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 democratic 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).