dipam
DİPLOMATİK İLİŞKİLER ve POLİTİK ARAŞTIRMALAR MERKEZİ
CENTER for DIPLOMATIC AFFAIRS and POLITICAL STUDIES

ANALYSIS

CYBER SECURITY POLICIES OF CHINA:
CYBER SPACE AS A NEW ARENA OF COMPETITION FOR GREAT POWERS

Larissa KUMAŞ

April 2024 No: 28

CYBER SECURITY POLICIES OF CHINA: CYBER SPACE AS A NEW ARENA OF COMPETITION FOR GREAT POWERS

The concept of cyber space holds significant importance in today's increasingly digitalized world. Countries and global companies, which are becoming more interconnected day by day, are facing growing competition and security threats in cyber space. Cybercrimes have become a serious problem threatening not only individuals or institutions but the security of entire nations. In fact, cyberattacks have revolutionized warfare in the military, leading to the emergence of a new battlefield. This reality shapes the foreign policies of countries, forming the cornerstone of international relations today.

Cyber Space in International Security

What is cyber space, that has become an integral tool in the foreign policies of countries? Cyber space, by definition, is the place where consumers are connected to the world, consisting of consumer computers, electronics, and communication networks. Since cyber space does not belong to the physical world, physical laws are not applied to cybercrimes. In countries where cybercrimes are intensively observed, separate sets of cyber laws have been enacted by governments, aimed at providing cyber security to cyber users. Such cyber laws are necessary to monitor and prevent individuals' immoral or illegal activities. Common cybercrime activities include hacking, theft, money laundering, terrorism, and piracy.

According to estimates by Cybersecurity Ventures, the annual cost of cybercrimes worldwide is estimated to reach $10.5 trillion by 2025.[1] The United States in particular has been the world leader in terms of data breach costs for many years. According to reports by International Business Machines (IBM), the cost of a data breach in the United States exceeded $5 million in 2023.[2] These figures indicate that cyber security is no longer just a technological issue but has also become an economic and political issue.

Meanwhile with the increase in geopolitical tensions, cyber threats have also increased. Particularly with the Russia-Ukraine war that began in 2022, 97% increase in cyber threats for organizations was observed. [3] With the increasing use of cyber space in interstate relations, concerns about cyber security are also growing. In this context, understanding and effectively addressing the importance of cyber security has become one of the top priorities of the international community.

In terms of states, it is possible to examine their intentions to expand these threats and cyber capabilities with three

[1] Esentire, 2023 Official Cybercrime Report https://www.esentire.com/resources/library/2023-official-cybercrime-report

[2] IBM, Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach

[3] Accenture, State of Cybersecurity Resilience 2023, p. 25 https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf

objectives[4]: Infiltrating the critical infrastructures of other states to deter them from security threats; Increasing knowledge accumulation by cyber espionage to advance states' military developments faster; and obtaining economic gains in areas where technological advancements are made. In this sense, analyzing the state capabilities of China as a major cyber power is extremely important, considering its position in this field in contrast to other states.

The Rise of China as a Cyber Power and Its Vision of Centralized Cyber Control

Cyber power has become a strategic priority for China, which aims to assume a leadership role in the digital realm alongside its goal of being a great power. In recent years, there has been a significant increase in political importance given to digital technologies. China's cyber objectives encompass military, economic, and political domains, adopting strategies such as intelligence gathering, internal surveillance, and ensuring general security. The primary purpose of these steps can be attributed to strengthening the power and legitimacy of the party-state.

At the core of China's cybersecurity policies are prominent initiatives such as the Social Credit System. The Social Credit System aims to create a security and control mechanism within the society by evaluating individuals' reliability based on personal and behavioral data. Underneath the Social Credit System lie significant cyber security risks: Third-party services, through collaboration with Chinese technology firms, often acquire consumers' data to offer benefits related to credit scores, while vast amounts of personal data typically move through an invisible network of companies. [5] This system can be interpreted as a form of cyber warfare conducted by China against its own citizens, as it intervenes in individuals' private lives and restricts personal freedoms.

Indeed, the Cybersecurity Law passed in 2017 has further shaped China's cybersecurity policies. This law has institutionalized the party's determined vision of cyber sovereignty and strengthened the party-state's control by providing various data access capabilities. Under the military-civil fusion policy and the framework of the 2017 law, Chinese telecommunications and technology companies have been compelled to collaborate with the government on data sharing and cybersecurity technology, where companies like Huawei have been encouraged to support developments that create a series of cyber and data security vulnerabilities in some of the developing and developed countries. [6] The Chinese government integrates cybersecurity and 5G connectivity due to the need for internal party surveillance, expanding access to foreign networks for the Chinese Communist Party (CCP) while generating revenue for local tech giants.

[4] Hjortdal, China's Use of Cyber Warfare: Espionage Meets Strategic Deterrences. p. 3 DOI:10.5038/1944-0472.4.2.1

[5] UC Berkeley (2020). Uncovering the Risk Networks of Third-Party Data Sharing in China's Social Credit System.

[6] Williams, B.K.(2021) "Evaluating China's Road to Cyber Super Power" p.4 https://www.osti.gov/servlets/purl/1830481

It is observed that these domestic policies, reflecting the need to strengthen regime integrity necessary to reach leadership capacity, subsequently influence foreign policy. China is understood to continue actively implementing its cybersecurity policies to increase its power in the cyber domain and achieve an effective position in the international arena.

Cyber Warfare in the Asia-Pacific Region

The 14th Five-Year Plan for National Economic and Social Development and the 2035 Long-Range Objectives of the Chinese Communist Party (CCP) openly express its desire to become a Cyber Superpower. [7] In line with these aspirations, China, which is striving to expand its cyber capabilities, can be observed carrying out cyberattacks against the United States with the objectives of infiltrating critical infrastructures to deter security threats, increasing its knowledge accumulation through cyber espionage for faster military development, and obtaining economic gains in areas of technological advancement.

In this context, it can be considered that the cyber weapons developed by China against the US are practical manifestations of the abovementioned objectives of expanding cyber capabilities. The cyberattacks, defined by scholars as "preemptive reconnaissance", conducted by China may be interpreted as aiming to surpass the American economy and military power in the long run. [8] According to the IP Commission report, the estimated annual economic loss to the US due to intellectual property theft exceeds $300 billion, with 50% to 80% of such thefts attributed to China.[9]

Indeed, Operation Aurora, which is considered a turning point in industrial espionage, was a series of cyberattacks originating from China targeting US private sector companies in 2010. Council on Foreign Relations explains attackers targeted companies such as Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google, and many others with a phishing campaign jeopardizing their networks to steal trade secrets. Google, being the only company to confirm being a victim and publicly attributing the incident to China, disclosed that specific Chinese human rights activists' Gmail accounts were compromised.[10]

Following Operation Aurora, after nine months of a comprehensive agreement between the then US President Barack Obama and Chinese President Xi Jinping aimed at preventing intellectual property theft, there was a significant decrease in cyberattacks by China on Silicon Valley companies, military firms, and other commercial targets. [11] However, it is stated with the onset of the Trump administration

[7] Xinhua News Agency (2021) "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," https://cset.georgetown.edu/publication/china-14th-five-year-plan/

[8] Rugina, J.M. 2023, Economic Cyber Espionage: The US-China Dilemma. https://doi.org/10.5152/JIRS.2023.23014

[9] The Commission on the Theft of American Intellectual Property Report (2013) https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf

[10] Council on Foreign Relations, 2010. Operation Aurora. https://www.cfr.org/cyber-operations/operation-aurora

[11] FireEye Report, (2021), Red Line Drawn: China recalculates its use of cyber espionage. https://www.mandiant.com/sites/default/files/2021-09/rpt-china-espionage-1.pdf

and the escalation of trade wars and other tensions with China, computer hacking activities resumed.[12] The increase in tariffs supported by President Donald J. Trump's 'Make America Great Again' policies, combined with efforts to become a global technological leader in the interests of US businesses, posed a significant threat to cybersecurity when combined with diplomatic tensions.

The threats in cybersecurity further exacerbate the trade war in the technology and big data sectors. This cyclical threat structure between trade and cybersecurity has added a new dimension to the 21st-century US-China competition, intensifying and continuing to grow. In the short term, it may seem challenging for China to surpass the United States, the leader of cyber security in the world. China may continue to target US data exports and map out foreign states' networks to gain military superiority. Economic or diplomatic gains from cyber espionage may be beneficial to the CCP, leading to accelerated cyber espionage campaigns.

In response to these risks, the Biden administration is taking steps both at the state and individual levels. At the individual level, the ban on the TikTok application in the US, which has been a point of discussed in recent years but not acted upon, can be cited as an example. The bill banning the application nationwide in the US has been introduced to the Senate, due to concerns over a Chinese company that owns 60% of TikTok, ByteDance, collaborating with the Chinese government on data sharing. Similarly, the decision to ban the application for European Commission employees was made based on cybersecurity threats.

At the state level, there are some developments, such as commitments with Japan and South Korea to enhance cybersecurity cooperation in the Indo-Pacific region. [13] In these commitments, partners acknowledge the importance of sharing cyber threat intelligence related to critical infrastructure threats, and the primary objective of this cooperation is to enhance cybersecurity in the region.

All these developments indicate a new stage in the US-China relations, trade and technology wars are now intertwined with cyber warfare. These conflicts are perceived to carry traces of the Cold War, characterized by intelligence gathering activities and a threat of sabotage, accompanied by digital conflicts. The question of whether these risks of cyber warfare could bring these two countries closer to a hot war remains unanswered for now. One thing is clear however, there are serious dangers posed by the increasing threat of US-China cyber warfare.

[12] Rugina, J.M. (2023), Economic Cyber Espionage: The US-China Dilemma; Larres, K. (2020). Trump's trade wars: America, China, Europe, and global disorder.

[13] Atlantic Council, Şubat 2024. "To combat Chinese cyber threats, the US must spearhead a new Indo-Pacific intelligence coalition" https://www.atlanticcouncil.org/blogs/new-atlanticist/to-combat-chinese-cyber-threats-the-us-must-spearhead-a-new-indo-pacific-intelligence-coalition/

ABOUT THE AUTHOR

Larissa Kumaş, completed her undergraduate degree in International Relations at Koç University and obtained a double major in Business Administration. Kumaş, who specializes in the impact of technological developments on international relations at DIPAM, writes analyses on topics such as cybersecurity, space, and artificial intelligence. She plans to pursue a master's degree in cybersecurity governance.