THE PEOPLE'S REPUBLIC OF CHINA AND THE THREATS TO NATO'S CYBER SECURITY

Lieutenant Colonel (N) Claudiu-Cosmin RADU, PhD Student
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.17

In recent years, many NATO member states have reported violations of cyber sovereignty, accusing the People's Republic of China (PRC). PRC has its own vision of cyberspace, employing technological advances to strengthen its position as a global leader. This article addresses NATO's cyber security challenges, analysing how Beijing's actions influence international politics and cyber stability. Utilizing a combination of qualitative and quantitative analysis, the research explores the ways in which the PRC pursues its geopolitical goals in cyberspace, as well as NATO's response measures. From the analysis of cyber security policies, we draw insights into the strategic directions each side is pursuing. The article also assesses the long-term impact of cyber tensions between the PRC and NATO and exposes the importance of international collaboration in promoting a stable and secure cyberspace. The conclusions emphasize the need for a coordinated and proactive approach to counter cyber threats and strengthen the Alliance's cyber defence.

Keywords: People's Republic of China; cyber security; NATO; cyber threats; cyberspace;

INTRODUCTION

The accelerated progress in information and communication technology in recent years has been of significant importance in the development of cyber capabilities worldwide. With this technological advancement, the People's Republic of China, hereafter referred to as the PRC, has become a major force not only economically and militarily, but also in cyberspace, strengthening its presence in this key area of international security. In the context of these developments, NATO, the alliance of Western democratic states, is facing unprecedented challenges posed by aggressive cyber-aggression in cyberspace. In the view of the member states, the main countries funding non-state actors or conducting offensive cyber activities are considered to be the Russian Federation, the People's Republic of China, North Korea and Iran (Diotte, 2020).

The PRC's expansion into cyberspace has attracted the attention of major Western powers, especially the United States of America, which sees Beijing as the main cyber security threat. According to reports by NATO and other international organizations, the PRC has developed complex cyber espionage strategies, using sophisticated methods of infiltration and intelligence collection to gain economic, military, and geopolitical advantages (Hamilton, 2020). The PRC is increasingly manifesting its influence in cyberspace through policies and strategies specifically designed and tailored to achieve sovereignty in cyberspace. Its conception of this operational domain is considered innovative and forward-looking, as it views cyberspace as a virtual extension of its territory, which it seeks to control in the same way it manages its physical territory. This approach creates particular challenges for the North Atlantic Alliance, which promotes a free, open, peaceful and secure cyberspace and strives to increase stability and reduce friction between countries. These goals are intended to be achieved through international law and accepted norms of responsible state behaviour in cyberspace (NATO, 2024).

The PRC's cyber strategy focuses on deterrence and coercion in cyberspace (Hamilton, ib.), where Beijing conducts offensive actions against government entities and critical infrastructures of its adversaries, including NATO member states. This tactic is part of a broader strategy of geopolitical influence, through which the PRC seeks to expand its presence and consolidate its status as a global power.

The PRC's intense cyber activities are one of the main concerns for NATO, due to the complexity and high frequency of cyber attacks launched. These attacks range from DDoS (Distributed Denial of Service) attacks to sophisticated infiltration of government, civilian or even military networks, with the aim of weakening networks and obtaining information critical to national security. The big challenge for NATO is to strengthen its defences against these increasingly advanced cyber attacks. In this context, the Alliance has implemented initiatives to foster coordination and cooperation among member states in the field of cyber security. However, the PRC's rapid advances in cutting-edge technologies, such as artificial intelligence and quantum computing, are amplifying the complexity of this landscape, prompting NATO to intensify its efforts to develop more effective countering techniques.

The main purpose of this paper is to analyse the cyber developments and activities of the PRC and their impact on the security of the North Atlantic Alliance. In this context, the proposed objectives are: to analyse the tactics employed by the PRC in cyberspace and to correlate the North Atlantic Alliance's responses to counter PRC threats in this environment. Furthermore, the paper also aims to analyse the long-term implications of this cyber conflict and how international alliances can play a decisive role in maintaining global security in the digital age.

The research methodology consists mainly of qualitative methods, but includes some quantitative methods by analysing the content of laws, strategies and policies governing cyberspace in the PRC and NATO, as well as the scientific literature. Based on this analysis, the present study aims to answer the following research question: *Is NATO prepared to effectively counter the increasingly sophisticated cyberspace actions initiated by the PRC?*

The content analysis of the Beijing administration's cyber policies underlines its intention to use cyberspace to achieve its geopolitical, economic and national security ambitions. A strategy that integrates technological advancement with rigorous domestic control, cyber sovereignty and information control, are critical for Beijing, both for maintaining domestic stability and for expanding its global influence. At the same time, the PRC's ability to offensively develop and deploy advanced technologies poses significant risks to global cyber security, requiring a coordinated response from NATO and its partners.

THE EVOLUTION AND PERSPECTIVES OF THE CYBER POLICIES OF THE PEOPLE'S REPUBLIC OF CHINA

To understand the actions of the PRC in cyberspace, it is essential to analyse some of the motivations and goals behind these actions. It is not intended to justify the PRC's behaviour, but to provide insight into the factors influencing the decisions and strategies adopted. After the end of the Cold War, when there were basically two major centres of power, new international actors emerged to claim their authority in various areas. As these new powers asserted their influence, many of them, including the PRC, experienced a rapid rise in areas such as technology, economics and military power. The PRC, with clear ambitions to become a major player in the global economy, has invested heavily in the development of advanced technologies, as it seeks to consolidate its geopolitical influence and reduce its dependence on other states. This global competition, fuelled by the egos and political ambitions of China's leaders, has led to an accelerated pace of research and innovation in emerging technologies such as artificial intelligence, 5G and 6G technology, Internet of Things (IoT) and quantum computing. In this context, the PRC has quickly recognized the value and potential of cyberspace, not only as a medium for economic development, but also as a strategic area for gaining competitive advantage over other states, whether through cyber espionage, intellectual property theft, or attacks on critical infrastructure (Chafetz, 2023). These actions are motivated by the PRC's desire to expand its global influence, protect its economic interests, and position itself as an international technological leader. Through this aggressive, politically and administratively driven approach, Beijing seeks not only to assert its supremacy in cyberspace, but also to consolidate its role as a global power capable of influencing the international order and asserting itself in an increasingly competitive geopolitical landscape. These actions are deeply rooted in the autocratic structure of the state, which favours centralized control and the subordination of economic and legal interests to the Communist Party.

Over the past decade, the overall competition between the People's Republic of China and the United States of America has intensified significantly, and a new front of this rivalry has emerged in cyberspace. In this context, both countries accuse each other of cyber espionage, unfair competitive practices and interference in national critical infrastructures. Critical infrastructure, which includes electricity grids, transportation systems and communications, is a particularly sensitive national asset and the security of these systems is essential to the functioning of any modern nation. Moreover, intrusion into these networks is perceived as a threat

to national security and is addressed by most states in their national strategies and cyber security strategies.

Much of the tension in cyberspace between the PRC and the USA centres on accusations of espionage, both in the military and economic spheres. Although both nations accuse each other of extensive espionage, the practice is not limited to just the two states. Most NATO member states have experienced a wider range of cyber incidents from state or non-state actors with ties to the PRC. Paradoxically, the complexity and economic interdependencies between states lead to a certain caution in carrying out such actions. Nonetheless, competition continues to be waged through DDoS attacks, infiltration of government institution networks and disinformation influence campaigns, all of which fall within the boundaries of hybrid warfare. However, cyberattacks are often considered a component of contemporary diplomatic and military strategy without escalating the threshold that would trigger direct armed conflict (Jinghua, 2019).

Beginning in the 1990s, the PRC began to understand the profound impact that new technologies could have on the future. Officials in Beijing saw the potential of developing cyber capabilities, first for their low cost, and second for the efficiency with which they could replace conventional technologies. Internet networks were put under tight control as the leadership was concerned about controlling access to the internet and digital infrastructure. There were fears that the country could become vulnerable to attacks from other nations, which had already begun to integrate advanced digital solutions into their military strategies (Jiang, T., 2022).

This period has been one of consolidation, influenced by military conflicts in which advanced technologies for the time were used in conflicts such as the 1991 Gulf War, which served as a clear demonstration of American technological advantage. The conflict is considered by many analysts as the first *"computerized war"* due to its extensive use of modern technologies such as advanced communications systems, radar, satellites, and guided weapons. Essentially, electronic warfare techniques were used to disrupt and intercept Iraqi communications as well as to precisely coordinate attacks. Although no actual cyber-attacks were launched, the war demonstrated the increasing reliance on cyber technologies in warfare, foreshadowing the importance of cyberspace actions in future conflicts. It was only during the Kosovo conflict in 1999 that cyber-attacks were employed, marking the event as the first *"internet war"*. Governmental and non-governmental actors alike used the internet to disseminate information, spread propaganda, spread fake news and solicit support for their positions (Denning, 2001). In the wake of global events,

the PRC perceived the need to accelerate its own cyber capabilities as a preventive measure. At the same time, the groundwork is being laid to strengthen control over the PRC's national cyber infrastructures. The ambitions for cyberspace security are heavily shaped by the trajectory of the PRC's informatization strategy. In 2000, it set the goal of becoming an advanced information society, where businesses, scientists, and citizens use the latest information and communication technologies (ICTs) to improve performance and enhance social benefits (Austin, 2018, p. 11).

At the national level, cyber research and development has been stepped up to secure its territory against external threats. Moreover, Beijing's strategy focuses heavily on *"network sovereignty"*, which translates into the government's ability to control the flow of information on the internet. It has included the implementation of strict censorship and data traffic monitoring measures designed to prevent external infiltration and protect national interests (Jiang, T., ib.). According to the same author, since 2008, the PRC has become the largest internet market in the world with over 253 million users. This rapid expansion of the internet has coincided with its rise to the global economic podium. However, the growth of the internet has not only been an engine of economic growth, but also a source of vulnerabilities, and it has become increasingly focused on the dangers associated with cyber security. Above all, the state has begun to realize the need to protect its critical infrastructures, such as financial institutions and energy grids, against potential threats from cyberspace. Like most countries, the PRC is heavily dependent on technology, prompting the government to closely monitor developments related to the internet and the flow of information it generates. The Chinese authorities perceive uncontrolled information as a threat to the regime and make considerable efforts to take advantage of the economic opportunities offered by the internet while maintaining political control over it (Grauman, 2012).

In this context, the Chinese Communist Party perceived the Internet as a threat to the regime's stability, given the possible impact of external influences on the Chinese population. To combat these risks, the PRC began in 1998 to develop a strategy based on surveillance and restricting access to information. A key first step was the launch, in 2003, of the *Golden Shield Project*, the basis of the *PRC's "Great Firewall",* which allows the regime to censor online content and block access to foreign information sources deemed harmful or subversive. The project is intended to filter and control internet traffic, blocking access to content outside the country's borders that is deemed sensitive (Austin, p. 11), effectively isolating the national internet from the global internet. In other words, the authorities combine digital

censorship with social surveillance, allowing them to track and control citizens' online behaviour. As part of this project, since 2009, the PRC has made efforts to block certain US software applications (such as Facebook, Twitter and YouTube) because of their incompatibility with its censorship laws (The International Institute for Strategic Studies, 2021).

To ensure regulatory compliance, the project also integrates digital identification measures whereby citizens are obliged to use real names on online platforms as a goal of maintaining cyber security (Triolo, Sacks, 2017). Users thus become directly responsible for their online activities, reducing the possibility of anonymous dissent and increasing self-censorship. Moreover, the *Golden Shield* has thus become a central pillar in the PRC's cyber strategy, setting standards for control and internet censorship. It thus marks a fundamental aspect of the PRC's broader cyber security and information sovereignty policies, establishing a model for a state-controlled internet that closely aligns with national security priorities. This framework is critical for understanding the development and implementation of Chinese cyber policies in the future.

After 2007, several events took place in cyberspace. Russia was accused of using cyberspace for offensive actions against Estonia and Georgia, and the USA was accused of being behind the Stuxnet attack. Moreover, the uprisings during the Arab Spring underlined the importance for the PRC to strengthen its cyber capabilities in order to protect its critical infrastructure and maintain national stability. The Stuxnet incident demonstrated the vulnerabilities of industrial networks to sophisticated attacks, prompting the PRC to reassess cyber strategies to prevent such threats. During this period, the USA recognized cyberspace as a new operational domain in addition to land, air, sea, and space (The White House, 2011). This recognition emphasized Beijing's focus on technology development to protect national interests and maintain internal security in an increasingly complex global landscape. Consequently, during this period, as the PRC rose to become the world's second-largest economy, its political, economic, and social development became deeply intertwined with global cyberspace (Jiang, T., ib.).

In 2010, the PRC published a White Paper on the status of IoT, emphasizing the need for cyber security to protect national security and state interests within its sovereign territory (Hwang, 2023), which reveals the recognition of the importance of cyber security in the context of national security. A year later, the PRC together with other states, including Russia, Tajikistan and Uzbekistan, presented an *International Code of Conduct for Information Security* to the UN General Assembly.

It reaffirmed the belief that rights and decision-making responsibilities for Internet-related public policies should be under the jurisdiction of the host state (United Nations General Assembly, 2011).

A new stage in the PRC's cyber security was ushered in when the country's President Xi Jinping announced the country's intention to become a cyber power. He initiated a series of institutional changes to achieve this goal. One of the most significant developments was the establishment of the *Cyberspace Administration of China* (CAC) in 2014. This institution becomes responsible for regulating, administering, and licensing the Internet in the PRC. The official view in the PRC, as in most rich and middle-income countries, is that cyber security affects and shapes the entire range of government, economic, social, technological, political, and security activities in the country (Austin, p. 7).

In 2015, the *China Information Technology Security Evaluation Centre* was established under the CAC with a role in strengthening national defence against cyber threats. Through its research work, the centre has provided key insights and strategies for effectively protecting the PRC from cyberattacks (Jiang, T., ib.). Also in the same year, the government issued new regulations targeting foreign IT companies that supply Chinese banks, requiring them to disclose the source codes of the IT products they supply. The measure was imposed to strengthen both domestic cyber security and localization of the cyber security industry (Austin, p. 14). The response came along political-diplomatic lines when PRC-USA bilateral relations cooled, prompting the PRC to suspend the measures also in the same year.

As the internet and cyber technologies have become an essential part of the economy and national security, the PRC's strategy has evolved from control and offense to defence and deterrence. Against this backdrop, Beijing has adjusted its policies to address both internal and external challenges, focusing on preventing cyberattacks and protecting its critical infrastructure. Its ascent as a cyber superpower has been marked by a transition from aggressive expansion to strategic protection as it has become more deeply integrated into the global economy. Since 2015, the PRC has begun to adopt a more defensive posture in its cyber strategy. While in the early stages the strategy was focused on pre-emptive attacks and strengthening cyber sovereignty, gradually the focus shifted to defence and deterrence (Jiang, T., ib.). This shift reflects a growing awareness of the risks of large-scale cyber warfare and its associated economic and political costs (Soesanto, 2022).

Politically, the current Chinese administration has fully recognized the importance of cyber security and declared it part of national security. As a result,

it has issued several national laws and strategies to strengthen the country's cyber defence capabilities. The 2015 *National Security Law of the People's Republic of China* provides the general framework for national security and cyber security (Jiang, M., 2020). Moreover, Article 25 of the *National Security Law* emphasizes the importance of scientific development, innovation and national control over core information technologies, critical infrastructures, important information systems and data. It also sets goals of preventing, stopping and managing cyber-attacks, network intrusions, cyber-theft, online distribution of compromising information, ultimately leading to achieving security and sovereignty in cyberspace. In terms of the cyber strategies published by the Chinese Cyberspace Administration, the *International Strategy for Cyberspace Cooperation,* approved in 2016, stands out as the PRC seeks to take the lead in international cyber governance, following President Xi's call to *"establish a community of common future in cyberspace"* (Jiang, M., ib.). This strategy particularly emphasizes the principles of peace, sovereignty, shared governance and upholds peace through cooperation and strategic mutual trust.

At the national level, several institutions have implemented laws or issued policies on personal data protection, administrative regulations or rules on information activities in cyberspace. In terms of criminal activity, China's Criminal Law has been revised several times in 2005, 2009 and 2015 to reflect the increase in criminal activities involving personal information. The 2017 *Cyber security Law* of the PRC similarly contains several provisions regulating the collection, storage, transmission and use of *"personal information"* by network and critical information infrastructure operators (Jiang, M., ib.). This law was created to protect national network infrastructure and control the activities of foreign companies in Chinese cyberspace. The law requires companies to implement strict security standards and report information about vulnerabilities in their networks to the authorities. We can say that this law reiterates the concept of cyber sovereignty as a national security tool.

In terms of cyberspace as an operational domain, the Beijing administration is publishing *China's National Defence in the New Era* White Paper in 2019. This lays out an assessment of the current national and international security situation and outlines the PRC's defence missions, reforms, and spending. This paper provides a detailed analysis of the current state of national and international security, outlining the PRC's missions, reforms, and spending in the defence sector. Moreover, it emphasizes the need for the Chinese military to adapt to the *"new era"* of strategic competition by improving training and increasing combat capabilities, thus aligning

with the PRC's global status, as well as its commitment to maintaining *"world peace"*. In the area of cyber defence, the White Paper highlights Beijing's interest in adopting the most advanced technologies in the military sector, including artificial intelligence, big data, cloud computing, quantum computing and the internet of things (IoT) (The State Council Information Office of the People's Republic of China, 2019). In addition, the military modernization program entails a *"civil-military fusion"* strategy, strengthening the relationship between civilian companies and defence establishments. Through this fusion, the Chinese military could benefit from technological advances in many areas, such as nuclear technology, aerospace, aviation, semiconductors, cloud computing, robotics, and Big Data processing (Ford, 2019).

Similar to other states, the PRC aims to dominate cyberspace while recognizing the need for a substantial transformation of its armed forces to achieve this strategic goal. President Xi Jinping and his team have laid the groundwork for transforming the People's Liberation Army (PLA) into a *"world-class army"* by 2050. Achieving it depends on the state's ability to adapt emerging technologies and artificial intelligence to existing military doctrine (Burke, Gunness, Cooper III, Coza, 2020). Further, the authors expound that the PLA Strategic Guidelines emphasize the importance of cyberspace as an operational domain and a critical tool in the conduct of military operations in an era dominated by confrontation between *"information-driven systems of systems"*. In this context, one of the most important developments in the field of *"informatization"* is the establishment of the PLA Strategic Support Force, a structure dedicated to coordinating all information aspects of warfare, including cyber attack and defence as well as electronic warfare. These state structures may be joined by other forces specially trained to conduct offensive or defensive actions in cyberspace such as state-sponsored state actors, non-state actors or even patriots acting out of their own convictions.

For the future, the PRC aims to develop the digital infrastructure globally, creating economic and thus political dependencies for many countries. This strategy strengthens the PRC's role as a global player and gives it considerable influence in international decision-making processes, especially in relation to its policies on Taiwan. As the US Ambassador-at-Large for Cyberspace and Digital Policy pointed out in 2023, the PRC's strategy to build the global internet infrastructure – from fibre optics and satellites to data centres and wireless technology – shows that focusing solely on data and application security would ultimately mean *"delivering highly secure and uncorrupted packages directly to Beijing in an untrusted architecture"* (Hamilton, 2024).

NATO POLICIES IN CYBERSPACE

NATO has had a significant evolution in its policy and vision in cyberspace. The analysis of the evolution of NATO's cyber policy reflects a continuous adaptation to the increasingly complex and diverse threats in the digital environment. Starting from the Cold War, where global power had a bicephalous component, we arrive at the contemporary situation where the *"Thucydides trap"* may be more valid than ever. As the PRC, the Russian Federation or any other country seeks to become increasingly influential on the global stage, there are fears that economic, cyber, military or geopolitical frictions could escalate into a major conflict, although there is also the possibility of avoiding them through diplomacy and cooperation. Thus, the concept highlights how risky the geopolitical landscape can become when a rising economic, military or other nation challenges an established one.

Whether it is the PRC or NATO, their actions in cyberspace are closely linked to their history and political leadership. For example, the autocratic regime in Beijing seeks to control and censor activities in cyberspace, while NATO advocates a common, open and secure cyberspace. Cyber security and cyber defence are part of NATO's core mission of collective defence. Its main objectives in this area are to protect its own networks, to operate in cyberspace, to help allies build resilience to protect national networks and to provide a platform for consultation and collective action.

NATO's cyber security policy direction is being driven by the growing threat of state-sponsored cyber attacks. In response, North Atlantic Organization member states are increasingly adopting active cyber defence strategies. These combine real-time attack detection with proactive countermeasures to reduce potential damage. The United States and the United Kingdom are leading the way in their implementation, using technical and policy responses, including hackbacks, to deter and attribute cyber threats (Jun, 2023).

Cyber defence appeared on NATO's agenda at the *Prague Summit* in 2002 and was subsequently confirmed as a priority in 2006 at the *Riga Summit*. For the first time a policy was agreed by Heads of State and Government at the *Bucharest Summit* in April 2008. The rapid evolution, sophistication and increasing frequency of cyber threats and attacks to the Alliance's security have put the issue back on NATO's security agenda. The Strategic Concept adopted at the *Lisbon Summit* in 2010 recognizes that attacks in cyberspace can affect the security of national critical infrastructures and jeopardize *"national and Euro-Atlantic prosperity, security and stability"* (NATO Strategic Concept, 2010) and their impact could be as damaging

as a conventional attack. Accordingly, Lisbon laid the foundations for the Alliance to develop the capacity to prevent, detect, defend against and recover from such threats.

In 2014, at the *Welsh Summit,* no one denied that cyberspace operations could have an impact equal to that of conventional attacks. Moreover, for the first time, it was recognized that a member could invoke Article 5 following a cyber attack of significant magnitude, similar to those faced by Estonia in 2007. Following these cyber attacks in Estonia, NATO approved its first cyber defence policy in 2008 and established the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

At the Munich Security Conference in 2011, NATO adopted a new cyber defence policy that focuses on preventing cyber attacks and building resilience. The creation of the Rapid Response Team was the result of the review of the Alliance's cyber defence policy, as well as the implementation of a cyber defence capability of its own networks (Hasanov, Iskandarov, Sadiyev, 2019). As a result of the lessons identified and learned from cyber threats and attacks to date, the major powers have stepped up their activity in the digital environment concomitant with the development of laws, strategies, policies, and doctrines regulating the activity.

As a consequence of cyber activities to that point, in July 2016, at the *Warsaw Summit*, the Allies recognized cyberspace as an operational area in which NATO must defend itself as *"effectively as in the air, on land and at sea"* (NATO, 2016). The Allies agreed on a military vision and strategy for cyberspace operations and committed to prioritize action to strengthen national cyber capabilities by making a political commitment to do so *(Cyber Defence Pledge*), to increase the resilience of national networks and infrastructure, and to improve the responsiveness, responding quickly and effectively to cyber attacks. Predictably, at the *2018 NATO Summit in Brussels*, the Allies agreed to establish a *Cyber Operations Centre (CYOC)* as part of NATO's consolidated command structure. They also agreed that NATO can draw on member states' national cyber capabilities for Alliance operations and missions. A year later, in February 2019, the Allies endorsed a NATO Guidance that sets out a range of tools (political, diplomatic, military) to strengthen NATO's ability to respond to malicious cyber actions (NATO, 2024).

At the *2023 NATO Summit* in Vilnius, the Allies adopted a new *Concept* aimed at enhancing the Alliance's contribution to cyber defence and deterrence. Alliance members also reaffirmed and strengthened their commitment to cyber defence, setting more ambitious goals for strengthening national cyber defences, including

critical infrastructure. Recognizing the need for rapid assistance, NATO has initiated the *Virtual Cyber Incident Support Capability* to assist national efforts to mitigate significant cyber incidents (NATO, 2023). It is interesting that the name of the People's Republic of China appears twice in the communiqué preceding the Summit. The coercive interests and policies of the People's Republic of China are recognized as directly challenging international interests, security and values. The PRC uses a variety of political, economic and military tools to expand its global influence and project power. It also conducts harmful hybrid and cyber operations, uses aggressive rhetoric and practices disinformation, targeting allies and compromising the security of alliances. The PRC seeks to dominate key technological, industrial and critical infrastructure sectors and control strategic materials and supply chains. It uses economic leverage to create strategic dependencies and increase its influence, striving to undermine the rules-based international order, including in the space, cyber, and maritime domains (Ib.). Also in the same communiqué, it is stated that instability in Africa and the Middle East directly affects the security of both NATO and partners. The Alliance is facing cyber, space, hybrid and other asymmetric threats, and the clear intentions and coercive policies of the Beijing government defy NATO's interests and jeopardize its security (Ib.). Practically, as of this moment, the People's Republic of China is officially recognized by NATO as, if not an adversary, at least a significant competitor in the cyber domain.

At the *2024 NATO Summit* in Washington, DC, the allies decided to establish a new *Integrated Cyber Defense Center* at SHAPE to improve network protection and cyber deployment in various peace, crisis and conflict scenarios. NATO also encourages a unified approach in developing cyber defence capabilities by setting specific objectives for allied countries, supporting them to strengthen their national cyber defence by sharing information and best practices and organizing specialized exercises. This facility allows member states to voluntarily contribute to strengthening the cyber capabilities of other allies (NATO, 2024).

Over the last decade, NATO's cyber policies have also facilitated the development of links with the civilian institutions of the European Union, thereby strengthening civil-military partnerships. This dynamic takes place in a context where most EU member states are also NATO member states. Cyber defence is one of the areas of enhanced cooperation between NATO and the EU, as part of the two organizations' increasingly coordinated efforts to counter hybrid threats. NATO and the EU exchange information and best practices. Cooperation is also strengthened in training, research and exercises with tangible results in combating cyber threats. The North

Atlantic Alliance and the European Union cooperate on cyber defence through a technical agreement, which was signed in 2016. Given common challenges, NATO and the EU are strengthening their cooperation in the field of cyber defence, in particular in training and responses to cyber attacks.

CYBER THREATS FROM THE PEOPLE'S REPUBLIC OF CHINA AND IMPLICATIONS FOR NATO CYBER SECURITY

The rise of the People's Republic of China has fuelled competition between it and the USA, particularly in trade and technology. Even the USA has recognized the PRC as *"the only one country that has both the will and the ability to reshape the regional and international order"* (Zhang, 2024). The competition between the two superpowers is also taking place at a time when internet-based economies and cyber policymaking increasingly revolve around the three main models established by the USA, the PRC and the EU. Chinese cyber security policies remain at the centre of global debate and research (Jiang M., 2023). Cyberspace is an inherently insecure environment, so the cyber threats posed by the PRC to NATO security are multiple and complex, with significant implications for the security of the Alliance and its member states.

Thousands of cyber threats are reported worldwide every day, and many of them are attributed to the People's Republic of China. A recent study ranked the PRC as *"the most comprehensive cyber power"* after the USA, which is due to its prioritization of education in information science and technology and training of specialists for military cyber operations (Hlavek, 2021). As expected, the main country targeted by Chinese cyberspace operations is the USA, the most powerful NATO member state. Washington has also identified Beijing as the most significant espionage threat, with over $300 billion in annual losses from intellectual property theft (Kobzova, 2023). In addition, other NATO member states, particularly in Europe, have reported attacks originating from Chinese hackers. These attacks intensified when a number of European states banned PRC firms from participating in the development of 5G technology in their respective states (Reuters, 2023). Chinese IT companies, including Huawei, are receiving substantial government support, including subsidies and investment in research and development, which has propelled some of them, Huawei in particular, to the forefront of the global 5G technology industry alongside other well-known Western companies. The introduction of 5G technology by Chinese firms in global markets has met vehement opposition from some Western states, whose political leaders are

concerned about the security risks associated with Chinese technology and its potential to be used for espionage or disruptive purposes (The International Institute for Strategic Studies, 2021).

Moreover, in July 2023, new cyber operations were identified in NATO countries such as the UK, Slovakia, Czech Republic and Hungary (Sharwood, 2023). Frequent targets were diplomatic entities, foreign ministries, the private sector and various other institutions. A few months earlier, the European Union Agency for Cyber Security (ENISA) had issued a report exposing numerous cases of cyber espionage attacks on member states, including activities directed against German companies, Belgian ministries, French organizations, EU institutions and many others (ENISA, CERT-EU, 2023). On the other hand, the collection of data and other information about citizens or institutions of NATO member states through various media platforms further enhances Beijing's strategic advantage over its competitors. Along with its massive investments in emerging technologies and in educating specialists, Beijing has improved its techniques, tactics and effectiveness through the complexities of operating in the digital environment. The combination of all these elements have strengthened the PRC's leadership position by becoming one of the most important challenges facing NATO (Kobzova, ib.).

The overall objective of the threats targeted by the PRC is to gain political, military and economic advantage over Western nations. From a cyber security perspective, Beijing's strategic approach differs from that of other significant actors in this field, such as the Russian Federation, North Korea or Iran. The goal is not to compromise critical infrastructure, but rather, cyber espionage. Over time, Beijing has gained notoriety for its sustained cyber espionage activities in both industrial and military sectors. However, it is worth noting that, on occasion, Chinese hackers have also been involved in attacks aimed at disrupting critical infrastructure (Ib.).

Another aspect of the confrontation between the PRC and the USA is the geostrategic Asia-Pacific area of influence, where the two great powers have interests. One of the PRC's most recent and worrying cyber campaigns targeted the US island of Guam (Sanger, 2023). The cyber operation in Guam has highlighted the strategic role of this territory, given its geographic location close to Taiwan and the important military facilities it possesses, which are essential to the USA response capability in the event of an escalation of the conflict in the South China Sea. These cyberattacks, which targeted critical infrastructure such as military bases and transportation and telecommunications systems, indicate a significant departure

from conventional methods of cyber espionage, suggesting a dual purpose: reconnaissance and potential preparation for disruptive action. In support of this, a report published by New Zealand and Canada indicated that the Chinese malware was not solely intended for cyber espionage (Kobzova, ib.).

In its 2022 *Global Threat Report*, US-based cyber security company *Crowd Strike* ranked the PRC as a world leader in exploiting cyber vulnerabilities. The report emphasizes the advanced exploitation skills possessed by the Chinese hacker community, highlighting the significant technical development capability of the Chinese (US-China Economic and Security Review Commission, 2022). According to other public reports, over the past two decades, the PRC has been continuously engaged in offensive cyber operations. With the expansion of its economic and political ambitions, its influence in cyberspace has grown significantly. It is reflected by the growing number of state-sponsored non-state actors developing and deploying offensive cyber capabilities in support of national objectives, ranging from economic to national security (Handler, 2023). In response to all the activities in cyberspace involving NATO or its members, heads of state and government have taken some measures, either reactive or proactive, depending on the situation.

With the proliferation and sophistication of threats – including terrorism, cyber-attacks, disruptive technologies, climate change and challenges from Russia and the PRC to the international order –, NATO has adopted the *NATO 2030 Initiative*. This document aims to strengthen transatlantic cooperation and proactively address security challenges related to emerging and disruptive technologies, responding to the PRC's ambitions to dominate the artificial intelligence sector. Through this initiative, NATO is committed to investing in broadening and deepening strategic partnerships that reflect shared values and common interests, thereby strengthening transatlantic cooperation. Also, the PRC's activities in cyberspace are considered threats that require deep and rapid strategic adaptation on NATO's part to remain effective and relevant in protecting the security and prosperity of its members (NATO, 2021).

As a result, in order to effectively manage cyber incidents, NATO engages in continuous and coordinated preparedness. To this end, member states' representatives have agreed on the establishment of dedicated institutions capable of preventing, promptly responding to and rapidly remediating security problems in Alliance networks. These structures are essential for strengthening NATO's

resilience against cyber threats and maintaining operational stability in the face of modern challenges.

Operationally, the North Atlantic Alliance established a Cyberspace Operations Centre at Allied Command Operations (ACO) in Mons, Belgium in 2019. The main purpose of this centre is to monitor cyberspace and to coordinate and synchronize cyberspace operations with land, sea, and air operations (Brzozowski, 2018). This centre is essential for the Alliance's cyber security, as it can act as a deterrent and allows NATO to respond quickly and effectively to potential cyber attacks. The centre also enhances collaboration between member states and can form the basis for a NATO Cyber Command essential in the face of evolving cyber threats.

From a technical perspective, the NATO Communications and Informatics Agency (NCIA) interacts with the NATO Cyber Security Centre (NCSC) and the NATO Computer Incident Response Capability (NCIRC), and is responsible for developing, managing and securing the Alliance's cyber infrastructure. In addition, the NCIRC, through a dedicated coordination centre, enables member states to share information and techniques on cyber threats, including some indicators that may provide clues to the nature of the attacks. These NATO structures have contracts with leading IT defence companies on cyber protection services for the Alliance. Moreover, NATO's cyber rapid response teams are available for prompt deployment in support of Allies suffering cyber attacks (Marrone, Sabatino, 2021). This type of civil-military partnership strengthens cooperation and resilience in cyber security and defence.

It is widely recognized that the challenges in cyberspace are considerably different from those in other operational domains because it is an artificial domain, which is almost entirely man-made and controlled. In this context, the human resource is essential. As a result, adequate training of personnel becomes crucial for the prevention of cyber incidents or the effective management of existing ones. NATO invests strategically in the training of its specialists by organizing intensive courses at various academic institutions affiliated to the Alliance.

The PRC's cyber capabilities are a concern within the North Atlantic Alliance, which is why numerous countermeasures have been taken. In cyberspace, NATO should take a leading role in the international community in terms of legislation and legal regulation. Accordingly, the Alliance has established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn to strengthen cyber defence capabilities. This centre serves as the main hub for cyber research and strategic thinking facilitating not only advanced research but also the development

of innovative cyber defence strategies. It also emphasizes doctrine development, training and education to support interoperability and the exchange of best practices among NATO members and partners. The centre has developed a comprehensive guide to the rules and laws applicable to cyber warfare called the *Tallinn Manual* (Pfannenstiel, Cox, 2024). It is an academic document developed to provide a detailed interpretation of how existing international laws apply to cyber conflicts. This treaty would strengthen global security and allow NATO to more effectively defend against Chinese threats. At the same time, NATO specialists benefit from numerous training opportunities through participation in joint exercises and activities, organized by the Alliance or in cooperation with other partners. For example, in 2023, more than 3,000 participants from 38 countries – including NATO Allies and partners – took part in the annual *Locked Shields* exercise hosted by CCDCOE. This is the world's largest cyber defence exercise, which involved protecting information systems from real-time attacks and simulating tactical and strategic decisions in critical situations (NATO, 2023).

Such exercises are fundamental to enhancing cooperation and facilitating the exchange of best practices, playing a key role in strengthening ties between member nations. They create valuable opportunities for allies to test and improve common procedures in simulated situations, thereby increasing the effectiveness of responses in real crises. Moreover, these activities provide a new perspective on the importance of civil-military cooperation. By involving civilian entities, including universities and private sector research institutions, the exercises contribute not only to improving cyber defence capabilities, but also to enhancing synergies between civilian and military assets, a crucial factor in adapting to new technological challenges and managing complex cyber threats.

In an increasingly technology-dependent global context, such initiatives are vital for maintaining a strategic advantage in cyberspace. They not only strengthen the individual capabilities of each member state, but also provide a solid basis for effective collective defence. Exercises, together with other similar initiatives, also play a very important role in deterring adversaries, enabling the Alliance to respond promptly and cohesively to emerging threats and to protect critical infrastructure in member states. These activities enhance NATO's ability to effectively anticipate and counter potential attacks, thereby ensuring the security and stability of the region.

Another measure that NATO should apply would be to invest more in equipment, in the development of emerging technologies, in the specialization of personnel and in the development of cyber hygiene among the population,

so as to counter the disruptive effect of offensive actions targeting the Alliance's security. NATO can also remain competitive in the field of cyber defence and cyber security only through close cooperation with civilian, academic and private institutions, and it is through this civil-military synergy that the Alliance will be able to have a comprehensive response to cyber threats. Moreover, improving information sharing and collaborative practices between member states through the use of common platforms to share threat and vulnerability data in real time is key.

Last but not least, cyber diplomacy can set international norms and rules for behaviour in cyberspace, seeking to build a global agreement on prohibiting disruptive practices that could harm critical data, networks and infrastructure without remedy.

CONCLUSIONS

This study is not intended to be exhaustive research. Therefore, its approach is limited to specific aspects of cyber security without fully exploring all the associated geopolitical dimensions and multivalences. It represents a deliberate delimitation of the scope and breadth of the analysis, focusing on specific contributions of existing policy and scientific literature.

The limitations in this research consisted in the choice of only one alliance for the study, which allowed for a detailed focus, but also restricted the generalizability of the findings to other states or alliances. In addition, open-source materials on this topic are often contradictory, sketchy and unclear. This methodological decision was driven by the need for an in-depth analysis, which, despite its specificity, provides a solid basis for further extrapolations and comparative research in the field of cyber security. As a result, future research directions could include the analysis of cyber activities and their impact on cyber security, both at EU and international level. Therefore, for a proper understanding, cyber security requires a holistic perspective that integrates and analyses its multiple dimensions and the interactions between them.

The answer to the research question is not simple. Cyber security within an alliance must be assessed from a multi-layered and comprehensive perspective. So far, the People's Republic of China has not challenged the North Atlantic Alliance; however, its ambitions to dominate cyberspace loom as imminent challenges for NATO. In order to better manage cyber incidents, various measures have been proposed.

Finally, NATO must take a comprehensive approach to the PRC's cyber threats by investing in emerging technologies, strengthening cooperation with civilian and military partners, and educating cyber specialists. Also, through joint exercises and cyber diplomacy, NATO can contribute to the development of an international framework to promote responsible behaviour in cyberspace. The Alliance's response must be one based on prevention, deterrence and cooperation to preserve stability and security in an increasingly contested area.

BIBLIOGRAPHY:

1. Austin, G. (2018). *Cybersecurity in China the Next Wave.* Canberra: Springer.
2. Brzozowski, A. (17 October 2018). *NATO sees new cyber command centre by 2023 as Europe readies for cyber threats*.
3. Burke, E.J., Gunness, K., Cooper III, C.A., Coza, M. (2020). *People's Liberation Army Operational Concepts.* Santa Monica: RAND.
4. Chafetz, G. (31 July 2023). *How China's Political System Discourages Innovation and Encourages IP Theft.* SUA.
5. Denning, D.E. (2001). *Chapter Eight – Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. In J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288). RAND Corporation.
6. Diotte, P. (2020). *The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online*. In *Canadian Military Journal*, pp. 32-42.
7. ENISA, CERT-EU (2023). *JP-23-01 – Sustained activity by specific.*
8. Ford, C.A. (11 September 2019). *U.S. Department of States*, https://2017-2021.state.gov/: https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/, retrieved on 22 July 2024.
9. Grauman, B. (2012). *Cyber-Security: The Vexed Question of Global Rules.*
10. Hamilton, B.A. (2020). *Same Cloak, More Dagger: Decoding How the People's Republic of China Uses Cyberattacks,* https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html#report, retrieved on 22 July 2024.
11. Hamilton, B.A. (2024). *How to succeed at annexation without really fighting – The PRC's Taiwan Cyber Strategy Explained.*
12. Handler, S. (31 January 2023). *The 5×5 – China's cyber operations*, https://www.atlanticcouncil.org/: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/, retrieved on 22 July 2024.
13. Hasanov, A.H., Iskandarov, K.I., Sadiyev, S.S. (2019). The Evolution of NATO's Cyber Security Policy and Future Prospects. In *Journal of Defense Resources Management,* vol. 10, no. 1(18), pp. 94-106.
14. Hlavek, A. (2021). *China cyber attacks: the current threat landscape.* Ironnet.
15. Hwang, J.-J. (2023). *Reframing China's Territory and Sovereignty in Cyberspace: Exploring Conceptual Territorialization and Claims of Cyber Sovereignty*. In *Issues & Studies A Social Science Quarterly on China, Taiwan and East Asian Affairs,* vol. 59, no. 4, 21.

16. Jiang, M. (2020). *Cybersecurity policies in China*. In L. Belli, *Cyber BRICS: Cybersecurity Regulations in BRICS Countries* (pp. 95-212). Berlin: Springer.
17. Jiang, M. (2023). *Chinese Cybersecurity Policies in the Age of Cyber Sovereignty*. In M. Timoteo, B. Verri, R. Nanni, *Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China* (pp. 77-90). Springer Nature Switzerland AG.
18. Jiang, T. (2019). *From Offensive Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar*. In *Chinese Journal of International Review,* vol. 1, nr. 2, pp. 195-218, www.worldscientific.com., retrieved on 17 July 2024.
19. Jiang, T. (2022). *The Shift of China's Strategic Thinking on Cyberwarfare Since the 1990s*. In *Journal of Chinese Political Science*, pp. 127-149.
20. Jinghua, L. (22 March 2019), https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/, retrieved on 29 June 2024.
21. Jun, O. (2023). *Direction of Japan's New Cybersecurity Policy*. In *Asia-Pacific Review*, pp. 63-78.
22. Kobzova, L. (2023). *China's Cyber Threat: Implications for NATO and Potential Remedies.* Adapt Institute.
23. Marrone, A., Sabatino, E. (2021). *Cyber Defence in NATO Countries: Comparing Models.* Instituto Affari Internazionali.
24. NATO Strategic Concept (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Lisbon: NATO.
25. NATO/North Atlantic Treaty Organization (2016). Warsaw Summit Communiqué. Warsaw.
26. NATO/North Atlantic Treaty Organization (2021). *NATO 2030.*
27. NATO/North Atlantic Treaty Organization (14 September 2023). *North Atlantic Treaty Organization*, https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 28 June 2024.
28. NATO/North Atlantic Treaty Organization (2023). Vilnius Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_217320.htm, retrieved on 27 June 2024.
29. NATO/North Atlantic Treaty Organization (30 July 2024). *Cyber defence*, North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 29 June 2024.
30. Pfannenstiel, M., Cox, D. (2024). *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations*. *Military Review Online Exclusive*.
31. Reuters (29 September 2023). *European countries who put curbs on Huawei 5G equipment*, https://www.reuters.com/: https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/, retrieved on 29 June 2024.
32. Sanger, D.E. (24 May 2023), in Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?, https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html, retrieved on 29 June 2024.
33. Sharwood, S. (4 July 2023). *Undiplomatic Chinese threat actors attack embassies.*
34. Soesanto, S. (4 July 2022). *Cyber Deterrence Revisited*. Alabama: Air University Press.
35. The International Institute for Strategic Studies (2021). *Cyber Capabilities and National Power: A Net Assessment.*

36. The State Council Information Office of the People's Republic of China. (July 2019). *China's National Defense in the New Era*. Beijing, China: Foreign Languages Press Co. Ltd.
37. The White House (May 2011). International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World. Washington.
38. Triolo, P., Sacks, S. (26 September 2017). *Center for Strategic and International Studies*, https://www.csis.org/analysis/shrinking-anonymity-chinese-cyberspace: https://www.csis.org, retrieved on 29 June 2024.
39. United Nations General Assembly (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.*
40. U.S.-China Economic and Security Review Commission (2022), https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf, retrieved on 29 June 2024.
41. Zhang, H. (12 July 2024). *What is the intention of NATO, the "war maker", to "directly warn" China?* China.