sector, which plays a significant role in cybersecurity governance[7].

However, we should not forget yet from the constructivism part of this research, which remembers us that these definitions of private and public are built and "powerful states can organize force in a manner that appears to be 'private' and/or foreign because this reduces political scrutiny" (Owens, 2008, 1986).

Anyway, as a result of this dynamic, there arises a need to redefine the distribution of responsibilities among civil, military, and private actors, putting them in a constant state of flux, requiring ongoing reassessment and adaptation. This evolution prompts critical questions about whether it is prudent for NATO to delegate authority and responsibility for the national defense of its member states, especially given the

was possible. In pursuit of imperialism, the delegitimization of the private sector was carried out by the dominant ideology and power, which defined what was public and private and how the war should develop (Owens, 2008).

7 As pointed out by Cavelty and Egloff (2019), those who currently own the most data and digital infrastructures are such companies. The US, for example, uses its cyberdefense strategies already assuming private partnerships (Carr, 2016), mainly after several cooperation stalemates that provoked shifts in the federal legislature (Fidler, Pregent & Vandurme, 2013).

challenges in sharing timely and sensitive information between the public and private sectors (Zibak & Simpson, 2019; Broeders, 2021) – although, as mentioned above, remains challenging to envision a scenario where the private sector does not play a significant role in assisting the state.

Even so, this questioning is necessary because decisions involving defense reach broad audiences and strengthen a politicization of the cyber theme that goes beyond its private space and passes to penetrate also into public spheres, generating debates about possible insecurities in proportions that even come to contest the legitimately instituted civil political authority (Cornish, 2021). Given their widespread presence across multiple jurisdictions, substantial scale, and technical expertise, these companies[8] employ various political constructs, thereby influencing the definition of what necessitates protection and fueling an escalation in the requirement for security measures (Egloff, 2018; Broeders, 2021).

Furthermore, private entities' pursuit of strategic cyber defense objectives may not ideally suit a civil-military balance (Cornish, 2021) because it introduces private interests into defense matters, potentially conflicting with public interests and democratic governance (Calcara *et al*., 2020; Pattison, 2020). In other words, on the one hand, the civil sector lacks complete control over defense operations, while on the other hand, there is inadequate accountability to society as a whole.

Despite guidance policies from those who hire them, the private agents that play a role as political agents act far from the essential protection function and approach the profit and market efficiency arena (Pattison, 2020). It is a concern because while state members of an organization cannot fail to rely on modern, up-to-date, and competent private companies, increasing the use of such companies represents a risk to the civil structure. After all, "the more infrastructure and services are provided by cyber mercantile companies, the more they will use their political power to advocate for their authority in making autonomous security claims to defend their monopolistic enterprises" (Egloff, 2018, p. 270). It causes "harm without going into the realm of emergency or exceptionality" (Backman, 2022, p. 60) since it continues to influence political will, obtain privileged information, and reduce other response capabilities (Harknett & Smeets, 2022).

In addition, there are dangers related to the problem of attribution (Nocetti, 2018) and legitimacy (Broeders, 2021) since private companies operate in complex environments where the lines between their activities and clients (governments, corporations, etc.) can become blurred. This ambiguity makes it difficult to determine whether the private company carried out a particular action under specific orders or on its initiative. Regulation (Sales, 2018; Cruz & Pedron, 2020) is also not easy because no

8 For Collier (2018), there is an active political role performed by these firms and he presents *Google* and *Microsoft* as examples.

comprehensive international regulatory framework is tailored explicitly to private companies that deal with security. This gap allows them to operate in regions where laws and regulations are either weak or poorly enforced, potentially exacerbating conflicts or destabilizing fragile environments.

More can be said about contract disputes (Anstett & Pullen, 2014) that often stem from disagreements over the interpretation of terms and ambiguities in initial expectations (Anstett & Pullen, 2014). Additionally, moral considerations come into play, questioning whether organizations fulfill their obligations to their member states when outsourcing security functions. According to Pattison (2020, p. 240), if states fail to protect their citizens or interests, as they potentially invest in firms, they may be seen as not fulfilling the social contract whereby citizens grant authority in exchange for protection. This moral dimension underscores broader concerns about accountability and the ethical implications of privatizing military and security responsibilities and can also be applied to organizations such as NATO.

Consequently, weaknesses can infiltrate NATO when member states relinquish control over regulatory and strategic defense matters to private military contractors, eroding political cohesion and commitment among members. Furthermore, deficiencies may arise within the military sector, stemming from potential inefficiencies in addressing defense issues independently of the organization (Calcara *et al*., 2020). This is due, for instance, to the inequality in access to cybersecurity provisions, which creates a sense of insecurity for those unable to afford enhanced protection, a phenomenon known as deflection (Pattison, 2020).

Moreover, it occupies a capacity for civilian work that, because it is part of a competitive market, is not always available at times of urgency in civil structures (Zekulić *et al*., 2017, p. 31). Thus, the potential externality of private cyber defense activities to provide democratic accountability is in there. While regulating this market is complex due to the range of varieties and functions that the private sector performs, it is known that "the challenges they pose to existing domestic and international law, civil-military relations, and political accountability are huge" (Owens, 2008, p. 977).

On the military side, the challenge presented to the military forces is to adapt their operating concepts to the information environment (Cardon, 2016, p. 16) while still being responsive to the civil command that administers them (Spidalieri & McArdle, 2016). This is complex because the policy decision for cyberdefense needs to be in harmony with the norms, beliefs, forms of interaction, and attitudes made by civilians and implemented by the military in all areas of defense (Segell, 2021) since the information revolution "informationized all conventional warriors" (Schneider, 2019, p. 843).

Besides, more questions were raised about how the military forces should use technology and "what constitutes military use in a domain where civilian and military users are inextricably entangled, and in which many cyber capabilities that are not military in

purpose can be used to generate militarily relevant effect" (Inkster, 2017, p. 28). So, it turns out that governments struggle to organize civil and military capabilities to achieve a joint response to the current cyber challenges in some organizations, such as NATO (Inkster, 2017, p. 29).

Navigating the cyber domain necessitates that NATO member states effectively integrate their offensive cyber capabilities into alliance operations. This strategic alignment aims to secure victories in future conflicts and mitigate potential tensions among Allies that might arise from unilateral cyber initiatives to protect critical infrastructure (Iftimie, 2020). Addressing these challenges requires enhanced coordination across all sectors, fostering trust, joint action, information sharing, and clearly defined responsibilities (Lété & Dege, 2017; Ablon *et al.*, 2019).

5. Conclusion

In conclusion, reorganizing boundaries across civil, military, and private sectors in response to cyber operations carries profound implications for global security, a concern underscored by entities such as NATO. The politicization and adaptation of security practices within organizations have notably augmented military involvement in domains historically managed by civilians, amplifying the risk of conflict escalation and reshaping threat perceptions. Moreover, the increasingly blurred distinction between defensive and offensive cyber activities has prompted intricate ethical and legal inquiries.

Furthermore, substantial increases in funding and investment for cyber defense have heightened the demand for skilled cybersecurity professionals, rendering the field more attractive and signaling the likely expansion of militarization.

Conversely, privatizing security, particularly in cyber defense, introduces challenges to competency, accountability, and the potential conflict between private interests and public governance.

The necessity for international norms and agreements governing behavior in cyberspace has become increasingly apparent, particularly amid mounting accusations of cyberattacks and the potential for diplomatic disputes and sanctions. The ramifications of militarization and commercialization are pivotal in this evolving landscape, where distinctions between civil, military, and private sectors undergo continuous redefinition.

Addressing these challenges effectively mandates coordinated efforts among all engaged sectors, fostering mutual trust, collaborative action, information sharing, and clear delineation of responsibilities in cyber defense. As the cyber domain expands, achieving equilibrium among these sectors is crucial for managing the implications of militarization and commercialization while safeguarding national security interests

and upholding democratic values. This complex issue remains central to governments and policymakers within the framework of NATO.

References

Ablon, L., Binnendijk, A., Hodgson, Q. E., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. A. (2019). *Operationalizing cyberspace as a military domain: Lessons for NATO*. RAND CORP ARLINGTON VA.

Adler, E. (2004). *Communitarian international relations: The epistemic foundations of international relations*. Routledge.

Aggarwal, V. K., & Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: a Framework for analysis. *Journal of Cyber Policy*, 3(3), 291-305.

Ahmad, N. F. (2020). *Brave New World: NATO, the EU and the New Age of Cyberspace.* Master's thesis. Department of Political Science, University of Oslo.

Anwar, S. S., & Yamin, T. (2021). Civil-Military Cooperation (CIMIC) in Cyber Security Domain.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, 44(2), 147-164.

Bogatinov, D. S., Bogdanoski, M., & Angelevski, S. (2016). AI-based cyber defense for more secure cyberspace. In *Handbook of Research on Civil Society and National Security in the era of cyber warfare* (pp. 220-237). IGI Global.

Bonacker, T. (2018). The militarization of security. A systems theory perspective. *Critical Military Studies*, 5(3), 276-294.

Broeders, D. (2021). Private active cyber defense and (international) cyber security – pushing the line? *Journal of Cybersecurity*, 7(1).

Bruneau, T. C., & Matei, F. C. (2008). Towards a new conceptualization of democratization and civil-military relations. *Democratization*, 15(5), 909-929.

Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: Towards a societal approach. *Journal of Cyber Policy*, 5(3), 449-470.

Buzan, B., & Hansen, L. (2012). *A evolução dos estudos de segurança internacional*. São Paulo: UNESP.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for Analysis*. London: Lynne Rienner Publishers.

Calcara, A., Csernatoni, R., & Lavallée, C., eds. (2020). *Emerging security technologies and EU Governance: Actors, practices, and processes*. Abingdon: Routledge.

Cavelty, M. D., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles Of the state. *St Antony's International Review*, 15(1), 37-57.

Clarke, R. A., & Knake, R. K. (2015). *Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito*. Brasport.

Cornish, P., ed. (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press.

Cusumano, E., & Corbe, M., eds. (2018). *A civil-military response to hybrid threats*. London; New York: Palgrave Macmillan.

Cusumano, E., & Kinsey, C. (2022). Advancing private security studies: Introduction to the special issue. *Small Wars & Insurgencies*, 33(1-2), 1-21.

Domingo, A., Pastor, V., Parmar, M., & Foote, S. (2021). Enabling NATO Cyberspace Operations by Building Comprehensive Cyberspace Situational Awareness. In *International Conference on Cyber Warfare and Security* (pp. 509-XIV). Academic Conferences International Limited.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense, and innovation at NATO. *Journal of Innovation and Entrepreneurship*, 8(1), 1-26.

Egloff, F. J. (2022). *Semi-state Actors in Cybersecurity*. Oxford University Press.

Ehrhart, H.G. (2017). Postmodern warfare and the blurred boundaries between war and peace. *Defense & Security Analysis*, 33(3), 263-275. https://doi.org/10.1080/14751798.2017.1351156

Ellison, D. (2022). The Screenwriter's Guide to NATO Civil-Military Relations. Military Strategy Magazine, 7 4, 39-44.

Feaver, P. D. (2009). *Armed servants*. Harvard University Press.

Gomez, M. A. N. (2016). Arming cyberspace: The militarization of a virtual domain. *Global Security & Intelligence Studies*, 1(2), 27786.

Hanağası, U. B. (2022). State's soldier or soldier's state: A glance at civil-military relations theory. *Journal of Human Sciences*, 19(3).

Harig, C., Jenne, N., & Ruffa, C. (2022). Operational experiences, military role conceptions, And their influence on civil-military relations. *European Journal of International Security*, 7(1), 1-17.

Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45(4), 534-567.

Heeren-Bogers, J., Moelker, R., Kleinreesink, E., Van der Meulen, J., Soeters, J., & Beeres, R. (Eds.) (2020). *The Yin-Yang Military: Ambidextrous Perspectives on Change in Military Organizations*. Springer Nature.

Henry, M., & Natanel, K. (2016). Militarisation as diffusion: The politics of gender, space And the everyday. *Gender, Place & Culture*, 23(6), 850-856.

Hillebrand, G. R. L. (2014). A privatização da guerra? a participação das empresas militares privadas em conflitos armados e o papel do Estado enquanto ator internacional.

Hristov, N. (2018). Nato Resilience, Deter and Profesional Military Education. *International E-Journal of Advances in Education*, 4(10), 72-76.

Huntington, S. P. (1981). *The Soldier and the State: The Theory and Politics of civil-military Relations*. Harvard University Press.

Iftimie, I. A. (2020). NATO's needed offensive cyber capabilities.

Inkster, N. (2017). Measuring military cyber power. *Survival*, 59(4), 27–34.

Jacobsen, J. T. (2021). Cyber offense in NATO: challenges and opportunities. *International Affairs*, 97(3), 703-720.

Kallberg, J., & Cook, T. S. (2017). The Unfitness of Traditional Military Thinking in Cyber. IEEE Access, 5, 8126-8130.

Kikuchi, M., & Okubo, T. (2019). Cyber governance complex in firms. In *Proceedings Of the 2nd International Conference on Control and Computer Vision* (pp. 116-120).

Kruck, A. (2014). Theorizing the use of private military and security companies: a synthetic perspective. *Journal of International Relations and Development*, 17(1), 112-141.

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, 10(1), 86-103.

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, 30(3), 139-148.

Lété, B., & Dege, D. (2017). *NATO Cybersecurity: A Roadmap to Resilience*. German Marshall Fund of the United States.

Lewis, J. A. (2018). Rethinking Cybersecurity. Center for Strategic and International Studies.

Libicki, M. C. (2012). *Crisis and escalation in cyberspace*. Rand Corporation.

Lindahl, J. (2015). *Understanding the American Use of Private Military Contractors* (Master's thesis).

Lutsenko, Y., Tarasiuk, A., Kryzhna, V., Motyl, V., & Dimich, A. (2021). Legal aspects of Civil-military cooperation in a comparative context. *Amazonia Investiga*, 10(48), 138-149.

Mabee, B., & Vucetic, S. (2018). Varieties of militarism: Towards a typology. *Security dialogue*, 49(1-2), 96-108.

Marrone, A., & Sabatino, E. (2021). *Cyber Defence in NATO Countries: Comparing Models*. Istituto Affari Internazionali.

McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. Politics and Governance, 6(2), 5-12. https://doi.org/10.17645/pag.v6i2.1335

McMahon, R. B., & Slantchev, B. L. (2015). The guardianship dilemma: Regime security Through and from the armed forces. *American Political Science Review*, 109(2), 297-313.

NATO (2002). Prague Summit 2002: Selected documents and statements. North Atlantic Council, (2002). Available in: https://www.nato.int/docu/0211prague/speeches-e.pdf

NATO (2008). Bucharest Summit 2008: Bucharest Summit Declaration. North Atlantic Council, (2008). Available in: https://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO (2011) Defending the networks: The NATO Policy on Cyber Defence, https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf, accessed 1 February 2016.

NATO (2014). Wales Summit 2014: Wales Summit Declaration. North Atlantic Council, 2014. Available in: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO (2021). *NATO Glossary of Terms and Definitions*. AAP-06 Edition 2021.

Nocetti, J. (2018). The darkening web: the war for cyberspace; The virtual weapon and international order.

Nøkleberg, M. (2020). The public-private divide revisited: questioning the middle ground of hybridity in policing. *Policing and Society*, 30(6), 601-617.

Olszewski, B. (2016). Militarization of cyberspace and multidimensionality of security. *Zeszyty Naukowe/Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki.*

Onuf, N. (1989). *World of our making: Rules and rule in social theory and international relations*. Routledge.

Ooijen, M. V. (2020). *Cyber securitization or cyberization of conflict?–the militarization of Cyber Security in Estonia* (Master's thesis).

Owens, P. (2008). Distinctions, distinctions: ' public ' and 'private force? *International Affairs*, 84(5), 977–990.

Pačka, R. (2019). CSIRT: v prednı linii boje proti kybernetickym hrozbam. Centrum pro studium demokracie a kultury.

Pačka, R., & Mareš, M. (2021). Achieving Cyber Power Through Integrated Government Capability: Factors Jeopardizing Civil-Military Cooperation on Cyber Defense. *Journal of Applied Security Research*, 1-26.

Pattison, J. (2020). From defense to offense: The ethics of private cybersecurity. *European Journal of International Security*, 5(2), 233-254.

Pion-Berlin, D. (2009). Defense organization and civil-military relations in Latin America. *Armed Forces & Society*, 35(3), 562-586.

Pion-Berlin, D., Schiff, R., Bruneau, T. C., & Neto, O. A. (2020). New Challenges in Civil-Military Relations.

Poirier, C. (2021). Interdependences Between Space and Cyberspace in the Context of Increasing Militarization and Emerging Weaponization of Outer Space – A French Perspective. In *Outer Space and Cyber Space* (pp. 67-85). Springer, Cham.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1), tyz002.

Rosenberger, L. (2020). Making cyberspace safe for democracy: The new landscape of information competition. *Foreign Aff.*, 99, 146.

Rubinson, E. (2021). Flexible democratic conditionality? The role of democracy and human rights adherence in NATO enlargement decisions. *Journal of International Relations and Development*, 24(3), 696–725.

Salminen, M., & Kerttunen, M. (2020). The becoming of cyber-military capabilities. In *Routledge Handbook of International Cybersecurity* (pp. 94-107). Routledge

Schneider, J. (2019). "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War." *Journal of Strategic Studies*, 42(6), 841–863. doi:10.1080/01402390.2019.1627209.

Shea, J. (2017). NATO: Stepping up its game in cyber defense. *Cyber Security: A Peer-Reviewed Journal*, 1(2), 165-174.

Shuya, M. (2018). Russian cyber aggression and the new Cold War. *Journal of Strategic Security*, 11(1), 1-18.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*.

Soeters, J. (2018). Organizational cultures in the military. In *Handbook of the sociology of the military* (pp. 251-272). Springer, Cham.

Spidalieri, F., & McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: The role of cybersecurity education in US service academies. *The Cyber Defense Review*, 1(1), 141-164.

Stevens, T., Ertan, A., Floyd, K., & Pernik, P. (2021). Cyber Threats and NATO 2030: Horizon Scanning and Analysis.

Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, 30(4), 1151-1168.

Szenes, Z., Efthymiopoulos, M. P., & Murray, C. (2021). NATO's cyber defense: Strategic challenges and institutional adaptation.

Tosbotn, R. A., & Cusumano, E. (2020). NATO in a Changing World. In *The Changing Global Order* (pp. 321-336). Springer, Cham.

Zekulić, V., Godwin, C., & Cole, J. (2017). Reinvigorating Civil-Military Relationships in Building National Resilience. *The RUSI Journal*, 162(4), 30-38.

Zhaohong, L. J. N. (2022). Striking the Balance between Civilian Control and Military Adaptability.

Zibak, A., & Simpson, A. (2019, August). Cyber threat information sharing: Perceived benefits and barriers. In *Proceedings of the 14th International Conference on availability, reliability, and security* (pp. 1-9).

Cabos Submarinos: Natureza Crítica e Vulnerabilidade Estratégica no Contexto da Aliança do Atlântico Norte

Inês Aguiar Branco
Consultora de Política do Mar.

Resumo

Num mundo cada vez mais global e tecnológico, as infraestruturas que suportam a conetividade digital, célere e permanente, adquirem um carácter imprescindível, uma vez que a transmissão da mesma quantidade de dados por outras vias é mais lenta, mais dispendiosa e insuficiente para atender às necessidades atuais a nível mundial.
Eventos recentes tornaram claro que os cabos submarinos estão em risco. Os adversários da OTAN estão não só cientes das vulnerabilidades existentes e conexas a este tipo de infraestrutura como, também, prontos e dispostos a explorá-las. Isto origina, inevitavelmente, implicações diversas para a segurança e interesses dos Estados aliados, às quais Portugal, como único país do mundo com ligações diretas de cabos submarinos estabelecidas com todos os continentes, à exceção da Antártida, não se deve alhear.

Palavras-chave: Cabos Submarinos; OTAN; Segurança Marítima; Infraestrutura Crítica; Vulnerabilidades; Danos; Ameaças.

Abstract
Subsea Cables: Critical Nature and Strategic Vulnerability in the North Atlantic Alliance Context

In an increasingly global and technological world, the infrastructures that support rapid and permanent digital connectivity become essential as the transmission of the same amount of data by other means is slower, more expensive, and insufficient to meet current needs worldwide.
Recent events have made it clear that subsea cables are at risk. NATO's adversaries are not only aware of the existing vulnerabilities related to this type of infrastructure, but also ready and willing to exploit them. This inevitably gives rise to numerous implications for the security and interests of allied States, implications which Portugal, as the only country in the world with direct subsea cable connections established with all continents, apart from Antarctica, should not ignore.

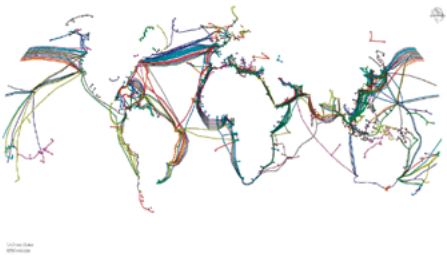
Keywords: *Subsea Cables; NATO; Maritime Security; Critical Infrastructure; Vulnerabilities; Damages; Threats.*

Artigo recebido: 31.01.2024
Aprovado: 16.04.2024
https://doi.org/10.47906/ND2024.168.04

Introdução

A conjuntura das sociedades contemporâneas está tão intrinsecamente dependente de uma ligação rápida e permanente à Internet que vários relatórios e estudos falam do acesso à Internet como sendo um Direito Humano (Kravets, 2011; Tully, 2014; Howell e West, 2016; Euronews, 2016; United Nations Human Rights Council 47th Session, 2021). Os cabos submarinos, artérias principais da Internet e da conectividade global, asseguram esse acesso, sendo responsáveis por 99% das telecomunicações mundiais, transmitindo rapidamente enormes quantidades de dados de origem pública e privada (Pérez, 2023; Miranda, 2023; Davenport, 2023; Medeiros e Pinto, 2023).

Figura 1
Traçado Mundial de Cabos Submarinos



Fonte: Symington (2023).

Figura 2
Rotas de Comércio Mundial

Fonte: Symington (2023).

O desenho traçado por estes cabos (Figura 1) mostra não só como circula a informação, mas também como flui o poder económico entre os diferentes continentes (Miranda, 2023; Medeiros e Pinto, 2023; Bueger *et al.*, 2022). Note-se que África é um dos continentes menos conectados, contrariamente à Europa e à América do Norte, e que, maioritariamente, os cabos submarinos seguem as rotas marítimas mais utilizadas pelos navios comerciais (Miranda, 2023; Medeiros e Pinto, 2023; Bueger *et al.*, 2022) (Figura 2).

O Atlântico Norte torna-se, assim, na rota marítima digital mais movimentada e densa do mundo (Medeiros e Pinto, 2023; Bueger *et al.*, 2022). Este facto, traduz-se em inúmeras oportunidades e desafios. Se, por um lado, este aumento da capacidade e qualidade da transmissão de dados permite comunicar de forma instantânea e permanente entre continentes, diminuindo as possibilidades de perda de ligação – por existir muita redundância –, por outro, o aumento da dependência societária desta infraestrutura gera preocupações securitárias com a manutenção do seu regular funcionamento (Bueger *et al.*, 2022). Assim, o Sul Global está mais vulnerável e suscetível a sofrer interrupções e demoras nos seus serviços de comunicações e Internet, em virtude do menor número de ligações que possui. Isto traduz-se numa

menor redundância e capacidade de resposta em caso de danificação da estrutura de cabos submarinos em toda esta área geográfica (Bueger *et al.*, 2022).

Embora a maior parte dos danos a cabos submarinos tenha, atualmente, carácter não intencional, a elevada dependência desta infraestrutura, para efeitos de comunicações sensíveis de natureza financeira e militar, preocupa, cada vez mais, a Organização do Tratado do Atlântico Norte (OTAN) e a União Europeia (UE) que, no atual contexto geopolítico, perspetivam a ocorrência de danos intencionais, coordenados e maliciosos (Bafoutsou *et al.*, 2023; Bueger *et al.*, 2022). Esta mudança de paradigma, relativamente ao carácter intencional dos danos a infraestruturas críticas, origina diversas preocupações a nível nacional e internacional tendo provocado a criação de vários grupos de trabalho e estudos para a identificação e mitigação de vulnerabilidades associadas a este tipo de infraestrutura (Pérez, 2023).

Em janeiro de 2023, a OTAN e a UE criaram um grupo de trabalho conjunto para proteger estas infraestruturas críticas. Meses mais tarde, a OTAN criou, ainda, uma Célula de Coordenação da Infraestrutura Crítica Submersa (EuroNews, 2023; NATO, 2023). Este novo organismo pretende coordenar esforços para mapear e dirimir vulnerabilidades entre os seus aliados, parceiros e setor privado.

Em outubro de 2023, o Conselho Europeu aprovou a Estratégia de Segurança Marítima da UE revista, bem como o seu Plano de Ação, justificando a revisão com a necessidade de fazer face a novas ameaças e desafios securitários, incluindo os ataques híbridos e cibernéticos contra as infraestruturas marítimas (Conselho Europeu, 2023). Este documento identificou a necessidade estratégica de aumentar a resiliência e a proteção das infraestruturas críticas submersas, reforçando as recomendações que o próprio Conselho já tinha emitido, em 2022 (Conselho Europeu, 2022).

Em Portugal, o Decreto-Lei n.º 20/2022, de 28 de janeiro veio aperfeiçoar o regime legal de identificação e proteção de infraestruturas críticas nacionais veiculado pelo Decreto-Lei n.º 62/2011, de 9 de maio, passando a incluir os setores das comunicações e infraestruturas digitais como setores onde deve ser feita a identificação de infraestruturas críticas nacionais. No entanto, trata-se de um processo de elevada complexidade pelo que, até ao momento, nenhuma infraestrutura crítica foi ainda identificada. Consequentemente, a infraestrutura nacional de sistemas de cabos submarinos permanece sem qualquer proteção jurídica ou securitária relevante[1].

1 A título de exemplo, a danificação intencional de um cabo submarino de comunicações, se excluirmos a criminalização desta conduta pelos crimes de terrorismo ou de sabotagem, que preconizam dolos específicos, só pode ser feita pelo Art.º 5.º n.º 2 do Decreto-Lei n.º 507/72 – cujas sanções são uma pena de multa de "20.000$00 a 100.000$00" e uma pena de prisão de 4 meses a dois anos, sendo a tentativa punível com pena até quatro meses de prisão – ou, em alternativa pelo crime de dano (Art.º 212.º do Código Penal português), cuja sanção é uma condenação até três anos de prisão ou uma pena de multa. Acresce, ainda, a existência de um amplo leque de normas sancionatórias que, de forma direta e indireta, contribuem para a segurança dos cabos

Este artigo aborda, simultaneamente, a natureza crítica e a vulnerabilidade estratégica que os cabos submarinos representam para a OTAN e, por maioria de razão, para o nosso país.

1. A Natureza Crítica dos Cabos Submarinos

No fundo do mar operam, presentemente, mais de 500 cabos submarinos suportados por mais de 1.400 estações de amarração (Telegeography, 2023). Estes cabos são essenciais para o funcionamento regular da sociedade global já que, constituindo a base estrutural da atividade social, governamental, militar e económica, a sua danificação, e consequente interrupção no fornecimento de serviços, pode provocar a paralisação total de um Estado (Guimarães, 2023; Miranda, 2023; Davenport, 2023; Medeiros e Pinto, 2023).

Quando comparados com outras tecnologias de transmissão de dados sem fios[2], os cabos submarinos oferecem vantagens imbatíveis nos campos da capacidade, velocidade e segurança de transmissão de dados (Submarine Telecoms Forum, 2022/2023). Estes adquirem, assim, natureza crítica uma vez que a transmissão da mesma quantidade de dados por outras vias não se coaduna com as necessidades mundiais atuais por ser, incomparavelmente, mais lenta e dispendiosa (Miranda, 2023; Pérez, 2023).

Não obstante a importância crítica, a abrangência geográfica e a dificuldade de monitorização deste tipo de infraestruturas, dispersas por diferentes ambientes operacionais e reguladas por distintos regimes jurídicos, há várias vulnerabilidades que tornam os cabos submarinos alvos atrativos para atores hostis (Guimarães, 2023; Medeiros e Pinto, 2023; Davenport, 2023). Prova disso é o interesse persistente da Federação Russa[3] na recolha de informação sensível sobre estas infraestruturas através da presença, frequentemente reportada, de cruzeiros científicos deste país em território marítimo de diversos Estados da OTAN (Medeiros e Pinto, 2023; Nunes, 2023; Donn, 2023; Colavito, 2023). Prova adicional é a preocupação generalizada dos Estados Aliados com o quase monopólio da República Popular da China como proprietária destas infraestruturas (Pérez, 2023; Brock, 2023; Schochet e Carr, 2023; Colavito, 2023).

submarinos de comunicações, mas que, além de serem de natureza contraordenacional, incidem sobre aspetos que não se reconduzem à sua proteção contra atos hostis.

2 Onde se incluem, por exemplo, as tecnologias de transmissão de ondas rádio (TV/Satélites), Wi-Fi, Bluetooth, NFC (comunicação por campo de proximidade) e RFID (ou identificação por radiofrequência).

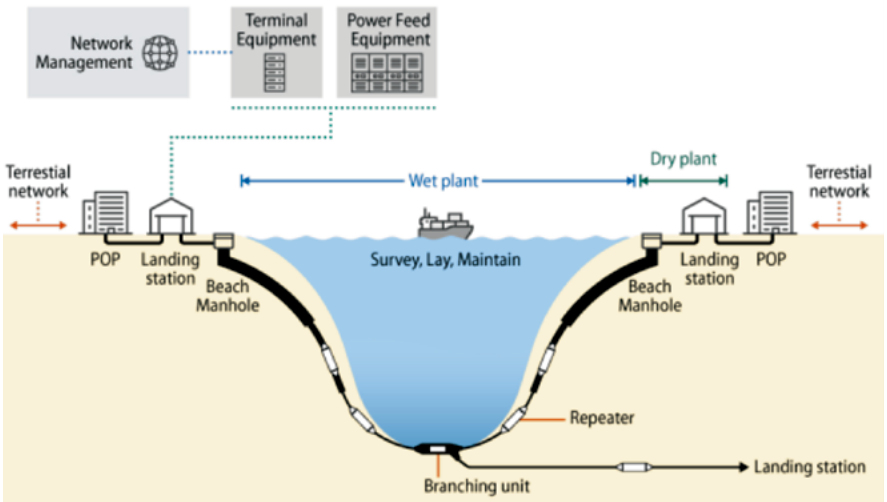
3 Neste domínio, importa referir que a possibilidade de a Rússia vir a realizar ataques contra cabos submarinos de comunicações e do sector energético tem sido veiculada por declarações de altos responsáveis políticos russos.

Este tipo de interesses e monopólio adivinham-se potenciadores de ações de mapeamento e, no contexto geopolítico atual de conflito armado, preocupam profundamente os Aliados da OTAN (Siebold, 2023; Davenport, 2023). Tal preocupação deve-se à potencial utilização desse mapeamento para ações de disrupção simultânea de vários cabos submarinos que, devido às limitadas e morosas capacidades de reparação existentes, bem como à dificuldade de atribuição de responsabilidade pelos danos ocorridos, representam um risco significativo para toda a Aliança (Davenport, 2015; Trakimavičius, 2021; Bueger *et al.*, 2022; Miranda, 2023; Pérez, 2023).
Assim, pela sua relevância estratégica, económica e securitária, importa analisar mais em pormenor as vulnerabilidades associadas a este tipo de infraestrutura crítica, bem como o aproveitamento que os Estados não aliados poderão fazer dessas vulnerabilidades.

2. Vulnerabilidades dos Cabos Submarinos

Para melhor se compreenderem as vulnerabilidades associadas à infraestrutura dos cabos submarinos, é importante considerar que estes são estruturas complexas que atravessam dois ambientes operacionais distintos (Figura 3): o ambiente marítimo que inclui o cabo em si, os repetidores nele instalados (para amplificação de sinal) e as unidades de derivação; e o ambiente terrestre, que inclui o "ponto de ligação"

Figura 3
Estrutura de Sistema de Cabo Submarino



Fonte: Gallagher (2022).

(Beach Manhole) que se liga à "estação de amarração" (Landing Station)[4]. Nas suas proximidades são, normalmente, instalados ainda os "pontos de presença" (PoP), que ficam alojados em centros de dados, que são a verdadeira origem e destino dos cabos submarinos e dos dados que neles circulam (Pérez, 2023; Gallagher, 2022).
Além de atravessarem diversos ambientes operacionais, os cabos estão, também, sujeitos a diferentes regimes jurídicos, por transporem e estarem "fixos" – tanto em mar, como em terra – a territórios sob soberania e/ou jurisdição de diferentes Estados e, ainda, fora da soberania e/ou jurisdição de qualquer Estado[5] (Davenport, 2018; Medeiros e Pinto, 2023).
Adicionalmente, os cabos submarinos são infraestruturas particularmente onerosas, normalmente financiadas através da constituição de consórcios entre empresas de tecnologia ou operadoras de telecomunicações de forma a partilhar os custos e os riscos associados a este modelo de negócio (Brock, 2023; Pérez, 2023; Medeiros e Pinto, 2023). Assim, na gestão e operação de um cabo submarino, participam diferentes entidades muito especializadas e diferenciadas, desde proprietários, fabricantes, instaladores e reparadores, até entidades governamentais.
Esta multiplicidade de parceiros, ambientes operacionais e regimes jurídicos, está na génese de uma série de vulnerabilidades que se manifestam em ambiente marítimo, terrestre e digital.

2.1. Vulnerabilidades Marítimas

As vulnerabilidades marítimas relacionam-se com os componentes do sistema de cabos submarinos que estão submersos (Figura 3). O isolamento geográfico e as condições ambientais adversas do ambiente marinho de grande profundidade, traduzem-se numa capacidade de monitorização e reparação reduzida, morosa e onerosa (Pérez, 2023).
Para além disso, existe uma concentração elevada de cabos em regiões específicas do oceano (Figura 1) o que, aliado ao facto de o traçado dos cabos ser do conhecimento público, favorece o conhecimento exato da localização e do número de cabos que é necessário danificar para provocar interrupções de grande escala ao fornecimento de serviços (Sunak, 2017).
Em 2013, a marinha egípcia deteve três mergulhadores, numa embarcação de pesca, perto da costa da Alexandria, sob suspeita de tentativa de corte do cabo submarino SeaMeWe-4, responsável por um terço do tráfego entre a Europa e o Egito (Arthur,

4 Local físico do país onde o cabo se liga à rede global de cabos submarinos, onde é feita a ligação às redes terrestres e onde residem as capacidades de gestão dos cabos e os equipamentos que fornecem a energia de que o sistema precisa para funcionar.
5 *Vide* Artigos 112.º e 113.º da *Convenção das Nações Unidas sobre o Direito do Mar*.

2013). Muito embora não haja detalhes adicionais, este caso demonstra que, para indivíduos determinados e munidos de equipamento adequado, não é necessário um elevado grau de sofisticação para causar uma disrupção séria às comunicações de Internet (Sunak, 2017).

2.2. Vulnerabilidades Terrestres

As vulnerabilidades terrestres dizem respeito aos componentes do sistema de cabos submarinos que estão em terra (Figura 3). Estes estão, normalmente, localizados na orla costeira e, por razões tanto de adequação geográfica como de redução de custos, alojam vários cabos submarinos criando, desta forma, diversos pontos de estrangulamento da rede (CSRIC, 2016).

A existência de pontos de estrangulamento é exacerbada, em grande medida, pela falta de segurança física característica destas infraestruturas, usualmente localizadas perto de zonas que, embora remotas, são de fácil acesso por não possuírem qualquer proteção por parte de estruturas físicas ou serviços de segurança especializados (Bueger *et al.*, 2022).

Em 2007, o Reino Unido conseguiu impedir uma tentativa de destruição das instalações da sede da Telecom Europe – empresa de centro de dados – por parte da Al-Qaeda (Leppard, 2007). Considerando que, ao contrário da maioria dos componentes terrestres de cabos submarinos, por ser um edifício-sede, este complexo estava dotado de medidas protetivas acima da média, é preocupante a possibilidade de ocorrência de ataques noutros locais (Sunak, 2017).

2.3. Vulnerabilidades Digitais

As vulnerabilidades digitais estão intimamente ligadas aos sistemas de gestão da rede de cabos submarinos, instalados nos centros de dados. Os centros de dados, por serem propriedade privada, oferecem aos seus operadores o controlo centralizado sobre os componentes físicos e digitais dos cabos submarinos, através de uma única localização. Esta localização, pelas suas capacidades integrais de controlo de rede, funciona como um botão de ligar e desligar a transmissão de dados (Sechrist, 2012).

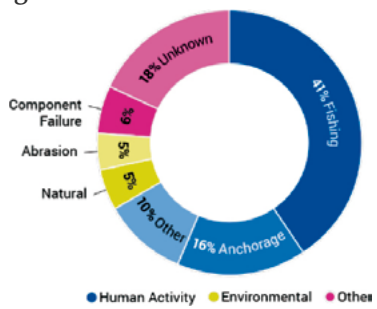
Esta vulnerabilidade é intensificada pela existência de sistemas, de gestão de redes de cabos submarinos, com operação remota. A multiplicação das formas de acesso que cada administrador pode utilizar para aceder ao sistema de gestão da rede de cabos submarinos aumenta o número de dispositivos que podem ser comprometidos para efetuar ações maliciosas contra a infraestrutura (Sunak, 2017).

Em 2022, foi reportado nos Estados Unidos da América o único ataque, desta natureza, contra cabos submarinos (Temple-Raston e Powers, 2022). De acordo com as autoridades americanas, um grupo internacional de *hackers* teve como alvo a infraestrutura em Oahu, violando os servidores de uma empresa privada que gere um cabo submarino que liga o Hawai aos restantes países da região do Pacífico (Boylan, 2022). Independentemente do meio em que se manifestam as vulnerabilidades descritas, destas advêm, forçosamente, ameaças à segurança física dos sistemas de cabos submarinos e à informação digital que neles circula. Essas ameaças originam, anualmente, centenas de danos que afetam a integridade dos sistemas e a capacidade de transmissão dos cabos submarinos (Clare, 2021).

3. Ameaças e Danos aos Cabos Submarinos

Relativamente à origem dos danos a cabos submarinos, podemos identificar três categorias: Humana, Ambiental e Outras (Figura 4). Os danos de origem humana são os mais frequentes por resultarem da atividade de navegação marítima regular – pesca de arrasto, dragagem ou ancoragem. Embora menos comuns, os danos de origem ambiental também podem ocorrer, resultantes da normal atividade geológica e biológica dos oceanos, como terramotos e mordidas de tubarão. Os restantes danos, aqui categorizados como de outra origem, acontecem muito raramente. É o caso das falhas de componentes e, sobretudo, das ações deliberadas de atores estatais e não estatais (Davenport, 2023).

Figura 4
Origem de danos a cabos submarinos



Fonte: Clare (2021).

Dentro das ações deliberadas não estatais encaixam os ataques cibernéticos realizados por *hackers* ou grupos de *ransomware*, com capacidade para perturbar os sistemas operativos dos cabos submarinos (Temple-Raston e Powers, 2022). Não obstante, o

principal desafio para a OTAN, no atual contexto geopolítico, são as ações deliberadas de atores estatais com recurso a sabotagem e espionagem (Davenport, 2018; Clare, 2021; Bueger *et al*., 2022; Pérez, 2023; Davenport, 2023). A este propósito, desde a explosão dos gasodutos[6] Nord Stream 1 e 2, muitos têm sido os relatos europeus de danos a cabos submarinos cuja causa se suspeita ser a sabotagem, deliberada e premeditada, destas infraestruturas submersas, por parte de atores estatais (ZMScable, 2022; Chiappa e Ngendakumana, 2023; Davenport, 2023; Kania, 2023).

Em outubro de 2022, três cabos submarinos foram cortados, interrompendo as ligações de internet entre Marselha, Lyon, Milão e Barcelona, o que tornou o acesso à Internet mais lento para os utilizadores europeus, asiáticos e americanos (PPLWARE SAPO, 2022; BBC NEWS, 2022). Na mesma altura, o cabo submarino que liga as Ilhas Faroé à Escócia, através das Ilhas Shetland e Orkney, foi danificado em dois incidentes separados, deixando a maioria das ilhas sem Internet (BBC NEWS, 2022).

Em fevereiro de 2023, os dois cabos que ligam as ilhas Matsu – controladas por Taiwan –, perto da costa chinesa, foram cortados, impedindo as 14 mil pessoas que lá habitam de aceder à Internet, durante dois meses (Wu e Lee, 2023; Kania, 2023). As autoridades de Taiwan identificaram a passagem de dois navios chineses perto do local onde o dano ocorreu, o que as levou a refletir sobre a falta de segurança e capacidade de reparação própria das 14 ligações por cabo submarino que garantem a sua conectividade (Wu e Lee, 2023; Kania, 2023).

Em outubro de 2023, o gasoduto Balticconector foi danificado, juntamente com dois cabos submarinos de comunicações que ligam Estónia, Finlândia e Suécia (Euronews, 2023). As autoridades finlandesas identificaram a passagem de um navio chinês e de um navio russo perto das zonas onde ocorreu o dano, suspeitando de ação estatal russa e chinesa neste incidente (Kubiak, 2023).

A ocorrência de falhas múltiplas de carácter simultâneo no mesmo cabo submarino ou em cabos submarinos próximos, excluindo causas naturais, é altamente incomum (PPLWARE SAPO, 2022; Bueger *et al*., 2022). O atual contexto geopolítico, aliado aos exemplos descritos *supra,* sustenta as preocupações da OTAN e da UE no domínio dos cabos submarinos, originando uma nova realidade quanto à possibilidade de os danos a esta infraestrutura passarem a ser de ações estatais deliberadas e maliciosas (Bueger *et al*., 2022).

Esta nova realidade acarreta implicações securitárias e políticas significativas, não só para a OTAN mas também para Portugal que, pela sua centralidade atlântica, tem vindo a assumir uma importância cada vez mais nevrálgica nas rotas de cabos

6 A 26 de setembro 2022, uma série de explosões e vazamentos de gás ocorreram nos gasodutos Nord Stream 1 e Nord Stream 2, construídos para transportar gás natural da Rússia para a Alemanha. Sabe-se que os vazamentos foram causados por sabotagem intencional.

submarinos, contando já com ligações de cabos submarinos a todos os continentes, exceto a Antártida (ANACOM, 2020).

4. Implicações Securitárias e Políticas para a Aliança

As implicações securitárias e políticas, decorrentes de ações estatais de sabotagem e espionagem a sistemas de cabos submarinos, não são totalmente desconhecidas, especialmente, em contexto de conflito armado (Davenport, 2023; Pérez, 2023; Guilfoyle, *et al.*, 2022; Medeiros e Pinto, 2023). A dependência militar desta infraestrutura, para efeitos defensivos e de guerrilha, é bem conhecida, tendo a danificação de sistemas de cabos submarinos sido, historicamente, utilizada para destabilizar inimigos durante conflitos armados[7] (Davenport, 2023; Guilfoyle *et al.*, 2022; Sunak, 2017; Kania, 2023). Apesar disso, a evolução da tecnologia dos cabos submarinos, agora considerada como universal e indispensável para o funcionamento "normal" das sociedades, bem como de outras tecnologias de sensorização, recolha, tratamento e armazenamento de dados, aporta novas ramificações. As capacidades e meios disponíveis para efetuar ações hostis desta natureza foram ampliadas, ao mesmo tempo que se maximizaram as consequências resultantes dessas ações (Guilfoyle *et al.*, 2022). Assim, Estados não aliados estão capacitados para efetuar ações coordenadas e simultâneas a vários cabos submarinos, o que poderá isolar e paralisar os Estados-alvo, comprometendo as suas capacidades militares, económicas e políticas de defesa e fragilizando a atuação da OTAN.

4.1. Implicações Securitárias de Ação Estatal: os Modi Operandi *da China e da Rússia*

A República Popular da China, com a crescente relevância mundial de empresas estatais chinesas, como a HMN Technologies, principal fabricante de sistemas de cabos submarinos, e operadoras de telecomunicações estatais, como a China Mobile e a China Telecom, constitui uma ameaça à integridade digital da informação que circula nos cabos submarinos (Brock, 2023; Pérez, 2023; Kania, 2023). Mudanças nos padrões de roteamento da rede teriam um efeito direto no tráfego, e o monopólio de negócios internacionais relacionados com o fabrico, a instalação e a reparação de cabos submarinos, pode gerar dependência tecnológica entre os países que interligam os sistemas de cabos (Schadlow e Helwig, 2020). Adicionalmente, os Estados Aliados, muito embora descartem, de momento, a capacidade para extração de dados

7 A 5 de agosto de 1914, a primeira ação militar do Reino Unido contra a Alemanha, após a declaração de guerra, foi o corte dos seus cinco cabos submarinos transatlânticos.

a grandes profundidades, estão convencidos de que existe a capacidade tecnológica para interferir nas comunicações, através de *backdoors* inseridos nos sistemas de cabos submarinos, durante o processo de fabrico e instalação (Schadlow e Helwig, 2020; Pérez, 2023; Walland e Morcos, 2021).

Já a Federação Russa representa um tipo de ameaça mais convencional à integridade física dos sistemas de cabos submarinos. O seu extenso programa de rearmamento, focado no aumento das suas capacidades navais e submersas, resultou na criação da maior frota de embarcações de profundidade do mundo (GFP Strenght in Numbers, 2024; Sunak, 2017; Nilsen, 2018). Esta frota de submarinos e navios de superfície equipados com submergíveis tripulados e não tripulados permite à Rússia manipular objetos a grandes profundidades, intercetar comunicações e destruir infraestrutura submersa (Metrick *et al*., 2016; Sunak, 2017).

É sabido, por isso, que tanto a Rússia como a China dispõem dos meios navais necessários para realizar ataques contra os sistemas de cabos submarinos em águas profundas: submarinos, embarcações submergíveis tripuladas e não tripuladas, e embarcações de superfície com capacidade cartográfica e grande alcance de profundidade (Sunak, 2017). Além destes meios operacionais, ambos os países possuem meios científicos e tecnológicos que permitem a colocação de sensores nos cabos submarinos, que aliados ao mapeamento das rotas de cabos submarinos e ao estudo do comportamento dos objetos submersos, poderá, a longo prazo, informar, de forma inédita, a atividade militar, comprometendo a capacidade de as embarcações Aliadas, tripuladas e não tripuladas, circularem de forma indetetável (Chen *et al*., 2022; Iqbal, 2023; Hlongwa, 2021; Jankowski, 2021; NATO STO-CMRE, 2023).

4.2. Implicações Políticas: a Gestão e Manutenção dos Cabos Submarinos

Pela sua natureza crítica, seria desejável que a gestão e manutenção dos sistemas de cabos submarinos fosse delineada de forma estratégica e coordenada, entre as entidades estaduais e os proprietários da infraestrutura. No entanto, tal não acontece (Kania, 2023).

Sendo a maior parte da infraestrutura de cabos submarinos propriedade de entidades privadas, essas entidades têm o poder de decidir quais os cabos que instalam, quando instalam e onde os instalam. Daqui resultam jogos de poder financeiro e geopolítico entre estas empresas e os Estados, verificando-se uma concentração de cabos muito maior no Atlântico Norte do que no Atlântico Sul (Figura 1) (Medeiros e Pinto, 2023; Pérez, 2023).

A fragilidade e dependência que os Estados do Atlântico Sul possuem em relação à estrutura de cabos submarinos existentes no Atlântico Norte traduz-se, de forma inequívoca, numa menor capacidade para desenvolvimentos tecnológicos e de defesa

cibernética (Medeiros e Pinto, 2023). Desta forma, é expectável que, na pendência de regime jurídico internacional específico para o efeito, haja a ocorrência de conflitos sobre que cabos devem ser instalados, que traçado devem seguir e que pontos de amarração devem utilizar.

Se a mera decisão sobre a instalação de cabos gera conflitos e desigualdades, as decisões relativamente à manutenção e reparação dos cabos trazem ainda mais dificuldades. Sendo propriedade privada, o ónus da manutenção e reparação dos cabos recai sobre o proprietário da infraestrutura danificada e, como tal, é este que decide que cabos reparar e porque ordem o deve fazer. No entanto, perspetivando-se a ocorrência de danos múltiplos e simultâneos, por parte de ator estatal, parece-nos dúbio que o ónus de reparação continue a recair sobre o proprietário da infraestrutura, estando esta questão pendente de regime jurídico próprio (Burnett, 2022).

O referido regime jurídico deverá acautelar, simultaneamente, a dificuldade de atribuição de culpa/responsabilização pela danificação simultânea de vários cabos por parte de ator estatal, bem como assegurar a existência de equidade relativamente ao ónus da obrigação de cobrir os custos de reparação do cabo em si (Davenport, 2023). Reformulando, muito embora a infraestrutura em causa seja propriedade privada, dada a sua inegável utilidade pública e, podendo a mesma ser alvo de ação hostil estatal causadora de dano, não deve o ónus de reparação recair apenas sobre o proprietário da infraestrutura.

5. Conclusões e Recomendações

À medida que aumenta a dependência societária, económica, militar e governamental dos sistemas de cabos submarinos, aumentam as preocupações relativas à sua segurança. Desta forma, é expectável que a temática da natureza crítica dos cabos submarinos continue a ganhar relevância a nível global. Não só por trazer consigo o desejado aumento da conectividade e de avultados investimentos, mas sobretudo pelas implicações e vulnerabilidades securitárias que acarreta, especialmente, no contexto geopolítico atual.

A este propósito, muitas têm sido as situações reportadas de danos a cabos submarinos em que existe forte suspeita sobre o carácter intencional e estatal do dano. A OTAN e a UE já reconheceram tanto a natureza crítica como a vulnerabilidade estratégica adjacente aos cabos submarinos. Os esforços individuais e conjuntos para identificação e mitigação de vulnerabilidades a estas infraestruturas, bem como o desenvolvimento de estratégias e planos de ação, são prova disso mesmo.

Assim, também Portugal deve mapear as vulnerabilidades existentes e desenvolver os mecanismos jurídicos necessários para regular a proteção física, cibernética e geopolítica dos cabos submarinos que atravessam o seu território, em estreita coo-

peração com as entidades privadas proprietárias da infraestrutura e com todos os parceiros envolvidos na operação e reparação dos sistemas de cabos submarinos. A Segurança Nacional e da Aliança disso depende.
As recomendações que se seguem são um contributo para que Portugal comece a caminhar na direção certa:

- **Assegurar a segurança física dos componentes terrestres dos sistemas de cabos submarinos** – é necessário adotar medidas de segurança física de forma a manter os colaboradores, as instalações e ativos dos sistemas de cabos submarinos protegidos das ameaças existentes. Isto inclui, de forma não exaustiva, a obrigatoriedade de implementação de medidas relativas à instalação de controlos de acesso (cartões de identificação e restrições biométricas) e a adoção de medidas de vigilância ativa permanente (por exemplo, alarmes, guardas e videovigilância).
- **Tornar obrigatória a instalação de equipamentos de monitorização nos componentes marítimos dos sistemas de cabos submarinos** – a instalação de sensores para frequências sonar nos cabos submarinos permitirá identificar, em tempo real, a ocorrência de situações suspeitas nas proximidades dos cabos (como a passagem de veículos submersíveis) e originar uma comunicação célere às autoridades responsáveis pela sua segurança.
- **Aumentar a diversidade geográfica tanto das rotas de cabos como das estações de amarração** – a dispersão geográfica de rotas e estações de amarração (por exemplo, no Algarve e no norte de Portugal continental) aumentará a redundância e a resiliência da rede diminuindo eventuais pontos de estrangulamento.
- **Acelerar a classificação dos sistemas de cabos submarinos como infraestruturas críticas** – embora já esteja em curso o processo espoletado pelo Decreto-Lei n.º 20/2022, de 28 de janeiro, que veio alargar às comunicações, infraestruturas e prestadores de serviços digitais, os procedimentos para a identificação e designação de infraestruturas críticas, até hoje não se veem avanços neste processo. Dada a necessidade de agir rapidamente, para garantir o reforço da proteção deste tipo de infraestruturas, será importante que seja atribuída aos sistemas de cabos submarinos prioridade máxima.
- **Criar uma estrutura de coordenação para a proteção dos sistemas de cabos submarinos** – esta estrutura, que deverá servir de mecanismo para a partilha de informação sobre incidentes com os cabos submarinos e com a sua infraestrutura terrestre, deverá incluir, não só todas as entidades envolvidas na instalação e operação dos cabos submarinos, mas também todas aquelas que têm competências legais e capacidades operacionais para contribuir de forma efetiva para a segurança destas infraestruturas; a sua criação deverá, também, ser independente do processo de identificação de infraestruturas críticas atualmente em curso neste setor.

- **Incentivar a criação/robustização do regime jurídico internacional para proteção dos cabos submarinos** – os sistemas de cabos submarinos, pela sua criticidade e complexidade, requerem uma abordagem holística e punitiva. Um novo tratado internacional sobre a temática deverá proteger estes sistemas e tornar a interferência com os mesmos mais onerosa para o infrator, incluindo normas sobre cooperação mútua, partilha de informação e facilitadoras da atribuição da responsabilidade em casos de dano.
- **Fomentar a realização de exercícios nacionais e no âmbito da OTAN sobre a proteção de cabos submarinos** – a realização de exercícios/simulacros para proteção dos sistemas de cabos submarinos, contra ameaças internacionais, permitirá instruir todos os intervenientes e identificar oportunidades de melhoria nos procedimentos existentes, incluindo cenários de reconhecimento hostil como os perpetrados, de forma persistente, pela Rússia no Atlântico Norte.

Bibliografia

ANACOM, 2020. *ANACOM* [Online]. Disponível em: https://www.anacom.pt/render.jsp?contentId=1538121 [Acedido 09 01 2024].

Arthur, C., 2013. *The Guardian* [Online]. Disponível em: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests [Acedido 25 01 2024].

Bafoutsou, G., Papaphilippou, M., Dekker, M. e ENISA, 2023. *SUBSEA CABLES – WHAT IS AT STAKE?,* Luxembourg: ENISA.

BBC NEWS, 2022. *BBC NEWS* [Online]. Disponível em: https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102 [Acedido 25 01 2024].

Boylan, P., 2022. *Star Advertiser* [Online]. Disponível em: https://www.staradvertiser.com/2022/04/12/breaking-news/cyberattack-on-hawaii-undersea-communications-cable-thwarted-by-homeland-security/ [Acedido 25 01 2024].

Brock, J., 2023. *REUTERS* [Online]. Disponível em: https://www.reuters.com/investigates/special-report/us-china-tech-cables/ [Acedido 08 01 2024].

Bueger, C., *et al.*, 2022. *Atlantic Centre* [Online]. Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_13.pdf [Acedido 25 01 2024].

Bueger, C., Liebetrau, T. e Franken, J., 2022. *Europarl* [Online]. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf [Acedido 08 01 2024].

Burnett, D. R., 2022. *A Reboot of Wartime Submarine Fiber Optic Cables,* Virginia, USA: Submarine Telecoms Forum Magazine.

Chen, J., *et al.*, 2022. A Critical Examination for Widespread Usage of Shipping Big Data Analytics in China. *Journal of Marine Science and Engineering,* 10(12), pp. 1-19.

Chiappa, C. e Ngendakumana, P. E., 2023. *Politico* [Online]. Disponível em: https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/ [Acedido 09 01 2024].

Clare, M., 2021. *International Cable Protection Committee* [Online]. Disponível em: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf [Acedido 08 01 2024].

Colavito, C., 2023. *GNOSIS* [Online]. Disponível em: https://gnosis.aisi.gov.it/Gnosis/Rivista74.nsf/ServNavig/74-20.pdf/$File/74-20.pdf?openElement [Acedido 25 01 2024].

Conselho Europeu, 2022. *Consilium Europa* [Online]. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/ [Acedido 24 01 2024].

Conselho Europeu, 2023. *Consilium Europa* [Online]. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2023/10/24/maritime-security-council-approves-revised-eu-strategy-and-action-plan/ [Acedido 24 01 2024].

CSRIC, W. 4. S. C. R., 2016. *Clustering of Cables and Cable Landings,* Washington: CSRIC - Communications Security, Reliability and Interoperability Council.

Davenport, T., 2015. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. *Catholic University Journal of Law and Technology,* 24(1), pp. 57-109.

Davenport, T., 2018. *Cambridge University* [Online]. Disponível em: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/C67248AD17B1F960E885C83EA-8F537AB/S239877231800048Xa.pdf/the-high-seas-freedom-to-lay-submarine-cables-and-the-protection-of-the-marine-environment-challenges-in-high-seas-governance.p [Acedido 08 01 2024].

Davenport, T., 2023. *Hoover Institution* [Online]. Disponível em: https://www.hoover.org/sites/default/files/research/docs/Davenport_finalfile_WebReadyPDF.pdf [Acedido 09 01 2024].

Donn, N., 2023. *Portugal Resident* [Online]. Disponível em: https://www.portugalresident.com/russia-spies-on-underwater-cabling-has-portugal-on-its-radar/ [Acedido 08 01 2024].

Euronews, 2016. *Euronews* [Online]. Disponível em: https://pt.euronews.com/2016/07/05/acesso-a-internet-e-um-direito-humano-diz-onu [Acedido 08 01 2024].

Euronews, 2023. *Euronews* [Online]. Disponível em: https://www.euronews.com/2023/10/10/baltic-gas-pipeline-leak-likely-caused-by-external-activity-says-finlands-president [Acedido 25 01 2024].

EuroNews, 2023. *EuroNews* [Online]. Disponível em: https://pt.euronews.com/2023/01/11/ue-e-nato-aliam-se-para-proteger-as-infraestruturas-criticas-da-europa [Acedido 12 01 2024].

Gallagher, J. C., 2022. *Congressional Research Service Reports* [Online]. Disponível em: https://crsreports.congress.gov/product/pdf/R/R47237 [Acedido 08 01 2024].

GFP Strenght in Numbers, 2024. *GFP Strenght in Numbers* [Online]. Disponível em: https://www.globalfirepower.com/navy-ships.php [Acedido 11 01 2024].

Guilfoyle, D., Paige, T. P. e Rob, M., 2022. The Final Frontier Of Cyberspace: The Seabed Beyond National Jurisdiction And The Protection Of Submarine Cables. *International & Comparative Law Quarterly,* 71(3), pp. 657-696.

Guimarães, A., 2023. *CNN PT* [Online]. Disponível em: https://cnnportugal.iol.pt/cabos-submarinos/espionagem/a-ameaca-que-se-esconde-no-mar-de-portugal-sabotagem-dos-cabos-submarinos-seria-uma-catastrofe/20230619/6478cc60d34ef47b87548052 [Acedido 05 01 2024].

Hlongwa, L. N., 2021. Artificial intelligence and big data in the Maritime Silk Road Initiative: The road towards Sea Power 2.0. *South African Journal of Military Studies*, 49(2), pp. 113-131.

Howell, C. e West, D. M., 2016. *Brookings* [Online]. Disponível em: https://www.brookings.edu/articles/the-internet-as-a-human-right/ [Acedido 08 01 2024].

Iqbal, A., 2023. *Paradigm Shift* [Online]. Disponível em: https://www.paradigmshift.com.pk/chinas-artificial-intelligence/ [Acedido 11 01 2024].

Jankowski, D. P., 2021. *Center for Strategic e International Studies* [Online]. Disponível em: https://www.csis.org/analysis/russia-and-technological-race-era-great-power-competition [Acedido 11 01 2024].

Kania, E. B., 2023. *Rajaratnam School of International Studies* [Online]. Disponível em: https://www.rsis.edu.sg/wp-content/uploads/2023/08/CO23113.pdf [Acedido 26 01 2024].

Kravets, D., 2011. *WIRED* [Online]. Disponível em: https://www.wired.com/2011/06/internet-a-human-right/ [Acedido 08 01 2024].

Kubiak, M., 2023. *The Jamestown Foundation* [Online]. Disponível em: https://jamestown.org/program/balticconnector-leak-highlights-need-for-stronger-coordination-in-protecting-critical-infrastructure/ [Acedido 25 01 2024].

Leppard, D., 2007. *The Times* [Online]. Disponível em: https://www.thetimes.co.uk/article/al-qaeda-plot-to-bring-down-uk-internet-b8vb32twcwt [Acedido 25 01 2024].

Medeiros, S. E. e Pinto, D. J. A., 2023. *Defesa* [Online]. Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_11.pdf [Acedido 05 01 2024].

Metrick, A., Weinberger, K. e Hicks, K. H., 2016. *Center for Strategic e International Studies* [Online]. Disponível em: https://www.csis.org/analysis/undersea-warfare-northern-europe [Acedido 11 01 2024].

Miranda, N., 2023. *Mapfre Global Risks* [Online]. Disponível em: https://www.mapfreglobalrisks.com/pt-br/gerencia-riscos-seguros/estudos/cabos-submarinos-a-maior-rede-mundial-de-telecomunicacoes/ [Acedido 05 Janeiro 2024].

NATO STO-CMRE, 2023. *CMRE* [Online]. Disponível em: https://www.cmre.nato.int/research/publications/technical-reports/special-publications/1701-cmre-ar-2022/file [Acedido 11 01 2024].

NATO, 2023. *NATO* [Online]. Disponível em: https://www.nato.int/cps/en/natohq/news_211919.htm [Acedido 12 01 2024].

Nilsen, T., 2018. *The Barents Observer* [Online]. Disponível em: https://thebarentsobserver.com/en/node/3381 [Acedido 11 01 2024].

Nunes, F., 2023. *Eco* [Online]. Disponível em: https://eco.sapo.pt/2023/05/04/russia-esta-a-espiar-cabos-submarinos-e-tem-portugal-no-radar/ [Acedido 08 01 2024].

Pérez, R. G., 2023. *IEEE* [Online]. Disponível em: https://www.ieee.es/Galerias/fichero/docs_marco/2023/DIEEEM10_2023_RAFGAR_Submarinos.pdf [Acedido 05 01 2024].

PPLWARE SAPO, 2022. *PPLWARE SAPO* [Online]. Disponível em: https://pplware.sapo.pt/informacao/cabos-submarinos-europeus-de-comunicacoes-foram-cortados-nesta-quarta-feira/ [Acedido 25 01 2024].

Schadlow, N. e Helwig, B., 2020. *Defense News* [Online]. Disponível em: https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/ [Acedido 12 01 2024].

Schochet, N. e Carr, E., 2023. *The Diplomat* [Online]. Disponível em: https://thediplomat.com/2023/08/navigating-china-us-subsea-cable-competition/ [Acedido 08 01 2024].

Sechrist, M., 2012. *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems,* Boston: Harvard Kennedy School.

Siebold, S., 2023. *REUTERS* [Online]. Disponível em: https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/ [Acedido 08 01 2024].

Submarine Telecoms Forum, 2022/2023. *Industry Report* [Online]. Disponível em: https://issuu.com/subtelforum/docs/submarine_telecoms_indsutry_report_issue_11?fr=xKAE9_zU1NQ [Acedido 10 01 2024].

Sunak, R., 2017. *Policy Exchange* [Online]. Disponível em: https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf [Acedido 11 01 2024].

Symington, A., 2023. *The Wold's Shipping Lanes.* [Art] (PhytonMaps).

Symington, A., 2023. *The World's Undersea Cables.* [Art] (PhytonMaps).

Telegeography, 2023. *Submarine Cable Map* [Online]. Disponível em: https://submarine-cable-map-2023.telegeography.com/ [Acedido 10 01 2024].

Temple-Raston, D. e Powers, S., 2022. *The Record* [Online]. Disponível em: https://therecord.media/who-tried-to-hack-hawaiis-undersea-cable [Acedido 10 01 2024].

Trakimavičius, L., 2021. *NATO ENSEC COE* [Online]. Disponível em: https://www.enseccoe.org/data/public/uploads/2021/12/the-hidden-threat-to-baltic-undersea-power-cables-final.pdf [Acedido 08 01 2024].

Tully, S., 2014. A Human Right to Access the Internet? Problems and Prospects. *Human Rights Law Review,* 14(2), pp. 175-195.

United Nations Human Rights Council 47th Session, 2021. *The promotion, protection and enjoyment of human rights on the Internet,* New York: United Nations.

Walland, C. e Morcos, P., 2021. *Center for Strategic e International Studies* [Online]. Disponível em: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security [Acedido 12 01 2024].

Wu, S. e Lee, Y., 2023. *REUTERS* [Online]. Disponível em: https://www.reuters.com/world/asia-pacific/fear-dark-taiwan-sees-wartime-frailty-communication-links-with-world-2023-03-15/ [Acedido 25 01 2024].

ZMScable, 2022. *ZMScable* [Online]. Disponível em: https://zmscable.es/pt/cortan-cables-submarinos-britanicos-franceses/ [Acedido 09 01 2024].

O Yin e o Yang da NATO – Desarmonias na Defesa da Europa

António Eugénio
Assessor de Estudos do IDN.

Resumo

A Guerra da Ucrânia trouxe uma urgência ao debate da integração da defesa europeia e uma renovada legitimidade à Organização do Tratado do Atlântico Norte (NATO), com a adesão rápida da Finlândia e da Suécia, dois países tradicionalmente neutros. No entanto, a existência da Aliança, liderada pelos EUA, que vêm demonstrando uma posição ambígua face à emergência de mais um novo ator geopolítico como a União Europeia (UE), além da China, tem causado algumas dúvidas sobre o verdadeiro interesse norte-americano no desenvolvimento de capacidades de defesa modernas e autónomas no continente europeu. Daí a utilidade de uma perspetiva como a do *yin* e *yang*, pela noção de uma dinâmica complementar que aqui se esboça e que poderá conduzir a uma solução harmoniosa, como a existência de um pilar de defesa europeu dentro da OTAN. Indo para lá do debate teórico e como proposta executiva, defende-se uma maior integração, modernização e digitalização da base tecnológica europeia de modo a poder concorrer com as suas congéneres norte-americanas e examina a desejável divisão de encargos entre países aliados, de modo a esta passar a incluir o valor comercial dos dados dos cidadãos, empresas e organizações europeias, aos quais as gigantes tecnológicas norte-americanas têm acesso sem reciprocidade.

Palavras-chave: Defesa; Europa; Yin; Yang; Ucrânia; NATO; EUA; Tecnologia.

Artigo recebido: 22.05.2024
Aprovado: 11.06.2024
https://doi.org/10.47906/ND2024.168.05

Abstract
NATO's Yin and Yang – Disharmonies in Europe's Defence

The war in Ukraine put the spotlight on European defense integration, as well as a renewed legitimacy to NATO, with the rapid accession of Finland and Sweden, two traditionally neutral countries. However, the sole existence of the Alliance has caused some doubt about the true intentions of its leader, the USA, in the development of modern and autonomous defense capabilities in the European continent, confronted with yet another new geopolitical actor besides China, such as the European Union. Hence, the usefulness of a sketch of a perspective such as that of yin and yang carries the notion of complementary dynamics that could lead to a harmonious solution, such as the existence of a European defense pillar within NATO. Going beyond the theoretical debate and as an executive proposal, the author advocates greater integration, modernization and digitalization of the European technological base in order to be able to compete with its North American counterparts and examines the desirable division of burdens between allied countries, so that this includes the commercial value of the data of European citizens, companies and organisations, to which North American technology giants have access without reciprocity.

Keywords: *Defence; Europe; Yin; Yang; Ukraine; NATO; USA; Technology.*

Introdução

Para a filosofia confuciana, é impossível separar assuntos conflituantes em qualquer tópico. Deste antagonismo básico, entre o *yin*, débil e inerte, e o *yang*, ativo e vigoroso, resulta o progresso e a harmonia, numa continuidade eterna. É nosso entender que é esse o caso das duas maiores tendências antagónicas no âmbito da segurança e defesa europeias atuais e que poderão ser entendidas como desarmonias. Por um lado, existe uma ameaça da retirada dos Estados Unidos da América (EUA) da OTAN, propalada pelo ex-presidente e novamente candidato Donald Trump (*yin*), e, por outro, a perspetiva da Guerra da Ucrânia (*yang*) ser o catalisador definitivo que a Europa precisa para encarar a sua defesa com maior autonomia face aos EUA. Através da análise das dinâmicas proporcionadas pelas lentes do *yin* e do *yang*, podemos vislumbrar como a OTAN pode navegar no futuro da segurança europeia, ainda que sob enormes tensões, mantendo o equilíbrio entre os países membros e adaptando-se às novas realidades geopolíticas.

Pedimos emprestados estes conceitos da filosofia taoista por duas razões principais. A primeira diz respeito à originalidade da referência que é feita objetivamente à República Popular da China (RPC) no último conceito estratégico da OTAN[1], apresentada como um desafio aos interesses, à segurança e aos valores aliados, dados os instrumentos obscuros de projeção de poder que utiliza para subverter a ordem internacional baseada em normas[2]. A RPC pertence a um espaço não vestefaliano de nações (Wang, 2024). Portanto, parece-nos útil invocar conceitos normalmente associados à sua cultura estratégica, para estimular o seu estudo, num contexto de competição entre grandes potências (He, 2023), de modo a evitar o viés cognitivo da imagem espelhada. A segunda razão é que esta abordagem pode ser útil para revelar as tensões internas no interior da Aliança, a que chamámos desarmonias, que objetivamente revelam o interesse dos EUA na manutenção do *statu quo* de um relacionamento de um para muitos (30 países europeus atualmente) em vez de um para um, que resultaria de uma negociação com a União Europeia. Procuram, assim, limitar a emergência de um pilar europeu de defesa, ao mesmo tempo que acusam os aliados europeus de não cumprirem as suas obrigações na divisão de encargos. Como veremos, existe uma ligação da OTAN à região da Ásia-Pacífico desde a sua origem

Nota: as ligações a sites da internet mencionadas neste artigo foram acedidas durante os meses de abril a junho de 2024.

1 A primeira menção à RPC surge na Declaração de Londres, de 2019, na sequência da Cimeira comemorativa dos setenta anos da OTAN, em que se afirma: "reconhecemos que a crescente influência e políticas internacionais da China apresentam oportunidades e desafios que teremos de encarar em conjunto, como uma aliança. Cf. https://www.nato.int/cps/en/natohq/official_texts_171584.htm

2 Cf. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

que é raramente referida e investigada numa perspetiva abrangente, em especial por aqueles que confinam regionalmente a Aliança. Seja por razões geopolíticas, seja por uma expansão dos domínios de confronto, cada vez mais desmaterializados, ou pela instrumentalização de setores não tradicionais como a energia e as relações comerciais, é necessário alterar a nossa perceção dos desafios securitários que estão no horizonte para podermos agir em conformidade.

Em vez de uma discussão exaustiva sobre a dialética *yin-yang* aplicada, oferece-se apenas um esboço do que poderá ser um método de gestão de contradições persistentes (Qin, 2018) que permitam à OTAN viver com elas, necessitando apenas de uma reinterpretação do contributo europeu para o esforço coletivo, em alternativa a uma linha metodológica ligada à dialética hegeliana, produzindo sínteses de alto nível das teses e antíteses. Deste modo, alcança-se um meio-termo do pensamento, que acomoda contradições sem que as posições sejam mutuamente exclusivas, obtendo a desejada harmonia (He, 2023). Um dos contributos maiores desta aproximação é que a realidade está sempre presente na construção de uma via para alcançar os objetivos, em vez da utilização de modelos abstratos que depois serão aplicados (Jullien, 2004).

Situando o tema do nosso artigo na área dos Estudos de Segurança Internacional, a abordagem metodológica mencionada alinha-se com as teorias de nível intermédio que utilizam múltiplos paradigmas no tratamento académico de questões concretas ou de eventos correntes com relevância política, em vez de um acantonamento a uma escola de pensamento específica.

A pergunta que iluminou a nossa pesquisa é a seguinte: Face à ambiguidade dos EUA quanto à emergência de um pilar europeu de defesa, como conviver com as tradicionais dificuldades de desenvolvimento das capacidades militares europeias e ao mesmo tempo satisfazer os compromissos assumidos na divisão de encargos no contexto da OTAN? A problemática é complexa e intrincada porque liga elementos históricos, geopolíticos, diplomáticos, industriais, tecnológicos, psicológicos, culturais, económicos, etc., obrigando a um esforço de contenção expositiva. Privilegiaram-se fontes primárias para obter os dados da investigação.

A Europa do século XXI parece tolhida entre os *Big States* e as *Big Techs*. Como um todo, é um gigante económico, uma potência demográfica e até científica. Porém, nos assuntos de defesa está profundamente balcanizada e completamente dependente de um *Big State* que dispõe de *Big Techs*, que é o caso dos Estados Unidos da América e de uma aliança, a OTAN, que garantiu uma "longa paz" (Gaddis, 1986) na Europa, mesmo quando a guerra aqueceu nos Balcãs, na década de 90 do século passado. Porém, quando a Rússia decidiu atacar a ordem unipolar[3] que afirmava

3 Um dos momentos mais marcantes do novo posicionamento estratégico da Rússia face ao Ocidente foi o discurso do presidente russo na Conferência de Segurança de Munique de 2007. http://en.kremlin.ru/events/president/transcripts/24034

estar estabelecida, nenhuma dissuasão aliada a conteve. Atacou a Geórgia em 2008[4], perante a indolência da comunidade internacional, segurou o regime de Assad, na Síria, a partir de 2011[5] (com envolvimento militar direto a partir de 2015), anexou a Crimeia e ativou os secessionistas do Donbass em 2014 (tubos de ensaio para o experimentalismo russo no setor dos grupos paramilitares "privados", que mais tarde passaram a operar desafogadamente em África), com o beneplácito de potências europeias, mas sem os EUA[6]. Interferiu nas eleições presidenciais norte-americanas e no referendo ao Brexit no Reino Unido, em 2016. Conduziu uma "anexação suave" com a Bielorrússia, depois da manobra eleitoral de 2020, e assinou uma declaração de "amizade sem limites"[7] com a China nas vésperas do evento que marcou o fim da passividade ocidental ao ressurgimento russo: a invasão plena da Ucrânia, em 24 de fevereiro de 2022.

Mais de dois anos depois e perante o impasse na guerra mais violenta do séc. XXI na Europa, uma ameaça como a que o candidato presidencial norte-americano Donald Trump fez em fevereiro último de "encorajar a Rússia a atacar qualquer país membro da OTAN que não cumpra as suas obrigações financeiras para com a aliança"[8] tem de ser equacionada como um forte abalo à confiança que os europeus depositam no seu maior aliado e protetor da atual ordem política europeia. Mesmo que não passe de uma insinuação torpe, dita, desdita e reinterpretada, a perspetiva de uma Europa da Defesa sem os Estados Unidos pode, afinal, ser o estímulo necessário e suficiente para obrigar os aliados a aceitar um pilar europeu da OTAN mais unificado, capacitado e resolvido a atuar sozinho quando lhe faltarem os apoios políticos norte-americanos ou tropeçarem em nós górdios securitários como o de Chipre[9].

A argumentação principal deste artigo é que os contributos dos 30 países membros na Europa para a divisão de encargos da OTAN devem ser revistos, atendendo ao valor dos dados que as grandes empresas tecnológicas obtêm deste espaço, que nunca foram valorizados. Para sustentarmos este argumento, em primeiro lugar, constatamos

4 Naquela que é referida como a primeira guerra europeia do séc. XXI, que ocorreu quatro meses depois da Cimeira da OTAN de Bucareste, onde foi aberta a possibilidade da Geórgia e da Ucrânia poderem vir a ser membros da Aliança.

5 Bloqueando a ação do Conselho de Segurança das Nações Unidas, entre outras medidas.

6 O formato da Normandia, usado para chegar aos acordos de Minsk (I e II), revelou o fracasso das fórmulas exclusivamente europeias de resolução de conflitos. Cf. https://cepa.org/article/minsk-and-normandy-failed-whats-next/

7 http://www.en.kremlin.ru/supplement/5770

8 https://www.politico.eu/article/trump-says-he-would-encourage-russia-to-attack-nato-members-that-dont-pay-enough/. Para outras citações de Trump sobre a OTAN, consultar: Donald Trump on NATO: Top quotes – DW – 07/09/2018.

9 Chipre representa as tensões que podem emergir dentro da OTAN e da União Europeia, por força das posições antagónicas da Grécia e da Turquia e das bases britânicas ali instaladas, em especial porque Chipre não é membro da OTAN e porque a Turquia não é membro da União Europeia. Cf. https://www.unav.edu/web/global-affairs/eu-nato-cooperation-on-the-cyprus-conflict

que as capacidades militares dos países europeus estiveram sempre aquém dos EUA e que isso foi mais evidente nas operações "fora de área". Essa condição agravou-se com a transformação da base industrial de defesa de uma época industrial para uma era em que a principal fonte de riqueza é derivada da economia de dados. Tendo presente as tendências emergentes da Guerra da Ucrânia e também por causa das tensões securitárias da região do Indo-Pacífico, manifestada pela ameaça chinesa a Taiwan e às forças americanas, os EUA aceleraram o desenvolvimento de novas capacidades e instaram os países europeus a aumentarem os seus orçamentos de defesa. Porém, continuam a tratar das vendas do seu armamento num plano bilateral e a não encorajar os esforços para o desenvolvimento de uma base tecnológica de defesa integrada na Europa, que seja concorrencial com a sua. Por causa da possibilidade dos EUA se tornarem mais isolados num eventual segundo mandato de Donald Trump, o que terá consequências na resolução da guerra na Ucrânia, será necessário arranjar novas interpretações para a divisão de encargos e para a possibilidade de os europeus terem de enfrentar esse e outros desafios securitários com maior autonomia. Este artigo está estruturado em três secções. Na primeira, olhamos para a tradição de adaptação estratégica da OTAN ao longo dos seus 75 anos, destacando dois elementos fundamentais para a sua continuidade: não existência de interesses antagónicos entre os Estados-membros e o mecanismo de decisão liberal que permite o consenso perante o desacordo e daí uma adaptabilidade estratégica com provas dadas. O contexto dessa secção é o da evolução dos conceitos estratégicos e das principais operações aliadas, para salientar a dificuldade do desenvolvimento de capacidades militares que satisfizessem as necessidades requeridas pelos EUA, em especial nas operações "fora de área", como o Afeganistão e a Líbia. Na segunda secção voltaremos a nossa atenção exatamente para as duas matérias que têm, desde sempre, ameaçado a ordem interna da Aliança Atlântica: a divisão de encargos (o famoso *burden sharing*) e as capacidades de defesa dos países europeus (muitas vezes confundidas com capacidades de defesa europeia). Por fim, o foco vai para o cerne atual do desenvolvimento dessas capacidades, constituído pelos ecossistemas de defesa moderna, propondo que a almejada autonomia europeia em matéria de defesa, possa ser alcançada dentro da OTAN, se houver a necessária coordenação estratégica entre os dois lados do Atlântico. Para isso, será necessário que o emergente mercado único de defesa europeu se afirme e concorra com o complexo militar-industrial americano, se não for em pé de igualdade, que seja em nome da reciprocidade. A chave para a resolução do problema estará na abertura do mercado de defesa americano às indústrias de defesa europeias, como moeda de troca daquilo que os Estados Unidos obtêm da Europa: influência, dados europeus que têm vindo a alimentar os lucros desmesurados das suas empresas tecnológicas e uma conciliação estratégica para enfrentar a emergência da China. Não será fácil, sob um eventual segundo mandato Trump, mas será, no mínimo, negociável.

OTAN – Uma Aliança Maleável

A OTAN é uma aliança notável. Em 75 anos de história, cresceu de 12 membros fundadores para 32 e apesar de haver oposição interna à participação na organização em alguns países, nenhum deles apresentou, até à data e formalmente, um pedido de saída, previsto no Artigo 13.º do Tratado do Atlântico Norte[10]. Curiosamente, o primeiro alargamento ocorreu em Lisboa, numa cimeira em fevereiro de 1952, onde foram admitidos, como Estados-membros, a Grécia e a Turquia[11]. Data dessa reunião a criação do cargo de Secretário-Geral, depois de ter sido nomeado o primeiro comandante militar aliado, o general norte-americano Dwight Eisenhower, em dezembro de 1950. Se pensarmos que a criação da República Popular da China ocorreu no mesmo ano da assinatura do Tratado de Washington (4 de abril de 1949) e que a institucionalização da estrutura militar permanente da OTAN é simultânea da Guerra da Coreia (1950), conseguimos estabelecer a ligação da segurança europeia à região do Indo-Pacífico, para lá da ameaça soviética que então despontava, conseguindo novas explicações para a continuidade da Aliança Atlântica, mesmo após o fim da Guerra Fria e renovando desafios geopolíticos absolutamente atuais. O primeiro Secretário-Geral da OTAN, o britânico *Lord* Ismay, dizia que a NATO tinha sido criada para manter "a União Soviética fora, os americanos dentro e os alemães em baixo"[12]. Nesse sentido, a OTAN cumpriu integralmente os seus propósitos. Mais concretamente, o arranjo que surgiu na Cimeira de Lisboa de 1952, com a criação de um organismo internacional de apoio ao Secretário-Geral (*International Staff*), onde os países dispõem de representações diplomáticas em simultâneo com um Estado-Maior militar permanente, contribuiu decisivamente para uma institucionalização da Aliança que é marca distintiva do seu *modus operandi*, face a outras alianças regionais antissoviéticas patrocinadas pelos EUA no pós-Segunda Guerra Mundial[13]. Outra curiosidade da Cimeira de Lisboa de 1952 é que foi nessa altura que a OTAN começou a ser ligada à dissuasão nuclear americana[14], muito por força

10 https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt

11 Durante muitos anos, a única fronteira entre a União Soviética e a OTAN.

12 https://www.nato.int/cps/en/natohq/declassified_137930.htm

13 Nomeadamente, a Organização do Tratado do Sudeste Asiático, que apenas teve interesse para as potências ocidentais e foi desmantelada em 1977. Cf. https://history.state.gov/milestones/1953-1960/seato. E das organizações relacionadas com a segurança no Atlântico Sul, que não passaram de especulações, com o seu auge em 1982, por ocasião da Guerra das Falkland/Malvinas. Cf. https://www.jstor.org/stable/2619934

14 Data desse ano, também, a criação do Comando Estratégico para o Atlântico (*Strategic Allied Command Atlantic* – SACLANT). O Grupo de Planeamento Nuclear, um dos principais corpos da orgânica da Aliança, só foi formado em 1966, na sequência da saída da França da estrutura militar integrada.

da incapacidade de os países europeus gerarem o nível de forças convencionais anteriormente acordadas[15].

Uma vida longa tem, naturalmente, assistido a sucessos e a intervenções mais polémicas. Dos primeiros, destacamos a Guerra Fria e a estabilização dos Balcãs, que ainda está por concluir. As intervenções "fora de área" no Afeganistão, no Iraque[16] e na Líbia têm sido muito criticadas, mas não deixam de conter diversas lições que podem orientar decisões futuras.

A inesperada hecatombe soviética, que culminou em 26 de dezembro de 1991, com a dissolução da URSS, foi percebida por todos como uma vitória ocidental sem combater e pôs em evidência a discussão em torno da continuidade da OTAN, perante a ausência de inimigo. De todo o processo de quatro décadas resultava um facto irrefutável: a dissuasão funcionou e o conflito entre as duas superpotências teve de ganhar contornos de procuração noutras geografias, mas a Europa foi preservada.

As décadas que se seguiram foram de esperança na cooperação entre anteriores inimigos. A declaração da Cimeira de Roma de 8 de novembro de 1991[17] falava num novo capítulo na história da Aliança e numa comunidade de interesses partilhados entre a América do Norte e "toda" a Europa. Desafiava-se o desenvolvimento da democracia na União Soviética e nos outros países da Europa Central e de Leste e anunciava-se a complementaridade da OTAN com outras organizações de segurança no espaço europeu, nomeadamente, a Conferência de Segurança e Cooperação na Europa (CSCE), a Comunidade Europeia, a União Europeia Ocidental (UEO) e o Conselho da Europa[18]. Sinal dos tempos, foi aprovado um novo Conceito Estratégico aliado[19], tornado público pela primeira vez. Ao contrário dos outros quatro documentos estratégicos anteriores, não era identificado claramente um inimigo. Uma breve leitura pelos sucessivos conceitos estratégicos[20] permite-nos salientar o caráter

15 https://www.nato.int/acad/fellow/94-96/mccalla/3b1b.htm.

16 Atualmente existe uma missão de aconselhamento e capacitação militar designada "NATO Mission Iraq", que substituiu outra, designada "NATO Training Mission-Iraq (NTM-I)", que se ocupou da reforma das forças armadas iraquianas e que decorreu entre 2004 e 2011. https://www.nato.int/cps/en/natohq/topics_166936.htm

17 https://www.nato.int/docu/comm/49-95/c911108a.htm.

18 Questões persistentes no atual panorama de segurança europeia. Em 2022, o presidente francês lançou uma iniciativa, designada Comunidade Política Europeia, com ligações quer à União Europeia, quer ao Conselho da Europa, para integrar todos os países que "subscrevem os nossos valores centrais para procurar um novo espaço de cooperação nas questões políticas, de segurança, energia, infraestrutura, investimento e migrações". Este fórum mantém um observatório (https://epc-observatory.info/), já conduziu três cimeiras e a quarta ocorreu a 18 de julho de 2024, no Reino Unido, designadamente no local de nascimento de Winston Churchill, uma semana depois da cimeira comemorativa dos 75 anos da OTAN, em Washington.

19 https://www.nato.int/cps/en/natohq/official_texts_23847.htm.

20 Para uma revisão dos documentos estratégicos da OTAN entre 1949 e 1969 consultar https://www.researchgate.net/publication/280287417_NATO_Strategy_Documents_1949-1969.

adaptativo da estratégica aliada, muito por força dos processos de negociação interna e da ausência de antagonismos entre os Estados-membros.

O primeiro dos documentos mencionados, intitulado *The Strategic Concept for the Defense of the North Atlantic Area*, com o código DC 6/1[21], foi aprovado em 6 de janeiro de 1950. Estabeleceu as orientações para o desenvolvimento de planos regionais com um horizonte de quatro anos, que rapidamente tiveram de ser revistos, perante a impossibilidade de geração das forças convencionais necessárias e pela perturbação provocada pela Guerra da Coreia. Durante a década de 50, foram produzidos mais dois documentos dessa natureza, o MC 14/1 *Strategic Guidance*[22], de 9 de dezembro de 1952, que afirmava que "o conceito para a defesa da Europa Ocidental é suster o inimigo o quanto mais a Leste na Alemanha for viável, usando todos os meios ofensivos e defensivos disponíveis, de modo a negar ou limitar ao máximo a sua liberdade de ação", e o MC 14/2 *Overall Strategic Concept for the Defense of the North Atlantic Treaty Organization Area*[23], de 23 de maio de 1957, já depois da adesão da República Federal Alemã à Aliança Atlântica, em 6 de maio de 1955 (segundo alargamento aliado) e da consequência desse facto: a assinatura do Tratado de Amizade, Cooperação e Assistência Mútua, em Varsóvia, no dia 14 de maio 1955, que instituiria o Pacto de Varsóvia, entendido como esteio militar da organização económica conhecida por Conselho para Assistência Económica Mútua (COMECON), que, por sua vez, representava a resposta de Moscovo ao Plano Marshall americano.

Durante a Guerra Fria, só foi produzido mais um documento desta categoria. Em 16 de janeiro de 1968 foi aprovado o MC 14/3, com o mesmo título do anterior[24], que defendia dois princípios básicos: a flexibilidade e a escalada, em oposição à retaliação nuclear massiva, que não tinha impedido a instalação de mísseis soviéticos em Cuba nem o início da Guerra do Vietname. Induzia-se um sentimento de incerteza sobre a verdadeira resposta a dar pelos aliados em caso de agressão soviética. Por outro lado, a retirada da França da estrutura militar integrada[25], em 1966, sinalizava as dúvidas perante os reais compromissos do empenho americano "até aos extremos" em caso de confrontação na Europa[26].

No já mencionado conceito de 1991, perante a ausência de inimigo, identificava-se um conjunto de riscos à segurança dos Estados-membros e abriam-se as portas da Aliança ao espaço soviético através de um conjunto de parcerias, diálogos e

21 https://www.nato.int/docu/stratdoc/eng/a491201a.pdf.

22 https://www.nato.int/docu/stratdoc/eng/a521209a.pdf.

23 https://www.nato.int/docu/stratdoc/eng/a570523a.pdf

24 https://www.nato.int/docu/stratdoc/eng/a680116a.pdf

25 A França haveria de regressar à estrutura militar integrada por ocasião do sexagésimo aniversário da OTAN, em 4 de abril de 2009.

26 As dúvidas persistem, atualmente, levando a questões hipotéticas sobre se os americanos estariam dispostos a trocar Nova Iorque por Vilnius. Cf. https://warontherocks.com/2022/04/russias-invasion-of-ukraine-and-natos-crisis-of-nuclear-credibility/

plataformas de cooperação. Foi este enquadramento que tornou possível a atuação da OTAN nos Balcãs e áreas adjacentes (portanto, *stricto sensu*, "fora de área", cumprindo o desafio de "out of area or out of business", lançado pelo senador norte-americano Richard Lugar[27]) enquadrada pelas resoluções das Nações Unidas, pela primeira vez em combate[28]. Esta intervenção, fora do contexto tradicional,[29] abriu as portas a uma revisão das tarefas aliadas que viriam a ser reformuladas no conceito estratégico aprovado por ocasião dos 50 anos da Aliança em 1999, com o título *The Alliance's Strategic Concept*[30], marcado, também, pelo quarto alargamento, desta vez para Leste[31]. A adaptação estratégica, conceptual e pragmática, em linha com a resposta flexível anterior, passava a ser uma característica essencial da Aliança e indicava uma agilidade institucional muito importante, num contexto de segurança internacional bastante fluido. Nesse documento, mais uma vez, não foi identificada nenhuma ameaça proveniente de um Estado. É de sublinhar que a Rússia era referida como parceira para a "construção de uma Europa una, estável e pacífica", depois de ter integrado o programa da Parceria para a Paz, em 1994, e de ter assinado o Ato Fundador com a OTAN[32], em 1997, sendo que a Organização para a Segurança e Cooperação na Europa (OSCE), sucedânea da CSCE, era tida como a única organização de segurança pan-europeia, estando ambos os lados comprometidos com o seu reforço, em linha com o "Documento de Lisboa"[33], na prossecução de um "Modelo de Segurança Comum e Abrangente para a Europa do Século XXI". Apesar disso, estipulava o conceito aliado que embora uma agressão convencional de larga escala contra a Aliança fosse altamente improvável, a possibilidade de uma ameaça desse tipo vir a materializar-se no longo prazo não podia ser descartada. Sinal dos tempos de desanuviamento, foi avançada uma nova definição de segurança, mais abrangente, de modo a incluir fatores políticos, económicos, sociais e ambientais, para além da tradicional defesa, e identificado um conjunto de riscos que afetavam

27 https://collections.libraries.indiana.edu/lugar/items/show/342#?c=0&m=0&s=0&cv=0&xywh=-2764%2C-375%2C10601%2C7495

28 A primeira ação de combate envolvendo meios da OTAN ocorreu a 28 de fevereiro de 1994, quando foram abatidos quatro caças sérvios que violavam a Zona Aérea Interdita sobre a Bósnia Herzegovina, no âmbito da operação "Deny Flight". Cf. https://shape.nato.int/page2148121621

29 A OTAN conduziu diversas operações nos Balcãs e uma ainda se mantém, Força do Kosovo – KFOR (https://jfcnaples.nato.int/kfor). Cinco países da região são hoje membros da Aliança (Albânia, Croácia, Eslovénia, Macedónia do Norte e Montenegro), enquanto três ainda não (Bósnia e Herzegovina, Kosovo e Sérvia).

30 https://www.nato.int/cps/en/natohq/official_texts_27433.htm

31 O terceiro alargamento tinha acontecido com a adesão da Espanha em 1982.

32 https://www.nato.int/cps/su/natohq/official_texts_25468.htm Previu-se, inclusive, a abertura de um Gabinete de Informação e Documentação da OTAN em Moscovo. Este gabinete funcionou junto da Embaixada da Bélgica desde 2001 até 2021, ano em que a Federação Russa solicitou o seu encerramento. https://www.politico.com/news/2021/10/18/russia-suspends-mission-nato-shuts-office-516189

33 https://www.osce.org/files/f/documents/1/0/39539.pdf

os Estados-membros, nomeadamente o terrorismo, o conflito étnico, as violações dos direitos humanos, a fragilidade económica e a proliferação das armas de destruição massiva e dos seus vetores de lançamento. Perante isto, o portefólio de tarefas fundamentais alargou-se, passando a integrar a segurança, consultas, dissuasão e defesa, gestão de crises e parcerias. As forças aliadas deveriam ser modernizadas para poderem enfrentar o espetro total de operações, com a combinação apropriada entre capacidades convencionais e nucleares para três tipos básicos de intervenções: defesa coletiva, operações de apoio à paz e operações de resposta a crises. Quanto à União Europeia, referia-se o apoio ao estabelecimento de uma Identidade Europeia de Segurança e Defesa dentro da OTAN, compatível com o Tratado de Washington, em que os aliados europeus assumissem maiores responsabilidades.

Foi precisamente um quadro de defesa coletiva e uma ação terrorista que levou a OTAN, mais uma vez, para "fora de área", em 2003, para um envolvimento que poderá ser entendido como o maior insucesso aliado até à data: o longínquo Afeganistão[34]. Com efeito, o 11 de setembro de 2001 desencadeou um acontecimento histórico para as relações transatlânticas: a primeira e única, até à data, invocação do Art.º 5.º do Tratado de Washington, do qual resultaram duas operações[35]: a "Eagle Assit", de reforço ao dispositivo de defesa aéreo norte-americano e a "Active Endeavour", de controlo do Mar Mediterrâneo. A primeira contou com o destacamento de aeronaves de aviso aéreo antecipado (AWACS)[36] da OTAN, normalmente estacionadas em Geilenkirchen, na Alemanha, para os Estados Unidos e decorreu entre 9 de outubro de 2001 a 16 de maio de 2002. A segunda durou 15 anos, entre outubro de 2001 e outubro de 2016. Estas alcançaram plenamente os seus objetivos, mas não evitaram o fracasso da intervenção no Afeganistão.

Voltando à análise dos conceitos estratégicos, a relação com a Rússia, cuja colaboração auspiciosa da década de 90 tinha alcançado resultados práticos na estabilização dos Balcãs e na primeira fase das operações no Afeganistão, foi bastante afetada depois da chegada ao poder de Vladimir Putin, um antigo oficial do KGB que assistiu, em Dresden, ao estertor da República Democrática Alemã. Putin assumiu as funções de primeiro-ministro da Rússia, em agosto de 1999, dois meses depois do fim da operação "Allied Force"[37], que foi conduzida sem mandato das Nações Unidas e pôs à prova a consistência interna da OTAN durante os 78 dias que durou o bombardeamento aéreo do que restava da Jugoslávia. Nesse ano, a Federação Russa estava a ferro e fogo, com a violência a deflagrar em diversas cidades russas, Moscovo incluída, protagonizada por forças islâmicas do Cáucaso. O modo contundente como Putin começou a resolver esses problemas, incluindo o seu desempenho temporário do

34 https://www.nato.int/cps/en/natohq/topics_8189.htm
35 https://www.nato.int/cps/en/natohq/topics_110496.htm#invocation
36 *Airborne early Warning And Control System*.
37 https://www.nato.int/cps/en/natohq/topics_49602.htm

cargo de presidente interino, favoreceu a eleição para a sua primeira presidência em março de 2000.

A primeira década do século XXI assistiu a um ressurgimento russo, simultâneo de um intervencionismo americano, liderado pelos neoconservadores da administração do presidente George W. Bush, pouco dados a soluções multilaterais. O auge desta atuação unilateral foi a invasão do Iraque, ultimada na Cimeira das Lajes[38], nos Açores, a 15 de março de 2003, por dirigentes dos EUA, Espanha e Reino Unido, acolhidos pelo primeiro-ministro português Durão Barroso. Onze dias mais tarde, Bulgária, Eslováquia, Eslovénia, Estónia, Letónia, Lituânia, e Roménia[39] assinavam os protocolos de adesão à OTAN. O alargamento da Aliança Atlântica foi visto como uma afronta por Moscovo, ligado ao pendor da política americana neoconservadora. Entretanto, a Rússia foi consolidando as suas posições no Cáucaso, encaminhando-se para uma vitória na Segunda Guerra da Chechénia, à medida que começava um ciclo de maior ingerência noutras anteriores repúblicas soviéticas, para evitar que seguissem o mesmo caminho dos Estados bálticos. São disso exemplo as interferências nas eleições presidenciais na Ucrânia em 2004 e a invasão da Geórgia em 2008. Apesar de tudo, a chegada ao poder dos democratas à Casa Branca, em janeiro de 2009, parecia indicar a vontade dos norte-americanos em estabelecer uma nova fase de relações com a Rússia, tendo ficado célebre a oferta pela Secretária de Estado Hillary Clinton de um botão de *reset* ao seu homólogo russo Sergei Lavrov[40], praticamente no início do mandato da nova administração. Um novo conceito estratégico aliado estava em elaboração. A sua aprovação final ocorreu na segunda cimeira da OTAN em Lisboa[41], em 2010, que contou com a presença do presidente russo Dimitri Medvedev[42] e continuava a não identificar nenhum país como ameaça. Estranhamente, esta situação ambígua teimava em perpetuar-se, tanto mais que, apenas três anos antes, Putin havia deixado claro de modo assertivo, na conferência de Munique, que a época da aproximação da Rússia ao Ocidente tinha terminado.

A erupção de uma vaga de revoltas que ficou conhecida como Primavera Árabe, levou a OTAN, mais uma vez, para "fora de área", através da operação "Unified Protector"[43], em 2011, de imposição de uma Zona de Exclusão Aérea sobre a Líbia, com mandato das Nações Unidas. Iniciada de forma precipitada e com muita pressão de alguns países europeus, os EUA foram convencidos a empregar as suas capacidades

38 https://arquivos.rtp.pt/conteudos/cimeira-nas-lajes/

39 https://www.nato.int/docu/update/2003/03-march/e0326b.htm

40 https://www.reuters.com/article/idUSN06402140/

41 https://www.nato.int/cps/en/natohq/official_texts_68828.htm

42 Putin era, então, primeiro-ministro, naquilo que mais tarde foi designado por presidência em tandem, com Medvedev. https://www.publico.pt/2010/11/21/mundo/noticia/nato-abre-nova-era-nas-relacoes-com-a-russia-1467324

43 https://www.nato.int/cps/en/natolive/71679.htm

estratégicas de comando e controlo, reabastecimento aéreo e de aviso antecipado, entre outras, dada a sua exiguidade entre os aliados europeus, mas afastaram-se das intenções da França para apoiar as atividades em terra contra as forças de Kadhafi. Durante esta operação foi revelada uma escassez significativa de munições de precisão por parte das forças aéreas inglesas e francesas, obrigando, mais uma vez, ao recurso das reservas americanas (Beaver e Fein, 2024).

Toda a cooperação prática entre a OTAN e a Rússia, estabelecida sob os auspícios do Conselho OTAN-Rússia (um mecanismo de diálogo e cooperação criado em 2002, em substituição do Conselho Conjunto Permanente OTAN-Rússia, formado na sequência do Ato Fundador com a OTAN, de 1997) cessou em abril de 2014, na sequência da anexação da Crimeia e do comportamento agressivo russo perante a Ucrânia. Entre 2016 e 2022, este Conselho ainda reuniu por seis vezes, mas o diálogo não tem sido possível, face às exigências russas de redesenho da Arquitetura de Segurança Europeia, impondo condições sobre o alargamento para Leste da Aliança, incompatíveis com o Art.º 10.º do Tratado de Washington, e do posicionamento de forças e armamento nos estados-membros que aderiram depois de 1997 (Pifer, 2021).

É num cenário de guerra aberta pela Rússia, num dos flancos da OTAN, que o Conceito Estratégico de 2022[44] é aprovado. O quarto documento desta natureza, desde que foram tornados públicos, afirma, sem margem para dúvidas, que a Federação Russa é a ameaça mais significativa e direta à segurança dos aliados. Nesse sentido, representa um contraste absoluto com o conceito estratégico anterior. Adotando uma linguagem abrangente[45], menciona o caráter regional da organização (euro-atlântica), mas refere "ameaças globais interligadas", ao ponto de identificar, pela primeira vez, a China como desafiadora estratégica, em especial nos domínios do espaço[46], ciberespaço e marítimo e nas operações de influência. É referido que uma ação hostil em cada um desses domínios ou várias, de um modo concertado, poderá conduzir a Aliança a invocar o Art.º 5.º, em virtude das consequências conjugadas poderem ser semelhantes às de ataque armado, com especial referência a operações híbridas, provenientes de Estados ou de agentes que utilizem organizações que atuem por procuração em nome desses Estados.

Esta breve revisão dos conceitos estratégicos e das principais operações, permite-nos aquilatar a agilidade da OTAN para se adaptar a um ambiente de segurança internacional em revisão permanente. Grande parte da atratividade da Aliança

44 https://www.nato.int/cps/en/natohq/topics_210907.htm

45 De notar o uso da expressão "aproximação 360 graus" em linha com a Bússola Estratégica para a Segurança e a Defesa da União Europeia (um documento adotado três meses antes). Cf. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf

46 Em 2019, os aliados adotaram uma política espacial e reconheceram o espaço sideral como o quinto domínio operacional, a par da terra, mar, ar e o ciberespaço. Cf. https://www.nato.int/cps/en/natohq/topics_175419.htm

está nas capacidades unicamente detidas pelos EUA (em especial, o armamento nuclear, a defesa antimíssil, as capacidades de comando e controlo, mas também os contributos das grandes empresas tecnológicas do setor do espaço e dos sistemas de informação), que têm provocado um certo entorpecimento de muitos países europeus, mas também na simplicidade do articulado do Tratado de Washington, que sem identificar detalhadamente os propósitos da OTAN, nem especificar os mecanismos de coordenação interna, permite muita flexibilidade aos países membros para irem ajustando as suas posições negociais, sem antagonismos secessionistas. A deliberação por consenso, mesmo perante o desacordo, tem possibilitado a ação conjunta da Aliança no cumprimento das suas tarefas essenciais, sistematicamente reafirmadas, de dissuasão e defesa coletiva, prevenção e gestão de crises e segurança cooperativa. Para os aliados europeus não tem havido qualquer alternativa perante a falha em chegar a um acordo sobre uma arquitetura de paz e segurança pan-europeia longa e duradoura, em especial com a atitude revisionista da Rússia, sob a liderança de Putin, como se viu na falência dos Acordos de Minsk, de que resultou a paralisia da OSCE (Hernández, 2023). No entanto, o torpor no desenvolvimento de capacidades militares úteis ao combate moderno e na partilha de encargos por parte de alguns países europeus tem várias explicações que, não sendo novas, têm agravado a dissonância entre os dois lados do Atlântico. Disso trataremos na próxima secção.

Divisão de encargos e o desenvolvimento de capacidades de defesa de países europeus.

A divisão de encargos e o desenvolvimento de capacidades representam dois elementos da mesma equação relativa à segurança europeia. A primeira é, assumidamente, a componente de entrada (*input*) e a segunda, manifestamente, a componente de saída (*output*) de um sistema de segurança multinacional, pluricontinental, mas com um foco na Europa. Ou seja, para se alcançar um determinado estado de prontidão para a defesa, incluindo a dissuasão, os países-membros devem acordar nas regras que regulam os seus contributos na produção desse "bem coletivo" que é a segurança do conjunto. Esses cálculos são extremamente complicados de serem realizados, especialmente porque dizem respeito a países muito heterogéneos em termos de riqueza, população, território, perceção da ameaça, recursos industriais, etc. A atual transformação digital e o contexto securitário global agravam a complexidade da abordagem dos dois temas em questão.

Tal como não existe uma especificação concreta para a finalidade da Aliança nos seus documentos estratégicos, também não existe uma regra fixa para o seu financiamento e ou divisão geral de encargos. Esta é uma das questões mais permanentes nas

reuniões da Aliança, ao ponto de ser considerada uma característica duradoura das relações entre os Estados-membros e mais concretamente entre os EUA e os aliados europeus. Este assunto representa, acima de tudo, um teste ao espírito de coesão e solidariedade dos aliados, aludido no Art.º 3.º do Tratado de Washington, que estipula: "a fim de atingir mais eficazmente os fins deste Tratado, as Partes, tanto individualmente como em conjunto, manterão e desenvolverão, de maneira contínua e efetiva, pelos seus próprios meios e mediante mútuo auxílio, a sua capacidade individual e coletiva para resistir a um ataque armado"[47].

Julgou-se que a já mencionada operação "Unified Protector", na Líbia, em 2011, pudesse constituir um modelo para uma OTAN "pós-americana", em que os EUA liderassem a partir da retaguarda (*leading from behind*)[48], com alguns países europeus a assumirem maiores responsabilidades no fornecimento da maior parte das capacidades militares, em especial porque a campanha era exclusivamente aérea, de baixa intensidade e de objetivos limitados. Porém, o que se viu foi um desentendimento e uma fragmentação das prestações de alguns países europeus, fruto de uma fraca coordenação entre as diversas operações nacionais, tendo-se assistido, entre outros episódios, à retirada prematura do porta-aviões italiano Garibaldi[49] e de aeronaves norueguesas[50], por falta de fundos para continuar o empenhamento desses meios por um período prolongado. Em vez de ser um protótipo para o futuro da divisão de encargos entre os dois lados do Atlântico, a intervenção na Líbia mostrou mais as limitações da OTAN que o seu poder, pondo em evidência as lacunas europeias em meios operacionais críticos. Datam desse ano as declarações pungentes do Secretário da Defesa norte-americano Robert Gates acerca de um futuro sombrio para a Aliança, avançando premonitoriamente, "na verdade, se as atuais tendências de declínio das capacidades de defesa europeias não forem travadas e revertidas, os futuros líderes políticos dos EUA – aqueles para quem a Guerra Fria não foi a experiência formativa que foi para mim – poderão não considerar que o retorno do investimento da América na OTAN vale o seu custo"[51]. Para alguns autores, "qualquer movimento em direção a uma Aliança pós-americana requer uma mudança nas mentalidades quer dos EUA, quer dos seus aliados, porque enquanto aqueles continuarem a desempenhar uma liderança dominante na OTAN, os incentivos para os países europeus incrementarem os seus contributos serão reduzidos" (Hallams e Schreer, 2012).

47 https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt
48 https://www.nato.int/docu/review/articles/2011/09/06/nato-after-9-11-a-us-perspective/index.html
49 https://www.atlanticcouncil.org/blogs/natosource/italy-withdrawing-its-aircraft-carrier-from-natos-libya-operation/
50 https://www.defenceweb.co.za/joint/diplomacy-a-peace/norway-withdraws-f-16s-from-libya/
51 https://www.atlanticcouncil.org/blogs/natosource/text-of-speech-by-robert-gates-on-the-future-of-nato/

Alguns autores, como Kunertova (2017) e Mattelaer (2016), entre muitos outros[52], estudaram as origens do debate nos primeiros tempos de vida da OTAN para encontrarem pistas que alimentem as soluções políticas perante o desacordo da divisão de encargos. A primeira apresenta uma retrospetiva das sucessivas decisões que foram sendo tomadas pelos aliados, propondo uma viragem qualitativa na divisão de encargos, de modo a alcançar um equilíbrio entre os princípios da simplicidade, da justiça e da eficácia, tal como se de um sistema tributário se tratasse, em vez da persistência na fixação de uma regra quantitativa pura[53], que apenas satisfaz o princípio da simplicidade e se limita a focar as medidas de *input*, não as de *output* associadas às capacidades. De um modo geral, colocar mais dinheiro nos orçamentos de defesa e fazê-lo em relação ao Produto Interno Bruto (PIB) não garante, *per se*, a melhoria (e atualização) das capacidades de defesa da Aliança. A autora defende que o processo sempre foi dinâmico e que necessita de revisões e ajustamentos constantes. A evidência provém do processo de planeamento estratégico da OTAN (*NATO Defense Planning Process* – NDPP), focado nas capacidades existentes em cada país para a constituição do leque alargado das forças aliadas e no seu desenvolvimento futuro. O que conta, neste âmbito, é o planeamento de recursos, partilha de equipamento e infraestruturas e a mobilização dos efetivos que a Aliança necessita para defender o seu território, sendo este o mecanismo que incorpora, ainda que indiretamente, a divisão de encargos e tarefas de uma maneira mais pragmática. Nele não está explícita nenhuma divisão entre capacidades norte-americanas e europeias, nem implicitamente nenhuma referência às indústrias de defesa, numa perspetiva de benefício para os seus detentores. Este debate já aconteceu na Aliança. De facto, a primeira referência à divisão de encargos foi em 1951, quando houve que edificar as estruturas de comando permanente. Nessa altura, estabeleceram-se algumas regras, eminentemente práticas, para o financiamento do orçamento comum, que contemplava as componentes militares e civis da OTAN, bem como a parte relacionada com as infraestruturas físicas da Aliança, exclusivamente situadas em solo europeu. A participação de cada país para o orçamento comum foi inspirada pelas regras de financiamento da ONU, baseadas no rendimento nacional, e ainda hoje é usada para calcular a percentagem relativa das contribuições individuais. Além do fundo comum, também existem os projetos conjuntos, que são financiados voluntariamente pelos países aderentes. Estas duas

52 Para uma revisão exaustiva sobre a divisão de encargos na OTAN, consultar Koivula e Ossa (2022).

53 O debate em torno dos 2% do PIB surgiu na Cimeira de Gales de 2014 e contemplava compromissos até 2024, além dos 2% do PIB no orçamento de defesa, como mínimo; mais 20% desse orçamento deveria ser atribuído ao *procurement* e à modernização de equipamento e nenhum aliado sozinho deva contribuir mais do que 50%. Cf. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

componentes constituem o financiamento direto da Aliança, que representa apenas 0,3% dos gastos aliados com defesa.[54]

Embora os custos iniciais de funcionamento da OTAN não fossem muito altos, assim que a discussão foi colocada em termos de investimentos em infraestruturas, várias outras questões se levantaram, como fossem o valor dos terrenos onde iriam ser construídas e os benefícios que resultariam para o fornecedor dos trabalhos de construção para a economia do país que os acolhesse. Daqui resultou a autonomização da edificação e manutenção das infraestruturas, cada uma com um projeto próprio de financiamento, separado do orçamento comum, seguindo soluções de compromisso baseadas no grau de uso comum e a capacidade de cada país contribuir para o custo total.

Deve ser recordado que nos primeiros tempos de vida da OTAN ainda decorria o Plano Marshall, cujo financiamento se prolongou até 1952, tendo sido substituído pela Lei (norte-americana) de Segurança Mútua[55], que durou até 1961 no que se refere ao apoio pelos EUA a alguns países europeus em diversas áreas do seu desenvolvimento. A partir desse ano e já com a Comunidade Económica Europeia em pleno funcionamento, depois da entrada em vigor do Tratado de Roma, em 1958, ocorreu a fundação da Organização para Cooperação e Desenvolvimento Económico (OCDE) que concentrou algumas das responsabilidades de coordenação anteriormente detidas pela Organização para a Cooperação Económica Europeia (OCEE), que tinha gerido os contributos dos Estados Unidos e Canadá à reconstrução europeia no pós-guerra. Se, durante a Guerra Fria, os EUA estavam dispostos a assumir uma parcela acrescida dos custos da preparação para um eventual conflito com a União Soviética, porque atribuíam uma grande utilidade à sua presença na Europa para alcançar os seus próprios interesses, certo é que nas últimas décadas passaram a lançar alertas cada vez mais exacerbados para uma maior participação dos países europeus nos encargos da Aliança. Aparentemente, isso deveu-se à ida dos aliados para "fora de área", com os destaques do Afeganistão e da Líbia, tendo os EUA afirmado, em 2013, que a sua percentagem de contribuição, como um todo, para a Aliança, tinha crescido de 50%, durante a Guerra Fria, para 75%, ao mesmo tempo que os orçamentos de defesa europeus iam diminuindo, fruto da crise financeira e da perceção da ameaça, levando o Secretário de Defesa norte-americano Chuck Hagel a afirmar que "o excesso de dependência de qualquer país para [fornecimento] de capacidades críticas traz consigo os seus riscos".[56]

Portanto, algo semelhante poderá ser pensado nesta altura da evolução da organização, se forem confrontados os benefícios que os EUA e a Europa, como um todo,

54 https://www.nato.int/cps/en/natohq/topics_67655.htm
55 https://www.govinfo.gov/content/pkg/STATUTE-65/pdf/STATUTE-65-Pg373.pdf
56 https://www.defenseone.com/ideas/2013/10/will-us-rebalance-its-contribution-nato/72281/

derivam dos seus ecossistemas de defesa, um pouco à semelhança do que foi feito relativamente às infraestruturas aliadas nos anos 50 do século passado.

As discrepâncias em termos de capacidades de defesa europeias (assim referidas, mas dizendo respeito aos países europeus individualmente) e norte-americanas representam uma falha estrutural e uma incapacidade de resolução deste problema por parte de uma organização intergovernamental como é a OTAN (Bergmann e Svendsen, 2023). No âmbito da Aliança, essa questão pode ser rastreada desde a Iniciativa de Capacidades de Defesa de 1999[57], com a ênfase colocada na projeção e sustentação de forças, assim como na sua proteção, de modo a dar resposta aos problemas encontrados nos Balcãs na década de 90 do século passado. Data desse ano a transferência da responsabilidade de gestão de crises da União da Europa Ocidental (UEO) para a esfera da União Europeia, robustecendo as responsabilidades desta organização em termos de segurança e defesa, no âmbito da então designada Política Europeia de Segurança e Defesa (PESD) e na sequência de outras decisões coletivas anteriores. E foi exatamente nessa altura que os Estados Unidos puseram o primeiro travão na autonomização da defesa europeia integrada, com os designados três "D" da Secretária de Estado Madeleine Albright (discriminação da UE contra Estados europeus membros da NATO; duplicação da segurança europeia oferecida pela OTAN; dissociação da tomada de decisão europeia na tomada de decisão na Aliança)[58], depois de uma cimeira anglo-francesa em St. Malo em dezembro de 1998[59].

O assunto das capacidades europeias da OTAN foi recuperado em 2002, com os compromissos de Praga (*Prague Capabilities Commitment* – PCC), onde os aliados concordaram em desenvolver, individual e coletivamente, as suas capacidades em 400 áreas específicas, cobrindo oito campos essenciais às operações militares da época[60]. No ano seguinte, entrou em vigor o quadro de referência para uma cooperação mais institucionalizada entre as duas organizações, com os chamados acordos "Berlim Mais", que previam que a gestão de crises e as operações militares lideradas pela UE fizessem uso das capacidades e meios coletivos da OTAN, incluindo os arranjos de comando e controlo e a assistência no planeamento operacional, sem que a Aliança, como um todo, estivesse envolvida. Data desse ano a declaração de parceria estratégica, entre as duas organizações[61]. Os PCC foram reafirmados e quantificados em 2004, na Cimeira de Istambul. Sumariamente, 40% das forças terrestres teriam de

57 https://www.nato.int/cps/en/natohq/official_texts_27443.htm
58 https://www.jstor.org/stable/resrep06989.8?seq=1
59 Declaração conjunta em: https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf
60 https://www.nato.int/cps/en/natohq/topics_50087.htm
61 230110-eu-nato-joint-declaration.pdf

ser destacáveis e 8% teriam de ser apoiadas em missões "fora de área", em qualquer altura.[62].

A política americana face a uma maior autonomia estratégica europeia tem sido, no mínimo, ambígua, para não dizer bloqueadora. Outro exemplo da manipulação americana à integração de defesa europeia foi a carta enviada pelas duas Subsecretárias da Defesa norte-americanas Ellen Lord e Andrea Thompson à Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança, Federica Mogherini, em 2019, a propósito das regras de funcionamento do Fundo Europeu de Defesa e da Cooperação Estruturada Permanente (*Permanent Structured Cooperation* – PESCO)[63], perante um eventual bloqueio a terceiros países (leia-se Estados Unidos e Reino Unido, nesta altura já com data de saída da União Europeia), que foram designadas como o "veneno" das relações transatlânticas[64]. Bergmann e Svendson (2023) resumem a atitude norte-americana numa falta de articulação explícita sobre o que os EUA querem realmente da Europa. Por um lado, dizem que os Europeus não gastam o suficiente na sua defesa e por outro querem manter-se influentes com a sua presença no continente. Os EUA beneficiam do apoio de alguns países europeus para o avanço da sua política internacional, mas evitam enquanto podem a emergência de um bloco integrado como um todo. Estimulam e conseguem o alargamento da OTAN, mas negoceiam bilateralmente com os novos membros os seus programas de aquisição de sistemas de armas, em concorrência com o armamento europeu. Lamentando a paralisia na resolução de um problema que já havia sido identificado anteriormente, esses autores afirmam que o obstáculo principal do entendimento entre as duas partes é a atual dinâmica industrial de defesa norte-americana e europeia, ilustrada por um mercado de armamento norte-americano relativamente fechado e protegido e um mercado europeu aberto e dirigido pelos governos de cada um dos Estados. Portanto, no que se refere à política de defesa transatlântica existe uma desconexão estrutural que pode romper-se subitamente se a política norte-americana for de vistas curtas, centrada nos lucros das suas companhias (privadas) de defesa e não ajudar o conjunto de indústrias de defesa dominadas pelos governos europeus na modernização e transformação digital, uma vez que estas ainda estão focadas no desenvolvimento de sistemas de armas do tempo da Guerra Fria (navios, aeronaves, blindados, obuses, etc.), com elevados custos de produção e pouca interoperabilidade. Entretanto, na Europa a progressiva integração política tem sido resolvida através de negociações setoriais. Um dos últimos setores que resta negociar, por ser o mais difícil de resolver pela réstia de soberania que alberga, é o da defesa. A existência da OTAN tem permitido que uma boa fatia do orçamento tenha sido encaminhada

62 https://www.nato.int/cps/en/natolive/official_texts_19544.htm

63 https://www.euractiv.com/section/global-europe/news/pentagon-warns-eu-against-blocking-us-firms-from-defence-fund-2/

64 https://www.france24.com/en/20190514-us-warns-eu-over-poison-pill-defence-plans

para outros setores prioritários, como a saúde e a educação, obtendo-se, deste modo, a fruição do dividendo da paz, mas tem inibido o desenvolvimento de uma indústria de defesa moderna e competente, em especial quando comparada com a norte-americana. A soma dos contributos dos países europeus para a OTAN é seguramente menor que a soma das suas partes e não vão ser resolvidos apenas com um aumento substancial dos orçamentos nacionais de defesa. O sistema atual de divisão qualitativa de encargos (NDPP) só aponta caminhos, mas não os decide. Isso, por enquanto, ainda está nas diferentes capitais europeias e não em Bruxelas, nem em Washington.

O empoderamento da União Europeia enquanto ator de defesa é algo que nunca foi tentado na arquitetura de defesa europeia e isso pode ser alcançado pela continuidade da tradição da negociação setorial. O problema contemporâneo mais agudo é a necessidade existencial de decisões rápidas a este respeito[65], perante a desestabilização motivada pela agressão russa e o eventual cenário de uma invasão chinesa de Taiwan[66], resultando, de novo, numa interdependência entre a segurança europeia e do Indo-Pacífico[67]. Uma ajuda que os EUA podiam dar, em seu próprio benefício, para permitir o já célebre *pivot* para a Ásia[68], seria apoiar a emergência da UE como ator geopolítico e abrir o mercado de armamento norte-americano à concorrência europeia.

O desenvolvimento de capacidades de defesa europeias contribui obviamente para a partilha de encargos entre os dois lados do Atlântico Norte. Nessa tarefa, os aliados devem, desejavelmente, assegurar a coerência, a complementaridade e evitar a desnecessária duplicação de esforços[69]. Apesar destas declarações de

65 Veja-se a consideração do presidente francês que a Europa é mortal. Cf. https://www.economist.com/leaders/2024/05/02/emmanuel-macrons-urgent-message-for-europe

66 Confira-se, a este respeito, o cenário do envolvimento da OTAN descrito em Lee, J. (2024).

67 A NATO mantém relações bilaterais com a Austrália, Coreia do Sul, Japão e Nova Zelândia, num quadro de parcerias e partilha de informações sobre ciberdefesa, novas tecnologias e ameaças híbridas.

68 Lançado pelo presidente norte-americano Barack Obama, descrito como "the first Pacific president" https://www.brookings.edu/articles/the-american-pivot-to-asia/

69 Na prática, o caminho trilhado pelas duas organizações tem sido de duplicação. Alguns exemplos, não exaustivos: as Forças-tarefas Combinadas e Conjuntas (Combined Joint Task Forces-CJTF) da OTAN criadas em 1994 para integrar aliados e parceiros em missões de apoio à paz (Peace Support Operations – PSO) e servirem de ponte entre a OTAN e a UEO, que tinha criado as missões de Petersberg em 1992; o lançamento das Forças de Resposta OTAN (NATO Response Force – NRF) na Cimeira de Praga foi praticamente contemporâneo do estabelecimento dos Battlegroups da União Europeia, que resultaram da Estratégia de Segurança Europeia de 2003, tendo, na prática, ofuscado a sua eventual utilização; os conceitos de Smart Defense da OTAN e Pooling and Sharing da Agência de Defesa Europeia (European Defense Agency – EDA) equivalem-se; até as iniciativas mais recentes como o Acelerador de Inovação de Defesa para o Atlântico Norte (Defence Innovation Accelerator for the North Atlantic – DIANA) e o Fundo de Inovação da OTAN, tem praticamente os mesmos propósitos do Esquema de Inovação de

princípios, certo é que as repetições de conceitos e até de geração de forças têm persistido durante o debate em torno da designada autonomia estratégica europeia. Portanto, uma peça chave de todo este processo reside na colaboração entre a OTAN e UE[70] (Lima, 2009).

Atualmente, já foram anunciadas três declarações conjuntas OTAN-UE (2016, 2018 e 2023), revelando a expansão significativa da cooperação entre estas organizações nos últimos anos, bem como uma sincronia entre os documentos estratégicos (Conceito Estratégico da OTAN de 2022 e Bússola Estratégica para a Segurança e Defesa, também de 2022) onde ambas as organizações se reconhecem mutuamente como atores relevantes e alinhados ao mais alto nível, designadamente no enfrentamento de ameaças híbridas[71] e cibernéticas e pelos desafios protagonizadas pela Rússia e China. A Guerra da Ucrânia veio acelerar a reflexão sobre as matérias de defesa no seio da União Europeia, mas também agravou as divergências entre as respetivas capacidades que devem ser desenvolvidas no futuro. A secção seguinte aborda essas questões e o seu relacionamento com as bases tecnológicas e industriais que se encontram em profunda revisão.

A Guerra da Ucrânia e as novas capacidades de defesa transatlântica

A Guerra da Ucrânia, desencadeada ilegalmente pela Federação Russa a partir de 24 de fevereiro de 2022, veio demonstrar, mais uma vez, a impreparação dos países europeus para resolver um conflito no seu continente e a paralisia do arranjo anterior de segurança pan-europeia apoiado na OSCE. Só isso explica a adesão de dois países culturalmente neutrais à OTAN, como foi o caso da Finlândia e da Suécia. Por outro lado, a expansão do conflito a novos domínios como o espaço sideral e o ciberespaço, que nunca tinham sido testados simultaneamente numa guerra convencional entre Estados, pôs em evidência as limitações europeias para lidar com um conflito moderno, agravando a sua dependência dos EUA, pelo facto de estes disporem de um leque alargado de capacidades associadas à sua liderança tecnológica em praticamente todas as disciplinas da nova economia baseada em dados e sistemas de informação.

Ao fim de dois anos e meio de combate, algumas observações podem desde já ser recolhidas: a garantia da soberania ucraniana foi mantida pelas *Big Techs* americanas e as bases industriais de defesa estão em acelerada revisão em todo o lado. De facto,

Defesa da União Europeia (EU Defense Innovation Scheme), acionado pelo Fundo Europeu de Defesa.

70 https://www.nato.int/cps/en/natohq/topics_49217.htm

71 Note-se, a este respeito, o exemplo de colaboração entre a OTAN e a EU, no estabelecimento do Centro de Excelência contra Ameaças Híbridas que foi formado em Helsínquia, antes da Finlândia aderir à Aliança, na sequência da declaração conjunta de 2016, https://www.hybridcoe.fi/

foram os serviços de nuvem de empresas como a Microsoft, a Amazon e a Google que permitiram a continuidade dos serviços do Estado ucraniano face aos ataques cibernéticos e cinéticos russos (Sánchez e Torreblanca, 2023). Também a empresa de internet por satélite Starlink tem oferecido soluções de comunicações estratégicas absolutamente críticas para o governo, povo e forças armadas ucranianas, sendo inclusive procurada pelos próprios russos para equilibrar a vantagem ucraniana neste domínio[72]. Um dos primeiros líderes de uma empresa tecnológica americana a deslocar-se a Kyiv, a seguir à invasão russa, foi Alex Karp, líder da Palantir[73], uma firma que usa inteligência artificial para apoio a diversos governos ocidentais no domínio da segurança e defesa e fornece informação para aquisição de objetivos à Ucrânia. Muitas outras empresas têm sido envolvidas na Guerra da Ucrânia, tendo levado um jornal britânico a afirmar que a "Rússia analógica estava a ser flanqueada por munições das *Big Techs*"[74].

A Ucrânia atual representa um campo de experimentação não só no capítulo das tecnologias de apoio à guerra, mas também no domínio político[75]. Por um lado, as indústrias de armamento estrangeiras estão interessadas em recolher o maior número de dados possível de um conflito real, já que as simulações em tempo de paz não geram a mesma fiabilidade que os dados do combate, e por outro é disputada politicamente por um conjunto de países, designado genericamente por "Ocidente alargado", e por uma autocracia, como é a Rússia atual.

Central para o Ocidente foi a reforma conduzida no complexo industrial de defesa ucraniano, "UkrOboronProm", em março de 2023, que visa um incremento de produção interna e uma arquitetura de geometria variável com a participação de diversos países, com benefícios mútuos[76]. Também merece destaque o lançamento, em abril de 2023, da plataforma "Brave1"[77], que assegura a coordenação de projetos tecnológicos que interessam à área da defesa, sendo uma implementação conjunta entre diferentes áreas governamentais ucranianas (Ministério da Defesa, Ministério das Indústrias Estratégicas, Ministério da Economia, Estado-Maior-General das Forças Armadas e Conselho de Segurança e Defesa Nacional), mas sob a tutela do Ministério da Transformação Digital. Foi também lançado um fundo internacional que tem levado a cabo diversas iniciativas bilaterais com os EUA e com a União

72 https://breakingdefense.com/2024/04/pentagon-working-with-ukraine-spacex-to-prevent-russian-exploitation-of-starlink/

73 https://www.defensenews.com/land/2022/06/02/palantirs-karp-is-first-western-ceo-to-visit-zelenskyy-amid-invasion/

74 https://www.thetimes.co.uk/article/ukraine-is-outflanking-russia-with-ammunition-from-big-tech-lxp6sv3qz

75 https://time.com/6691662/ai-ukraine-war-palantir/

76 https://www.understandingwar.org/backgrounder/ukraine%E2%80%99s-long-term-path-success-jumpstarting-self-sufficient-defense-industrial-base

77 https://brave1.gov.ua/en/

Europeia, entre outros. Digno de nota para a indústria de defesa europeia é a declaração da abertura de um gabinete de inovação de defesa da UE em Kyiv, até final do corrente ano[78].

As guerras têm um efeito acelerador do fator tecnológico, dada a urgência dos beligerantes obterem vantagens no campo de batalha. A guerra da Ucrânia não é exceção. Com efeito, depois de muitos anos a combater inimigos de uma categoria inferior, os EUA despertaram para a competição geopolítica a Oriente, protagonizada pela China, que durante décadas estudou as modalidades de ação americana no mundo e desenvolveu antídotos para colocar em causa a vantagem potencial que os EUA terão num eventual apoio a Taiwan, resumidos naquilo que é descrito como técnicas anti-acesso e de negação de área (*Anti-acess and Area Denial* – A2/AD) (Impson, 2020), sustentadas por um aumento sistemático das despesas militares ao longo de várias décadas.

Nas vésperas da invasão plena da Ucrânia, a Rússia assinou uma "parceria sem limites" com a China[79]. O conflito também trouxe para primeiro plano a atuação russa no campo da guerra híbrida contra o Ocidente[80], as operações de influência global[81] e as dificuldades em desenvolver plataformas de combate moderno, que obrigaram a Rússia a estabelecer uma parceria com o Irão para fornecimento de *drones*[82]. Por seu lado, a intensificação de relações com a Coreia do Norte[83], de que é exemplo a visita de Putin a Pyongyang, em junho de 2024, sugerem a emergência de um eixo mundial de autocracias reunidas em torno da ideia de afrontar a ordem mundial dominada pelos EUA e seus aliados. Daqui se infere que o desenlace da Guerra da Ucrânia provocará consequências que vão para lá do continente europeu. Portanto, nada será mais urgente e crítico para o futuro da Europa, tal como esta tem vindo a ser construída nas últimas sete décadas, do que a mobilização das bases tecnológicas e industriais de defesa (BTID) dos dois lados do Atlântico Norte para fazer face ao aparelho militar russo na Ucrânia, mantendo a atenção nos acontecimentos no Indo-Pacífico e aquilo que se passa no flanco Sul, onde os grupos armados sob as ordens do Kremlin têm substituído as forças ocidentais, secundados pelo apoio financeiro da China aos regimes entretanto instalados.

78 https://www.eunews.it/en/2024/05/06/defense-eu-opens-innovation-office-for-industry-s-tartups-in-kyiv/

79 http://en.kremlin.ru/supplement/5770

80 https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html

81 https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/

82 https://www.c4isrnet.com/unmanned/uas/2024/03/27/attack-drones-at-heart-of-military-partnership-between-russia-iran/

83 https://www.iiss.org/publications/strategic-comments/2023/the-surge-of-activity-in-relations-between-north-korea-and-russia/

Perante a exposição anterior, não devem então surpreender as medidas tomadas pela atual administração Biden, tentando blindar os efeitos nefastos de uma eventual eleição de Donald Trump, que possa quebrar ou pôr em causa a ligação transatlântica. Vai nesse sentido a legislação aprovada pelo Congresso norte-americano, precavendo a retirada unilateral dos EUA da OTAN, sem autorização do Senado ou de uma Lei do Congresso[84]. Além disso, todos os instrumentos de planeamento de defesa norte-americanos foram revistos, desde a Estratégia de Segurança Nacional[85], a Estratégia de Defesa Nacional, Defesa Antimíssil e Revisão da Postura Nuclear[86], onde foi avançado o novo conceito de dissuasão integrada, com aliados e parceiros[87], revelando a natureza intrincada da política mundial contemporânea. Também deve ser destacada a publicação de uma Estratégia de Ciência e Tecnologia para a Defesa Nacional[88] e, pela primeira vez, de uma Estratégia Industrial de Defesa Nacional[89], cujos objetivos principais são assegurar cadeias logísticas resilientes, formação de mão-de-obra qualificada, aquisições flexíveis e dissuasão económica. Antes, em 2015, foi fundada uma unidade de inovação de defesa[90], em Silicon Valley, tentando captar e integrar tecnologias disruptivas desenvolvidas pelo dinâmico setor comercial na área de defesa, dando-lhe escala, fora das formalidades tradicionais do Pentágono. Em dezembro de 2022, foi inaugurado um gabinete de capital estratégico no Departamento de Defesa[91], com a finalidade de desenvolver, integrar e implementar estratégias de parcerias de capital, para moldar e dar dimensão ao investimento em tecnologias críticas e nas cadeias logísticas. Uma comissão chegou à conclusão de que os EUA não tinham um problema de inovação, mas sim de adoção dessa inovação na esfera militar, produzindo um relatório final com recomendações relacionadas com um novo portfolio de capacidades e restantes alterações processuais[92]. Um dos conceitos relacionados com os novos meios é que eles sejam desgastáveis (*attritable*), sem comprometerem a missão, ágeis, resilientes, inovadores, equilibrados, decisivos e integrados. A iniciativa emblemática desta nova aproximação é designada "Replicator", com a ambição de obter milhares de *drones* e outros dispositivos num

84 https://thehill.com/homenews/4360407-congress-approves-bill-barring-president-withdrawing-nato/
85 https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
86 https://www.defense.gov/News/News-Stories/Article/Article/3202438/dod-releases-national-defense-strategy-missile-defense-nuclear-posture-reviews/
87 https://www.defense.gov/News/News-Stories/Article/Article/3237769/official-says-integrated-deterrence-key-to-national-defense-strategy/
88 https://media.defense.gov/2023/May/09/2003218877/-1/-1/0/NDSTS-FINAL-WEB-VERSION.PDF
89 https://www.businessdefense.gov/NDIS.html
90 https://www.diu.mil/
91 https://www.cto.mil/osc/
92 https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-defense-innovation-adoption/

período entre 18 a 24 meses[93]. Em dezembro do ano passado, foi nomeada mais uma comissão para estudar a guerra baseada em software[94] e em março último, uma comissão conjunta bicamaral do Congresso e do Senado produziu um relatório sobre a reforma do sistema de planeamento, programação, orçamentação e execução da área da defesa[95].

A União Europeia reagiu à invasão russa e ao pedido de adesão formal da Ucrânia a esta organização quatro dias depois do seu início, na sequência de uma reunião informal do Conselho Europeu, a 11 de março de 2022 em Versalhes[96] e tem vindo a constituir-se como a principal fornecedora de apoio de longo prazo ao país assolado pela guerra[97]. Mobilizou as suas instituições, num esforço abrangente à Ucrânia[98], incluindo a utilização de 11 mil milhões de euros do seu mecanismo de apoio à paz[99], numa ação concertada com a Noruega estabeleceu uma missão de assistência militar à Ucrânia[100], aberta a terceiros países, e lançou um programa para a produção conjunta de armamento[101]. O objetivo geral será aumentar a sua autonomia estratégica face aos EUA.

Também a Agência Europeia de Defesa reviu no ano passado as suas prioridades no desenvolvimento de capacidades[102] e a Comissão Europeia publicou a sua primeira Estratégia Industrial de Defesa (*European Defense Industry Strategy* – EDIS)[103], em conjunto com a proposta de um programa imediato no valor de 1,5 mil milhões de euros do orçamento da União Europeia, para o período de 2025 a 2027 (*European Defence Industry Programme* – EDIP)[104]. No entanto, como afirmam Bergmann e Svedson (2023)[105], na Europa ainda são os Estados que tratam da Defesa e não a União Europeia e a EDIS não é de execução obrigatória, cabendo a cada país a seleção dos programas em que pretende participar.

Para se ter uma noção da discrepância de valores, refira-se que só o investimento em 17 centros de dados de "soberania" da Microsoft na Europa ultrapassa os 12 mil

93 https://www.defensenews.com/pentagon/2023/12/19/replicator-an-inside-look-at-the-pentagons-ambitious-drone-program/
94 https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/forward-defense/commission-on-software-defined-warfare/
95 https://ppbereform.senate.gov/
96 https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf
97 Para o seguimento deste apoio, consultar a seguinte base de dados: https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/
98 https://european-union.europa.eu/priorities-and-actions/eu-support-ukraine_en
99 https://www.consilium.europa.eu/en/policies/european-peace-facility/#ukraine
100 https://www.eeas.europa.eu/eumam-ukraine_en
101 https://defence-industry-space.ec.europa.eu/eu-defence-industry/asap-boosting-defence-production_en
102 https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf
103 https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-strategy_en
104 https://defence-industry-space.ec.europa.eu/eu-defence-industry/edip-future-defence_en
105 Op. cit., p. 4.

milhões de dólares[106]. Para agravar as divergências entre a realidade norte-americana e europeia saliente-se que 90% dos dados da União Europeia são geridos por empresas americanas, que menos de 4% das plataformas online são europeias e que os micro-processadores de fabrico europeu representam menos de 10% do mercado interno. Estes números impressionantes constam da "Bússola Digital 2030: a via europeia para a década digital"[107], documento este que não faz qualquer menção à defesa.

As preocupações reguladoras da União Europeu, cujo último episódio foi a aprovação de legislação, designadamente a Lei dos Mercados Digitais e a Lei dos Serviços Digitais da UE, que visa conter a posição dominante dos designados "guardiões" (Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft) e incentivar um comportamento responsável *online*, não escondem a debilidade da indústria tecnológica europeia contemporânea neste domínio. O estado da arte é perfeitamente ilustrado pelo domínio do mercado europeu de *smartphones* por marcas exteriores ao continente[108]. Numa altura em que a digitalização progride na economia e na sociedade e se fala da Internet das Coisas Militares[109] e a indústria de defesa europeia está fortemente fragmentada e voltada para o passado, só poderemos concluir que este processo agrava a dependência da Europa dos EUA e que a única via possível de encarar o futuro da defesa europeia é através da concertação estratégica entre a OTAN e a União Europeia, em especial no que se refere às bases industriais de defesa norte-americana e europeia.

As opiniões fundamentadas para um aumento da cooperação industrial de defesa entre os dois lados do Atlântico Norte vêm de longe. Em 1997, advogava-se que essa cooperação devia ser formalizada através de um "Acordo Comercial de Defesa Transatlântico", mas reconhecia-se a sensibilidade política do assunto[110]. Por outro lado, um estudo de 2017, conduzido por especialistas em economia de defesa, analisou a relação entre as bases industriais de defesa dos EUA e de cinco países membros da UE (Alemanha, França, Itália Reino Unido e Suécia), numa perspetiva de consolidação do mercado comum de defesa europeu, com vista a uma maior autonomia estratégia. As recomendações principais foram no sentido de criar regras que governem as relações entre as BTID americanas e da UE e destas serem baseadas na reciprocidade e em princípios de regulação comuns, definidos através de diálogo

106 https://blogs.microsoft.com/eupolicy/2022/12/15/eu-data-boundary-cloud-rollout/

107 https://commission.europa.eu/europes-digital-decade-digital-targets-2030-documents_en?prefLang=pt . Uma explicação sobre os propósitos da transformação digital pode ser encontrado em: https://www.europarl.europa.eu/topics/pt/article/20210414STO02010/transformacao-digital-importancia-beneficios-e-politica-da-ue

108 https://www.gsmarena.com/canalys_apple_reaches_top_spot_in_europe_as_the_market_slowly_heals-news-61672.php

109 https://www.computer.org/publications/tech-news/research/internet-of -military-battlefield-things-iomt-iobt

110 https://www.nato.int/acad/conf/ameuro97/04-b.htm

entre a União Europeia e os Estados Unidos e não entre cada um dos países europeus e os Estados Unidos. O estudo afirmava ainda que quanto mais os países europeus colaborassem entre si na pesquisa e desenvolvimento de defesa, mais aptos estariam para estabelecer um conjunto de regras mutuamente benéficas para a relação com os Estados Unidos (Belin et al, 2017). Em 2023 e fruto da invasão russa da Ucrânia, um estudo alemão designado *European Defense In New Age* – EDINA (Mölling e Hellmonds, 2023), falava da necessidade de um alinhamento entre as BTID transatlânticas. A Declaração da Cimeira de Vilnius de 2023 assume que a cooperação industrial deve ser melhorada entre os aliados, prometendo reduzir ou eliminar as barreiras às trocas e ao investimento relacionado com a defesa, conforme for o caso, para o desenvolvimento das capacidades necessárias[111], mas não foram avançados os mecanismos de implementação.

Existem propostas para a resolução do problema da melhoria da eficiência do mercado da defesa europeia, através de investimentos de longo prazo (Gotev, 2024) e de *procurement* conjunto[112]. Se a Europa conseguir implementar um mercado único de defesa dentro da União Europeia, poderá vislumbrar-se uma maior institucionalização do relacionamento ente a OTAN e a UE ao nível do topo. Duff (2024), por exemplo, sugere a criação de um comando conjunto permanente, que assegure a interoperabilidade, acelere e racionalize o *procurement* de armamento e estabilize o planeamento de defesa no longo prazo, mantendo os EUA envolvidos e aproximando o Reino Unido da UE. Esse comando teria uma estrutura civil, guarnecida por pessoal do Serviço de Ação Externa da UE e do Quartel-General da OTAN (SHAPE) e comandaria a campanha ocidental para resolver a agressão russa no Leste da Europa.

No setor comercial, já foi estabelecido um acordo sobre o lucrativo mercado transatlântico de dados, no valor de 7,1 biliões de dólares, para permitir o livre fluxo entre os dois continentes[113]. Normalmente, a preocupações da Comissão Europeia vão mais no sentido de exigir o cumprimento dos requisitos da privacidade dos dados dos cidadãos europeus, para os proteger do eventual uso e abuso pelos serviços de informações norte-americanos, no âmbito de um quadro de referência mútua[114], do que a concentração no seu valor comercial. Isto é francamente vantajoso para a atividade dos "guardiões" e devia ser reequacionado face à inexistência de um mercado equivalente do lado europeu, pela falta de grandes plataformas. Focando o assunto deste modo, é possível criar espaço negocial para desmontar a narrativa que os europeus não cumprem as suas obrigações na divisão de encargos da OTAN. Nos anos 50, os países europeus contribuíram com os seus terrenos e empresas, quando o assunto versou as infraestruturadas aliadas. Atualmente contribuem com os seus

111 https://www.nato.int/cps/en/natohq/official_texts_217320.htm
112 https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739294
113 https://www.politico.eu/article/eu-signs-off-on-data-transfers-deal-with-us/
114 https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

dados para a vantagem informacional que os EUA detêm à escala global e isso deve ser contabilizado[115].

Havendo o necessário entendimento político, todas estas questões poderão ser debatidas durante a sequência de importantes eventos, nomeadamente, a Conferência de Paz para a Ucrânia,[116] Conselho Europeu, cimeira dos 75 anos da OTAN (9 e 11 de julho) e cimeira da Comunidade Política Europeia (18 de julho), que reúne o maior número de líderes políticos da Europa. Tudo isto, antes da data da eleição mais falada em todo o mundo, a 5 de novembro de 2024. Qualquer que seja o candidato reeleito, a Europa poderá, nessa altura, estar mais bem apetrechada para a sua defesa.

Assim, a OTAN pode perfeitamente ser descrita numa lógica de *yin* e *yan*, composta de balanço e harmonia (quando há desequilíbrios ou excessos de um sobre o outro, pode ocorrer desarmonia, disrupções e até caos), em interação dinâmica (os dois não são entidades estáticas, interagindo dinamicamente, produzem mudança, crescimento e renovação); e têm uma natureza cíclica (seguem ritmos e padrões naturais, alternando-se num ciclo continuo de criação, manifestação e dissolução).

Conclusão

A visão do presidente norte-americano George Bush (pai) para uma Europa unida e livre, partilhada no final da Guerra Fria[117], está por cumprir. Nas últimas quase oito décadas, a paz na porção ocidental e central do continente tem sido garantida por um processo negociado de integração eminentemente económica e tendencialmente política, protegido pela OTAN. No entanto, a dissuasão oferecida pela Aliança deixou de funcionar como era hábito durante a Guerra Fria, o que terá levado uma Rússia revisionista a tentar a sua sorte na reparação das perdas verificadas no processo de decomposição da URSS. A ameaça de Leste regressou à ordem do dia e deu uma nova legitimidade à existência da OTAN, ao mesmo tempo que acentuava a debilidade da União Europeia no domínio da defesa. A emergência da China, enquanto potência regional, provocou um autêntico dilema nas preocupações norte-americanas que conduziram a sistemáticas queixas quanto à exiguidade das despesas no setor da defesa dos aliados europeus, levadas a um extremo retórico pelo antigo e candidato a futuro presidente Donald Trump, ao afirmar que encorajaria a Rússia a atacar qualquer país que não cumprisse com as suas obrigações. De certa maneira, o cenário geopolítico atual não é muito diferente daquele que conduziu à institucionalização da estrutura de comando permanente da OTAN na Europa: conter uma ameaça na

115 Veja-se, a este respeito, Cabugueira (2024).

116 https://www.swissinfo.ch/eng/foreign-affairs/ukraine-peace-conference-50-countries-have-agreed-to-attend-so-far/77614755

117 https://usa.usembassy.de/etexts/ga6-890531.htm

frente Leste, atendendo à situação no Indo-Pacífico, sem esquecer as perturbações no flanco Sul. Se regressarmos às origens do debate sobre a divisão de encargos, desde a fundação da Aliança, verificamos que nunca houve rigidez na fixação dos contributos dos aliados, tendo-se privilegiado as soluções pragmáticas. Atualmente, o processo de planeamento estratégico de defesa da OTAN (NDPP) agrega os compromissos em termos de capacidades aliadas correntes e futuras, não contemplando divisões entre os dois lados do Atlântico e não levando em conta a perspetiva dos benefícios obtidos pelo complexo militar-industrial norte-americano nas vendas bilaterais de equipamento militar aos países europeus.

Atendendo aos ensinamentos que chegam da Guerra da Ucrânia, onde uma mistura de material mais antigo e outro emergente, como *drones* e outros sistemas autónomos, opera em diversos domínios e é incorporado rapidamente nas operações militares, assistimos a uma vaga de revisão dos mecanismos de planeamento de defesa e das bases industriais e tecnológicas de defesa, muito centradas em processos digitais. As alterações visíveis são mais acentuadas nos EUA que tentam capitalizar o seu avanço tecnológico nessas áreas, o que agrava a divisão entre capacidades norte-americanas e europeias pela falta de consolidação da indústria de defesa europeia e uma ausência de competências digitais comercialmente competitivas. Deste modo, a União Europeia terá de desenvolver um mercado interno de defesa para evitar a sua sistemática fragmentação e convencer os EUA que existem mecanismos de concertação entre as duas organizações intergovernamentais, que garantam a sua assistência à Europa para que esta os auxilie num eventual enfrentamento da China, caso essa necessidade se manifeste, através de um pilar de defesa autónomo, mas ligado à OTAN. Uma análise mais circunstanciada, com base na dialética *yin-yang*, poderá enriquecer o debate sobre o futuro da Aliança com mais sucesso da história mundial.

Bibliografia

Beaver, W. e Fein, J. (2024). "America Must Remedy Its Dangerous Lack of Munitions Planning", *The Heritage Foundation Issue Brief Defense*, 26 de fevereiro de 2024. Disponível em: https://www.heritage.org/sites/default/files/2024-02/IB5341.pdf

Belin, J., Hartley, K., Lefeez, S., Linnenkamp, H., Lundmark, M., Masson, H., Maulny, J. P., Ungaro, A. (2017). "Defence Industrial Links Between the EU and the US", *Armament Industry European Research Group*, setembro de 2017. Disponível em: https://www.iris-france.org/wp-content/uploads/2017/09/Ares-20-Report-EU-DTIB-Sept-2017.pdf

Bergman, M. e Svendsen, O. (2023). "Transforming European Defense, A New Focus in Integration", *Center for Strategic & International Studies*, junho de 2023. Disponível em: https://www.csis.org/analysis/transforming-european-defense-new-focus-integration

Cabugeira, M. (2024). "Open data and Open Finance in the EU: it's not only about the data!", *Magazine des Professions Financières et de l'Économie*, 28 (junho de 2024). Disponível em: https://professionsfinancieres.com/sites/professionsfinancieres.com/files/Article%205%20-%20Manuel%20CABUGUEIRA.pdf

Duff, A. (2024). "NATO and the European Union: Bridging the gap", *European Policy Centre Discussion Paper*, 13 de maio de 2024. Disponível em: https://epc.eu/content/NATO.pdf

Gaddis, J. L. (1986) "The long peace: Elements of stability in the postwar international system", *International Security*, 10(4), 99-142.

Gotev, G. (2024). "The name is Bond, European defence bond", *Euractiv – The Brief*, 27 de fevereiro de 2024. Disponível em: https://www.euractiv.com/section/global-europe/opinion/the-brief-the-name-is-bond-european-defence-bond/

Hallams, E. e Schreer, B. (2012). "Towards a 'post-American' alliance? NATO burden-sharing after Libya", *International Affairs,* 88(2), 313-327. Disponível em https://doi.org/10.1111/j.1468-2346.2012.01073.x

He, B. (2023). "Chinese great power management: Managing War through the Yin-Yang Strategy", *Swiss Institute for Global Affairs*, 7 de agosto de 2023, [blog]. Disponível em: https://www.globalaffairs.ch/2023/08/07/chinese-great-power-management-managing-war-through-the-yin-yang-strategy/

Hernández, G. R. (2023). "OSCE in Crisis Over Russian War on Ukraine", *Arms Control Association*, janeiro/fevereiro 2023. Disponível em: https://www.armscontrol.org/act/2023-01/news/osce-crisis-over-russian-war-ukraine

Impson, N. (2020). "The Next Warm War: How History's Anti-Access/Area Denial Campaigns Inform the Future of War", *Small Wars Journal*, 14 de Janeiro de 2020. Disponível em: https://smallwarsjournal.com/jrnl/art/next-warm-war-how-historys-anti-accessarea-denial-campaigns-inform-future-war

Jullien, F. (2004). *A Treatise on Efficacy: Between Western and Chinese Thinking*. Hawaii: The University of Hawaii Press.

Koivula, T. e Ossa, H. (2022). "NATO's Burden-Sharing Disputes: Past, Present and Future Prospects". Cham: Palgrave Macmillan.

Kunertova, D. (2017). "One measure cannot trump it all: lessons from NATO's early burden-sharing debates", European *Security*, 26(4), 552-574. Disponivel em: https://doi.org/10.1080/09662839.2017.1353495

Lee, J. (2024). "NATO and a Taiwan contingency", *NDC Outlook* 02-2024. Disponível em: https://www.ndc.nato.int/download/downloads.php?icode=816

Lima, B. P. (2009). "As relações entre a NATO e a União Europeia pós-11 de setembro", *Relações Internacionais*, março 2008, 87-99. Disponível em: https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri21/RI21_artg6_BPL.pdf

Mattelaer, A. (2016). "Revisiting the Principles of NATO Burden-Sharing", *Parameters,* 46(1), 25-33. Disponível em: https://doi:10.55540/0031-1723.2821

Mölling, C. e Hellmonds, S. (2023). "Security, Industry, and the Lost European Vision, How Russia's War in Ukraine Is Changing the European Defense Technological and Industrial

Base", German Council on Foreign Relations, 31 de outubro de 2023. Disponível em: https://dgap.org/en/research/publications/security-industry-and-lost-european-vision-edina-ii

Pifer, S. (2021). "Russia's draft agreements with NATO and the United States: Intended for rejection?", Brooking Institution, 21 de dezembro de 2021. Disponível em: https://www.brookings.edu/articles/russias-draft-agreements-with-nato-and-the-united-states-intended-for-rejection/

Qin, Yaqing (2018). *A Relational Theory of World Politics*. New York: Cambridge University Press.

Sánchez, I. e Torreblanca, J. I. (2023). "Ukraine one year on: When tech companies go to war", *European Council on Foreign Relations*, 7 de março de 2023. Disponível em: https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/

Wang, F. L. (2024). *The China Race: Global Competition for Alternative World Orders.* Albany, NY: State University of New York Press.

Gaddis, J. L., 1986. The Long Peace: Elements of Stability in the Postwar International

System. *International Security,* Vol 10(No 4), pp. 99 – 142.

Gaddis, J. L., 1986. The Long Peace: Elements of Stability in the Postwar International

System. *International Security,* Vol 10(No 4), pp. 99 – 142.

Gaddis, J. L., 1986. The Long Peace: Elements of Stability in the Postwar International

System. *International Security,* Vol 10(No 4), pp. 99 – 142.

Gaddis, J. L., 1986. The Long Peace: Elements of Stability in the Postwar International

System. *International Security,* Vol 10(No 4), pp. 99 – 142

Extra Dossiê

África no Tabuleiro de Xadrez Mundial: Estruturas, Desafios e Oportunidades

Teresa Rodrigues
IPRI-NOVA
José Félix Ribeiro
IPRI-NOVA

Resumo

África é hoje um "Continente do Mundo", no duplo sentido dos desafios que a sua evolução coloca à economia mundial e das oportunidades que o seu grau de (in)sucesso abrirá aos múltiplos parceiros externos que, em número crescente, têm manifestado interesse em reforçar os laços geoeconómicos e geopolíticos com os Estados africanos. Com base na análise de vários indicadores, este artigo tem como objetivos: (i) identificar as múltiplas realidades internamente coexistentes no continente africano hoje; (ii) propor uma divisão macrorregional para África; (iii) discutir os relacionamentos externos que nos próximos anos consideramos poderem desempenhar um papel significativo no posicionamento do continente africano no xadrez internacional.

Palavras-chave: África; Regiões; Demografia; Desenvolvimento; Política Externa.

Abstract

Africa is today a "Continent of the World", in the double sense of the challenges that its evolution poses to the world economy and the opportunities that its degree of (un)success will open up to the multiple external partners who, in increasing numbers, have expressed an interest in strengthening geo-economics and geopolitical ties with the African States. Based on the analysis of several indicators, this article aims to: (i) identify the multiple realities internally coexisting in the African continent today; (ii) propose a macro-regional division for Africa; (iii) discuss the external relationships that in the coming years we consider to be able to play a significant role in the positioning of the African continent in the international chessboard.

Keywords: *Africa; Regions; Demography; Development; Foreign Policy.*

Artigo recebido: 10.09.2024
Aprovado: 13.09.2024
https://doi.org/10.47906/ND2024.168.06

Introdução

África é hoje um "Continente do Mundo", no duplo sentido dos desafios que a sua evolução coloca à economia mundial e das oportunidades que o seu grau de (in)sucesso abrirá aos múltiplos parceiros externos que, em número crescente, têm manifestado interesse em reforçar os laços geoeconómicos e geopolíticos com os Estados africanos.

Com base na análise de vários indicadores, este artigo tem três objetivos principais: (i) identificar as múltiplas realidades internamente coexistentes no continente africano; (ii) propor uma divisão macrorregional para África; (iii) discutir os relacionamentos externos que nos próximos anos consideramos poderem desempenhar um papel significativo no posicionamento do continente africano no xadrez internacional.

Tendo em vista a concretização destes objetivos, o texto está dividido em seis pontos e uma conclusão final. Numa primeira parte falaremos dos aspetos estruturais que permitem traçar um retrato do continente africano, composto por 54 Estados políticos e uma significativa diversidade em termos étnicos, linguísticos e religiosos, mas também do tecido económico e social e estabilidade política, a que acrescem ainda as características de ordem geográfica e riquezas naturais. Segue-se a identificação do que consideramos serem os principais desafios, oportunidades e riscos que emergem da estrutura previamente identificada e uma proposta de visão diferenciadora em termos macrorregionais da história, da geoeconomia e da geopolítica africanas. O ponto quatro é dedicado às dinâmicas demográficas e discute o modo como as características e dinâmicas atuais e futuras da população africana se distinguem de todas as outras e representam riscos, mas também oportunidades de caráter endógeno para a atualidade e sobretudo para as próximas décadas. A esta visão atual e também prospetiva sobrepõe-se, no ponto cinco, a rede de conetividade global do continente africano e das redes de proximidade internas, que permitem dividir África em sete sub-regiões. O texto termina com quatro exemplos de atores externos que se destacam pelo seu interesse nessas regiões africanas previamente identificadas: Estados Unidos, República Popular da China, Índia e Federação Russa.

1. Aspetos Estruturais

Em termos metodológicos, começamos por olhar a realidade atual do continente africano de um modo abrangente. Esse exercício prevê a identificação de um conjunto de aspetos ou vetores que entendemos geográfica e historicamente estruturantes e permitem explicar a atual diversidade interna e abrir caminho para futuros também diversos. Esse conhecimento multidimensional permitirá encontrar sub-regiões com identidades distintas. Como veremos, essas sub-regiões nem sempre coincidem

com as divisões geográficas por norma reconhecidas e utilizadas pela bibliografia académica especializada e nas estatísticas e relatórios de organizações internacionais, que por norma distinguem África Setentrional, África Meridional, África Central, África Ocidental e África Oriental (Figura 1).

Figura 1
A África Política

Fonte: https://www.guiageo.com/africa-politico.htm#google_vignette

A primeira, também conhecida como Norte da África, compreende a Argélia, Egito, Sudão, Marrocos, Líbia e Tunísia. Localiza-se próximo do Mar Mediterrâneo e concentra um considerável número de habitantes; a segunda, a África Meridional, conhecida também por África Austral, é a região localizada na parte sul do continente africano. Integram essa região a África do Sul, o Zimbabué, o Botsuana, a Namíbia e a Zâmbia. Geograficamente, encontra-se entre o Oceano Índico, a leste, e o Oceano Atlântico, a oeste. Destaca-se economicamente pela agricultura e extração mineral; por seu turno, a África Central situa-se na faixa central do continente africano e nela se encontram o Chade, Gabão, República do Congo, Angola, Camarões e República

Democrática do Congo. É uma região que difere das restantes zonas, porque não é construída com base em similaridades históricas, políticas ou económicas; o quarto grupo de países forma a África Ocidental. Está localizado entre o deserto do Saara e o Golfo da Guiné e inclui os territórios do Níger, Senegal, Mauritânia, Gana, Cabo Verde, Guiné-Bissau, Guiné, Serra Leoa, Togo, entre outros; por fim, a África Oriental, composta por países situados entre a bacia hidrográfica do Congo e o Oceano Índico (Mundo Educação, 2024).

Partindo desta proposta de divisão territorial do continente efetuamos um primeiro esforço de análise baseado em indicadores de natureza diversa, que permitiram identificar um total de dez vetores que consideramos constituírem o ponto de partida para uma nova proposta de divisão macrorregional (Ribeiro, 2023). São eles:

1. A geografia física africana e o seu impacto na geografia do povoamento, incluindo neste vetor o papel das estruturas familiares na dinâmica demográfica e o papel da mulher nas sociedades africanas;
2. A especialização internacional de África, nomeadamente uma total dependência face à exportação de *commodities* agrícolas, mineiras e energéticas, com ciclos de preços que se repetem e com limitado impacto na criação de emprego;
3. O papel-chave da agricultura de subsistência para a maioria da população rural, agravada pela sua elevada dependência face às condições climatéricas, designadamente de pluviosidade;
4. Os recursos hídricos e o modo como condicionam a abundância física e/ou escassez alimentar, condições sanitárias da população e dinamismo económico;
5. A urbanização de África, feita a ritmos intensos e a importância das megacidades, onde predomina uma oferta limitada de condições básicas e qualidade de vida;
6. Os padrões de urbanização e respetiva interação com o ambiente natural, de que decorrem riscos permanentes de zoonoses;
7. Os grupos étnicos e diversidade linguística e cultural que fragmentam o continente e que coexistem com migrações internas seculares que atravessaram o continente – veja-se, por exemplo, as migrações dos povos *bantus*;
8. A importância para os Estados pós-coloniais e nas relações entre Estados, que decorrem de formas de governação tradicional das populações com estruturas tribais e em muitos casos com uma implementação transfronteiriça;
9. A multiplicidade e potencial confronto entre as religiões autóctones e as religiões vindas do exterior, como o islamismo e o cristianismo, e respetivo mapa atual da sua influência;
10. Uma "tinta invisível" de antigos impérios e reinos, que constituíram as formas mais avançadas de governação antes da colonização europeia.

2. Desafios, Oportunidades e Riscos

Das características que parecem definir o perfil do continente africano em termos estruturais decorrem sete principais desafios, associados a dois grandes conjuntos de oportunidades, que coexistem com riscos de diferentes tipologias. O cruzamento destes desafios, oportunidades e riscos originam impactos de ordem e grau distintos nas diferentes sub-regiões que compõem e coexistem em África.
Desde logo destacamos entre os principais desafios os seguintes:

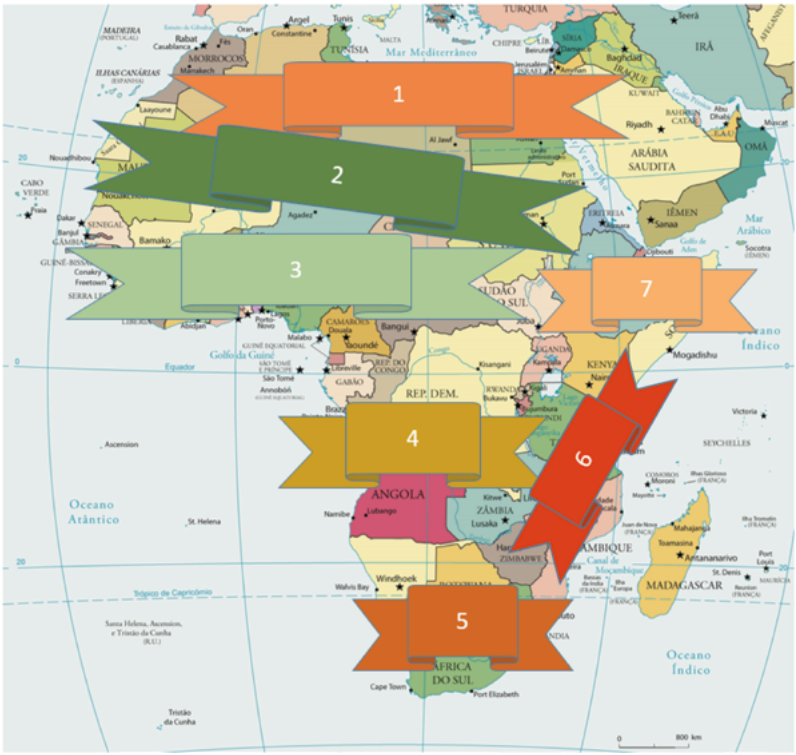
1. As alterações climáticas e a pressão sobre alguns recursos vitais, que podem ser especialmente gravosas atendendo ao ritmo de crescimento da população residente e ao aumento do consumo *per capita*;
2. A intensidade e a complexidade dos fluxos migratórios intercontinentais, explicados por fatores ambientais, instabilidade política e conflito, com um crescente número de migrações forçadas e aumento do volume de refugiados e de deslocados internos;
3. Indicadores pouco favoráveis em termos de governança, estabilidade política e corrupção;
4. Indicadores pouco favoráveis de desenvolvimento humano, em alguns casos a registarem uma tendência decrescente, acompanhados pelo aumento da desigualdade interna;
5. Indicadores pouco favoráveis de desenvolvimento económico e escassa flexibilidade do mercado de trabalho;
6. Indicadores pouco favoráveis de desenvolvimento e qualidade de vida, designadamente nos centros urbanos, que vão continuar a aumentar e colocam problemas complexos de gestão;
7. Escassa projeção global do continente africano e de cada um dos seus Estados nos domínios económico, militar e de *soft power*.

Estes desafios coexistem com as oportunidades abertas pela transformação tecnológica em curso e com oportunidades de carácter geoeconómico, que poderão traduzir-se na redução dos níveis de dependência alimentar das populações africanas. Mas estas oportunidades só podem ser rentabilizadas caso seja possível reduzir os efeitos negativos dos riscos associados à segurança e à estabilidade dos regimes políticos africanos. Na verdade, o continente apresenta indicadores pouco favoráveis ao nível de governança, solidez política e níveis elevados de corrupção. A escassa flexibilidade do mercado de trabalho, a luta pela posse de recursos, a distribuição assimétrica de riqueza e as tensões sociais e étnicas são causa e consequência da falta de estabilidade política e do falhanço das infraestruturas críticas.

3. Uma Visão Diferenciadora

Por todos os aspetos identificados nos pontos anteriores, e da ponderação do seu grau relativo de importância em termos das entidades nacionais presentes em África, foi possível criar um conjunto de sete sub-regiões, distintas em termos geoeconómicos e geopolíticos (Figura 2). Cada uma delas foi construída tendo em conta: as ligações que a história política destas sub-regiões anteriores à colonização europeia permitiu criar em África e fora dela (Figura 3); as tribos ainda hoje dominantes em cada região e respetiva relação histórica com o Islão; a importância externa dos recursos naturais e territoriais de cada região e a natureza dos fluxos comerciais em torno desses recursos (Figura 4); e os apoios externos (militares, políticos, económicos e financeiros) que caracterizam atualmente os países que compõem cada um dos grupos identificados.

Figura 2
A África das 7 sub-regiões



Fonte: Elaboração dos autores, com base em:
https://www.guiageo.com/africa-politico.htm#google_vignette

Figura 3
África. Mapeamento da Colonização Europeia em 1914

Fonte: The Metropolitan Museum of Art, Heilbrunn Timeline of Art History.

Figura 4
África. Recursos Naturais mais Abundantes por País (2020)

Fonte: https://www.aljazeera.com/news/2018/2/20/mapping-africas-natural-resources

Identificam-se de seguida cada uma dessas sete sub-regiões, os Estados que as compõem e respetivos elementos caracterizadores e diferenciadores face às restantes – as cores correspondem à proposta de divisão contemplada na Figura 2.

1
ÁFRICA DO NORTE – **ESPAÇO MEDITERRÂNICO**
Argélia – Egito – Líbia – Marrocos – Tunísia

· Estados que são herdeiros de Impérios e reinos pré colonização europeia, sob influência política islâmica e fortes relações com a Andaluzia;
· Estados com estreita relação estabelecida durante a colonização europeia com Estados do sul da Europa (França, Itália e Espanha) exceto o Egito, sob influência britânica;
· Países exportadores de petróleo e gás natural, como a Argélia, a Líbia e atualmente o Egito;
· Estados com fortes fluxos de emigração para a Europa e que funcionam também como países de trânsito de vagas migratórias provenientes da África subsaariana;
· Estados com diferentes alinhamentos atuais com potências exteriores à União Europeia (EUA, Rússia, Turquia e mais recentemente a República Popular da China);
· A Líbia a atravessar atualmente uma segunda guerra civil, depois de ter estado envolvida numa guerra por fronteiras com o Chade (1978-1987);
· Contágio possível com movimentos islamitas/terroristas da África saheliana.

2
ÁFRICA SAHELIANA – **ESPAÇO SUDANÊS**
Burkina Faso – Chade – Mali – Mauritânia – Níger **– República Centro Africana – Sudão**

· Espaços herdeiros dos Impérios islâmicos do Sahel (Gana, Mali, Songa e Bornu-Karen);
· Estados com insurreições islâmicas radicais ou movimentos secessionistas (caso do Darfur no Sudão);
· Estados que contam (ou contaram) com a presença de tropas francesas e de outros países europeus no combate a grupos terroristas e mais recentemente com mercenários de origem russa.

3
ÁFRICA OCIDENTAL
Benim – Cabo Verde – Camarões – Costa do Marfim – Gâmbia – Gana – Guiné-Bissau – Guiné Conacri – Guiné Equatorial – Libéria – Nigéria – S. Tomé e Príncipe – Senegal – Serra Leoa – Togo

· Espaço em que se concentram as maiores tribos africanas, várias delas islamizadas, e que participam atualmente em vários destes Estados, com destaque para a Nigéria;
· Centro de Reinos e Impérios anteriores à colonização europeia, intensamente envolvidos no comércio de escravos antes da colonização do seu interior pelas potências europeias, que aí instalaram feitorias costeiras para negociar ouro e escravos;
· Atualmente a Nigéria e a Guiné Equatorial são exportadores de petróleo e os restantes são exportadores de produtos agrícolas e de alguns minérios (como a bauxite).

4
ÁFRICA CENTRAL + ÁFRICA ATLÂNTICA + REGIÃO DOS GRANDES LAGOS
Angola – Burundi – Gabão – Congo e República Democrática do Congo – Ruanda – Uganda – Zâmbia

· Grande região mineira e energética de África, em torno da República Democrática do Congo, da Zâmbia e de Angola;
· Região articulada por laços tribais da República Democrática do Congo com Estados da região dos Grandes Lagos (Ruanda e Burundi), onde se verificaram os conflitos mais violentos da África pós-colonial.

5
ÁFRICA AUSTRAL
África do Sul – Botsuana – Lesoto – Malawi – Namíbia – Suazilândia

· Outra grande região mineira de África, rica em ouro, diamantes e vários outros minérios de elevada procura atual (como o titânio);
· Local de implantação das tribos mais ricas de África (zulus, choças, sotos);
· Sem presença islâmica significativa;
· A África do Sul é o maior polo industrial e empresarial de África, integra o grupo dos BRICS e tem forte influência na União Africana.

6
ÁFRICA ORIENTAL
Cômoros – Madagáscar – Maiote – Maurícias – Moçambique – Quénia – Reunião – Seicheles – Tanzânia – Zimbabué

· Região com forte ligação geoeconómica às Áfricas Austral e Central;
· Com presença islâmica histórica na Tanzânia, no norte de Moçambique e no norte do Quénia, assente em relações com Estados do Médio Oriente e Golfo Pérsico;
· Moçambique tem uma longa história de envio de trabalhadores para as minas da África do Sul;
· Em Moçambique e na Tanzânia têm vindo a ser descobertos importantes jazigos de gás natural, que coincide com o início de atuação do Estado islâmico em Cabo Delgado no Norte de Moçambique;
· Macrorregião com vocação de relacionamento com a Ásia do Sul e com a Ásia Pacífico;
· O Canal de Moçambique é um corredor de importância estratégica no acesso à África Austral.

7
CORNO DE ÁFRICA
Djibouti – Eritreia – Etiópia – Somália – Sudão do Sul

· Região de grande importância estratégica, na proximidade com o Mar Vermelho e com Estados árabes do Golfo Pérsico, o que explica a presença de bases militares de quatro Estados no Djibouti (França, EUA, China, Japão);
· A Somália tem funcionado como base de pirataria associada a movimentos islâmicos radicais;
· O papel geopolítico central nesta macrorregião cabe à Etiópia, império africano com uma longa história, atravessada na atualidade por conflitos tribais, que ameaçam a sua integridade territorial.

4. O *Puzzle* Demográfico

A análise demográfica ajuda a compreender os equilíbrios de poder do sistema internacional, as tensões entre Estados e dentro de um mesmo Estado e a probabilidade destas tensões se virem a agravar, permitindo atuar com base em informação objetiva a curto e médio prazo e prevenir fatores de risco. Consideramos o fator demográfico essencial para entender a realidade africana e queremos saber de que modo as características e dinâmicas atuais e futuras da população africana se distinguem de todas as outras e representam riscos, mas também oportunidades de caráter endógeno na atualidade e sobretudo nas próximas décadas. Será essa evolução uniforme em termos continentais ou marcada por diferenças significativas entre as sete sub-regiões identificadas? E qual o papel desempenhado pelos oito gigantes populacionais africanos, que em 2024 contam entre 50 e 230 milhões de residentes?

Com 1495 milhões de residentes, África é de longe o continente mais jovem do mundo, com 41% da sua população menor de 15 anos e apenas 3% maior de 65 anos (2024). A média etária ronda os 18 anos, consequência direta dos elevados níveis de fecundidade que se continuam a verificar na maioria dos 54 Estados que a compõem. Os 10 países com maior número médio de filhos por mulher do mundo são todos africanos. Também por este facto, África será o continente onde se espera o maior aumento populacional até 2050, podendo mesmo duplicar. Dos atuais 18,4% que hoje representa em termos mundiais, subirá para 25,6% até 2050 (Tabela 1). As Nações Unidas preveem que até meados do século XXI metade do aumento populacional do mundo estará concentrado em nove países, cinco dos quais africanos (Índia, Nigéria, Paquistão, R. D. Congo, Etiópia, Tanzânia, EUA, Indonésia, Uganda).

Desconhece-se, no entanto, como irá evoluir a trilogia população, recursos e desenvolvimento e até que ponto esta relação poderá originar focos de tensão a nível local e regional, dadas as dinâmicas sociodemográficas hoje existentes. Entre estas cumpre destacar o facto de os ritmos intensos de crescimento natural coexistirem com níveis de morbilidade e mortalidade elevados; com migrações que continuam a ser sobretudo de saída, permitindo até certo ponto reduzir tensões sociais nas zonas mais povoadas, mas com custos em termos de competitividade – "dividendo demográfico"; com níveis de urbanização em aumento rápido – em 2030 cerca de metade da população africana viverá em zonas urbanas, algumas muito populosas –, mas em condições socioeconómicas pouco satisfatórias – em bairros degradados, onde coexistem níveis elevados de desemprego, exclusão social, insegurança e economia paralela. Embora apresentem uma tendência média positiva, o Produto Interno Bruto (PIB) e o Índice de Desenvolvimento Humano (IDH) em África continuam a ser inferiores à média mundial e registam crescentes diferenças entre Estados.

Com efeito, confrontamo-nos na atualidade com uma África a várias velocidades, que comunga de realidades sociodemográficas maioritariamente idênticas, mas com um conjunto de situações distintas, observáveis nas sete sub-regiões consideradas neste artigo. Falamos de diferenças regionais entre as partes norte e sul do continente – com perfis demográficos mais semelhantes entre si – face às restantes; da vantagem socioeconómica das regiões dos "polos" – maior taxa de urbanização e PIB –, que embora apresentem estruturas etárias jovens têm um crescimento populacional mais lento. Este facto pode facilitar a existência um desenvolvimento económica mais regular e permitir melhorar os níveis de bem-estar e de segurança dos seus residentes. O contexto de segurança relativa e a existência de uma situação económica favorável torna a parte sul do continente um espaço atrativo para a imigração extra e sobretudo intracontinental.

Várias características e tendências sociodemográficas representam vantagens para o futuro próximo do continente, a primeira das quais resulta do potencial humano sem precedentes, que pode constituir uma janela de oportunidades em termos de equilíbrio ativos/inativos. Espera-se um aumento da esperança média de vida superior à média mundial resultante da redução da mortalidade infantil e juvenil e do aumento do número de anos de vida com saúde, que permitirá esbater parte das assimetrias internas de distribuição de bem-estar e qualidade de vida e terá impacto positivo em termos de acesso a cuidados de saúde e infraestruturas essenciais.

Na verdade, tudo pode melhorar em termos de indicadores demográficos e sociais. De destacar o aumento do nível de instrução e formação e maior equilíbrio de género; emprego mais qualificado e redução da percentagem dos jovens que não estudam e não trabalham; melhoria das condições de habitabilidade, sobretudo em contexto urbano; benefícios trazidos pela tecnologia e avanço da ciência, postos ao serviço da população para resolver parte da pressão sobre os recursos; e o esbater das assimetrias internas de distribuição de bem-estar e qualidade de vida.

O futuro depende da forma como serão resolvidos os maiores riscos que África como um todo enfrenta, nomeadamente de caráter geopolítico e económico (consolidação de estabilidade política, maior flexibilidade e especialização do mercado de trabalho e criação de infraestruturas essenciais), que continuam pautados por grandes diferenças regionais.

Tabela 1

África. Principais Indicadores Demográficos (2024-2050)

ANOS	2024						2030	2050
MUNDO	8 118 836						8 546 141	9 709 491
% Pop. Africana	18,41						20,02	25,59
ÁFRICA	1 494 989						1 710 661	2 485 131
	População	Idade Média	ISF	Densidade (P/ Km²)	% Pop. Urbana	Saldo Migratório	População estimada	População estimada
GRUPO 1 – ÁFRICA DO NORTE – ESPAÇO MEDITERRÂNICO								
Argélia	45,606,480	28	2,8	19	75	-10,0	49787,283	60001,114
Egipto	112,716,598	24	2,8	113	41	-30,0	125151,725	160339,888
Líbia	6,888,388	27	2,4	4	82	-2,0	7394,813	8539,976
Marrocos	37,840,044	29	2,3	85	66	-40,0	40226,396	45044,99
Sahara Ocidental	587,259	32	2,2	2	95	5,6	662,726	851,066
Tunísia	12,458,223	32	2	80	69	-4,0	13100,768	14315,778
%	**14,7**	**28,7**	**2,4**	**50,5**	**71,3**	**-13,4**	**13,8**	**11,6**
GRUPO 2 – ÁFRICA SAHELIANA – ESPAÇO SUDANÊS								
Burkina Faso	23,251,485	17	4,6	85	32	-25,0	27523,563	40541,548
Chade	18,278,568	15	6,1	15	24	-2,0	22460,393	36452,035
Mali	23,293,698	15	5,8	19	44	-40,0	28712,294	47439,803
Mauritânia	4,862,989	18	4,3	5	61	3,0	5830,562	8914,673
Níger	27,202,843	15	6,7	21	17	1,0	35217,942	67043,296
República Centro Africana	5,742,315	15	5,8	9	40	-14,7	7104,274	11533,423
Sudão do Sul	11,088,796	17	4,3	18	28	-23,3	12570,402	17460,846
%	**7,8**	**16,0**	**5,4**	**24,6**	**35,1**	**-14,4**	**8,2**	**9,2**

GRUPO 3 – ÁFRICA OCIDENTAL								
Benim	13,712,828	18	4,9	122	48	-200,0	16393,827	25264,035
Cabo Verde	598,682	27	1,9	149	67	-1,2	638,84	727,457
Camarões	28,647,293	18	4,3	61	58	-4,8	34051,102	51279,56
Costa do Marfim	28,873,034	18	4,3	91	52	6,0	34211,272	51358,242
Gâmbia	2,773,168	17	4,5	274	58	-3,0	3263,651	4673,742
Gana	34,121,985	21	3,5	150	57	-10,0	38775,85	52231,784
Guiné	14,190,612	18	4,2	58	40	-4,0	16622,387	23711,7
Guiné Equatorial	1,714,671	21	4,1	61	67	4	1999,678	2790,533
Guiné-Bissau	2,150,842	19	3,8	76	45	-1,4	2484,863	3445,289
Libéria	5,418,377	18	4	56	54	-5,0	6282,074	8890,7
Nigéria	223,804,632	17	5,1	246	54	-60,0	262580,426	377459,883
São Tomé e Príncipe	231,856	19	3,7	242	77	-600,0	265,036	366,663
Senegal	17,763,163	18	4,3	92	52	-20,0	21125,872	32562,869
Serra Leoa	8,791,092	19	3,8	122	43	-4,0	10105,188	13595,023
Togo	9,053,799	19	4,1	166	44	-2,0	10558,178	15478,883
%	**26,8**	**19,1**	**4,0**	**131**	**54**	**-60**	**26,9**	**26,7**

GRUPO 4 – ÁFRICA CENTRAL + ÁFRICA ATLÂNTICA + REGIÃO DOS GRANDES LAGOS								
Angola	36,684,202	16	5,1	29	68	-1,0	44911,664	72328,068
Burundi	13,238,559	16	4,9	516	15	2,0	15800,53	24208,671
Congo	6,106,869	18	4	18	70	-1,0	7114,987	10378,911
Gabão	2,436,566	22	3,4	9	85	1,0	2774,522	3757,053
R. D. do Congo	102,262,808	16	6,1	45	46	-15,0	127582,053	217494,004
Ruanda	14,094,683	19	3,7	571	18	-9,0	16375,704	23030,046
Uganda	48,582,334	16	4,4	243	29	-126,2	58380,262	87622,081
Zâmbia	20,569,737	17	4,2	28	46	-5,0	24676,418	37460,435
%	**16,8**	**17,5**	**4,5**	**182,4**	**47,1**	**-19,3**	**17,4**	**19,2**

GRUPO 5 – ESPAÇO DA ÁFRICA AUSTRAL								
África do Sul	60,414,495	28	2,3	50	69	58,5	64659,278	73529,753
Botsuana	2,675,352	24	2,7	5	69	3,0	2972,271	3679,34
Lesoto	2,330,318	22	2,9	77	31	-4,0	2501,946	2898,368
Malawi	20,931,751	17	3,8	222	19	-6,0	24944,243	37159,3
Namíbia	2,604,172	21	3,2	3	60	-3,9	2910,056	3779,918
Suazilândia	1,210,822	22	2,8	70	31	-5,3	1305,985	1655,122
%	**6,1**	**22,3**	**3,0**	**71,2**	**46,5**	**7,1**	**5,8**	**4,9**

GRUPO 6 – ÁFRICA ORIENTAL								
Cômoros	852,075	20	3,8	458	33	-2,0	959,412	1246,206
Madagáscar	30,325,732	19	3,7	52	40	-1,5	35604,443	51592,965
Maiyotte	335,995	17	4,3	896	40	0,0	407,579	664,141
Maurícias	1,300,557	37	1,4	641	40	0,0	1305,425	1226,235
Moçambique	33,897,354	17	4,5	43	40,00	-5,0	40920,707	63044,497
Quénia	55,100,586	20	3,2	97	31	-10,0	63103,942	85211,739
Reunião	981,796	34	2,2	393	93	-630,0	1031,822	1127,252
Seychelles	107,66	33	2,3	234	5	-200,0	111,317	116,644
Tanzânia	67,438,106	17	4,6	76	38	-40,0	81885,304	129931,521
Zimbabué	16,665,409	18	3,4	43	37	-10,0	19179,393	26438,588
%	**14,2**	**23,2**	**3,3**	**293,3**	**39,7**	**-89,8**	**14,3**	**14,5**

GRUPO 7 – CORNO DE ÁFRICA								
Djibouti	1,136,455	24	2,7	49	72	900,0	1247,129	1502,575
Eritreia	3,748,901	19	3,7	37	67	-15,3	4283,354	5964,021
Etiópia	126,527,060	19	4	127	22	-12,0	149296,378	214812,309
Somália	18,143,378	15	6,1	29	46	-30,0	22316,857	36462,83
Sudão	48,109,006	19	4,3	27	35	-10,0	56997,098	84494,269
%	**13,6**	**19,2**	**4,2**	**53,8**	**48,4**	**166,5**	**13,7**	**13,8**

Fonte: Elaboração dos autores com base em Worldometer, UNPFA, 2024.

Os dados da Tabela 1 evidenciam os contrastes entre o Sahel, a África Ocidental, Central e Atlântica *versus* a África do Norte, do Sul e Oriental. Desde logo em termos de peso percentual de cada um deles no total de população. Mais de 26% dos africanos reside na África Ocidental. A África Austral e a Saheliana representam 6,1% a 7,8% da população do continente, respetivamente, repartindo-se os restantes 60% de forma quase igualitária por quatro outras sub-regiões.

Os dados permitem também observar assimetrias significativas em termos de idade média da população residente, que oscilam entre um máximo de 28,7 anos na África do Norte e apenas 16 anos na África Saheliana e Sudão, como consequência dos níveis de fecundidade. Com efeito, o número médio de filhos por mulher (ISF – Índice Sintético de Fecundidade) é de 2,4 no Norte de África, próxima de não garantir a renovação das gerações (como já sucede na Tunísia), mas é estimado em mais do dobro (5,4) na região do Sahel e Sudão.

Existe igualmente uma relação direta positiva entre as regiões com ritmos de crescimento mais moderado, médias etárias mais elevadas e maior percentagem de população urbana, embora não se possa estabelecer uma relação causal entre os três vetores. Acresce a esta realidade a questão migratória. Os saldos migratórios parecem indicar uma menor repulsão nas zonas de maior percentagem urbana, embora tal não signifique forçosamente desenvolvimento económico ou qualidade de vida das populações urbanas. Não devemos esquecer que todo o continente africano está sujeito a fluxos migratórios intensos, que incluem uma percentagem crescente de migrantes forçados, sejam deslocados internos ou refugiados. Estes últimos procuram por norma países vizinhos, o que explica valores migratórios positivos improváveis em alguns casos – Benim e Uganda, por exemplo. Por seu turno, as ilhas são espaços onde os saldos migratórios são quase sempre de saída, sendo por vezes muito elevados – São Tomé e Príncipe, Reunião, Seychelles. O dinamismo económico explica os resultados positivos da África do Sul, que desde há muito atrai população de países vizinhos e de outros continentes.

Como consequência destas diferenças, o futuro do continente africano será marcado pelo crescimento absoluto da sua população e pelo aumento do seu peso relativo em termos mundiais. Em 2050, mesmo considerando um cenário de crescimento moderado, uma em cada quatro pessoas será africana. As sub-regiões dois e quatro terão quase o dobro dos residentes, as sub-regiões três, seis e sete registarão subidas de 65% a 70% e as sub-regiões um e cinco pouco mais de 30% (Tabela 2).

Tabela 2
África. Estimativas de População por Sub-Regiões, 2024-2050 (%) – Cenário Médio

SUB-REGIÕES	2024	2030	2050	Taxa Var. 2024-50 %
1	14,7	13,8	11,6	31,9
2	7,8	8,2	9,2	95,8
3	26,8	26,9	26,7	65,5
4	16,8	17,4	19,2	89,6
5	6,1	5,8	4,9	34,2
6	14,2	14,3	14,5	70,0
7	13,6	13,7	13,8	69,3

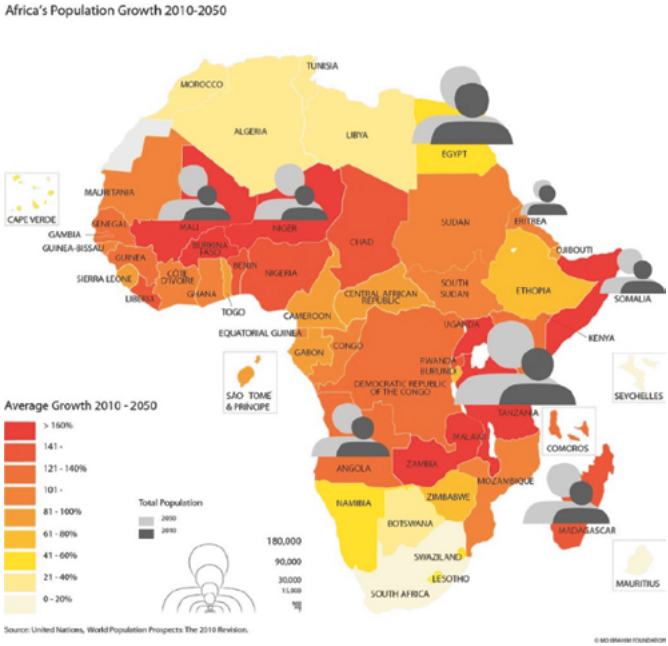
Fonte: Elaboração dos autores com base em UNPFA, 2024.

Esta visão simples esconde, no entanto, a diversidade interna de cada grupo de países, o que pode ser relevante caso essa diversidade coincida com os líderes demográficos intrarregionais. Referimo-nos aos nove grandes Estados africanos e ao modo como as suas características atuais irão condicionar futuros distintos e mudar a sua importância relativa na sub-região a que pertencem enquanto atores de âmbito continental ou mundial (Figura 5).

Em 2024, existe um gigante demográfico com quase 230 milhões de residentes – a Nigéria, o 6.º maior país do mundo –, três com mais de 100 milhões – Etiópia, Egito e República Democrática do Congo –, curiosamente todos em sub-regiões distintas, e cinco outros com volumes entre os 50 e os 70 milhões – Tanzânia, África do Sul, Quénia, Uganda e Sudão. Os grandes Estados africanos são, no entanto, distintos em termos de percentagem de população urbana, saldos migratórios, perfil etário e níveis de fecundidade. E será este último o fator determinante para que venham a ter futuros diferenciados.

O gigante nigeriano é o líder demográfico indiscutível do Grupo 3. Representa 57% do seu total e até 2050 manterá essa importância, devido ao aumento populacional previsto de cerca de 64,7%, embora ligeiramente inferior à média do grupo. O segundo gigante africano é a Etiópia, que corresponde a 64% do total de população no Grupo 7 e perde até 2050 apenas dois pontos percentuais (passa de 64% a 62,6%). No mesmo Grupo 7 figura o Sudão, que irá aumentar mais de 70% entre 2024 e meados do século, mas que corresponde a pouco mais de 24% do efetivo humano do grupo. O terceiro maior Estado é o Egito, com mais de 112 milhões de habitantes em 2024 e um aumento esperado de 40% até meados do século. Corresponde na atualidade a 52,3% do total de população do Grupo 1, valor percentual que deverá ascender a 55,5% em 2050. É, portanto, o líder indiscutível do Norte de

Figura 5
África. Estimativas de Crescimento Populacional (2010-2050)



Fonte: *Spiegel online* https://live.staticflickr.com/6054/6334485690_6e362e5fd4_b.jpg

África. O conjunto que inclui a África Central e Atlântica e a região dos Grandes Lagos tem dois grandes países, a República Democrática do Congo e o Uganda. O primeiro corresponde a 42% do total do Grupo 4 e irá representar 45,7% em 2050, na sequência da esperada duplicação do volume de residentes. Mais modesto, o Uganda acomoda em 2024 19,9% do grupo e irá descer 1,5% até 2050, malgrado continue a crescer. Outros dois grandes países africanos situam-se na sub-região da África Oriental: a Tanzânia, o 5.º maior país africano, e o Quénia, o 7.º. Prevê-se uma quase duplicação de efetivos (87%) no primeiro caso e um crescimento mais modesto no segundo (51,6%), o que permitirá uma subida relativa do peso da Tanzânia no contexto do Grupo 6 (em 2050 corresponderá a 36% do total do grupo) e uma descida do Quénia (de 26,5% atuais, para 23,6%). A 6.ª posição pertence à África do Sul, líder indiscutível do Grupo 5, onde representa dois terços do total de habitantes. Estima-se, no entanto, um aumento populacional de apenas 20,5% até 2050, facto que explica a descida da sua representatividade dos atuais 66,7% para 59,9%.
Vejamos em síntese:

		População	Idade Média	ISF	% Pop. Urbana	Saldo Migratório	% Var. Pop. 2024-50
1	Nigéria	223,804,632	17	5,1	54	-60,0	64,7
2	Etiópia	126,527,060	19	4,0	22	-12,0	65,6
3	Egipto	112,716,598	24	2,8	41	-30,0	40,1
4	R.D. do Congo	102,262,808	16	6,1	46	-15,0	105,9
5	Tanzânia	67,438,106	17	4,6	38	-40,0	87,2
6	África do Sul	60,414,495	28	2,3	69	58,5	20,5
7	Quénia	55,100,586	20	3,2	31	-10,0	51,6
8	Uganda	48,582,334	16	4,4	29	-126,2	75,5
9	Sudão	48,109,006	19	4,3	35	-10,0	71,2

5. Rede de Conetividade Global e Redes de Proximidade

Neste ponto procede-se a uma leitura analítica das relações geoeconómicas de uma amostra de países integrados em cada uma das sete sub-regiões identificadas anteriormente, incluindo, entre outros, aspetos relacionados com transações comerciais, de investimento, tecnológicas, de informação e comunicação, bem como de movimentação de efetivos. Utilizamos como base de informação os dados publicados pela DHL (*DHL Global Connectedness Index 2022*). O estudo criou fichas individuais para todos os países do mundo e estima o seu padrão de conectividade internacional, elencando ainda em cada caso os dez países do mundo com quem o respetivo país mantém maiores relações de caráter económico, populacional, informacional e outras.

A análise realizada com base nessa informação permitiu identificar duas tipologias de países africanos: aqueles que nas suas conexões geoeconómicas apresentam um perfil de relações com potências externas e privilegiam, nomeadamente de contactos com os EUA, a China, a Índia, os Emirados Árabes Unidos e o Reino Unido; e países que sustentam as suas relações externas numa rede com Estados vizinhos, designadamente os integrados na sua própria sub-região.

Adicionalmente, a Figura 6 retrata três níveis distintos no que respeita às dez maiores conexões externas nas relações entre estes três níveis:

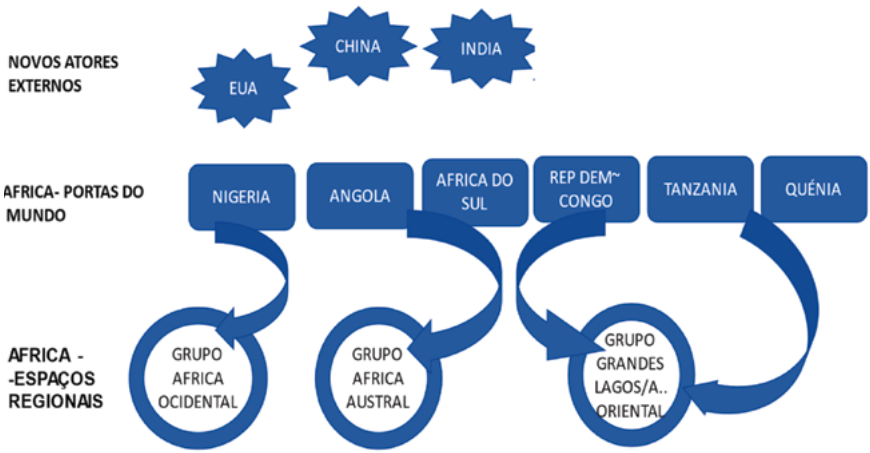
1.º NÍVEL – ÀS PORTAS DE UM NOVO MUNDO – Este grupo inclui os Estados africanos que privilegiam de conexões com atores externos (EUA, República Popular da China, Índia). Falamos da **NIGÉRIA, ANGOLA, REP. DEMOCRÁTICA DO CONGO, QUÉNIA, TANZÂNIA E ÁFRICA DO SUL.**
Neste grupo, a **ÁFRICA DO SUL** é o único com uma forte conexão em termos de parcerias prioritárias com a maioria dos outros Estados do Grupo a que pertence.

2.º NÍVEL – AS ILHAS DO MUNDO – Constituído por Estados de menor dimensão (três insulares e três continentais), mantém também conexões privilegiadas com os EUA, a República Popular da China e a Índia. Referimo-nos à **SERRA LEOA, LIBÉRIA, GÂMBIA, CABO VERDE, MADAGÁSCAR E MAURÍCIAS.**

3.º NÍVEL – OS ESPAÇOS MACRORREGIONAIS AFRICANOS – Inclui Estados em cujas 10 maiores conexões predominam outros Estados africanos. Quase todos têm também conexões com os novos parceiros externos, embora com intensidade menor que o grupo do 1.º Nível. Neste conjunto de Estados podemos identificar três subgrupos regionais diferenciados:
África Ocidental – Inclui a **COSTA DO MARFIM, NÍGER, BURKINA FASO, MALI, BENIN E TOGO**. Vários deles apresentam fortes conexões com a Nigéria, pertencente ao Grupo do 1.º Nível;
África Austral – Inclui **MOÇAMBIQUE, MALAWI, NAMÍBIA, BOTSUANA** e **ZIMBABWE.** Todos têm fortes conexões com a África do Sul e com a Tanzânia, pertencentes ao Grupo do 1.º Nível;
Grandes Lagos – Inclui o **UGANDA, RWANDA E BURUNDI**, Estados que apresentam fortes conexões com a República Democrática do Congo e com a Tanzânia e o Quénia, que pertencem ao Grupo do 1.º Nível.

Fonte: Elaboração dos autores com base em DHL, 2023.

Figura 6
África. A Rede de Conetividade Global



Fonte: Elaboração dos autores com base em DHL, 2023.

Revendo as sete sub-regiões inicialmente identificadas no ponto dois e sobrepondo a essa imagem a divisão decorrente da identificação da rede de conectividade, concluímos que os Estados do 1.º nível se incluem em apenas cinco sub-regiões:

3 – ÁFRICA OCIDENTAL

- Estado Inserido na Conetividade Global de África – NIGÉRIA.
- Estados Inseridos na rede macrorregional da África Ocidental – COSTA DO MARFIM, NÍGER, BURKINA FASO, MALI, BENIN e TOGO, podendo englobar-se também o GANA e quatro Ilhas do mundo, SERRA LEOA, LIBÉRIA, GÂMBIA E CABO VERDE.

4 – ÁFRICA CENTRAL + ÁFRICA ATLÂNTICA + REGIÃO DOS GRANDES LAGOS

- Estados Inseridos na Conetividade Global de África – ANGOLA e REPÚBLICA DEMOCRÁTICA DO CONGO.
- Estados inseridos na rede macrorregional – GABÃO, REPÚBLICA DO CONGO, RUANDA e BURUNDI.

5 – ESPAÇO DA ÁFRICA AUSTRAL

- Estados inseridos na Conetividade Global de África – ÁFRICA DO SUL .
- Estados inseridos na rede macrorregional – MOÇAMBIQUE, MALAWI, NAMÍBIA, BOTSWANA e ZIMBABWE.

6 – ÁFRICA ORIENTAL

- Estados inseridos na Conetividade Global de África – TANZÂNIA e QUÉNIA.
- Estados inseridos na rede macrorregional – UGANDA, RUANDA e BURUNDI (dupla pertença com macrorregião quatro).

7 – CORNO DE ÁFRICA

- Estados Inseridos na Conetividade Global de África – ETIÓPIA.
- A Etiópia não está incluída nas *Fichas Países do Relatório da DHL*, razão pela qual não surge nas listagens anteriores, mas vamos considerá-la neste exercício.
- Estados inseridos na rede Regional Corno de África – DJIBOUTI, SUDÃO DO SUL, ERITREIA e SOMÁLIA.

Vejamos com maior precisão como estes novos atores interagem com a realidade africana, incluindo nesta análise a Federação Russa, que tem vindo a aumentar nas últimas décadas, e de forma muito clara, o seu interesse em se posicionar também como ator externo em África.

Esta transformação do padrão de relações externas dos Estados africanos pode ser comparada com outra realidade, que é a dos Estados observadores da CPLP. O interesse de atores políticos como os EUA, a Índia, o Japão, a Turquia e o Qatar por integrarem a coroa de Estados Observadores da CPLP deveria levar-nos a refletir sobre o papel do mundo lusófono no processo atual de transformação geopolítica e geoeconómica global, dando prioridade a África.

6. Atores Externos nas Sub-Regiões

Neste ponto vamos centrar a nossa análise em quatro atores, os dois primeiros mais direcionados para a concretização de projetos na área geoeconómica e os restantes dois empenhados em garantir uma presença em África na esfera da defesa e cooperação militar.

6.1. Geoeconomia, Tecnologias e Sociedade

6.1.1. EUA *versus* a China e a Índia

Os EUA têm privilegiado uma abordagem integrada e abrangente de relacionamento com África, centrada em diferentes áreas. Em 2022 presidiram a uma cimeira com líderes de vários Estados africanos, assinalando a intensificação dessa relação e da qual resultaram novos acordos bilaterais de comércio e investimento envolvendo dezenas de biliões de dólares.
A International Development Finance Corporation e o Departament of Commerce foram responsáveis pela criação de um conjunto alargado de apoio a infraestruturas estratégicas e ao setor de pequenas e médias empresas. Amplos financiamentos foram alocados para garantir acesso a minerais críticos, bem como ao aumento da produtividade agrícola, incentivando inclusivamente práticas agrícolas climaticamente inteligentes. Visaram também a melhoria da oferta de cuidados de saúde.
A criação do *President´s Advisory Council on doing business in Africa* (PAC -DBIA), com 18 novas recomendações para fortalecer a colaboração comercial em setores prioritários, dá conta da aposta e interesse americano na presença em África, de que um dos grandes momentos foi a celebração da parceria US-Kenya Strategic Trade and Investment Partnership.
Outro campo relevante consistiu na celebração de acordos de parceria em setores prioritários, como digitalização, tecnologias energéticas limpas e indústrias criativas. O lançamento da iniciativa *Digital Transformation with Africa* (DTA) foi um dos mais relevantes, mas podemos referir múltiplos projetos – nomeadamente a criação de novos Data Centers no Gana e no Quénia; a criação do Women in Digital Economy Fund, com envolvimento da Microsoft; ou o apoio à criação de PME na esfera do digital que os EUA estabeleceram com o governo da Costa do Marfim.
Na esfera do suporte dado a infraestruturas destaca-se a US Trade and Development Agency. O Presidente Biden escolheu o continente africano para o lançamento em maio de 2023 do primeiro grande projeto de apoio a corredores de transporte. De destacar, no âmbito da iniciativa *Partnership for Global Infrastructure and Investment*, o projeto destinado à modernização do caminho de ferro de Benguela e ao novo

terminal de minérios do porto do Lobito, reforçando a ligação ferroviária entre Angola, República Democrática do Congo e Zâmbia.

6.1.2. A República Popular da China (RPC). Investimento em África

A China tem vindo a realizar avultados investimentos no continente, privilegiando duas áreas particulares de intervenção: em corredores ferroviários macro e intrarregionais e portos associados aos mesmos e em zonas económicas especiais e parques industriais.

No respeitante à construção e modernização de corredores ferroviários, tem vindo a realizar um forte investimento na construção e modernização de corredores ferroviários a nível nacional – criando corredores centrados nas capitais – e em sub-regiões de África – com corredores que em vários casos estão associados à construção ou expansão de portos que permitem assegurar a interface do continente africano com os oceanos Atlântico e Índico. Estes corredores são construídos com financiamento chinês e a responsabilidade de construção está também entregue a firmas chinesas. Iremos destacar quatro desses investimentos. O primeiro na África Ocidental, onde a RPC se envolveu, na Nigéria, na construção da linha ferroviária Lagos-Ibadan, que liga a capital à segunda maior cidade do país e está vocacionada para o transporte de passageiros. Representou o maior projeto ferroviário do país desde a independência, e após falência da companhia ferroviária estatal.

O segundo investimento compreendeu o corredor ferroviário Atlântico-Índico (Figura 7). Este corredor tem uma natureza diferente dos restantes três, porque se destina a garantir acesso a uma sub-região mineira, que abrange parte da República Democrática do Congo (no Catanga) e a Zâmbia, encravadas no interior do continente. Garante acesso quer ao Oceano Atlântico, através de Angola e do caminho de ferro de Benguela, também ele renovado com investimento chinês; quer ao oceano Índico, através da Tanzânia e do TANZAM – projeto ferroviário apoiado pela China nos anos 70, que liga a Zâmbia aos portos na Tanzânia. Este corredor está a ser acompanhado pela construção de um novo porto na Tanzânia, o porto de Bagamoyo.

O corredor África Oriental e Grandes Lagos é o terceiro grande investimento. Além de ligar Nairobi, capital do Quénia, ao porto queniano de Mombaça, procura ligar o Quénia à África dos Grandes Lagos (Uganda, Ruanda e Burundi), chegando mesmo até à cidade de Kisangani, no norte da República Democrática do Congo, e desta forma conectando países situados mais no interior do continente através do oceano Índico.

Por fim o investimento no Corno de África. Este corredor quando foi planeado destinava-se a ligar a capital da Etiópia, Addis Ababa, situada no interior do continente, com o porto de Djibouti no Corno de África, à entrada do Mar Vermelho, numa altura em que a independência da Eritreia – em choque com a Etiópia – cortava o acesso

Figura 7
África. Os Corredores Ferroviários Financiados pela RPC

Corredor Atlântico-Índico

Corredor África Oriental-Grandes Lagos

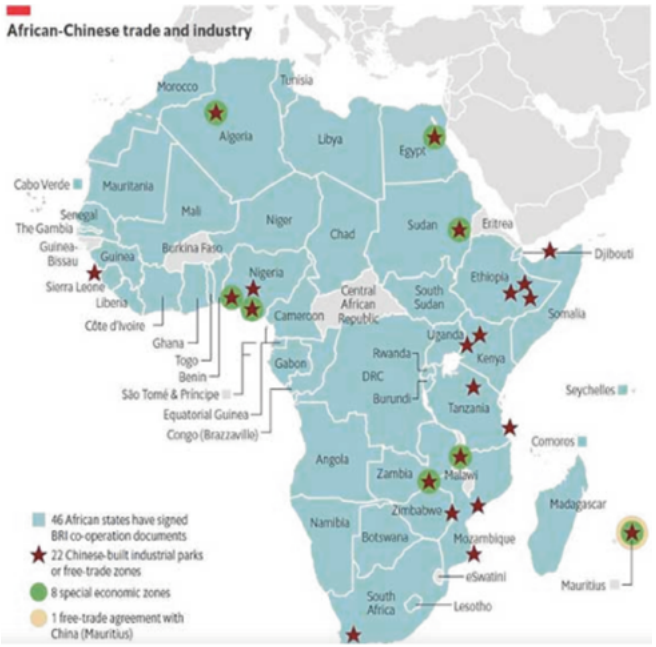
Corredor Addis Ababa ao porto de Djibouti

tradicional desta ao porto eritreu de Asmara – situação que se modificou, graças ao acordo de paz assinado entre os dois países.

Que retorno efetivo resultou destes investimentos, que envolveram montantes em rápido crescimento – de 75 milhões em 2003 para 27 mil milhões de dólares em 2019? A indústria de construção representava no ano de 2019 cerca de 30% do investimento total da China em África. Nestes projetos as empresas chinesas forneceram as locomotivas, adaptadas a mudanças de altitude de 2.000 metros e a temperaturas que podem atingir os 50 graus Celsius de dia e temperaturas geladas de noite. Uma das promessas que estes investimentos ferroviários se propuseram concretizar foi assegurar viagens confortáveis, com ar condicionado para o transporte de passageiros, muito necessário em várias regiões de África. No entanto, o número dos passageiros não

foi tão elevado como o previsto e o serviço nem sempre foi confiável em termos de horários. Contudo, o transporte de mercadorias representa uma parte significativa do potencial de longo prazo das novas ferrovias e pode vir a ser um ativo valioso para se conseguir desenvolver o comércio intracontinental em África (Fabio Scala, 2020).
No que diz respeito às Zonas Económicas Especiais e Parques Industriais construídos pela China em África, a observação da Figura 8 testemunha a importância da Nigéria na África Ocidental, contando com a combinação de três zonas económicas com três parques industriais construídos pela China; da Etiópia no Corno de África, com três parques industriais construídos pela China; e de dois Estados da África Oriental com dois parques industriais contruídos pela China, no Quénia e na Tanzânia.
Da observação destas duas áreas de intervenção da China em África, investimento ferroviário e criação de zonas económicas, ressalta a estratégia de privilegiar o relacionamento com os países que, em cada sub-região, estão mais inseridos na conetividade global de África, tendo igualmente a preocupação de "desencravar" o núcleo mineiro no centro do continente – República Democrática do Congo e Zâmbia –, reforçando os acessos ferroviários a portos no Atlântico e no Índico.

Figura 8
Zonas Económicas Especiais e Infraestruturas Criadas e Construídas pela China para Captação e Localização de Investimento Externo



Fonte: Chinese Trade and Investment in Africa – The Economist Intelligence Unit.

6.1.3. Índia, África e Índico

A Índia é um dos cinco maiores investidores em África, com um investimento acumulado de 73,9 biliões de dólares entre 1996 e 2022. Na verdade, a Índia e África têm uma já longa parceria baseada em valores partilhados e no bom relacionamento que a Índia tem com África. Refira-se que o comércio da Índia com África passou de 68,5 mil milhões de dólares em 2011-2012 para 90,5 mil milhões em 2022-2023.
Realizaram-se Cimeiras do Fórum Bilateral Índia-África a partir de 2008 (em Nova Dehli), 2011 (em Adis Abava), em 2015 (Nova Deli), esta última com a participação de 54 Estados africanos. A quarta cimeira do Fórum teve de ser adiada, devido à pandemia Covid-19. Em 2023 a Índia utilizou a sua presidência do G20 para garantir à União Africana (UA) o estatuto de membro permanente do G20.
A Índia promoveu ainda a criação de uma organização de integração regional no Índico, a IORA, que inclui membros da África Oriental, do Golfo Pérsico, do Indo-Pacífico (ASEAN e OCEANIA) e tem como Estados observadores os EUA, a China, o Reino Unido, França e Alemanha.

6.2. Segurança e Defesa – os EUA versus *a Rússia*

6.2.1. EUA em África, uma Intervenção Militar Poli Direcionada

Os EUA têm uma presença efetiva em termos geoeconómicos, à qual agregam ainda uma componente militar, talvez de ambas a mais distintiva. Em termos militares possui bases militares dispersas pelo território de África do Sahel, África Central e do Sul (Figura 9).
Através do *Africa Command*, os EUA apoiam os seus parceiros em África utilizando uma abordagem 3D, que envolve Diplomacia, Desenvolvimento e Defesa. Assim, enquanto as Embaixadas utilizam Diplomacia e Desenvolvimento no apoio aos governos africanos, o *Africa Command* ajuda esses governos na área da Defesa. E fá-lo ajudando-os a capacitar as suas Forças Armadas para combater extremismos violentos e para responder a crises, nomeadamente no âmbito da *Security and Safety*, garantindo aos seus povos funções-chave, como educação, emprego e cuidados de saúde. O apoio dos EUA à consolidação das Forças Armadas inclui treino, realização de exercícios, vendas de equipamento e outros serviços de cooperação em segurança, que ajudam os militares africanos a respeitar os governos civis, as leis da guerra e os Direitos Humanos (*Africa Command*, 2024).

Figura 9
Bases Militares Estrangeiras em África

Fonte: https://issafrica.s3.amazonaws.com/site/images/2019-08-27-iss-today-foreign-military-map.png

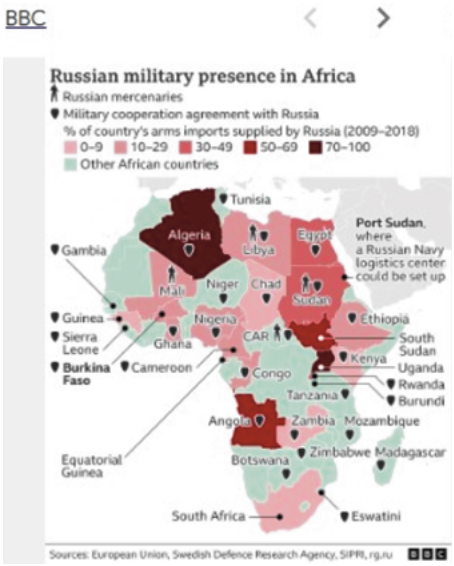
6.2.2. Rússia. Uma outra Forma de "Construir" Influência em África

A Rússia prolongou os relacionamentos criados no tempo da URSS, nomeadamente na África Austral e Oriental, e iniciou uma expansão em todo o Sahel e uma penetração na África Central. Tem procurado desenvolver a sua presença em África com base nas suas capacidades na área militar, mediante o estabelecimento de acordos de cooperação militar, venda de armamento e presença militar – inicialmente por via de grupos, como o Grupo Wagner, mas também com forças russas, como no caso recente do Níger (Figura 10). Em contrapartida desse tipo de intervenção tem procurado aceder de forma privilegiada a recursos mineiros e de obter facilidades militares.

…Voltando ao Princípio "África, um Continente do Mundo"

No início deste artigo referimos a transformação da África, no que designamos por "África, um continente do Mundo", procurando chamar a atenção para a profunda transformação em curso das relações externas dos países africanos.
No ponto seis podemos identificar esta transformação, patente no reforço das relações de países africanos com países fora da Europa, incluindo os EUA, a China, a Índia e a Rússia, mas também os Emirados Árabes Unidos e a Turquia, pese embora se

Figura 10
Presença Militar Russa em África



trate de relações com diferente grau de importância a nível económico, tecnológico, político ou mesmo militar.

Nos próximos anos África continuará a ser um espaço de competição entre as grandes potências, nomeadamente as quatro que analisamos neste texto. No entanto, no horizonte temporal de 2030, permanece a incerteza no relativo ao seu vizinho mais próximo, a União Europeia, e ao modo como esta vier a reavaliar a importância de África no seu relacionamento externo.

Bibliografia

Al Jazeera, 2022. Mapping Africa's natural resources. Al Jazeera Staff, 15 Feb. Disponível em: https://www.aljazeera.com/news/2018/2/20/mapping-africas-natural-resources

Chakrabarty, M., 2024. Time for a new chapter in India-Africa relations. Observer Research Foundation. Published on Feb 08. Disponível em: https://www.orfonline.org/expert-speak/time-for-a-new-chapter-in-india-africa-relations

CPLP, 2019. *Documento Estratégico de Cooperação da CPLP 2020-2026*. Disponível em: R3_Orientacao-Estrategica-da-Cooperacao_Anexo-1_DEC_2020_2026_APROVADO%20(1).pdf

DHL, 2023. *DHL Global Connectedness Index 2022*. Na in-depth report on the sate of globalization. Disponível em: https://www.dhl.com/content/dam/dhl/global/delivered/documents/pdf/dhl-global-connectedness-index-2022-complete-report.pdf

Mapa político de África. Guia geográfico. Disponível em: https://mundoeducacao.uol.com.br/geografia/paises-da-africa.htm

Partition of Africa, 2009. The Metropolitan Museum of Art, Heilbrunn Timeline of Art History. Disponível em: https://www.blackpast.org/global-african-history/partition-africa/

Ribeiro, J. F., 2023. África -uma Breve Vista (Documento policopiado), Lisboa, FCG.

Ribeiro, J. F., 2024. Reinos e Impérios em África antes da colonização Europeia – Um apontamento. (Documento policopiado), Lisboa, FCG.

Scala, F., 2020, Africa Day is every day. Celebrating the socio-economic renaissance of the African continent, Opinion, Further Africa. 24 May 2024. Disponível em: https://furtherafrica.com/2024/05/24/africa-day-is-every-day/

United States Africa Command. Disponível em: https://www.africom.mil/

UNPFA, 2022. *World Population Prospects 2022*, Population Division. Disponível em: https://population.un.org/wpp/

US Government, 2022. Fact Sheet: Accelerating the US – Africa Partnership After the 2022 US – Africa Summit. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/08/fact-sheet-president-biden-announces-the-americas-partnership-for-economic-prosperity/

Worldometer. Disponível em: https://www.worldometers.info/world-population/

REVISTA NAÇÃO E DEFESA
Números temáticos publicados

1998	84	Inverno	Uma Nova NATO numa Nova Europa
	85	Primavera	Portugal e o Desafio Europeu
	86	Verão	O Desafio das Águas: Segurança Internacional e Desenvolvimento Duradouro
	87	Outono	O Estado em Mudança
1999	88	Inverno	Mulheres nas Forças Armadas
	89	Primavera	Portugal na NATO: 1949-1999
	90	Verão	Economia & Defesa
	91	Outono	Operações de Paz
2000	92	Inverno	Portugal e as Operações de Paz na Bósnia
	93	Primavera	Novos Rumos da Educação para a Cidadania
	94	Verão	Democracia e Forças Armadas
	95/96	Outono-Inverno	Prevenção de Conflitos e Cultura da Paz
2001	97	Primavera	Nova Ordem Jurídica Internacional
	98	Verão	Forças Armadas em Mudança
	99	Outono	Segurança para o Século XXI
	100	Inverno	De Maastricht a Nova Iorque
2002	101	Primavera	Europa e o Mediterrâneo
	102	Verão	Repensar a NATO
	103	Outono-Inverno	Novos Desafios à Segurança Europeia
	Extra	Dezembro	Cooperação Regional e a Segurança no Mediterrâneo (C4)
2003	104	Primavera	Evolução das Nações Unidas
	Extra	Abril	A Revolução nos Assuntos Militares
	105	Verão	Soberania e Intervenções Militares
	106	Outono-Inverno	A Nova Carta do Poder Mundial
2004	107	Primavera	Forças Armadas e Sociedade. Continuidade e Mudança
	Extra	Julho	Educação da Juventude. Carácter, Liderança e Cidadania
	108	Verão	Portugal e o Mar
	109	Outono-Inverno	Segurança Internacional & Outros Ensaios
2005	110	Primavera	Teoria das Relações Internacionais
	111	Verão	Raymond Aron. Um Intelectual Comprometido
	112	Outono-Inverno	Número não Temático
2006	113	Primavera	Número não Temático
	114	Verão	Segurança na África Subsariana
	115	Outono-Inverno	Portugal na Europa Vinte Anos Depois

2007	116	Primavera	Número não Temático
	117	Verão	Número não Temático
	118	Outono-Inverno	Políticas de Segurança e Defesa dos Pequenos e Médios Estados Europeus
2008	119	Primavera	Transição Democrática no Mediterrâneo
	120	Verão	Número não Temático
	121	Outono-Inverno	Estudos sobre o Médio Oriente
2009	122	Primavera	O Mar no Pensamento Estratégico Nacional
	123	Verão	Portugal e a Aliança Atlântica
	124	Outono-Inverno	Que Visão para a Defesa? Portugal-Europa-NATO
2010	125	Primavera	Visões Globais para a Defesa
	126		O Conceito Estratégico da NATO
	127		Dinâmicas da Política Comum de Segurança e Defesa da União Europeia
2011	128		O Mar no Espaço da CPLP
	129		Gestão de Crises
	130		Afeganistão
2012	131		Segurança em África
	132		Segurança no Mediterrâneo
	133		Cibersegurança
2013	134		Ásia-Pacífico
	135		Conselho de Segurança da ONU
	136		Estratégia
2014	137		Reflexões sobre a Europa
	138		Brasil
	139		Portugal na Grande Guerra
2015	140		Nuclear Proliferation
	141		Arquipélago dos Açores
	142		India
2016	143		Terrorismo Transnacional
	144		The EU Comprehensive Approach: Concepts and Practices
	145		Leituras da Grande Guerra
2017	146		Drones
	147		Brexit
	148		Grupos Islamistas Radicais

2018	149		Europe and Refugees
	150		European Defence
	151		Geopolítica Aplicada
2019	152		Terrorismo e Violência Política
	153	Agosto	Segurança Energética e Economia do Gás
	154	Dezembro	Pontes Sobre o Atlântico
2020	155	Abril	Desafios Europeus
	156	Agosto	Segurança em Tempo de Crise
	157	Dezembro	Mulheres, Paz e Segurança
2021	158	Abril	Segurança Internacional
	159	Agosto	Desafios Geopolíticos
	160	Dezembro	Relações Europa-África
2022	161	Abril	Conflitos Armados
	162	Agosto	O Espaço Pós-Soviético
	163	Dezembro	Tecnologia, Cibernética e Defesa
2023	164	Abril	Conflitos e Disputas Regionais
	165	Agosto	Geopolítica e Soberania
	166	Dezembro	China 2049
2024	167	Abril	Dinâmicas Regionais de Segurança e Defesa

Política Editorial

A *Nação e Defesa* proporciona um espaço de reflexão que privilegia diferentes paradigmas e perspetivas relevantes para o conhecimento e análise de questões no quadro da segurança e defesa, no plano teórico e aplicado. A revista encontra-se vocacionada para a compreensão, exame crítico e debate de matérias no âmbito da segurança e defesa internacional e nacional.

Tem como prioridade promover o conhecimento e a reflexão pluridisciplinar, nomeadamente no campo dos Estudos de Segurança, Estudos Estratégicos, Ciência Política, História, Estudos Diplomáticos, Relações Internacionais, Sociologia, Direito Internacional Público e Economia.

Nação e Defesa é uma publicação periódica de natureza científica, que adota o sistema de arbitragem por pares na admissão e aprovação dos artigos submetidos.

Editorial Policy

Nation and Defense provides a space for reflection that privileges different paradigms and perspectives relevant to theoretical and applied analysis of security and defense matters. The journal is dedicated to the critical examination and scientific debate on international security and defense.

Its priority is to promote a multidisciplinary approach to Security Studies, Strategic Studies, Political Science, History, Diplomatic Studies, International Relations, Sociology, International Law and Economics.

Nation and Defense is a scientific publication, which adopts the peer review system in the admission and approval of submitted articles.

NORMAS DE COLABORAÇÃO

O artigo proposto para publicação, em português ou inglês, deve ser enviado via correio eletrónico para idn.publicacoes@defesa.pt devendo observar as seguintes normas:

- Ter entre 5.000 a 8.000 palavras (espaços incluídos) em Word;
- Ser acompanhado de um resumo em português e em inglês (até 150 palavras cada);
- Ter título e palavras-chave em português e inglês;
- Ser redigido de acordo com o sistema de referências de Harvard.

Os textos submetidos devem ser inéditos, não editados ou apresentados em quaisquer outras publicações.

O artigo, sem indicação do autor e acompanhado pela Ficha de Identificação (disponível em https://www.idn.gov.pt/conteudos/documentos/FichadeAutor.pdf) devidamente preenchida, será apreciado em regime de anonimato (*blind peer review*).

A revista *Nação e Defesa* adota o sistema de referência bibliográfica de Harvard, disponível em https://library.aru.ac.uk/referencing/harvard.htm. Este sistema emprega a referência autor e data no corpo do texto e uma lista de referências bibliográficas no final do artigo escrito, organizada por ordem alfabética. A lista de referências contém uma relação detalhada dos livros, revistas e fontes eletrónicas citadas.

Os artigos publicados são da inteira responsabilidade do autor.

Cada autor receberá dois exemplares da revista na morada indicada.

Ao submeter um manuscrito à revista, o(s) autor(es) declara(m) que autoriza(m), a título gracioso, a digitalização, o carregamento e a divulgação do referido artigo nas plataformas de conteúdos digitais do IDN e em repositórios e bases de dados bibliográficos. Os casos não especificados nestas normas de colaboração deverão ser apresentados ao Editor.

COLLABORATION RULES

The article submitted for publication, in Portuguese or English, must be sent by email to idn. publicacoes@defesa.pt observing the following rules:

- Length between 5,000 and 8,000 words (spaces included) in a Word format;
- Abstract in Portuguese and English (up to 150 words each);
- Title and keywords in Portuguese and English;
- Adoption of the Harvard reference system.

Submitted texts must be unpublished, unedited or presented in any other publications.

The article, without the author name and accompanied by the Identification Form available in https://www.idn.gov.pt/conteudos/documentos/author_form.pdf duly completed, will be evaluated anonymously (blind peer review).

Nation and Defense adopts the Harvard bibliographic reference system - https://library.aru. ac.uk/referencing/harvard.htm. This system uses the author and date in the text body and a list of references at the end of the article, organized in alphabetical order. The reference list contains a detailed list of cited books, journals and electronic sources.

Published articles are the sole responsibility of the author. Each author will receive two copies of the journal.

By submitting a manuscript to the journal, the author (s) declare that they gracefully allow the digitization, upload, and dissemination of the article on IDN digital content platforms, repositories and bibliographic databases. Cases not specified in these collaboration rules should be submitted to the Editor

NAÇÃO E DEFESA

Revista quadrimestral

Nome/Name _____

_____

Morada/Adress _____

_____

Localidade/City _____

Cód. Postal/Zip _____ - _____ _____

_____ NIF _____

Country _____

E-mail _____

Tel./Phone _____

☐ Renovação/Renewal – Assin. nº/Subscrip. nr. _____

☐ Nova assinatura/New subscription

Assinatura/Signature _____

Data/Date _____

Assinatura Anual/Annual Subscription (3 nºs /issues)

☐ Instituições/Institutions 40,00 €

☐ Individuais/Individuals 25,00 €

☐ Estudantes/Students 20,00 € (anexar comprovativo deste ano)

Números Anteriores/Previous Issues – 8,50 € cada/each + portes/ /postage charges

☐ ☐ ☐ ☐ ☐ ☐

Pré-Pagamento/Prepayment

☐ **Numerário**

☐ **Cheque** nº _____ Banco _____ à ordem do IDN

☐ **Transferência Bancária** NIB 0781 0112 0000 000 7777 20
(anexar comprovativo da Transferência)

☐ **Bank Transfer** (compulsory for foreign subscriptions)

IBAN – PT50 0781.0112 0000 000 7777 20
BIC (SWIFT) – IGCPPTPL

INSTITUTO DA DEFESA NACIONAL
Calçada das Necessidades, 5, 1399-017 Lisboa
PORTUGAL

www.idn.gov.pt
idn.publicacoes@defesa.pt
tel. + 351 21 392 46 00 Fax + 351 21 392 46 58

idn nação e defesa

EXTRA DOSSIÊ

TERESA RODRIGUES E JOSÉ FÉLIX RIBEIRO ÁFRICA NO TABULEIRO DE XADREZ MUNDIAL: ESTRUTURAS, DESAFIOS E OPORTUNIDADES

idn Instituto da Defesa Nacional

ISSN 0870-757X 00168