Journal of Regional Studies Review (JRSR)
Volume 4, Issue 1 (Winter 2025) | Pages: 503–515
ISSN (Online): 3006-6646
Digital Object Identifier (DOI): 10.62843/jrsr/2025.4a096
Correspondence should be addressed to Baqir Hassan Haidery; Baqir.75hassan@gmail.com

RESEARCH ARTICLE

The US-China Cyber Conflict and Its Impact on the UK's Cybersecurity Policies

Baqir Hassan Haidery [a]

Abstract: This paper explores the geopolitical implications of the U.S.-China cyber conflict and its cascading effects on the United Kingdom's cybersecurity posture. As the United States and China engage in strategic cyber competition involving espionage, data theft, and digital infrastructure control, third-party states like the UK are compelled to recalibrate their cybersecurity strategies. Employing Realist theory in international relations, the paper explains how power maximization and national sovereignty guide cybersecurity policy decisions in a multipolar digital world. By analyzing the evolution of the UK's cybersecurity frameworks, alliances, and technological investments in response to this competition, the study reveals the cyber domain as an arena of influence where global power dynamics manifest. The research also reflects on how digital sovereignty and multiparty intelligence alliances reshape middle-power behavior in the international system.

Keywords: Cybersecurity, U.S.-China Cyber Conflict, UK Cyber Strategy, Realism, Digital Sovereignty, Cyber Espionage, Strategic Alliances, Cyber Governance, Geopolitics, International Relations

Introduction

The subject "The U.S.-China Cyber Conflict and Its Impact on the UK's Cybersecurity Policies" pertains to the new frontier of cyber war, which has become the epicenter of strategic competition between great powers. The United States-China conflict is being waged with charges of cyber spying, data theft, and intellectual property theft. These cyber wars are not a two-way street but have international implications. The UK, as a close ally of the U.S. and a member of international intelligence-sharing bodies like NATO and the Five Eyes (United Kingdom National Cyber Security Centre, 2023) community, is impacted by this new space. Cybersecurity is no longer an information technology issue but a constituent of national security. As cyberattacks increase in size and sophistication, the UK is compelled to walk the tightrope of political alignment, economic ties, and technological vulnerabilities. The greater convergence of digital infrastructure and geopolitical competition has compelled the UK to redesign its cybersecurity policies. This paper presents an analysis of how the current U.S.-China cyber tensions impact the UK's policy decisions, threat perceptions, and international alliances. Through these dynamics, we understand how cyber power competitions in the international system impact third-party nations. This paper also employs the Realist framework to explain motivations behind such strategic actions.

The United States and Cybersecurity

The United States has been a leader in cyber and technological defense innovation, but leadership has also made it the most probable target for adversaries. The 2015 OPM breach (Office of the Director of National Intelligence [ODNI], 2023) and release of sensitive information of over 21 million federal employees and the 2020 SolarWinds hack (ODNI, 2023) are just some of the large-scale cyberattacks that demonstrate the increasing vulnerability of even the technologically most advanced states. These intrusions, attributively attributed to Chinese state actors, provoked a strong cybersecurity response from the U.S. Government. The

[a] Student, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan.

Cite this Article: Haidery, B. H. (2025). The US-China Cyber Conflict and Its Impact on the UK's Cybersecurity Policies. *Journal of Regional Studies Review, 4*(1), 503-515. https://doi.org/10.62843/jrsr/2025.4a096

government has established specialist agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) (U.S. Department of Homeland Security, 2022), established national cybersecurity strategies, and invested in AI driven threat detection. U.S. policy today is centered upon deterrence, resilience, and cooperation with the private sector. With cyberspace emerging as a central battleground for economic and military supremacy, the U.S. has also developed offensive capabilities, including the use of cyber operations for attacking enemy networks. Through international collaboration with private-public sectors and global coordination, the U.S. is enhancing its cybersecurity posture, which establishes de facto standards that indirectly affect its allies, such as the UK.

China's Role in Global Cyberspace

China's expanding footprint in cyberspace is political and strategic. In seeking technological autonomy and geopolitical influence, China has created sophisticated cyber capabilities under the control of its Strategic Support Force. These are believed to serve state purposes like economic espionage, political surveillance, and cyber sabotage. Western intelligence agencies routinely blame cyberattacks on critical infrastructure, businesses, and research institutions on Chinese-backed actors like APT10 (FireEye Mandiant, 2021) and APT41 (Council on Foreign Relations [CFR], 2023). While China has disavowed such accusations, its cyber activity reflects broader national aspirations in "Made in China 2025 (Ministry of Foreign Affairs of the People's Republic of China, 2023)" and Belt and Road policy. These are above economic reforms— they are to become leader in new domains of emerging technology like 5G, artificial intelligence, and quantum computing. As a result, cyber space becomes tool for China's influence expansion at the expense of competitors. China's opaque system of government and state-corporate convergence make attribution and accountability difficult, and thus international response even more challenging.

The United Kingdom's Cybersecurity Response

The UK is indirectly engaged in cyber war with China but is affected strongly by the war in its geopolitical position. Being a trusted ally of the U.S. and a member of the Five Eyes, the UK has shared intelligence responsibilities and is bound by Western cybersecurity standards. The most glaring example is the ban on Huawei (UK Government, 2022) in the UK 5G network on the basis of surveillance and foreign interference. This policy shift was a turning point in the management of the nexus of technological innovation and national security in the UK. The National Cyber Security Centre (NCSC) (United Kingdom National Cyber Security Centre, 2023) has since had its role expanded, issuing advice on cyber resilience and incident response across the private and public sector. Further, the UK 2022 National Cyber Strategy sets out visionary measures against state-sponsored attacks, enhancing collaboration with other nations, and protecting critical infrastructure. These actions demonstrate how the broader geopolitical setting, in particular the U.S.-China cyber competition, affect the UK's global positioning and internal cybersecurity agenda.

Research Questions

1. How does the U.S.-China cyber conflict exemplify Realist principles in international relations?
2. In what ways has the UK's cybersecurity strategy evolved in response to the U.S.-China cyber tensions?
3. How does the Realist framework explain the UK's alignment with the U.S. in cybersecurity matters?

Theoretical Framework

The U.S.-China cyber war and spillover effects on UK cyber policy can be best comprehended with the help of Realism, the most prevalent theory of international relations (Nye, 2011). Realism in its simplest conception conceives the international system as anarchic, with no central power to impose rules or settle disputes (Nye, 2011). Under such an environment, states behave in their own self-interest to survive, maintain sovereignty, and seek power. Cybersecurity, once a technical area, has now become an important area of strategic competition, based on the principles of Realist philosophy.

Realism stresses the priority of the state, the inevitability of war, and the ongoing quest for relative power (Nye, 2011). The cyber domain, although virtual, is not exempt from these principles. Cyberspace, in return, offers new fields of conflict where the classic military encounter is substituted by cyber intrusions, cyber espionage, infrastructure attacks, and clandestine operations. The United States-China cyber competition is the classic Realist competition for power and security. In the meantime, the United Kingdom, perceiving the dangers of the competition, re-prioritizes its cyber activities in an attempt to protect interests, preserve autonomy, and preserve strategic partnerships.

Cybersecurity as an Instrument of Power

Realist theory argues that power is at the heart of global politics. With the cyber age, power is no longer just military hardware or economic dominance—information dominance, technological dominance, and cyber dominance. States are spending more on cyber warfare, cyber defense systems, and offensive cyber capabilities in order to gain strategic dominance over rivals. The United States, the traditional dominant great power in the world, wants to keep its dominance through superior cyber defense systems, global surveillance programs, and alliances like the Five Eyes (United Kingdom National Cyber Security Centre, 2023). China, however, sees cyberspace as an arena where it can counterbalance U.S. dominance, promote its own national interests, and exercise its sovereignty in the digital age.

The United Kingdom is not a cyber superpower itself but feels immense pressure to modify its cyber policies in reaction to this power game. As a U.S. ally and a victim of past cyber operations (e.g., the 2017 WannaCry ransomware attack (European Parliament, 2022)), it is compelled into a Realist position—resilience spending, aligning itself with great powers, and contingency planning for retaliatory action if necessary.

Security Dilemma in the Cyber World

Another fundamental Realist idea is the security dilemma—a vicious cycle in which the quest for security by one country makes others insecure and hence they seek an arms race or increased tensions. The idea is well illustrated in the cyber rivalry between the United States and China. When the United States expands its cyber defenses and expands its surveillance capabilities, China sees it as an encroachment on its sovereignty and responds by expanding its cyber capabilities. It is tit-for-tat where both sides expand their capabilities but neither feels safe doing so.

The UK, while not a focal point for this bilateral conflict, sits in the middle of the crisis. It must respond to renewed threats without appearing to be actively aggressive or inviting retaliation. The result is a series of defensive and diplomatic measures—ranging from new national cybersecurity policy to international campaigning for cyber norms—that are reflective of Realist concerns on national interest and preservation in a rapidly evolving threat environment.

National Interest and Sovereignty

Realism anticipates that states will pursue their own national interest first and foremost. In cyberspace, this equates to protecting critical infrastructure, protecting sensitive information, and digital sovereignty (Nye, 2011). The United States justifies its cyber activity as a means to counter authoritarian powers and maintain international stability. China views cyber control as the key to national rejuvenation and domestic security. Both states employ cyber tools to promote their interests—whether to get economic intelligence, destabilize adversaries, or create the digital order.

The policy of the UK is also guided by national interest. Actively working with allies, especially the U.S., it also takes independent action in the interest of its people. These are, for example, rebalancing foreign tech firms, investing in domestically created innovation, and augmenting public-private partnerships in cyber security. Realism explains this action as a prudent step in reaction to the shifted balance of power, where the UK needs to act pragmatically to protect its national sovereignty (Nye, 2011).

Realism and the Shortage of Global Governance

Realism is skeptical of global institutions and international norms because it is convinced that they are likely to be weak or susceptible to manipulation by the great powers (Nye, 2011). In cyberspace, the lack of strong global governance only serves to feed this skepticism. Although institutions such as the United Nations have attempted to set norms of responsible state behavior in cyberspace, enforcement is far away. Great powers still operate in cyberspace with impunity, and attribution difficulties make it difficult to call out actors.

In this lawless world, Realist policies are dominant. States exercise self-help, build deterrence by building capabilities, and exercise cyber diplomacy to shape the rule in their interest. The U.S. and China, permanent members of the UN Security Council, exercise cyber actions which are an expression of the strategic interests rather than international consensus. The UK also values sovereignty, bilateral arrangements, and technological autonomy over multilateral cyber treaties.

Methodology

The research is based on carefully reviewing public strategies, expert reports and research papers. Rebus Ivuk analyzes how states conduct themselves based on the tenets of Realism, especially their actions in the cyber domain.

Cybersecurity strategy documents from the United States, China and the United Kingdom, along with official statements and intelligence assessments (e.g., by the UK Government, ODNI, NCSC), are types of primary sources. Some examples of secondary sources used are books and scholarly articles that study cyber warfare, state conduct and global security changes. Documents are carefully studied to find out how nations see these and other threats, align their efforts and update their cybersecurity policies due to tensions with the U.S. and China.

To understand how mid-level countries respond in a cyber conflict, the study looks at actions and decisions taken by the United States, China and the United Kingdom as main cases. Using this method, one can explain cybersecurity trends and changes in political behavior due to digital evolution.

Discussion

Answer to Research Question 1

The U.S.-China cyber war is a classic case of Realist dynamics in international affairs. Both nations seek relative gains over absolute gains, willing to make sure that their gains are at the cost of their competitors. America's strategic cyber warfare and China's cyber-enabled IP theft are both examples of a zero-sum game wherein technological dominance equates to national power. Even diplomatic gestures like cyber treaties aimed at limiting economic espionage are tactical maneuvers under Realist principles, designed to gain time, contain conflict, or divert attention.

Moreover, the conflict has also brought cyber resilience to broader national security policy in both countries. Cyber capabilities for offense have become mainstream as accepted tools of statecraft, further indicating that cyber activity is being considered from a power-maximization perspective and not from any form of idealist vision of collective cyber governance.

Answer to Research Question 2

The UK's cyber evolution, particularly post-2018, has been marked by a series of strategic shifts prompted quite prominently by the U.S.-China cyber rivalry. Before the heightening of tensions between the two great powers, the UK had more or less viewed cyber threat as primarily a criminal justice issue. But faced with intelligence of coordinated cyber-espionage campaigns involving Chinese and Russian actors, the UK radically shifted gears.

The establishment of the National Cyber Security Centre (NCSC) in GCHQ was an institutionalization of cybersecurity as a national security issue (United Kingdom National Cyber Security Centre, 2023). The increased remit for the NCSC is not merely incident response but, in effect, advising portions of the critical infrastructure on threat intelligence and risk mitigation. The 2022 National Cyber Strategy for the UK explicitly declares that hostile state actors are the UK's largest cyber sovereignty (Ministry of Foreign Affairs of the People's Republic of China, 2023) threats (UK Government, 2022).

Moreover, the UK Huawei ban also exhibited a deep convergence with U.S. intelligence estimates and geopolitics (UK Government, 2022). The move valued security above economic cost, as it would interrupt 5G deployment timelines and necessitate massive investment in new supply chain substitutes. From a Realist point of view, the UK valuing sovereignty and alliance obligations above market optimality shows the security prioritization of state action.

Response to Research Question 3

Realism explains the UK's strategic decision to cooperate closely with the U.S. in cyber issues in a rational manner (Nye, 2011). Since the UK is a middle power in a turbulent world, it benefits from security assurances and access to intelligence-sharing in alliances such as Five Eyes (United Kingdom National Cyber Security Centre, 2023). In world anarchy, trust is not easy to find; therefore, the UK decision to respond to U.S. warnings regarding Huawei as well as Chinese cyber activity is based on the Realist maxim of self-help (UK Government, 2022).

The "Bandwagoning" model fits best here: weaker or middle powers bandwagon with stronger states to guarantee their survival. With cyber alignment with the U.S., the UK ensures its access to vital threat intelligence and wields maximum deterrence against state-sponsored cyber-attacks. Additionally, the active engagement of the UK in championing international norms on cybersecurity—e.g., encouraging responsible state behavior in cyberspace in the UN Group of Governmental Experts (GGE) (The White House, 2023)—is not a utopian fantasy. It also helps the Realist objective to create the foundation of a cyber order that restrains aggressive action and maintains the strategic benefits of the West.

Discussion of Entities

The United States Acts as the Leader of the World in Cybersecurity Strategies

Cyber activities on a global scale are led by the United States. The country’s strong technology, intelligence and planning give it the highest standard in defensive and offensive cyber activities. Recognizing cyberspace as an area of war, the U.S. was an early leader in planning cyber defenses for its national security. Thanks to national cybersecurity strategies, the use of intelligence for surveillance, military online commands and international alliances, the U.S. has influenced the development of the global cyber system.

The U.S. treats cyberspace like land, sea, air and space in terms of its significance for warfare. As a result of this identification, countries have advanced offensive systems, launched new cyber intelligence actions and created doctrines for early defense. America has put a lot of effort into organizations like the Cybersecurity and Infrastructure Security Agency (CISA) (U.S. Department of Homeland Security, 2022), U.S. Cyber Command and by urging cooperation between federal agencies, the military and tech companies. They are designed to accomplish two purposes: support domestic needs and impact the global balance between countries, mainly those facing China.

The Competition between the US and China in Cyber Space

Deep suspicion between the U.S. and China forms the major reason behind their cyber confrontation. Officials in the U.S. accuse China of using cyber-attacks to investigate important industries, disturb key equipment and sway debates. In 2015, a breach that hit the Office of Personnel Management (OPM) was discovered, led by Chinese state hackers and affected the sensitive information of more than 22 million federal employees.

In that situation, the United States focused on a doctrine that involved constantly conducting actions in cyberspace to prevent threats and guide the moves of adversaries. Thanks to the doctrine, it is possible to track events closely, disrupt attacks just as they begin and manage how the situation escalates. Staying ahead of attacks by preventing them (left of boom) is one way the U.S. defends its superior position in cyber warfare without needing to engage in full-scale warfare.

The U.S. follows China's Digital Silk Road, part of the Belt and Road (Ministry of Foreign Affairs of the People's Republic of China, 2023) Initiative, because it might help China extend its control over global cyber affairs. As a result, the U.S. has urged its allies, including the UK, to block or limit Chinese companies from involvement in 5G networks because of fears over espionage and surveillance.

Working Together With Other Companies

USA engagement in cyber security is proactive as well as collaborative. Since cybersecurity affects everyone, the U.S. has built several alliances, including the Five Eyes (United Kingdom National Cyber Security Centre, 2023) (with the UK, Canada, Australia and New Zealand), the Quad (with India, Japan and Australia) and cyber-related arrangements with NATO.

They exist to allow countries to share information, participate in joint drills, implement the same response plans and shape technology standards together. The UK depends on these ties to get quick alerts about Chinese cyber activities and benefit from using advanced cyber ideas and inventions.

Clean Network shows how the U.S. is trying to form a worldwide digital system not under Chinese influence. By urging allies to work only with trusted firms and leave out Chinese technologies in sensitive fields, the U.S. hopes to prevent China from expanding in cybernation and improve Western sovereignty in technology.

How Security and Surveillance Are Used

Together with the CIA and others, the National Security Agency has the leading role in conducting cyber operations for the U.S. In the Edward Snowden leaks (Clarke & Knake, 2010), PRISM shown how powerfully the U.S. can monitor digital activities. Though some consider them controversial, these programs are based on Realist ideas that security and stability mean doing something intrusive.

The U.S also uses its intelligence to both guard against threats and learn more about Chinese cyber activities. When U.S. forces monitor networks that have been targeted by others, they can learn about Chinese tactics, better identify who is involved and plan counteractions.

The UK's decisions on cybersecurity rely heavily on the sharing of intelligence. Using Five Eyes (United Kingdom National Cyber Security Centre, 2023), the UK obtains early messages, technical support and insight into threats which help develop its domestic cyber policy. As a result, the U.S. both guards and guides the larger cyber world the UK is linked to.

The Guiding Principles for U.S. Cybersecurity and the Nation's Reach

Resilience, innovation and partnering with the private sector are central focus areas in the present U.S. National Cybersecurity Strategy. The U.S. supports close cooperation between the government and Microsoft, Google and Amazon to protect all types of networks. Besides, the stress on zero trust architecture and encryption technology that is protected from quantum attacks will build the world's cybersecurity standards in the coming years.

The doctrine reaches allies as well as opponents. The UK's national cyber strategy has been harmonized with U.S. suggestions by applying zero trust methods, investing in centers for the monitoring of cyber-attacks and sharing more information with NCSC. These decisions show the quiet influence of the U.S. cyber policy on friends in the global arena.

Also, the United States contributes to creating cyber norms around the world. In the UN Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG), the U.S. strives to form rules that keep states open, accountable and responsible in cyberspace. Often, these actions try to answer China's request for complete state control over internet matters.

Influence on the Cyber Policies of the UK

The way the U.S. deals with cyber threats matters a lot to the UK. Because the UK is part of Five Eyes (United Kingdom National Cyber Security Centre, 2023) and is a longtime ally, it frequently backs U.S. cybersecurity efforts. The ban of Huawei (UK Government, 2022) from the UK's 5G infrastructure was largely driven by U.S. lobbying and warnings from its intelligence services. The UK's cyber strategy for 2022 focuses on issues noted in U.S. policy such as joining efforts among private and public sectors, using new technology for security and collaborating with foreign nations.

Also, the U.S. participates in building the UK's cyber security stance by joining exercises, reviewing threats together and having regular talks involving strategy. American weapon development tools, databases with secure information and highly advanced threat detection are available to the UK. At the same time, the UK is seeking to remain independent and grow its own skills by handling its dependence with sovereignty in mind.

Entity 2: China – Digital Authoritarianism and Strategic Cyber Ambitions

China has grown quickly to become one of the most powerful players in cyberspace. From technology innovation to cyber espionage and cyber versions of governance, China's cyber policy is state-led, holistic, and an integral part of its geopolitics. As a cyber power, China values sovereignty, control of information, and the leverage of cyberspace to project its global power. Its cyber activities have become one of the core features in its overall competition with the United States, frequently countering Western democratic models of openness, transparency, and private-sector innovation.

China's distinctive cyber model has created a new kind of strategic challenge, one that dissolves the distinction between civilian technology and military power. By using state-subsidized networks, aggressive surveillance policies, and sweeping global infrastructure initiatives, China has reshaped the cyber space, thus affecting not just adversaries but even U.S. allies like the UK.

The Chinese Cyber Doctrine

China views cyberspace as a central area of national security and political influence. It has incorporated cyber policy into its overall state machinery under the rubric of "Cyber Sovereignty." This ideology does not believe in the Western concept of an open, uncontrolled internet. Rather, it propounds a regime where every state has the freedom to manage the internet within its borders—censoring information, controlling data flows, and monitoring users as and when needed.

This strategy is implemented through tight state control of the domestic internet, with robust institutions like the Cyberspace Administration of China (CAC) pushing regulation, censorship, and enforcement. The Chinese Communist Party (CCP) has employed this strategy to suppress dissent, manage public discourse, and exercise political power.

China's cyber doctrine also integrates its civilian tech sector with the military via the Military-Civil Fusion (MCF) initiative. These companies include Huawei (UK Government, 2022), ZTE, Alibaba, and Tencent, all of which are government-controlled and provide technological support to the military and the intelligence sector. This integration enables China to conduct cyber operations using both formal and informal means, making attribution more difficult and defense harder to achieve.

State-Sponsored Cyber Operations

China's offensive cyber activities are mostly credited to advanced persistent threat (APT) groups, including APT10 (FireEye Mandiant, 2021) (Stone Panda) and APT41 (Council on Foreign Relations [CFR], 2023), which are associated with the Ministry of State Security (MSS) and the People's Liberation Army (PLA). These entities have been active in cyber espionage against governments, multinational entities, defense contractors, and critical infrastructure.

Arguably the best known is the OPM hack in the US, but China also mounted large-scale cyber activity in Europe. The UK's National Cyber Security Centre (NCSC) (United Kingdom National Cyber Security Centre, 2023), for example, has openly credited Chinese actors with targeting research into COVID-19 vaccines, telecommunications sectors, and diplomatic networks. These activities are not only strategic in terms of intelligence gathering but also because they help improve the technological and geopolitical standing of China.

China also commits intellectual property (IP) theft, appropriating trade secrets to speed up indigenous innovation at no research cost. It has particularly affected areas such as aerospace, biotechnology, and supercomputing. The UK concern is not just that its own companies are vulnerable but that such actions erode the rules-based international order.

The Digital Silk Road (Ministry of Foreign Affairs of the People's Republic of China, 2023)

China's Digital Silk Road (DSR) is a key pillar of its cybersecurity strategy. Under the umbrella of the larger Belt and Road (Ministry of Foreign Affairs of the People's Republic of China, 2023) Initiative (BRI), the DSR seeks to construct digital infrastructure—5G networks, fiber-optic cables, data centers, and e-commerce platforms—across Asia, Africa, and Europe. This enables China to extend its technology, standards, and rules of governance to the rest of the world.

The UK and other Western countries' concern is that there is a built-in risk of espionage and manipulation of data. The technologies of Chinese companies carry backdoors or open the door for the Chinese state to potentially have access to foreign data. The allegations though are hard to substantiate because of the Chinese state-firm relationship's opaque nature, the ultimate UK decision to exclude Huawei (UK Government, 2022) from its 5G network rested on exactly these concerns.

The Digital Silk Road (Ministry of Foreign Affairs of the People's Republic of China, 2023) is also a challenge to the Western monopoly on internet governance globally. China, through its infrastructure and through its partners, advocates an alternative internet model—one that potentially will fragment the internet (a development referred to as the "splinternet"). This model advocates state control, censorship, and surveillance—something far removed from the liberal ideals advocated by the UK.

The risk in the UK and other Western countries is that surveillance and control over data can be embedded wherever necessary. Many times, businesses in China add secret entryways to their software which can grant the Chinese government access to foreign data. Because it is difficult to confirm such claims due to the lack of transparency in Chinese state businesses, UK authorities made their decision to reject Huawei (UK Government, 2022) for 5G on those exact fears.

The Digital Silk Road (Ministry of Foreign Affairs of the People's Republic of China, 2023) is also challenging the West’s control of the worldwide internet. China uses its infrastructure and alliances to back a different approach to the internet which may end on the internet being broken up into smaller networks (the “splinternet”). The way this model functions is not in line with liberal ideas popular in the UK: it supports control, censorship and surveillance.

Artificial Intelligence, Surveillance and the Way We Are Controlled

Facial recognition and biometrics collection in cities, among others, are all some of the most advanced in the world created by China. At home, these tools are employed to restrict people, including in Xinjiang where they closely watch and restrict the Uyghur Muslims.

China sends these technologies to countries in Africa, Latin America and Southeast Asia around the world. exporting surveillance systems helps bring money and improves China's influence in the world Not only does this add dependence on China, but it also gives the Chinese approach to digital control global prestige—a challenge for democratic nations including the UK.

The UK is worried that taking such technologies from third-party suppliers in Europe could lead to their misuse inside the UK and that more worldwide use of surveillance could threaten global agreements on rights and secure cyberspace.

Striving for a Competitive Relationship with the West

China wants to lead in cyber activities by fighting against the U.S. and its allies. By 2030, China wishes to lead the world in AI, create global rules for internet governance and establish worldwide standards in new telecommunications.

China has suggested at forums such as the International Telecommunication Union (ITU) that new rules should allow governments to monitor what people post on the internet and their identities. Like the U.S., the UK feels that these proposals may bring about authoritarianism.

We are now releasing Part 4: Entity 3 – the United Kingdom, the next section of the "Discussion of Three Entities," which covers the UK's stance on the U.S.-China cyber conflict and its result on its cyber and defense policies.

Entity 3: United Kingdom's Weight in the Digital Conflict

The United States' close ally in the UK and its prominent liberal democracy places it at the center of Washington's ongoing struggles with Beijing online. In response to defending Britain's interests along with considering the security of global digital matters, the nation's cybersecurity policy has transformed. Because the UK faces threats online and sets international cyber standards, its position is extremely varied. Instead of just reacting to threats, it is also taking part in guiding the worldwide answer to cybersecurity problems in the present century.

A plan for Protecting the Nation against Cyber Threats

The National Cyber Security Strategy updated regularly among the UK's cybersecurity guidelines. The strategy for 2022–2030 sets out plans to help Italy become more resilient, discourage its adversaries and work more with partners around the world. It explains that cybersecurity is essential to the security, prosperity and strong democracy of any country.

According to this approach, the National Cyber Security Centre (NCSC) (United Kingdom National Cyber Security Centre, 2023), an arm of GCHQ, takes charge of overseeing cyber defense in the country. The organization is in charge of spotting vulnerabilities, giving cybersecurity suggestions to important infrastructure and directing incident management. National security agencies regularly join forces with intelligence, law enforcement, private organizations and collaborate primarily with the Five Eyes alliance (UK, US, Canada, Australia and New Zealand).

According to the UK's national cybersecurity framework, public-private cooperation is key as most essential infrastructure and technology comes from private firms. Working together, government supervision and industry ideas contribute to the UK's goal of a society-wide approach to protecting against cyber-attacks.

Effects of the U.S. and China's Cyber Conflict on UK Policies

The growing cyber competition between China and the U.S. has strongly affected how the UK approaches strategy. In a number of ways, the UK is being pressed to pick between the strong tech expertise of the U.S.

and the economic openings offered by China. As a result, the UK's rules on digital security were reworked and given new weight.

Huawei (UK Government, 2022)'s situation greatly influenced the way countries see telecoms giants today. The UK allowed Huawei (UK Government, 2022) a small part in its 5G system, provided the company follows certain government rules. Yet, under extra pressure from the U.S. government and after receiving intelligence about risks of espionage, the UK changed their mind in 2020 and chose to remove all Huawei (UK Government, 2022) equipment from its 5G networks by 2027. It meant the UK was aiming to adopt the American approach of isolating itself from China in the cyber space.

At the same time, the UK is now applying its cybersecurity strategy to developments in foreign investment, especially regarding new fields of AI, quantum computing and semiconductors. The law gives the government the ability to prevent deals that might harm national security—the main purpose being to keep foreign acquisitions, often made by China, in check.

Being Strategically Independent While Leading the World

Though they share the same security goals, the UK also wants to be self-reliant in cybersecurity. You can see its support for digital sovereignty in placing importance on controlling important infrastructure, supply chains and data. The UK aims to rely equally upon its allies, not give too much power to any one country.
The UK has set itself apart by encouraging a system of rules in the global cyber environment. It acts in supporting roles in the United Nations, both in the United Nations Group of Governmental Experts (UNGGE) and the Open-ended Working Group (OEWG), to define standards for responsible state actions on the internet.

Besides, the UK backs skill development in developing countries to help protect against cyber problems and authoritarian rule. This work is motivated by a focus on national defense and the growing contest between the U.S. and China over how the internet should be run.

Cyber Attack Tools

Defending the UK from cyber-attacks is only part of what it does; it is also developing offensive capacities. In 2020, the government formed the National Cyber Force (NCF) as a combined operation between GCHQ and the Ministry of Defence to do cyber operations that interfere with enemies' plans, stop attacks and help military campaigns.

It has an important role in expanding national power in cyberspace. For example, it might carry out work that disrupts terrorists' ability to communicate, takes apart criminal ransomware groups or gets involved in state-sponsored misinformation. Its foundation marks a change in UK policy from the old style of passive defense to one of active deterrence.

This matches the NATO's latest cyber doctrine which considers cyberattacks a possible reason to invoke collective defense. As a member of NATO, the UK is part of a team response to cyber dangers and helps defend allies in Eastern Europe, where hybrid methods are used a lot.

Cybersecurity, Diplomacy and World Partnership

The UK has given special emphasis to cyber diplomacy in its efforts to encourage coalition-building and shape new cyber norms. The U.K. has Team up with the U.S. and EU regarding cybersecurity matters, even after Brexit created broader political disagreements. The UK keeps playing a major part in Five Eyes (United Kingdom National Cyber Security Centre, 2023), helping members access and use intelligence and sharing the work of tracking and investigating threats online.

Identifying foreign offenders in cyberattacks is significant and the UK has often helped do so publically. It was one of the countries that together with the U.S. and EU linked the 2021 attacks on Microsoft

Exchange Servers to Chinese state-sponsored groups. They make the actions taken against cyber criminals very clear to everyone.

Besides, the UK stands for "responsible state conduct in cyberspace", meaning that it opposes damaging civilian systems, respects each country's sovereignty and collaborates on stopping cybercrimes. They directly resist China's cyber strategy and focus on keeping the internet free, safe and easy to use.

Issues and Areas Where Security is at Risk

In spite of taking early action, the UK experiences many challenges. Because modern computing relies on internationally linked supply chains, it's at risk for cyber threats embedded by manufacturers. Furthermore, since changes in AI and quantum computing are so rapid, governments need to move fast, a thing often blocked by bureaucracy.

The UK has to handle domestic politics in relation to digital measurement, online threats and encryption. Ensuring civil liberties and strong security is very tricky when there are fears about laws like the Online Safety Act overstepping privacy protection.

Problems related to workers shortages in cybersecurity can last for years. Putting Cyberflirts and other programs in place, the UK intends to ensure cybersecurity skills are taught to young people. Even so, it will require patience and long-term spending to close this difference.

The UK's Plan for Future Cybersecurity

In the future, the UK wants its digital world to be safe, original and rooted in democracy. Now, its strategy on cybersecurity joins economic preparedness, defense readiness, new technology and being involved internationally.

Britain seeks to defend what the West considers important, ensure a security structure in cyberspace and preserve its independence against both attack and external pressures in the U.S.-China cyber rivalry. The improvement of its cybersecurity policies happens for more reasons than attacks; it's part of an overall plan to protect freedom and openness online.

Conclusion

Currently, the competition in cyberspace between the United States and China constitutes a key security problem for today's world. Because the United States and China are constantly competing in cyber areas such as espionage and stealing intellectual property and disrupting services, their rivalry is changing both their own relationship and the international cybersecurity landscape. Because of this, the UK and other secondary actors are making changes to their security strategies to defend their country in a competitive digital world.

Evidence from this discussion indicates that the main issue of the U.S.-China cyber conflict is competition for influence and authority online. Building on realist thinking, this competition occurs as states work to secure their country, use advanced technology and gain strategic influence because the world remains highly anarchic. Both nations believe that influence in cyber space can help achieve economic wealth, stronger defense and higher influence on the world stage. As a result, cyber activities now form key parts of the country's national security planning.

The United States puts importance on its cyber warfare, research and development and also brings other countries together to meet threats from China. US officials aim to keep the country's technology ahead and ensure its critical infrastructure is safe from advanced persistent threats created in China. The United States often makes public attributions of cyberattacks and uses consequences to stop any possible future attacks.

Unlike the U.S., China uses strong defenses, as well as gathers and controls a lot of intelligence through cyber means. In addition to state security, Beijing tries to boost its domestic technological independence and help form internet guidelines that fit its form of government. It appears China's cyber activities aim to oppose U.S. strength online and raise its position as a major cyber player.

Stuck between powerful tech firms led by China and the United States, the United Kingdom deals with a difficult security situation. Its cybersecurity approach now reflects balancing the country's alliance commitments, national control and business interests. The UK has moved to secure its critical digital infrastructure against China, at the same time as building up its existing partnership with the United States in intelligence and cyber defense. At the same time, the UK hopes to be independent in its strategies and backs the creation of guidelines for responsible state behavior online while improving its cyber strength.

The British experience shows how states with limited resources deal with the competition between big technology powers. To become safer from threats by all sorts of actors, the UK ensures close cooperation between the government, companies and other nations. Besides, China leads in cyber diplomacy and the development of cyber skills which qualify it to be a key factor in forming a stable and rule-based system for cyberspace.

That said, there are still difficulties. Quickly advancing technology, uncertain supply chains and trying to balance civil liberties with security ongoing, cause policy issues. To keep up its cyber security, the UK needs to focus on improving its people and technology. It should play a positive role in international conferences to help find common ground on methods for stopping and addressing cyber conflicts.

The tension between the U.S. and China in cyberspace is likely to remain a key element of world politics for years ahead. The effect of those attacks highlights that all cybersecurity policies in the United Kingdom should stress connectedness, adaptability and cooperation. Seeing the UK's strategies can show others the best ways for middle powers to remain democratic and help maintain stability in the cyber world and face challenges from larger competitors.

In short, this project makes clear that studying cyber conflict should include a realism approach which underlines the role of power and safety. It also points out that proper and adaptable cybersecurity rules are vital to deal with the uncertain and quick progress in the world today. Since each region is working hard to protect their digital interests, learning from the U.S.-China rivalry and the UK's approach will become very important for those committed to digital security.

References

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal (Buchanan, 2020) of Geopolitics.* Harvard University Press.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* HarperCollins.

Nye, J. S. (2011). *The Future of Power.* PublicAffairs.

Segal, A. (2016). The *Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs.

United Kingdom National Cyber Security Centre. (2023). *Annual Review 2023.* https://www.ncsc.gov.uk

U.S. Department of Homeland Security. (2022). *Cybersecurity and Infrastructure Security Agency Reports.*

Ministry of Foreign Affairs of the People's Republic of China. (2023). *China's Position on Cyber Sovereignty*. https://www.fmprc.gov.cn

Council on Foreign Relations (CFR). (2023). *Cyber Operations Tracker*. https://www.cfr.org

European Parliament. (2022). *Cybersecurity and Disinformation: Threats from China and Russia.* https://www.europarl.europa.eu

The White House. (2023). *National Cybersecurity Strategy of the United States.* https://www.whitehouse.gov

Office of the Director of National Intelligence (ODNI). (2023). *Annual Threat Assessment of the U.S. Intelligence Community.* https://www.dni.gov

UK Government. (2022). National Cyber Strategy (UK Government, 2022) 2022. Retrieved from https://www.gov.uk/government/publications/national-cyber-strategy-2022

FireEye Mandiant. (2021). *APT1: Exposing One of China's Cyber Espionage Units.*

Harvard Belfer Center. (2022). *U.S.-China Strategic Competition in Cyberspace*. https://www.belfercenter.org