The US Pivot and Great Cyberpower Competition in the MENA Region

Tamara Kharroub

Over the last few years, the United States' global strategy and national security priorities have shifted significantly from focusing on counterterrorism and Middle East conflicts to dedicating increasing attention to deterring the threat posed by China and Russia. Meanwhile, information and communication technologies (ICT) have emerged as vital tools in the global political order, as technology has become the backbone of political, economic, and military structures across the globe. In this ever-expanding environment of digital omnipresence, cyberspace has become the new battleground for power and influence. Countries around the world are prioritizing cyber strategies and investing in cyber capabilities and technological infrastructures, especially in the realm of cybersecurity, which includes cyber weapons and defense systems. With rapid advancements in technology and the relatively low-cost and high-impact nature of cyber tools compared to conventional weapons systems, cyberspace has become a major arena for global influence, and no less so when it comes to great power competition.

Recent US defense and national security postures have not only renewed America's strategic focus on great power competition with

Russia and China, they have also elevated the importance of cybersecurity. This chapter aims to explore the emergence of global cyber powers, to assess Chinese and Russian influence in the information and technology domains in the Middle East and North Africa (MENA), and to analyze the impacts of US shortcomings in the cyber environment of the Arab world. Although the US may not be completely pivoting away from the Middle East, its policy recalibration in the region reflects a renewed narrow focus on security while it continues to lose influence on other fronts, including cyberspace. Washington's cyber strategy prioritizes cybersecurity and cyberthreats from adversaries like China, Russia, Iran, and North Korea, but in the process loses much-needed leverage over information and technology infrastructures that are poised to determine the future of power and influence, especially in the MENA region.

The Global Battle Over Cyberspace

Cyberspace is becoming increasingly central to all political and geopolitical domains, including governance, diplomacy, economics, and defense; and it is also being used as a weapon of war and aggression, especially in the form of espionage and cyberattacks. While state and nonstate actors alike are leveraging cyber capabilities to advance their political agendas, a comprehensive understanding of cyberpower and information about various states' cyber capabilities remain limited. Cyberpower can be defined as the effective deployment of cyber capabilities and the use of cyberspace by a state or other actor to create both advantage and influence in other environments in order to achieve its (national) objectives.[1]

A few initiatives in recent years have begun assessing the cyberpower of some countries. According to a 2021 report by the International Institute for Strategic Studies (IISS), which analyzed the cyber capabilities of 15 countries, the United States is the world's dominant cyber power, partly because it has been building its cyberpower since the 1990s and has established cyber alliances like the Five Eyes.[2] The report lists Russia and China in the second tier (along with five other countries), but concludes that China

[1] Julia Voo et al., "National Cyber Power Index 2022," Belfer Center for Science and International Affairs, September 2022, https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

[2] "Cyber Capabilities and National Power: A Net Assessment," International Institute for Strategic Studies, June 2021, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf.

is on track to join the US in the first tier due to its "Made in China 2025" strategy and its focus on developing artificial intelligence (AI) and growing its indigenous technologies to achieve economic independence. However, the seven categories used by IISS to assess cyberpower are primarily security-focused, for example, national strategies, governance and military structures, cyber espionage abilities, defense and resilience against cyberthreats, and offensive cyber operations. Taking a more holistic approach to cyberpower, the 2022 National Cyber Power Index (NCPI), ranked 30 countries across eight categories that conceptualize cyberpower in terms of cyberwar components (similar to those found in the IISS study), in addition to a wide range of non-military capabilities, namely information manipulation and control, domestic surveillance, national commercial cyber competence, defining international cyber norms, and cyber operations to amass wealth.[3] The NCPI found that the United States tops the list, especially when it comes to destructive capabilities and intelligence, followed by China in the second spot and then Russia ranking third. Although the United States ranks first on most categories, China beats the United States when it comes to cyber surveillance, cyber commerce, and cyber defense.

The expanding cyberpower of China and Russia has presented the United States with an additional challenge in its strategic global competition. As cyber technologies are becoming ever more central in the realm of power and influence and as instruments of warfare, China and Russia are racing to develop their cyber capabilities and their malicious operations around the world—and especially against the United States—to achieve geopolitical and strategic goals. Russia has arguably carried out the most damaging cyberattacks against the United States, primarily in the form of information warfare, espionage, and destructive cyber operations.[4] The most prominent examples of Russian cyber aggression include the hacking and release of stolen emails and documents from the Democratic National Committee, disinformation operations to influence US presidential elections, and more recently the 2020 SolarWinds hack that compromised the supply chain and infiltrated US government networks. Other influential Russian operations to aid its political and expansionist geostrategic goals include a broad 2007 attack on the Estonian cyber grid that crippled both public and private organizations, a similar 2008 cyberattack

[3] Voo et. al, "National Cyber Power Index 2022."

[4] Andrew S. Bowen, "Russian Cyber Units," Congressional Research Service, updated February 2, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11718.

against Georgia, a 2015 attack on the power grid in Ukraine, a 2018 hack of a Saudi Petrochemical plant, and the 2017 NotPetya attack aimed at Ukraine, which paralyzed multinational companies and threatened global economic and political systems. Evidently, the Kremlin views the targeting of critical infrastructure and information environments in the United States and around the world as a key part of its cyber strategy for achieving its hegemonic aspirations.

Similarly, China's cyberthreats to the United States have relied on methods of espionage and information control, albeit with a larger focus on economic and industrial goals. Chinese President Xi Jinping has made it very clear that he plans to turn China into a "cyber superpower." The 2023 Annual Threat Assessment of the US Intelligence Community considers China the top cyber espionage threat to the American government and the US private sector, mainly due to its commitments to boost its indigenous commercial and military technologies to become self-sufficient and to continue to dominate global technology supply chains, and because of its growing dedication to information operations to shape public perception in the United States, spread Chinese propaganda, and undermine US leadership.[5] Commercial espionage in particular has become a trademark of Beijing's efforts to control the global economic environment through illegally acquiring technological and trade secrets and intellectual property.[6] Additionally, the Chinese Communist Party, through its Made in China 2025 plan, encourages private companies to develop dual-use technologies that can also be employed for military purposes.[7] Another major concern for the United States is China's attempts to politicize and take control over technical standards and protocols in order to dominate the global tech ecosystem, including by investing in a national standards strategy, pushing for membership and influence in standards development organizations like the International Organization for Standardization, and using its Belt and

[5] "Annual Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[6] Yudhijit Bhattacharjee, "The Daring Ruse That Exposed China's Campaign to Steal American Secrets," *New York Times Magazine*, March 7, 2023, https://www.nytimes.com/2023/03/07/magazine/china-spying-intellectual-property.html.

[7] Meia Nouwens and Helena Legarda, "China's Pursuit of Advanced Dual-Use Technologies," International Institute for Strategic Studies, December 18, 2018, https://www.iiss.org/research-paper//2018/12/emerging-technology-dominance.

Road Initiative to lock countries into its standards.[8] This is especially the case with the 5G wireless networks that provide the backbone for the next generation of connectivity, where Chinese company Huawei is leading the world in the race for 5G, having signed more 5G contracts than any company (including with European countries)—and this coming after it has already built 70 percent of the African continent's 4G network.[9]

Both Russia and China have recognized the importance of data and cyberspace in each country's competition with the United States and quest for global dominance. The more digitally connected society and governance become, the more susceptible they are to cyberattacks and information operations that can paralyze entire nations, compromise critical national security data and economic infrastructures, and change public opinion and the political landscape. As the opportunities and threats afforded by cyberpower are becoming apparent, states are racing to not only protect their national security but also to amass influence and control in the global digital ecosystem. In response, the United States is emphasizing the importance of cyber capabilities in its national security and defense strategies. For example, the Biden administration's 2022 National Security Strategy highlights the role of emerging technologies in the global political order and in geopolitical competition with major global powers.[10] However, cyberattacks appear to take center stage in the United States' concerns, as evidenced by the administration's Cybersecurity Strategy of 2023, which emphasizes cybersecurity components such as defending critical infrastructure and disrupting threat actors, investing in security and the resilience of data and systems, and forging international partnerships to counter cyberthreats and defend allies against them.[11]

Much of the United States' discussion about cyberpower is focused on the concept of cybersecurity, which involves defensive cyber tools to

[8] Tim Rühlig, "China, Europe and the New Power Competition over Technical Standards," Swedish Institute of International Affairs, January 2021, https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2021/ui-brief-no.-1-2021.pdf.

[9] David Sacks, "China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond," Council on Foreign Relations, March 29, 2021, https://www.cfr.org/blog/china-huawei-5g.

[10] "National Security Strategy," The White House, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[11] "National Cybersecurity Strategy," The White House, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

protect data and systems, cyber breaches to collect intelligence and information, and offensive cyber operations that cause harm and damage to rival governments' infrastructures. Understandably, Washington is especially prioritizing cyber defense and security capabilities with regard to Russian aggression, while at the same time focusing on containing China economically and decoupling it from the technology supply chain. However, this narrow focus on defense and cybersecurity underestimates the long-term impact of Chinese and Russian investments in the worldwide information environment and communications infrastructures. While the US is busy with its tech cold war with China and with Russia's conventional war on Ukraine, a different kind of cyber battle is emerging in the MENA region.

MENA: The Cyber Battleground the United States Is Losing

The tech ecosystem is rapidly evolving and emerging technologies will be the determining factor in strategic power competition, where control over information, access to data, artificial intelligence, and communication networks provide competitive advantages. Cyberspace in the Middle East and North Africa is a crucial battleground that both China and Russia are attempting to dominate. Both nations have been investing in long-term cyber strategies in the MENA region aimed at garnering influence and control and advancing their respective global and geopolitical agendas.

China's cyber strategy is being implemented through its Digital Silk Road (DSR), which is the technological component of its Belt and Road Initiative. By making the DSR one of its foreign policy priorities, Beijing is aiming to expand its digital footprint in the region and become the top technological global power, thereby amassing greater control over communication and data networks. Through the DSR, Chinese companies have built critical digital infrastructure across the MENA region, and Beijing has forged agreements with various countries there. The major components of this cyber architecture include memoranda of understanding (e.g., with Egypt, Saudi Arabia, and the UAE), comprehensive mass surveillance and Huawei's "safe cities" public monitoring projects, ICT training centers and labs, cloud services and quantum computing networks, subsea fiber-optic cables, 4G and 5G communication networks, and the BeiDou Navigation Satellite System, which is now more accurate in Asia than GPS.[12] Chinese

[12] Thomas Blaubach, "Chinese Technology in the Middle East: A Threat to Sovereignty or an Economic Opportunity?," Middle East Institute, March 2021, https://mei.edu/sites/default/files/2021-03/Chinese-Tech.pdf.

surveillance companies Hikvision and Dahua account for the production of almost 40 percent of surveillance cameras in the world, and comprehensive surveillance systems (including those using AI and big data analytics) have been sold to over 80 countries, including many in the MENA region such as the UAE, Morocco, and Lebanon.[13] When it comes to fiber-optics, HMN Technologies (formerly Huawei Marine Networks) is laying undersea fiber-optic cables to connect the Middle East with Europe and Africa as part of its Pakistan and East Africa Connecting Europe (PEACE) subsea cable. China is the fourth largest provider of international subsea cables, which transmit 95 percent of the world's data.[14] Huawei has also been developing the MENA region's 5G communication networks in eight countries, including the UAE, Saudi Arabia, Qatar, Morocco, and Egypt.[15]

As MENA countries plan to diversify their economies and embark on processes of digital transformation, China is taking advantage of this opportunity to take control over Arab technological infrastructures and the region's digital communications ecosystem. While many of the Chinese companies involved are private firms, their ties to the Chinese Communist Party present a significant concern. To be sure, Chinese companies are not the only ones with this level of control over communication and information systems, as American and other western companies also have large global market shares, but the close relationship between the Chinese private sector and the government, as well as China's laws, give the government greater control and access. These companies' access to massive amounts of data therefore grants Beijing unprecedented power and influence in the region. The Chinese government can use these tech networks to collect intelligence and monitor opponents, obtain intellectual property and trade secrets, and shut down entire communication channels and digital infrastructures to use them as leverage and implement coercive measures for strategic ends. Moreover, some analysts have referred to the affordability arrangements that Chinese companies provide to developing countries in exchange for supplying them with crucial technologies as debt traps, wherein an inability to pay results in the loss

[13] "Mapping China's Digital Silk Road," Reconnecting Asia, October 19, 2021, https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

[14] Ibid.

[15] Dale Aluf, "China's Tech Outreach in the Middle East and North Africa," *The Diplomat*, November 17, 2022, https://thediplomat.com/2022/11/chinas-tech-outreach-in-the-middle-east-and-north-africa/.

of critical infrastructure and a broader threat to national autonomy.[16] Such powerful control over the global tech ecosystem enables Beijing to become the global cyber power it envisions and to exert control over the international order to advance its political and economic interests.

While Russia has also invested in surveillance systems and exported them to some countries, including supplying the UAE's Oyoon surveillance system, it has primarily devoted its foreign cyber strategy to the arena of information operations, and especially cross-border political influence disinformation campaigns. Without a commercial tech industry and burdened by a weakened military in the post-Soviet era, Russia employs cyber operations as part of its great-power strategy to recover its global dominance. In the Arab world, Russia began waging a systematic disinformation war and deploying Arabic-language propaganda operations even prior to the Arab Spring uprisings of 2011, efforts that were led by the launch of *RT Arabic* (formerly *Russia Today*) in May 2007.[17] Today, the Kremlin operates a large network of Arabic media outlets and social media campaigns using bot factories and troll farms to spread Russian propaganda and anti-American content in the Arabic-language digital sphere. Narratives on social media platforms and those coming out of Russia's state-funded media outlets, such as the various outlets of *RT Arabic* parent company RT and the news agency *Sputnik*, aim to manipulate public opinion about the United States and the West and control current narratives, especially regarding Russia's war on Ukraine. The Russian playbook frames the war as one that challenges US imperialism and counters both encirclement by NATO and the American-led hegemonic global order. Russian media outlets have even propagated false claims, including a statement that Ukrainian President Volodymyr Zelenskyy had fled the country and conspiracy theories about the existence of secret laboratories for biological weapons in Ukraine. Another critical part of Russian cross-border political influence operations involves orchestrated social media campaigns in support of the Assad regime in Syria and military leaders in Libya and Sudan.[18]

[16] Blaubach, "Chinese Technology."

[17] Elene Janadze, "The Digital Middle East: Another Front in Russia's Information War," Middle East Institute, April 19, 2022, https://www.mei.edu/publications/digital-middle-east-another-front-russias-information-war.

[18] "Evidence of Russia-Linked Influence Operations in Africa," Stanford Internet Observatory, October 30, 2019, https://cyber.fsi.stanford.edu/io/news/prigozhin-africa.

Russian government perspectives are pervasive in the Arabic-language media sphere. Some evidence shows that *RT Arabic* ranks among the top three most watched news outlets in several Arab countries, and both *RT Arabic* and *Sputnik* have been found to post significantly more content on social media platforms than other major media outlets, thus flooding the Arabic-language digital sphere with the Kremlin's narrative.[19] Public opinion polling suggests that these information operations may be working. For example, according to the UAE-based Arab Youth Survey, young Arabs believe that the United States and its NATO allies are more to blame for the Ukraine war than Russia.[20] Multiple factors contribute to the success of Russian disinformation campaigns and help its information warfare rank among the world's most effective. First, Russian operations exploit existing sentiments and societal divides and employ them to augment its chosen narrative, often cloaking said narrative in supposedly authentic indigenous voices. For example, Russia builds on extant anti-American views and the history of the United States' failures and war crimes in the MENA region to demonize the United States and present itself as an anti-imperialist power fighting both US and broader western hegemony. Second, the Kremlin's information warfare strategy is premeditated, long-term, and ongoing, as it does not make a distinction between times of peace and times of war. Equally important is the lack of credible information sources in the MENA region's state-controlled media environment and the overreliance of a primarily young population on social media platforms for news and political engagement. Furthermore, social media platforms by design elevate and amplify extreme, unexpected, and inflammatory content and create online echo chambers and ideological silos that continue to perpetuate these disinformation campaigns.[21] Importantly for the United States, there is a severe lack of counternarratives in the Arabic-language digital environment to confront Russia's information campaigns in the MENA region, part of an information vacuum that Moscow has successfully exploited to win the hearts and minds of the Arab people. Control over the information ecosystem allows Russia to shape not only opinions but ultimately events on the ground.

[19] Janadze, "The Digital Middle East."

[20] "14th Annual ASDA'A BCW Arab Youth Survey," BCW Global, September 21, 2022, https://www.bcw-global.com/newsroom/global/14th-annual-asdaa-bcw-arab-youth-survey.

[21] Tamara Kharroub, "Identity Politics 2.0: Cyber Geopolitics and the Weaponization of Social Media," Arab Center Washington DC, June 1, 2019, https://arabcenterdc.org/resource/identity-politics-2-0-cyber-geopolitics-and-the-weaponization-of-social-media/.

Data and Connectivity Represent Power

While information and military technology have always been an important part of warfare, the evolution of cyberpower has no doubt significantly enabled China and Russia to rise on the world stage, to reemerge as serious threats to the US, and to expand their global influence. Both Russia and China are flexing their cyber muscles in the MENA region, and Washington should not underestimate the power that technological infrastructure and information hold for determining the future of the Middle East. As the United States moves forward with recalibrating its policies and strategies in the Middle East to prioritize the Abraham Accords, security alliances with oppressive and authoritarian regimes, and cybersecurity collaboration, it is losing the long-term cyber war in the region.[22] While it is true that both Russia and China are signing cyber agreements to support Iran's cyber capabilities and are helping Tehran build its cyber strategy and offensive technologies, a narrow US focus on the MENA region using the lens of an Iran-deterrence security strategy does not match up with the region's rapidly evolving technological ecosystem.

As the US intelligence community continues to prioritize espionage operations and cyberattack threats to American national security, the United States is underestimating the power and long-term impact of China and Russia's expanding investments in information and technology infrastructure around the world, and especially in the MENA region. Such heavy foundational operations undermine US influence and power, as Russia and China aim to set telecoms standards, control the information environment, and secure a monopoly over telecommunications infrastructure and data facilities. Data is a source of power, and increased connectivity brings additional layers of vulnerabilities that can be exploited for espionage, cyberattacks, sanctions, and shutdowns. The United States' overemphasis on security in the region and its miscalculations regarding the power of information and telecoms infrastructure risk it losing not only the cyber war but its ongoing great power competition as well.

To be sure, MENA countries, especially in the Gulf, are forging their own cyber strategies. States like Saudi Arabia and the UAE are emerging as regional (authoritarian) digital powers by leading disinformation

[22] On cybersecurity alliances under the Abraham Accords, see: Ines Kagubare, "US, Middle Eastern Allies Include Cyber Collaboration in Abraham Accords," *The Hill*, January 31, 2023, https://thehill.com/policy/cybersecurity/3838236-us-middle-eastern-allies-include-cyber-collaboration-in-abraham-accords/.

campaigns and political influence operations, obtaining and implementing large-scale surveillance systems, investing in smart cities and tech capabilities, passing laws that protect their data sovereignty, and harnessing AI, predictive policing, and spyware programs. Non-Arab MENA countries like Israel, Iran, and Turkey remain the largest cyber powers in the region, with extensive cybersecurity and cyberattack capabilities. But China and Russia are far ahead of the competition, representing the most capable cyber powers in the world after the United States. As part of their respective great-power strategies, they will continue to jockey for influence and control over both global and MENA cyberspace and to dominate the region's information and technology infrastructures for decades to come.