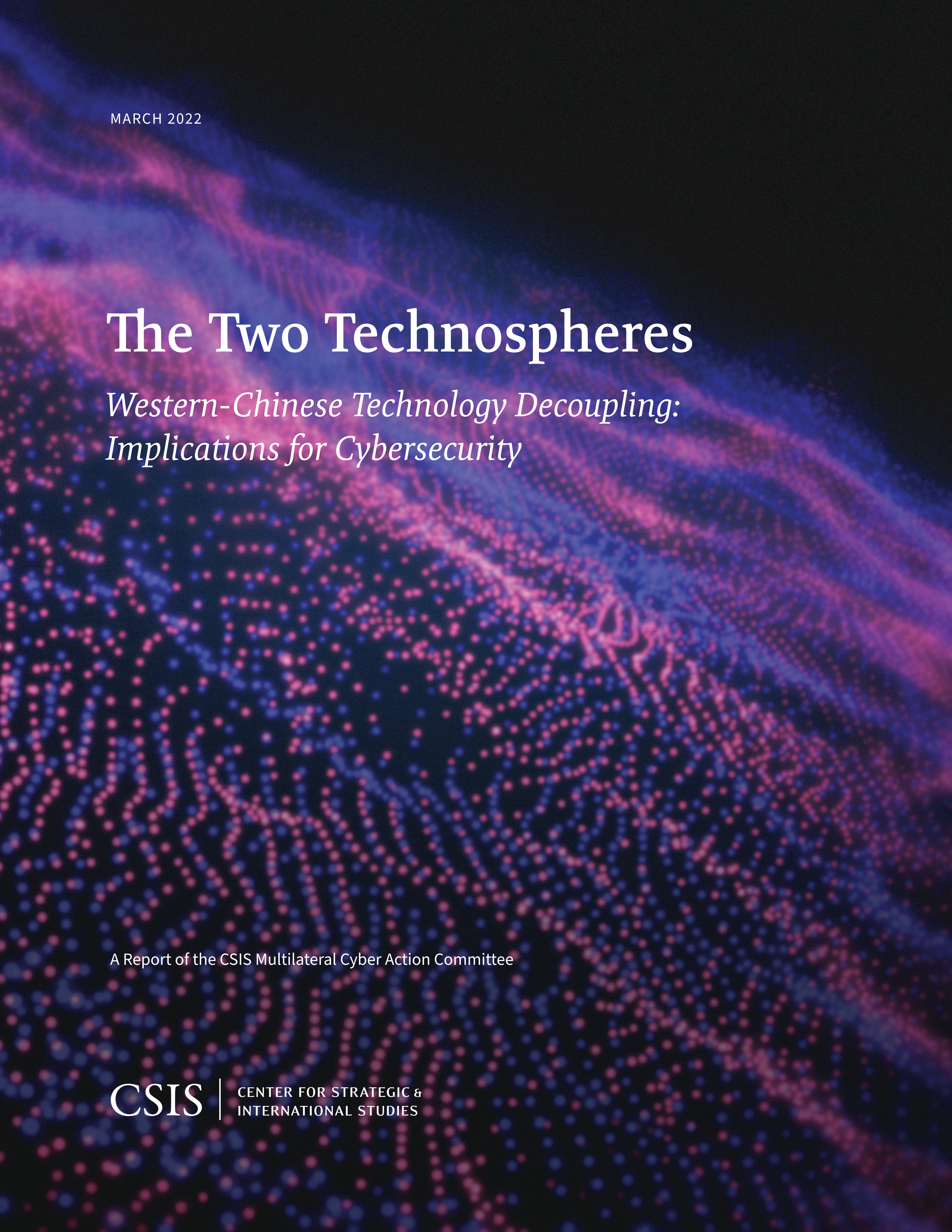


MARCH 2022

The Two Technospheres

Western-Chinese Technology Decoupling: Implications for Cybersecurity

A Report of the CSIS Multilateral Cyber Action Committee

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

MARCH 2022

The Two Technospheres

Western-Chinese Technology Decoupling: Implications for Cybersecurity

A Report of the CSIS Multilateral Cyber Action Committee

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

CSIS Multilateral Cyber Action Committee

Steering Committee

Dennis Blair
Former U.S. Director of National Intelligence

Michael Chertoff
Former U.S. Secretary of Homeland Security

Art Coviello
Former CEO, RSA

Timo Koster
Former Ambassador, Dutch Ministry of Foreign Affairs

Ciaran Martin
Professor, University of Oxford; Former CEO, UK National Cyber Security Centre

Kazuo Noguchi
Senior Researcher, Keio University

Executive Directors

James Lewis
Senior Vice President and Director of the Strategic Technologies Program, Center for Strategic and International Studies

Gregory Rattray
Cofounder, Next Peak; Former Chief Information Security Officer, JP Morgan Chase

Members

Isaac Ben Israel
Director, Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University

Niloofar Howe
Senior Operating Partner, Energy Impact Partners; Board Member of Morgan Stanley, Recorded Future, Dragos, and Tenable

Toomas Ilves
Former President of Estonia

Hiroshi Ito
Former Commander, Cyberwarfare, Japan Self-Defense Forces

Nobukatsu Kanehara
Former Deputy National Security Advisor of Japan

Sir Julian King
Ambassador to the United Kingdom; Former European Commissioner for the Security Union

Tzipi Livni
Former Minister of Justice of Israel

Stuart McClure
Founder and CEO, Cylance

James Mulvenon
Director of Intelligence Integration, SOS International; Chairman of the Board, Cyber Conflict Studies Association

Craig Mundie
Former Chief Research and Strategy Officer, Microsoft

Jun Murai
Distinguished Professor, Keio University

Masanori Nishi
Former Administrative Vice Minister of Defense of Japan

Junishi Nishiyama
Former Deputy General Manager, Mitsubishi Heavy Industries

Pamela Passman
Senior Associate (Non-Resident), Center for Strategic and International Studies; Chair, APCO Worldwide

Satoru Tezuka
Professor, Keio University

Staffan Truvé
Cofounder and Chief Technology Officer, Recorded Future

Jamie Saunders
Former Director of International Cyber Policy, UK Foreign and Commonwealth Office

Martin Schallbruch
Former Chief Information Officer, Government of Germany

Hideaki Watanabe
Former Facility and Procurement Head, Japanese Ministry of Defense

Christy Wyatt
President and CEO, Absolute Software

Sir Alex Younger
Former Chief of UK Secret Intelligence Service

Staff

Ian Pelekis
Program Coordinator

Acknowledgments

The authors of this report would like to thank the individuals from government, the private sector, and the cybersecurity community who gave the research team their time and insight in a series of workshops carried out as part of this project. Many of these individuals also participated in a workshop held to discuss this project's findings. These engagements provided significant insight into the technology decoupling issues explored by the Multilateral Cyber Action Committee and faced by the Western technology community, allowing the research team to derive fruitful findings to guide recommendations.

This CSIS report was made possible by the generous support of Tenable.

Contents

Executive Summary

The divergence of the Western and Chinese technospheres is a critical driver of cybersecurity concerns requiring the attention of both governments and the private sector around the world. During a survey of existing literature and a series of hosted workshops on this issue, the Multilateral Cyber Action Committee (MCAC) has not only assessed existing initiatives and studies, but also brought forth new recommendations. This MCAC report focuses on the growing cybersecurity implications of the Western-Chinese technology decoupling. In competition with Western nations, China has led in driving digital technology advancements across the globe. The rise of Chinese technological prowess comes at a time of rising geopolitical tensions made worse by growing Chinese power and aspirations, an increasingly divided Europe, and a United States in political turmoil. As cybersecurity is a central aspect of global affairs, the implications of the emergence of two separate technospheres have received much attention.

The origins of the initial technosphere were in Western nations, dominantly in the United States. This sphere grew organically, fostering innovation and competition without significant national-level coordination. As a result, differing approaches and incentives exist in key areas between Western nations. Now, China seeks to evolve a technosphere from the original foundations that provides an alternative related to products, services, and governance. China is consciously seeking to co-opt nonaligned nations around the globe to align with its technosphere. Western nations have a challenge and a choice regarding collaboration as they seek to engage with nonaligned nations in this realm.

The MCAC seeks to build on three recommendation areas from existing analysis and initiatives:

- Strengthen international cybersecurity norms focused on promoting transparency and impose consequences for malicious transgressions of these norms to ensure the global operation of the internet core

- Promote global standards for data connectivity focused on establishing operational approaches to allow cross-border data flows while ensuring security and privacy
- Foster an environment for continued Western leadership in critical technologies, including 5G systems and artificial intelligence, to ensure trust and security across the globe

Based on a series of hosted workshops, the MCAC recommends two additional areas for action:

- Enhance cybersecurity collaboration at the operational and technical levels among Western governments and private-sector partners to help deter and disrupt malicious actors and activities
- Strengthen long-term focus and collaboration on technology transparency, a fundamental Western advantage that can counter the growth of a Chinese-led technosphere in markets and governments around the world

While the MCAC inherently believes in the value of a global, open, interconnected cyberspace, geopolitical tensions will likely continue to drive a divergence of the two technospheres. Western nations should act now to mitigate the growing cybersecurity risks posed by this decoupling.

Introduction

Decoupling of digital innovation, systems, and data flows between Western nations and China is a global issue with high potential to destabilize cyberspace and increase risks in the digital world.[1] A global, open, safe, and secure cyberspace remains an aspiration that could empower economic growth, innovation, and social exchange. However, digital decoupling—defined as the separation of certain technology endeavors into two distinct and separate branches that can technically connect but impose legal and practical limits on interoperability—is leading to the establishment of two "technospheres."[2] This decoupling is accelerated by differences in language, standards, and regulatory frameworks. Among Western countries, its effects vary due to differing views on critical issues such as data privacy, innovation policy, and trade.

The growing presence of two distinct technospheres, one driven by China and the other by companies and governments in Western nations, has become a central aspect of managing national and global cybersecurity, also affecting economic competition, trade, and geopolitics. The MCAC assessed the effects of decoupling of the two technospheres, concluding that they are increasingly disconnected and suspicious of each other's technologies, with each seeking to create greater advantages in cyberspace and technology competition to protect and grow its own reach. This competition creates an increasingly complicated, inefficient, and risky digital world for governments and private enterprises alike.

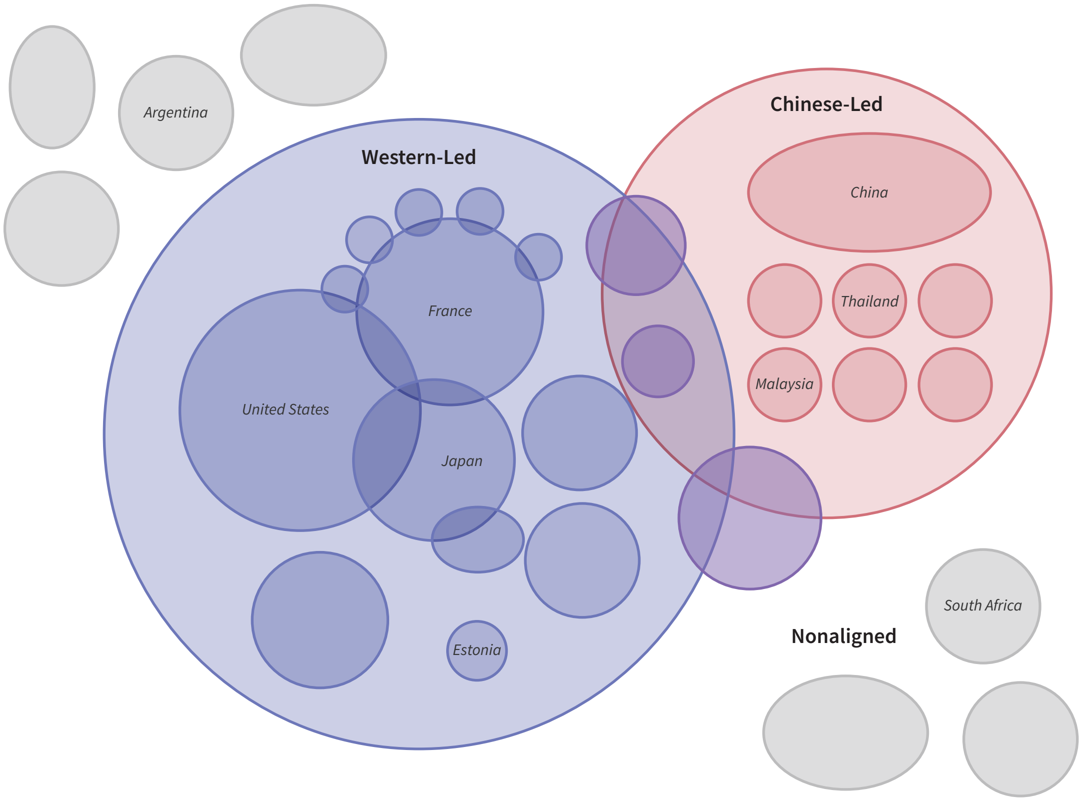
The MCAC promotes recommendations from previous studies and initiatives, as well as from its own investigation, to help guide collaboration where possible and mitigate cyber risk where necessary. The need for prescriptive, actionable recommendations motivated the MCAC to solicit direct experiences from organizations seeking to conduct business and operate across the technospheres so it could understand existing challenges and opportunities. The MCAC recommends five focus areas for increased collaboration and investment by Western nations. Additionally, the MCAC believes that the new recommendations focused on the two technospheres are also applicable to broader global cybersecurity challenges.

Study Scope and Approach

The MCAC has endeavored to assess the degree to which the two technospheres are decoupling and its implications at the enterprise, national, and global cybersecurity levels. The MCAC builds upon the findings of previous initiatives, adding the committee's insights to create actionable recommendations to mitigate the cybersecurity risks generated by technology decoupling. In addition to surveying existing activities, initiatives, and reports, the MCAC hosted workshops with leading outside experts to better understand the business and cybersecurity implications of technology decoupling. The MCAC focused on three types of industries: automotive manufacturing, the financial sector, and the information and communications technology (ICT) sector. Experts included both academic subject-matter experts and private-sector representatives experiencing the effects of technology decoupling firsthand. The MCAC examined Western (primarily U.S.) companies operating in China during the first workshop and turned its attention to Chinese companies operating in the United States during the second workshop. The MCAC, as noted above, recognizes the limits to this analysis, which does not capture the diverse range of Western experience in China nor of Chinese companies in the wide variety of Western states. For the MCAC workshop's findings, refer to the report appendix.

"Technology decoupling" is commonly used to describe the phenomenon of increased separation of two technology ecosystems, one driven by China and the other by Western nations, potentially decreasing global technological interdependence and interaction.[3] Decoupling has various facets, including increased geopolitical and economic competition, trade decoupling of supply chains and critical inputs, innovation decoupling of research and development (R&D), and digital decoupling of data governance, network standards, and telecommunications services.[4] The MCAC acknowledges that decoupling is occurring at multiple levels but focuses on digital decoupling as the most impactful on cybersecurity. The MCAC has specifically focused on risks to a safe cybersecurity environment that enables digital innovation and companies' global operations. The broader issues of geopolitical, economic, and trade competition are not central to the study, but the committee did seek to understand their intersection with cyber and digital security concerns. While the MCAC values intellectual property and wishes to enforce norms to protect it, this issue is also outside the scope of the report. The MCAC did address the key role technology innovation plays in the evolution of the global cybersecurity ecosystem.

Technosphere Structure

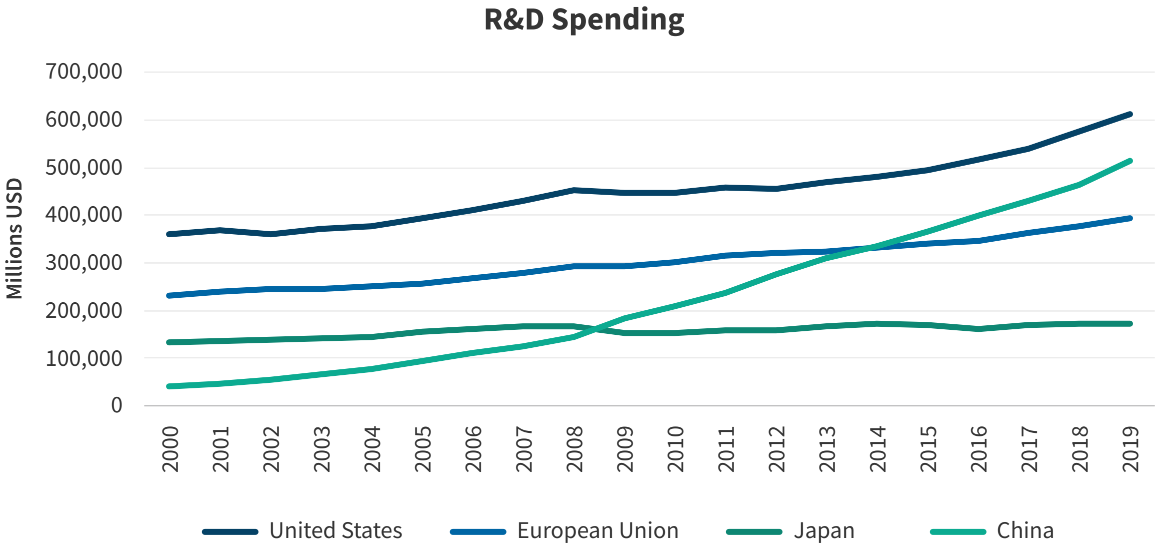


The Chinese-led technosphere emerged from the global technosphere, a primarily Western-driven ecosystem with limited coordination but shared values. As China separated, it created a top-down model for providing data and information controls, regulations, and policies. Many countries are caught between both spheres or remain unaligned to either.

Source: Based on MCAC members' analysis.

The MCAC recognizes that regions and countries in the West experience technology evolution differently. The committee seeks to identify concerns that impact all multilateral stakeholders; for instance, technology decoupling intersects with key issues such as trade, privacy, and innovation policy. MCAC recommendations call for joint government and private-sector actions, understanding that specific actions and implementations will differ depending on regional and national contexts and recognizing the differing intersections with and stances surrounding these key issues.

With respect to trade, the United States, Europe, and Japan have adopted varied stances. Under the Trump administration, the United States tried to link multiple aspects of competition, for example by connecting trade issues concerning soybeans with security issues surrounding fifth-generation (5G) network supply chains. This approach has made it more difficult for allies to understand U.S. priorities and how it will pursue competition with China. The United States now appears to be more coherently asserting a competitive approach across a broad front that seeks to include other Western nations. European nations, to varying degrees, are less inclined to subordinate economic opportunities. The European Union sees China as both a valuable trading partner and a systemic rival, and individual member states are trying to balance between the two. Japan, alternatively, seeks to align its strong national security concerns with those of the United States and the European Union. However, Japan's trade and manufacturing model has recently shifted to providing products for Chinese consumption while ensuring global supply chains can be decoupled. Most Japanese companies have the stance of "when in Rome, do as the Romans do," seeking to keep advanced intellectual property within the country and separating information systems when working with foreign partners while diligently following local regulations and business customs.



Source: "Gross Domestic Spending on R&D," OECD Data, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm.

Divergence over data-privacy issues also intersects heavily with technology decoupling. Europe has focused on government-led efforts to protect personal privacy, regarding data privacy as a fundamental right and issuing strong privacy regulations in the form of the General Data Protection Regulation (GDPR). EU efforts to enable a "digital single market" and recent European Digital Identity and digital wallet proposals provide examples of this mindset. Japan has also taken an approach that enables global digital interconnectivity and trade, promoting "data free flow with trust" (DFFT), an architecture for international cooperation on data flows between governments and businesses.[5] Furthermore, Japan and the European Union are working together on data-privacy regulations, seeking to establish strong standards to be supplemented by operational and technical approaches across Western nations. The joint EU-Japanese Pilot for the International Compatibility of Trust Services (IMRT)—which references electronic identification, authentication, and trust services (eIDAS) regulations[6]—aims to ensure that people and businesses can use their own national electronic identification schemes to access public services across borders. Cross-functionality has the added benefit of creating an internal trusted market for services, as all participating companies in these nations must follow the regulatory framework. The United States has generally been less active regarding private-sector data protection, though stances within the country on data privacy are changing; the California Consumer Privacy Act (CCPA) passed in 2018, and many industry organizations are pushing for the implementation of national data-protection and breach-notification laws. U.S.-based global companies have worked to meet other jurisdictions' data-protection standards, though with only partial success, as European governmental and regulatory scrutiny of U.S. tech companies continues to increase.[7]

Western stakeholders often differ greatly on innovation policy and the use of national champions. The United States has historically avoided promoting national champions, allowing global technology leaders to operate with little regulation. However, lack of coordinated Western prioritization of leadership in key areas of innovation has created major opportunities for a rising China to pursue its national strategy to gain greater access to global markets—even market dominance. Additionally, Western reliance on an international supply chain that heavily uses Chinese technology and products, for example semiconductors and 5G technology, has created security risks. These issues have motivated calls for a national innovation policy and government support for Western-sourced components in strategic industries. Japan is seeking to discover its twenty-first-century niche in collaboration with Western partners, hoping to identify strengths before committing to innovation policies. Part of this effort is reflected in Japan's Digital Agency, established on September 1, 2021, to help guide direction for innovation policy. With limited government and private-sector resources compared to the United States, Japan is focusing on a small number of joint innovation projects with Western partners to revitalize critical semiconductor technologies, develop quantum computing and cryptography, build 6G networks, and secure undersea cables.[8] The European Union has often championed national companies, yet European technology providers such as Nokia and Ericsson are not providing effective alternatives in the global 5G competition. However, technology decoupling is not simply an issue of China not cooperating with the West. The European Union itself is not fully united and has concerns about U.S. technology-platform dominance. Similarly, the United States is politically fragmented, and tensions exist between parties on important issues.

Emerging technologies simultaneously affect decoupling and global cybersecurity outcomes, regardless of differing national stances on individual issues. As new technologies emerge and become commonplace in industry—such as the internet of things (IoT), artificial intelligence (AI), machine learning (ML), and quantum computing—new market leaders will arise to provide competitive edges to each technosphere. Unfettered competition between the spheres has the potential to create new vectors for offensive cyber operations; and as the spheres become increasingly distinct, potentially creating a clearer "frontline" in the digital domain, belligerents could have less reason to display restraint in cyberspace. While emerging technology and global markets will affect cybersecurity outcomes in the face of decoupling, the MCAC notes that cybersecurity will remain an issue regardless. In a decoupled world, the internet and other digital lines of communication will continue to exist across the two spheres. The recommendations the MCAC makes in this report for increasing global cybersecurity are affected by decoupling but will not be solved by mending decoupling. As the balance and distance between the technospheres varies, so too will the related cybersecurity risks.

As the MCAC issues this report, the Russian invasion of Ukraine is ongoing. As this crisis unfolds, choices by the West and China may well also have an impact on the evolution of the two technospheres. The rapid coalescence of Western sanctions and other actions against Russia include cutting off access to advanced digital technologies. How China will react to the crisis and make decisions about its ties with Russia, including in the technosphere realm, is not yet clear. Chinese decisions to align more closely with Russia and Western reactions to such developments could accelerate technology decoupling and the impacts described in this report

Yet, the MCAC firmly believes that, in many ways, there is a fundamental convergence of interests among Western nations regarding the challenges posed by the emergence of the two technospheres. As the divergence of the technospheres continues, the MCAC has identified cybersecurity challenges at the national and global levels. The report further notes that although a future without these separate technospheres is more desirable, divergence is increasing. Given this dichotomy, any opportunities to build bridges between the technospheres and ensure Chinese participation are welcome and encouraged. Models for decelerating decoupling already exist. For example, the Regional Comprehensive Economic Partnership (RCEP), a free trade agreement bringing together the members of the Association of Southeast Asian Nations (ASEAN) and five regional partners, has come into effect in January 2022.[9] This agreement includes both China and Western-oriented countries such as Australia, Japan, and Canada, providing an example of a forum in which constructive dialogue can occur. The United States and China are also working to maintain a constructive dialogue, as displayed by the virtual meeting between President Joe Biden and President Xi Jinping on November 15, 2021, in which both leaders discussed the complex nature of relations and how to manage competition responsibly.[10] While these opportunities exist, recent government behavior indicates a push for further technology decoupling—but the future may still hold opportunities for Western nations to open the door for China to join multilateral frameworks.

While the impact of decoupling on cybersecurity and conflict dynamics is inherently intertwined with geopolitical, economic, and national security factors, the MCAC has identified the following four effects of decoupling that are of greatest cybersecurity concern to Western countries and companies:

- **Increased costs and difficulty for Western companies seeking to operate in China of managing supply chains due to regulation and the increased chance of malicious cyber activities.** Western companies operating in China are facing increased cybersecurity risk from intrusive regulations for foreign entities and from cyber operations against them, which are enhanced due to geographic and supply-chain access. Mitigating these costs leads Western companies to invest heavily in cybersecurity measures that are, for the most part, ineffective when operating in geographic areas with a Chinese-based technology stack. These risks and associated costs have caused many Western companies, particularly in the technology sector, to withdraw from operating in China. Many of the companies still operating there have chosen to use local technology stacks while in the country. Both these factors contribute to decoupling, as Western tech companies no longer work with Chinese partners, and companies continuing to operate in China have decoupled technology stacks.
- **Increased global restrictions on secure data flows both in and out of China and among Western countries as data becomes the fuel for AI and economic growth.** A major contributing factor to decoupling is the increasingly restrictive data-flow regulations that compromise the integrity of communications in and out of China. New Chinese regulations mandate that all data must pass through Chinese service providers who must, in turn, provide access to Chinese authorities. This imposes high costs on Western companies, which need to segment networks carefully and

be particular about which data is housed and transferred to entities in China, as well as blunts their competitive edge when operating in China. Additionally, these companies may not be able to provide the privacy and data protection sought by governments and companies. Rather than comply with Chinese regulations, many entities have chosen to withdraw from operations in China, further exacerbating decoupling.

- **Increased potential for Chinese technology dominance in the nonaligned world, which poses an increased cybersecurity risk to Western governments and companies operating globally.** Chinese technology solutions have become ever more present in nonaligned countries, including in the Middle East, South Asia, and Africa. As technology stacks become increasingly decoupled and less interoperable, it is more possible that a majority of global markets will align with a Chinese-led technosphere. If growth of a Chinese-led technosphere continues, Western governments and companies will discover that the number of high-risk environments for their operations will similarly increase because they will be more likely to encounter Chinese technology stacks abroad.
- **Increased difficulty of establishing and enforcing global cybersecurity norms that foster both security of global digital systems and economic growth.** As the technospheres grow further apart, so will the norms and standards that foster the health of the digital ecosystem. Consensus will not only become more difficult to create but also less relevant. As two spheres emerge, there is a high probability that each sphere will have distinct sets of norms and enforcement mechanisms, often at odds with each other. Furthermore, while some measures may be agreed upon in areas such as cybercrime, ransomware, ATM theft, and child pornography, enforcing norms will be increasingly difficult once certain malicious actors are out of reach of authorities in the other sphere. For example, cyber-criminal groups in opposing technospheres may feel an added layer of protection when targeting organizations across spheres because jurisdictional boundaries, enforcement authorities, and technology stacks are separate.

Recommendations

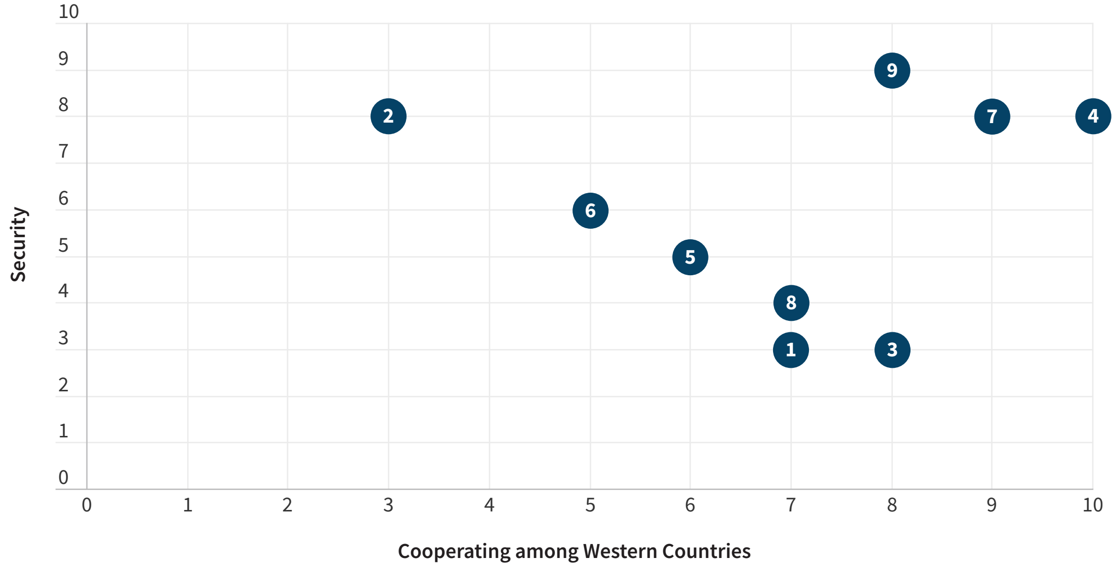
Considering the associated challenges to cooperation and security that both the United States and China are facing, the MCAC set out to evaluate existing recommendations from numerous studies and initiatives to mitigate the growing cybersecurity concerns arising from technology decoupling.

Building On Existing Insights

The MCAC makes three recommendations for mitigating cybersecurity risks, supporting those promulgated by existing initiatives and studies:

1. **Strengthen transparency and consequences for violating international cybersecurity norms.** Calls for strengthening international agreements on cybersecurity have existed for over 20 years, with efforts already underway to establish common global norms. The MCAC believes norm setting is an invaluable step in mitigating risks generated by technology decoupling and can help pave the way for cooperation within the international community. However, there need to be practical measures to coordinate efforts of norm-setting groups, as well as organizations and forums focused on norms enforcement. Seeking accountability in cyberspace can greatly enhance cybersecurity norms. For example, using the private sector's technical resources and data to identify events and transgressions that cause harm to digital infrastructure stability or users—and to push governments to act in response to these transgressions—can greatly enhance stability in cyberspace.

Recommendation Ranking from External Sources



1. Promote greater technology openness, interoperability, and standardization among countries
2. Double down on globalization to support a U.S. high-tech industry
3. Promote U.S. technology in global markets to gain competitive edge over competition
4. Form new defense organizations and alliance networks for cybersecurity
5. Seek out leadership roles in development of new tech and standards
6. Designate a lead federal agency to coordinate ICT supply-chain risk-management efforts into a cohesive strategy and act as a liaison for public-private partnerships
7. Prioritize the creation of objective standards and rules for data security, platform regulation, and digital connectivity
8. Promote innovation within the Western industrial base and cut back regulations, policies, and processes that stifle industry growth
9. Assess implications of decoupling where there are interdependencies between the West and China, and work together to create regulatory frameworks to allow for flexible architecture

This graph summarizes existing recommendations and ranks their effectiveness by increased security and increased cooperation.

Source: See Appendix 2 for list of existing recommendations and complete sources.

Key initiatives focusing on strengthening international cybersecurity norms that could mitigate the effects of decoupling include:

- *The Paris Call for Trust and Security in Cyberspace:* In 2018, a joint private-public effort bringing together stakeholders from across cyberspace called for actors to work together to adopt responsible online behavior and implement principles that apply in the physical world.[11] The Paris Call's ninth principle specifically urges the international community to promote the widespread acceptance and implementation of norms and responsible behavior in cyberspace.
- *The UN Open-Ended Working Group (OEWG) on Information and Telecommunications (ICT) in the Context of International Security:* The OEWG on ICT published its final report by consensus in March 2021, in which it promoted norms of responsible state behavior in cyberspace, recommending 11 voluntary, non-binding norms.[12]
- *The Global Commission on the Stability of Cyberspace (GCSC):* The GCSC has promoted norms as a foundational element of maintaining stability in cyberspace, publishing a

> final report in 2019. The commission specifically believes that responsibilities should be imposed on non-state actors, as they play a critical role in taking affirmative action in cyberspace. It promotes a wide set of norms, including non-interference with the public core of the internet, protection of electoral infrastructure, not tampering with ICT products in development, not commandeering ICT devices for use as botnets, creation of a vulnerability equities process, reduction and mitigation of significant vulnerabilities, implementation of basic cyber hygiene for defense, and prevention of offensive cyber operations by non-state actors.[13]

Building on these efforts, the MCAC specifically advocates establishing operational mechanisms to identify malicious activities that transgress these norms and forums to hold actors committing such transgressions internationally accountable. The CyberPeace Institute, announced during the Paris Peace Forum and established in November 2018, seeks to leverage the data and technological expertise present among participating private-sector organizations to help make transgressions more transparent. Its initial report, Playing with Lives: Cyberattacks on Healthcare Are Attacks on People, provides an example of the role such a private-sector body can play.[14] The private sector has similarly been involved in calling for the establishment of norms. Scott Charney at Microsoft has called for the creation of cyber norms for government actors.[15] His paper highlighted the need for such a framework, as private-sector actors lack the authority to engage in the legalistic regimes of governments yet are affected by government-led malicious activity in cyberspace. Additionally, with countries unsure of how cyberattacks may impact the full cyber ecosystem, a set of norms is necessary to help mitigate the associated risks. Moving beyond the efforts of the United Nations and others to articulate norms, the international community should seek to establish an approach for operational monitoring and identification of responsibility for transgressions. Furthermore, the MCAC envisions an organizational body—which is comprised of public- and private-sector actors with open-ended membership, hosts regular meetings, and has a dedicated staff—that will impose accountability and consequences on those who violate norms.

The MCAC recommends developing a spectrum of consequences like-minded nations can utilize in the event of transgressions. Although norms are voluntary, like-minded countries do have the ability to come together to impose consequences, whether these involve "name and shame" tactics, implementing economic sanctions, or seeking joint action to disrupt cyberattack infrastructures. For example, such mechanisms could be used to enforce already agreed norms like the non-interference with the public core of the internet, which protects both digital and physical network assets such as the domain-name system and undersea internet cables.

Seeking to ensure that those who commit transgressions suffer consequences may involve coercive action but can also offer a distinct opportunity for bridge building and cooperation between the technospheres. Multiple areas of cooperation and aligned visions exist in cyberspace between the West and China, for example regarding cybercrime, ransomware, ATM theft, and child pornography. While provisions for combating cybercrime are embedded in domestic laws in China and Western countries, the committee further hopes that common expectations regarding prosecution and punishment of transgressions can be promoted through law-enforcement collaboration and shared legal practices. Creating legal frameworks that promote collaboration and an associated spectrum of consequences for responding to cyber-criminal acts and actors, including China, can provide a forum for communication and bridge building. To find consensus, it may be necessary to separate efforts to create such a framework to address cybercrime with Chinese participation from efforts to address nation-state transgressions.

Such efforts can be modeled on existing frameworks in other realms. One approach could look to the International Observatory of Human Rights, which provides a forum for like-minded nations and nongovernmental organizations (NGOs) to communicate and condemn violators of human rights norms. While the organization would likely initially be comprised of Western governments and private-sector partners, a forum focused on providing transparency to uphold cyber norms could be open to any nation or partner willing to foster the norms established by the United Nations and other initiatives. The idea of a "T12" group of techno-democracies—which would be an informal group of states, rather than a formal alliance or international organization—is an alternative possible model under which to gather Western nations and private-sector partners.[16] A more intrusive approach at the government level could be modeled after the International Atomic Energy Agency's enforcement of the Non-Proliferation Treaty—in which the agency uses reporting and access requirements to gather information and make strong assertions about transgressions so it can hold nations accountable to their commitments—enabling members of an operational intergovernmental body to seek action.

2. **Promote global standards for data security and digital connectivity.** The MCAC strongly supports calls for setting global standards for data security and digital connectivity across the world. Common standards have the potential not only to mitigate cyber risk but also to provide a strong unified base from which to engage with China on mitigating the effects of technology decoupling.

   Key initiatives and reports focusing on the promotion of global standards for data security and digital connectivity that will mitigate the cybersecurity impacts of decoupling include:

   - *The Mercator Institute for China Studies (MERICS):* A 2021 MERICS report sponsored by the EU Chamber of Commerce in China assessed the calls for aligning data-governance models to ensure privacy and security while enabling management of data transfer across borders. Addressing like-minded democratic states, MERICS advocates launching pluralistic negotiations to set robust standards for data security and platform regulation.[17]

   - *The Center for Strategic and International Studies (CSIS):* Inspired by then prime minister Shinzo Abe's call for worldwide data governance during the 2019 Osaka Group of Twenty (G20) summit, CSIS created a set of data-governance principles for use by G20 member states. Principles include ensuring the interoperability of digital systems around the world and their compliance with global standards, holding data processors responsible for the security and integrity of data and digital systems, and discouraging data practices that serve as barriers to open competition.[18]

   - *EU electronic identification, authentication, and trust services (eIDAS):* In 2019, the European Union put in place a regulatory framework to oversee electronic identification and trust services, setting standards at an operational and technical level on how to conduct business online and create a trusted internal market. eIDAS encourages transparency and interoperability, promoting trust and connectivity among EU members. Japan is working with the European Union, as discussed above, to adopt eIDAS and the General Data Protection Regulation (GDPR), and the United Kingdom has also adopted eIDAS regulations, indicating the potential for establishing common standards in the digital world.

The MCAC will specifically build on these efforts by seeking the adoption of a standards and operational frameworks for data governance, connectivity, and digital privacy among Western nations willing to participate. Efforts to create data security and privacy norms among Western nations should include the establishment of a joint organization that aims to institutionalize operational processes and practices, building on such efforts as the Japan-EU mutual recognition agreement (MRA) on trusted services. The pilot project between the European Union and Japan, initiated in October 2020, focuses on creating best practices for technical requirements for trust building.[19] Efforts are aimed at the private and civilian sectors to ensure a trusted and secure digital market.

3. **Foster an environment for continued Western leadership in critical technologies.** China has developed and successfully implemented strategic planning around critical and emerging technologies, as well as identified key strategic dependencies. Successful strategic planning has enabled many of China's leaps in technological progress over the past decade in important areas such as 5G networks, AI/ML systems, and electric vehicles. Existing stakeholders have identified a lack of similar strategic planning in Western countries as a major shortcoming. The MCAC seeks to foster an environment for enabling Western leadership by Western companies and consortiums in critical and emerging technologies and to encourage coordinated action in the technology sector. Furthermore, organized planning at the national level and across Western nations will greatly aid in determining critical dependencies within national supply chains.

Key initiatives and reports focusing on enabling Western leadership in critical technologies that will mitigate cybersecurity impacts of decoupling include:

- *The Trilateral Cyber Security Commission (TCSC):* The TCSC, formed to strengthen U.S.-Japanese-UK relations in cyberspace, released its first report, National Security Strategy for 5G, in which it identified 5G as a critical technology requiring a unified strategy to mitigate cybersecurity risks. The commission recommends, for example, developing a robust and open domestic 5G sector for free-market democracies to build competitive solutions and forming a "5G International Security Council" for member states to coordinate 5G security and trade policies.[20]

- *The Cyberspace Solarium Commission (CSC):* The CSC's fourth white paper detailed the necessity for the United States to create an ICT industrial-base strategy to establish trusted supply chains for critical technologies. Of particular interest to the MCAC are the paper's fourth and fifth recommendations: to stimulate domestic markets to encourage a diversity of supply-chain choices in key technologies and to ensure global competitiveness in the provision of these critical technologies.[21]

- *Johns Hopkins University:* A national security report on the telecommunications industry, part of a series by the Johns Hopkins University Applied Physics Laboratory, projects that U.S.-China decoupling in the sector will move to near-complete bifurcation. One of its

> prominent recommendations for mitigating the effects of decoupling is to form a new industrial policy for telecommunications that shapes the deployment of next-generation networks, creates interoperable standards, and ensures private companies compete with China on an equal playing field.[22]

The MCAC recommends building on these efforts, specifically by establishing a public-private, long-term Western initiative involving both senior government and business leaders. The initiative will set out concrete, time-specific goals to establish a global environment that fosters the competitiveness of Western companies in emerging technologies, initially focusing on 5G, AI/ML, and quantum-computing technologies. This initiative could also provide private-sector and government leaders a forum to connect stakeholders so they can conduct joint and complementary R&D initiatives, enabling governments to coordinate efforts to provide funding for identified innovations. Stakeholders could synchronize global market-entry strategies, including implementing product transparency, to encourage global adoption of Western-sourced critical technologies. Such an initiative could enable Western countries to convene, set standards, and mitigate risks when technologies are initially deployed, bringing together participating countries well beyond Europe, Japan, and the United States. As recommended by the TCSC, it could build on such initiatives by providing a multilateral organizational body to foster technology-focused security and trade policies, including support for the Paris Call recommendations and the principles outlined in Microsoft's Cybersecurity Tech Accord.

MCAC-Originated Recommendations

In addition to building on previous work, the MCAC also conducted workshops to examine cybersecurity challenges for companies in the manufacturing, financial, and ICT sectors operating across the U.S. and Chinese technospheres, as described in the appendix. These companies suffer commercial impacts and cybersecurity risks from rules and regulations to various degrees, depending on their location, industry, and home nation's perceived security concerns. The MCAC, based on the workshops it held and its further deliberations, recommends two initiatives in addition to the existing efforts described above to mitigate cybersecurity risks generated by technology decoupling:

1. **Enhance cybersecurity collaboration at the operational and technical levels between Western government and private-sector partners.** In addition to the aforementioned efforts to seek accountability and consequences for transgressions against cyber-related norms, sustained, multilateral cybersecurity operational collaboration that links the human expertise and technical capabilities of Western government and private-sector partners is necessary to increase costs and raise challenges for malicious actors.

   To achieve this end, the MCAC recommends establishing a dedicated initiative made up of Western countries and private-sector partners, as well as actors such as NGOs and universities, to deepen a set of shared operational and technical capabilities to mitigate cyber risks. While similar efforts have existed for over a decade, with multiple governments and private-sector players working to disrupt botnets and other malicious activities, they remain sporadic and ad hoc and lack sufficient resources or sustained focus. The MCAC envisions such an organization reaching across multiple national efforts, enabling it to conduct joint technical analysis and forensic attribution, as well as thwart disruptive operations. Such an initiative could link government-led public-private partnerships—such as the U.S. Department of Homeland Security's Joint Cyber Defense Collaborative and other countries' national cybersecurity centers, including the UK National Cybersecurity Centre (NCSC) and Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)—with private-led initiatives like the CyberPeace Institute and the major technology infrastructure companies that operate globally. Establishing joint centers that house both government and private-sector stakeholders and personnel—fusing data, analytics, and insights to deliver merged capabilities—can provide the means to map, track, and plan to disrupt state malicious actors. Additionally, such an initiative could build on an increasing number of existing models of operational collaboration across Western nations.[23]

The MCAC notes that an effective initiative to establish multilateral cybersecurity collaboration and organizations will require significant investment from Western nations and their private-sector partners. The MCAC believes that senior leaders' long-term commitment to and investment in concrete steps to establish a safer cyberspace are necessary to reap the gains of ongoing digital transformations occurring among Western nations and companies.

2. **Strengthen collaboration on technology transparency for security, which could be a fundamental Western advantage to counter the growth of a Chinese-led technosphere and enable technology products to go to market globally.** The MCAC recommends Western stakeholders strengthen collaboration on secure technology transparency by enabling government and private-sector stakeholders to submit key elements of products (e.g., hardware and code) for evaluation by a multilateral review organization. Such an organization could function by allowing member private-sector companies to submit code and software bills of materials (SBOMs)—as well as necessary artifacts for evaluating hardware and firmware—creating an inventory of verified products for trusted use among Western nations. Such a collaborative program could help prevent such events as the 2020 SolarWinds breach and address security concerns stemming from Huawei's 5G dominance. If Chinese companies wish to enter the Western technosphere, they should be allowed to participate in these programs (and vice versa for Western companies operating in China), potentially building bridges across the technospheres. Such mechanisms could provide involved stakeholders the desired assurance of the safety of integrating technology into their infrastructure and mitigate supply-chain risks presented by the increasingly decoupled technospheres.

   Similar organizations already exist. Microsoft has transparency centers in the United States, Belgium, and China, likely providing the most mature model for such activities. Microsoft's transparency centers enable government technical professionals to test and assess technology to ensure that it does not pose security threats if deployed—all while maintaining intellectual property protections for Microsoft. Huawei has made similar efforts, submitting its code to the United Kingdom's Huawei Cyber Security Evaluation Centre (HCSEC), an entity under the Government Communications Headquarters, in order to provide transparency and security assurance regarding Huawei products.[24]

   Increasing transparency of key aspects of technology such as software code and update mechanisms has the added potential benefit of enabling faster go-to-market capabilities in countries whose governments fear security risks from foreign, including Western, technologies.

The possible maliciousness of Western technology is sometimes a concern to unaligned states: If Western and Chinese technologies pose equal risk, why not buy the cheaper technology from China? By providing transparency, not only does the West secure its own infrastructure, build trust, and counter technology decoupling, it also ensures transparency to unaligned stakeholders, providing potential cost advantages and a new value proposition that can counter Chinese influence.

Conclusion

The overall geopolitical rivalry between China and the West makes it unlikely that technology decoupling will decrease. Both see technology as a method to promote their respective worldviews while seeing each other's efforts as focused on national security competition. However, the MCAC notes that countering or limiting the extent of decoupling is a worthwhile effort. A unified and stable cyberspace provides advantages to governments, companies, and people across the globe, but decoupling will only further hinder opportunities for cooperation, trade, and capacity building. The MCAC finds the West requires a more collective approach that includes the private sector in addressing technology decoupling and mitigating associated cybersecurity risks. Western countries should seek a joint approach to identifying transgressions and enforcing norms, also using joint operational capabilities to mitigate the cybersecurity risks generated by decoupling. Such an effort will require significant investment, not just to implement the MCAC's recommendations, but also to act upon the well-founded recommendations generated by others. Even if two technospheres exist, the long-term benefits of investing in a stable cyberspace will far outweigh the upfront investment costs. Public and private leaders should join together, understand the challenge, and commit to the long-term actions necessary to keep cyberspace a vibrant and productive realm.

Appendix 1

MCAC Workshop Findings

The workshops that the MCAC held illuminated the significant variation among decoupling effects across sectors and technospheres. The automotive manufacturing sector has faced little impact in either technosphere. While regulations and risks of intellectual property theft were higher for Western automotive companies in China, these companies have largely accepted the risk; Chinese automotive manufacturers operating in the United States have similarly felt little to no effects. The growing technology decoupling had more impact on the functions of the financial sector, yet both Western and Chinese firms used each other's ecosystems as case studies in risk calculus, overall accepting greater cybersecurity risk in exchange for market access. The technology sector suffers major impacts due to technology decoupling, driven by perceived national security concerns that affect business operations. Overall, the MCAC found that technology decoupling is accelerating, largely driven by reciprocal laws and regulations from both sides, with the degree of sector impact being proportional to the perceived balance of corporate loss and gain and to national security concerns. As regulations, laws, and perceived risks grow, generating reciprocal actions, so have the cybersecurity risks.

Automotive

For Western companies operating in China, the risks of intellectual property and data theft already exist despite new cyber-generated risks. In the automotive industry, there is a high degree of risk acceptance among Western manufacturing firms. Western companies operating in China require a Chinese state-owned enterprise (SOE) partner in a joint-venture model. Foreign companies operating in China must share R&D and intellectual property data with their local partners despite the potential for data theft. This model enables technology transfer to China; however, cyber-based data theft enables an even more rapid acquisition of technical data and manufacturing knowledge, allowing the bypassing of network segmentation that companies operating in China may have implemented. Automotive manufacturing companies in China must rely on Chinese digital infrastructure when operating within Chinese borders, creating this cyber-based vector for data acquisition and intellectual property theft.

Conversely, a Chinese automotive-component manufacturing company operating in the United States reported not experiencing any regulatory challenges: the U.S. government has not imposed restrictions on its operations or use of technology systems. The company reported strong growth and return on investment in the United States. This growth indicates the few restrictions placed on automotive manufacturers operating in the United States have little commercial impact, as the United States does not view such activity as a national security concern. Chinese automotive manufacturers evidently share this view, as they use Western technology and data stacks in their Western-based operations.

Financial Services

Financial-services companies in both the West and China seek to continue global operations despite the growing challenges created by technology decoupling.

Although security challenges exist for the Western financial sector when operating in China, the MCAC found these companies are generally able to adjust and accept associated cybersecurity risks, maintaining and growing their business operations. The Western financial sector can and does take specific actions to address cyber risk when operating in China, especially regarding data flows. Transmitting and storing data in China is a major concern for U.S. banks operating there given recent Chinese national security laws and other regulations governing data security and privacy that seek China-based storage, control, and access. Data localization requirements for using Chinese technology, encryption, and data centers also generate major cyber risks for Western financial firms, driving them to create network and data enclaves for Chinese-based operations and business entities to avoid breaches of their global data and networks. While Western financial-services institutions work to limit how much data they hold in China—and, as necessary, store data in accordance with China's laws and regulations—they are simultaneously trying to balance the need to transfer information and conduct transactions globally against ensuring data security in the Chinese environment. Furthermore, China does not regard the financial sector as a specific national security risk and understands the sector's potentially key role in global economic competition. Its enforcement stance within this sector has so far focused on protecting the personal data of Chinese citizens. Its limited punitive regulatory and legal actions to this point reflect a desire to enable China's participation in global financial flows and to make the Chinese market a lucrative space for financial activity. However, China's current stance regarding Western financial firms operating in the country might simply be the calm before a storm, with other aspects of national competition driving increasing regulation and enforcement actions in the sector.

The MCAC workshop focusing on Western companies operating in China also discussed Hong Kong, where many global financial firms maintain significant operations based on their previous trust in its rule of law and lack of security risks. Many Western companies increasingly realize the risk posed by China's encroaching control and its efforts to extend provisions of the National Security Law and other legal requirements to Hong Kong. If these rules apply to Western companies' use of technology and data, as seems increasingly likely, this aspect of the decoupling—combined with cyber risks arising from physical proximity to China—will further impact the global financial-services industry.

Chinese banks operating in the United States currently do not face targeted restrictions on their operations and, in MCAC explorations, do not currently appear concerned about the cyber risks generated by increased decoupling of technology or how it impacts their overseas business. Chinese banks face the same regulations as other foreign banks operating in the United States. These regulations are heavy in terms of operational, technology, and cyber requirements but neither intrusive in terms of enforcement nor driven by national security imperatives. Chinese banks, like Western companies operating in China, have developed two separate technology and data enclaves. Branches in the United States use Western vendors whereas those in China use domestic technology for core banking systems; these banks, following Chinese rules, ensure that data on Chinese citizens is not stored in the United States. Chinese companies more broadly operate within and between the Chinese and Western technospheres, using a combination of international and Chinese software and hardware.

ICT Companies

The ICT sector faces the largest effects of technology decoupling. The MCAC finds that the Chinese and Western ICT sectors are mostly separated and trending to separate further. However, some global companies have worked to enable themselves to operate in each sphere. Key examples the MCAC examined include Microsoft's continued operations in China and Huawei's recurring efforts to operate in the United States.

Western ICT companies operating in China face a series of potentially draconian regulations and laws, including China's recent National Security Law and data privacy law, officially called the Personal Information Protection Law (PIPL). The new National Security Law's ambiguity gives Chinese authorities extensive power to target offenses such as "separatism," "subversion," "terrorism," and "collusion with foreign forces," enabling them to seize facilities and hardware and to shut down operations.[25] These measures inevitably increase companies' cyber risks by forcing them to provide network access to China, if demanded, or face punishments such as having operating licenses denied or their business operations closed. Companies have had a range of experiences in dealing with Chinese authorities, including being forced to install Chinese government-mandated tax software discovered to contain malware.[26] China has also created barriers to foreign ICT companies integrating their products in China. China's 2017 Cybersecurity Law specifically halts the use of foreign ICT equipment in government networks and installations. Furthermore, the adoption of China's Multi-Level Protection Scheme (MLPS) halts the adoption of any foreign firms' technology that is designated as above a certain level of national security interest. The MLPS 2.0 approach promulgated in China's Cybersecurity Law further strengthens these barriers, expanding their scope to critical technologies such as the IoT and cloud computing.[27] The recent National Security Law caused McAfee Corp., a U.S.-based security-software company, to remove its servers from China altogether. TunnelBear, a Toronto-based VPN service acquired by McAfee, announced its removal of all its Hong Kong servers so it could guarantee the safety and privacy of its users.

In addition, U.S. national security rules limit the ability of U.S. companies to supply and work with Chinese technology, further hindering their ability to operate effectively in China. These measures accelerate decoupling, as Western companies withdraw operations in the face of well-documented and well-understood risks stemming from Chinese cyber espionage—for example, as seen in Operation Aurora, a set of cyberattacks against Google in January 2010.[28] Over the past decade, numerous retreats have occurred. As recently as November 2021, Yahoo exited operations in China due to the country's tightened data and privacy regulations, and in October 2021 Microsoft's LinkedIn decided to shut down operations in China, citing difficulties "facing a significantly more challenging operating environment and greater compliance requirements."[29] While examples exist of Western tech companies operating in China—notably Microsoft, which is conducting ongoing efforts to address Chinese concerns—the majority have calculated that the risks outweigh opportunities, contributing to accelerated technology decoupling.[30] Exceptions to this general finding include major cloud service providers, namely Microsoft Azure and Amazon Web Services, which have decided to partner with local Chinese operators to provide versions of their cloud services that are specifically compliant with local regulations.

Chinese ICT companies operating in the United States have begun to face reciprocal constraints. For example, the U.S. Department of Commerce recently placed greater restrictions on technologies that can be exported to China and added major Chinese tech companies to its Entity List, effectively imposing additional licensing requirements if the company seeks to purchase U.S. technology or receive U.S. investment. The Secure and Trusted Networks Communications Act of 2019 codifies an earlier ruling by the Securities and Exchange commission, including prohibiting the use of universal service funds for purchasing Huawei equipment.[31] These restrictions were implemented in response to alleged cybersecurity risks posed by Chinese tech companies operating in the United States. Additionally, the Biden administration has amended licenses for companies selling Huawei products, further barring them from supplying items that can be used with 5G devices or systems. In the case Huawei brought against the Federal Communications Commission (FCC), the appellate court's final ruling established a prohibition on using universal service funds for purchasing products from companies on the Entity List, using a "predictive judgement" (rather than findings of past wrongdoing) to judge Huawei as a national security threat. The court justified use of "predictive judgement" in its decision by pointing to the difficulty in specifying national defense and public safety concerns, highlighting the complex correlation between these concerns and the degree of technology decoupling.[32]

As severe as effects on the ICT sector are, there are substantial differences across Western countries in the level of impact and how companies—especially European ones—interact with China in the sector. Many European tech companies maintain sizeable operations in China despite significant perceived cyber risks to intellectual property. While China, the European Union's biggest trading partner, presents important economic opportunities, national security plays a role in European nations' varied stances on governing the external actions of their ICT companies or use of Chinese ICT. Their approach to assessing security risks is generally "country neutral" and "vendor neutral," rather than directed against China or Huawei specifically. Furthermore, levels of risk acceptance regarding use of Chinese technology vary widely. Some countries, such as Sweden, have decided to ban the use of Chinese suppliers in implementing 5G, while others—such as Austria and the Netherlands—have demonstrated a hesitancy to ban Chinese 5G technology. In the middle of the pack are countries such as Germany and France, which have not banned Chinese tech companies altogether but have established the authority to block the acquisition of 5G equipment if deemed a threat to national security.[33]

Despite accelerated technology decoupling, global companies continue to seek opportunities to operate across the technospheres by complying with market-specific requirements. Huawei has displayed resilience in its campaigns to penetrate Western markets in face of the heavy regulation burdens and national security concerns. Huawei's efforts in the United Kingdom have generated mixed results, as the company does not yet face a complete ban. Additionally, Western companies such as Microsoft are maintaining their presence in China and working with Beijing to enable market access. Microsoft's Transparency Center provides an example of how companies can invest in engaging with a government to mitigate perceived cybersecurity risks and maintain access to the market. Similarly, Apple has chosen to continue Chinese operations, setting up a local data center and manufacturing the majority of its hardware in China.[34] Major enterprise-software companies such as Oracle and SAP do billions of dollars' worth of business in China. These efforts demonstrate that opportunities can exist for cooperation to facilitate global commerce between the technospheres—even in the ICT sector—that might help decelerate technology decoupling and mitigate its associated cyber risks.

Overall, the MCAC finds that technology decoupling is rapidly progressing. The effects on each sector vary depending on how heavily they intersect with national security and personal privacy concerns. To date, the manufacturing sector suffers little, if any, disruption. While Western manufacturing companies in China face some potential liabilities, opportunities heavily outweigh any presented risks; conversely, Chinese automotive manufacturers do not feel at risk. The financial sector feels the impacts of technology decoupling but has maintained an overall risk acceptance and associated operating and security costs—with organizations often willing to work within the confines of new regulations, using separate technology stacks and heavily segmenting networks in each other's technospheres—limiting the extent of technology decoupling. The ICT sector suffers from severe limitations and impacts from technology decoupling, forcing many companies to end operations in the other's technosphere, though specific outcomes vary by company. While the overall economic effects of technology decoupling have yet to become clear, trends in 2021 show a widening divide. If technology decoupling does not slow down, companies and nations will have to rapidly learn how to form tech and data enclaves based on sovereignty and local jurisdictions.

Appendix 2

Existing Recommendations and Initiatives

Christopher A. Thomas and Xander Wu, "How global tech executives view U.S.-China tech competition," Brookings Institute, February 25, 2021, https://www.brookings.edu/techstream/how-global-tech-executives-view-u-s-china-tech-competition/.

Toomas Hendrik Ilves, "A Digital Defense Alliance," Berlin Policy Journal, January 10, 2018, https://berlinpolicyjournal.com/a-digital-defense-alliance/.

Paul Triolo, *The Telecommunications Industry in US-China Context: Evolving toward Near-Complete Birfurcation* (John Hopkins Applied Physics Laboratory, 2020), https://www.jhuapl.edu/Content/documents/Triolo-Telecomms.pdf.

Angus King and Mike Gallagher, "Building a Trusted ICT Supply Chain," U.S. Cyberspace Solarium Commission, October 2020, https://www.solarium.gov/public-communications/supply-chain-white-paper.

Cañada Amela et al., *Decoupling – Severed Ties and Patchwork Globalisation* (European Union Chamber of Commerce in China and MERICS, January 2021), https://merics.org/en/report/decoupling-severed-ties-and-patchwork-globalisation.

Yan Luo, Samm Sacks, Naomi Wilson, and Abigail Coplin, "Mapping U.S.-China Technology Decoupling," DigiChina, Stanford University Freeman Spogli Institute for International Studies, August 27, 2020, https://fsi.stanford.edu/publication/mapping-us%E2%80%93china-technology-decoupling.

Charles Bradley et al., "Advancing U.S. Telecommunications Network Security: A Response to FCC Notice of Proposed Rulemaking in the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, FCC 18-42," Domain 5, n.d.

Endnotes

[1] The MCAC uses the term "Western" to describe those "like-minded" nations committed to global economic and security regimes and to rules established by international organizations and consensus.

[2] The divide between the two technospheres can been seen, for example, in UN voting patterns: https://www.un.org/en/ga/third/73/docs/voting_sheets/L.9.Rev.1.pdf.

[3] Yan Luo et al., "Mapping U.S.-China Technology Decoupling: How Disparate Policies Are Unravelling a Complex Ecosystem," Stanford University and New America, DigiChina Project, August 27, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/mapping-uschina-technology-decoupling/; Diego A. Cerdeiro et al., "Sizing up the Effects of Technological Decoupling," International Monetary Fund, Working Paper, March 12, 2021, https://www.imf.org/en/Publications/WP/Issues/2021/03/12/Sizing-Up-the-Effects-of-Technological-Decoupling-50125.

[4] Mercator Institute for China Studies, *Decoupling: Severed Ties and Patchwork Globalisation* (Beijing: European Union Chamber of Commerce in China, 2021), 4, https://merics.org/sites/default/files/2021-01/Decoupling_EN.pdf.

[5] Fikunari Kimura, "Developing a Policy Regime to Support the Free Flow of Data: A Proposal by the T20 Task Force on Trade, Investment and Globalization," Research Institute of Economy, Trade, and Industry (RIETI), July 30, 2019, https://www.rieti.go.jp/en/columns/a01_0526.html.

[6] "Building Trusted Digital Identity in the European Union: Efficient & Secure Digital Life," European Commission, 2019, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61682.

[7] Michael Becker, "GDPR Compliance: How It's Affecting U.S. Companies," Emarsys, November 6, 2018, https://emarsys.com/learn/blog/gdpr-united-states-companies/.

[8] The UN Office on Drugs and Crime now categorizes tampering with undersea cables as criminal behavior. See UN Office on Drugs and Crime, *Maritime Crime: A Manual for Criminal Justice Practitioners* (Vienna:

United Nations, 2019), https://www.unodc.org/documents/Maritime_crime/19-02087_Maritime_Crime_Manual_Second_Edition_ebook.pdf.

9 Peter A. Petri and Michael Plummer, “RCEP: A New Trade Agreement That Will Shape Global Economics and Politics,” Brookings Institution, November 16, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/11/16/rcep-a-new-trade-agreement-that-will-shape-global-economics-and-politics/.

10 The White House, “Readout of President Biden’s Virtual Meeting with President Xi Jinping of the People’s Republic of China,” November 16, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/16/readout-of-president-bidens-virtual-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china/.

11 “The 9 Principles,” The Paris Call for Trust and Security in Cyberspace, accessed December 21, 2021, https://pariscall.international/en/.

12 United Nations, “Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report,” United Nations General Assembly, March 10, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

13 Global Commission on the Stability of Cyberspace, *Advancing Cyberstability: Final Report* (The Hague: Global Commission on the Stability of Cyberspace, November 2019), https://cyberstability.org/report.

14 CyberPeace Institute, *Playing with Lives: Cyberattacks on Healthcare Are Attacks on People* (Geneva: CyberPeace Institute, March 2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

15 Scott Charney, “Governments and APTs: The Need for Norms,” Microsoft, December 2014, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtU.

16 Jared Cohen and Richard Fontaine, “Uniting the Techno-Democracies: How to Build Digital Cooperation,” *Foreign Affairs* 99, no. 6 (November/December 2020), https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

17 Mercator Institute for China Studies, *Decoupling: Severed Ties and Patchwork Globalisation*.

18 William A. Carter and Erol Yayboke, “Data Governance Principles for the Global Digital Economy,” Center for Strategic and International Studies, June 4, 2019, https://www.csis.org/analysis/data-governance-principles-global-digital-economy.

19 Soshi Hamaguchi, “Use Of Trust Lists in Japan to Build Global Trust Spaces,” The European Union Agency for Cybersecurity, September 22, 2021, https://www.enisa.europa.eu/events/trust-servicies-forum-ca-day-2021/ca-day-presentation/07_sip-1-_soshi-hamaguchi.pdf/@@download/file/07_SIP%20(1)_Soshi%20Hamaguchi.pdf.

20 Trilateral Cyber Security Commission, *National Security Strategy for 5G: Findings and Recommendations on Meeting the 5G Challenge* (Washington: DC: Sasakawa Peace Foundation USA, December 2019), 5–6, https://spfusa.org/wp-content/uploads/2019/12/TCSC-National-Security-Strategy-for-5G-Dec-2019.pdf.

21 Cyberspace Solarium Commission, *Building a Trusted ICT Supply Chain: CSC White Paper #4* (Washington, DC: Cyberspace Solarium Commission, October 2020), 15–16, https://www.solarium.gov/public-communications/supply-chain-white-paper.

22 Paul Triolo, *The Telecommunications Industry in US-China Context: Evolving toward Near-Complete Bifurcation* (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2020), 24–25, https://www.jhuapl.edu/Content/documents/Triolo-Telecomms.pdf.

[23] New York Cyber Task Force, *Enhancing Readiness for National Cyber Defense through Operational Collaboration* (New York: Columbia School of International and Public Affairs, 2020), https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF-%20Enhancing%20Readiness%20for%20National%20Cyber%20Defense%20through%20Operational%20Collaboration.pdf; Aspen Institute, "An Operational Collaboration Framework for Cybersecurity," Aspen Cybersecurity Group, November 8, 2018, https://www.aspeninstitute.org/publications/an-operational-collaboration-framework/; World Economic Forum, *Partnership against Cybercrime: Insight Report* (Geneva: World Economic Forum, November 2020), https://www.weforum.org/reports/partnership-against-cybercrime.

[24] Huawei Cyber Security Evaluation Centre Oversight Board, *Annual Report: 2019* (London: UK Cabinet Office and National Cyber Security Centre, March 2019), https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

[25] Angeli Datt, "The Impact of the National Security Law on Media and Internet Freedom in Hong Kong," Freedom House, October 19, 2021, https://freedomhouse.org/article/impact-national-security-law-media-and-internet-freedom-hong-kong.

[26] Yoichi Takita, "Global Finance Falls Victim to China's Spyware Campaign: U.S. and Germany Warn Companies about Backdoors in Chinese Tax Software," Nikkei Asia, December 6, 2020, https://asia.nikkei.com/Business/Technology/Global-finance-falls-victim-to-China-s-spyware-campaign2.

[27] Jim Fitzsimmons and Carly Ramsey, "Enforcement of China's Multi-Level Protection Scheme: The Rapid Roll-out of Cyber Security Compliance," Control Risks, October 2020, https://www.controlrisks.com/campaigns/china-business/enforcement-of-chinas-multi-level-protection-scheme.

[28] David Drummond, "A New Approach to China," Google Blog, January 12, 2010, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[29] Zen Soo, "Yahoo Pulls out of China, Citing 'Challenging' Environment," AP News, November 2, 2021, https://apnews.com/article/yahoo-inc-leaving-china-f3b589754224bc663d5e83ec385eb49a; Mohak Shroff, "China: Sunset of Localized Version of LinkedIn and Launch of New InJobs App Later This Year," LinkedIn Blog, October 14, 2021, https://blog.linkedin.com/2021/october/14/china-sunset-of-localized-version-of-linkedin-and-launch-of-new-injobs-app.

[30] Scott Charney, "New Beijing Transparency Center Announced," Microsoft, September 16, 2016, https://blogs.microsoft.com/on-the-issues/2016/09/19/new-beijing-transparency-center-announced/.

[31] U.S. Congress, *Secure and Trusted Communications Networks Act of 2019*, HR 4998, 116th Cong., 2nd sess., introduced in House November 8, 2019, https://www.congress.gov/bill/116th-congress/house-bill/4998.

[32] U.S. Court of Appeals for the Fifth Circuit, "Fifth Circuit Decision - Huawei Technologies v. FCC & USA, No. 19-60896," June 18, 2021, https://www.fcc.gov/document/fifth-circuit-decision-huawei-technologies-v-fcc.

[33] Annabel Murphy and Jack Parrock, "Huawei 5G: European Countries Playing 'Politics' with Network Bans, Chinese Company Says," Euronews, July 28, 2021, https://www.euronews.com/next/2021/07/28/huawei-eyes-a-place-within-europe-s-digital-future-despite-5g-bans-in-some-countries.

[34] "Apple Supplier List: Fiscal Year 2020," Apple Inc., May 2021, https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf.

COVER PHOTO PESHKOVA/ADOBESTOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**