China’s Internet of Things

John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green,
Jonathan Ray, and James Mulvenon

Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission

October 2018

Disclaimer: This research report was prepared at the request of the U.S.-China Economic and Security Review Commission to support its deliberations. Posting of the report to the Commission's website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 113-291. However, it does not necessarily imply an endorsement by the Commission or any individual Commissioner of the views or conclusions expressed in this commissioned research report.

About the SOSi Special Programs Division

This project was conducted within SOSi's Special Programs Division (SPD), the premier open source and cultural intelligence exploitation cell for the U.S. intelligence community. Staffed by an experienced team of cleared analysts with advanced language skills, SPD's mission is to provide cutting-edge, open source and cultural intelligence support to the collection, analytical, and operational activities of the U.S. intelligence community, with the goal of achieving national strategic objectives. SPD accomplishes its mission through the conduct of objective, independent, and relevant research and analysis, under strict quality guidelines.

Comments may be sent to the General Manager of the Special Programs Division, Dr. James Mulvenon.

Dr. James Mulvenon
General Manager
Special Programs Division
SOS International
2650 Park Tower Drive, Suite 300
Vienna, VA 22180
TEL: 571-421-8359
Email: James.Mulvenon@sosi.com

Executive Summary

The Internet of Things (IoT)—the interconnection of physical and virtual things via information and communication technologies—is emerging as the next front in global network infrastructure, with potentially transformative benefits across a range of applications and services. Due to its potential adoption in essentially all economic sectors, analysts expect the IoT to expand exponentially over the next few years, ultimately involving billions of connected devices and dozens or more vertical markets around the world. However, pressing questions about the IoT's operation, safety, and security have yet to be answered. What international standards will guide the development of IoT technologies and supporting infrastructure like 5G networks? How secure is the IoT and what are the risks of its vulnerabilities? How will U.S. consumer data be used and protected here and abroad?

China features prominently in all of these issues, and its drive to become a leader in the IoT poses sobering challenges to U.S. economic and security interests. This report examines how China's development of the IoT—bolstered by the Chinese government's efforts to harness national resources for its promotion—has put China in a position to credibly compete against the United States and other leaders in the emerging IoT industry. China's pursuit of IoT dominance constitutes a significant challenge to U.S. economic and national security interests. Its robust participation in international standards committees has given Beijing greater opportunities to dictate the rules of the road. Its research into IoT security vulnerabilities and its growing civil-military cooperation raise concerns about gaining unauthorized access to IoT devices and sensitive data. Its authorized access to the IoT data of U.S. consumers will only grow as Chinese IoT companies leverage their advantages in production and cost to gain market share in the United States.

For now, China's large market size, production capacity, and government support offer some significant advantages, but China is still behind leading international levels in many IoT technologies. Therefore, U.S. companies and the U.S. government still have time to maintain a technological edge and influence future IoT development, standards, and roll-out. By comparison, the world is on the cusp of 5G with commercial rollouts beginning in 2018. The countries with the largest and most reliable 5G networks will have a head start in developing the technologies that 5G enables–first among them, the IoT. China has laid a solid groundwork for a comprehensive rollout, relying on a whole-of-country approach that has created an entire ecosystem for domestically manufactured 5G technologies and furthered their inclusion in international technical standards. With ten times the 5G sites per person as in the United States, China appears likely to lead early 5G deployment.[1]

Chinese dominance in the IoT will likely come at considerable cost to U.S. companies and consumers, hurting both U.S. economic and national security interests. China sees technology development as a decisive strategic resource and believes other countries' control of key technologies is a significant strategic liability. Its determination to lead in IoT development is grounded in these considerations, as well as a high sensitivity to the cost of ceding dominance in next-generation technologies to other powers. As such, China's IoT development strategy to date has been designed to narrowly serve Chinese interests. The Chinese government is unlikely to

[1] Dan Littmann, Phil Wilson, Craig Wigginton et al., "5G: The Chance to Lead for a Decade" (London: Deloitte, 2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf?mod=article_inline.

show much consideration for the protection of U.S. consumers, let alone U.S. companies competing in the IoT space.

China’s Approach to IoT Development

As this report describes, China’s commitment to becoming a leader in IoT development is predicated on the belief that its security requires it to become a technological power, particularly in emerging technologies that the country considers strategically vital. The potential effect of the IoT on the global economy led Chinese leaders to designate it as a priority area for development in 2009. China subsequently took steps to catalyze domestic IoT research and development (R&D) and infrastructure development through robust planning initiatives and extensive financial support. After years of this support, the Chinese IoT market has grown rapidly, passing 1 trillion RMB (approx. $154 billion) in value in 2017, with expectations that it will reach 1.8 trillion RMB (approx. $264 billion) in value by 2020. Global IoT industry growth trends have been similarly robust: by way of comparison, some experts believe that IoT infrastructure investment is expected to reach $421 billion in the United States and $274 billion in Europe by 2021.[2] Chinese experts anticipate that an “Internet of Everything” era will arrive once IoT is adopted widely in developed countries, and some assess that China has already developed a relatively complete IoT supply chain, including chips, components, devices, software, systems integration, operators, and applied services.

China’s top leaders have long viewed technological advancement as a bellwether of national strength and security and are keen to avoid falling behind other international competitors in technological advancement. Driven by this sense of urgency, China’s policies to promote IoT development have included the creation of IoT industrial clusters and demonstration bases, extensive financial support for IoT R&D, restrictions on foreign investment, selective enforcement of Chinese laws to hinder the operation of foreign IoT firms in China, and the ever-looming prospect of technology transfer.

These policies pose serious challenges for U.S. firms competing with Chinese firms in the IoT industry, who must be aware that the Chinese government considers them to be strategic rivals, if not outright threats. China is likely to engage in protectionist and unfair trade practices to favor its own IoT companies over foreign competitors, creating an austere and tacitly hostile market environment for foreign firms. In response, this report recommends that the U.S. government:

- Commission a blue-ribbon panel with a mandate to assess the ability of the United States to compete in emerging commercial information and communications technologies;
- Publish a list of federal guidelines laying out “best practices” for IoT firms seeking to operate within China;
- Continue to seek legal redress against coercive Chinese trade practices through international institutions; and
- Collaborate with partner nations to counter coercive Chinese trade practices and expand existing trade partnerships in the Asia-Pacific region to build a larger shared market that could act as a counterweight to China’s economic power.

[2] “Worldwide Semiannual Internet of Things Spending Guide,” IDC, accessed September 5, 2018, https://www.idc.com/getdoc.jsp?containerId=IDC_P29475

China’s Race to Set International Technical Standards

The Chinese government is actively attempting to influence international technical standards for the IoT that would benefit Chinese companies at the expense of U.S. and other foreign counterparts. As information technology (IT) industry precedents have shown, the competition over technical standards touches on a larger contest about intellectual property ownership, market advantage, international prestige, and approaches to privacy, security, and control of data. Once a global standard is established and accepted it can put pressure on countries or companies developing other standards to conform to the existing norm, ceding these important benefits to whichever nation’s preferences manage to be adopted as the international standard. This advantage is magnified from a security viewpoint, as the originator of a standard technology has an intimate understanding of how it operates inside and out. China’s increased effort to influence and set international IoT standards is a critical part of China’s ambitious state-directed plan to achieve dominance in the IoT. These efforts may lock-in Chinese preferences for standards in IoT and supporting infrastructure sooner rather than later, as nascent IoT and 5G standards exist in a fragmented and complex standards-setting environment rife with incompatible proprietary solutions and an alphabet soup of standards-setting bodies.

China is currently leveraging a more coordinated and comprehensive strategy than the United States to influence relevant standards for the IoT, and U.S. entities are often absent from key international standardization processes. Consequently, some international standards have been developed with reduced U.S. input. In contrast, China’s international standardization efforts are increasing, following a centralized plan to effect change at both high and ground levels. On the high level, China has increased its participation in international standards institutions, where it shows a preference for multilateral (one country, one vote) standards institutions over U.S.-backed multi-stakeholder institutions. Chinese nominees leading these organizations work in tandem with national Chinese standards development efforts and push China’s agenda from their official platforms. On the ground level, China is leveraging the country’s sizable economy, state investment in new technologies, and state-subsidized foreign policy initiatives like the Belt and Road Initiative (BRI) to encourage other countries to adopt its technology, and with it, its standards. China is explicit in its support for “standardization work” and will likely continue emphasizing this work and strategy for the IoT and other new and emerging technologies.

To address China’s aggressive pursuit of international technical standards and ensure U.S. leadership and advantages in the IoT and other related industries, the U.S. government should:

- Conduct additional open source reporting and research on China’s international standards efforts;
- Encourage more U.S. participation in international standards committees through additional funding and incentives;
- Where acceptable, adopt proposals and processes agreed upon by multi-stakeholder international standardization bodies while continuing to counter Chinese attempts to re-define internet governance as a matter of national sovereignty that requires the devolution of control to nation-states; and
- Create a government-industry advisory body charged with studying corporate foreign interactions in the interest of national security.

Unauthorized Access to IoT Devices and Chinese Exploitation Efforts

The IoT is inherently vulnerable to attack as billions of devices are added and connected to networks. These products, from industrial controls to smart watches, can become attack surfaces through their internet connections. Worse, market demands for lower costs paired with low barriers to entry in the IoT market mean there is currently little incentive to build more secure IoT devices. Unauthorized access to IoT devices has already resulted in physical consequences, including attacks on industrial machinery and power grids around the world. Future unauthorized access is likely to open a Pandora's box of negative consequences as IoT devices are deployed in greater numbers around the world.

Because of its market size, China has the potential to wield an outsize impact on the security of IoT devices against unauthorized access (i.e., technical compromise). Chinese-manufactured IoT devices have already become common targets for unauthorized access, thanks in part to insecure device configurations that have resulted in surreptitious data collection and the commandeering of devices for use in botnets. The widespread usage of Chinese IoT devices and components suggests that the aggregate negative consequences of unauthorized access to Chinese devices may be proportionally larger than for devices from other countries.

China is also actively researching IoT vulnerabilities, both for security purposes and almost certainly to collect intelligence, conduct network reconnaissance for cyberattacks, and enhance its domestic surveillance powers. Chinese IoT security research exhibits a familiarity with exploitation methods that could lead to unauthorized access and is already leveraging machine learning and algorithmic techniques to accelerate the pace of research and develop adaptable malicious code that could affect multiple types of IoT devices. China's IoT security research entities are also part of a broader and increasingly fused civil-military research ecosystem that increases the chances that PRC intelligence and military actors will have access to any breakthroughs in IoT vulnerability research.

The combination of widespread adoption of IoT products and Chinese research into exploits raises the threat of unauthorized access to U.S.-based IoT devices and the networks they connect to. To counter Chinese potential exploits of IoT vulnerabilities and safeguard U.S.-based devices against state and non-state threats, the U.S. government should:

- Encourage adoption of security best practices for IoT products in the form of an industry-backed cybersecurity program;
- Increase funding and support for IoT security research, especially in areas that could yield proportionately greater gains for IoT security;
- Document Chinese entities that conduct IoT security research for, alongside, and supported by Chinese military and security services; and
- Overhaul the oversight process for green-lighting Chinese investment in U.S. IoT industry in order to better account for the unique security concerns posed by China's blending of its military and civilian IoT research ecosystems.

Authorized Access to IoT Data and Privacy Concerns

While authorized data access, collection, and processing are indispensable parts of the IoT's transformative potential, the Chinese government is uniquely empowered to access the IoT data of U.S.-based consumers. Authorized access, or access that is agreed to by the consumer in lengthy terms and conditions documents, allows companies and governments to gather massive amounts of data that can translate into substantial economic and strategic advantages. While this practice is the norm across the world, China poses a grave threat to U.S. privacy as its government and surveillance apparatuses are empowered to access this data well in excess of accepted international norms. Chinese companies can access U.S. IoT data in four main ways:

1. At the user-level, Chinese entities can access U.S. data simply from sales and usage of their IoT products by U.S. consumers who authorized data collection and transmission by agreeing to terms of use.
2. Device-level access through the device manufacturing and design process opens up opportunities for outside entities to collect even more information at scale.
3. At the corporate level, Chinese companies could buy U.S. IoT companies and the data they have accumulated through their products, or buy U.S. data through a third-party vendor or a data broker.
4. Last, Chinese government data appropriation powers could expose U.S. IoT data to Chinese government collection.

Chinese access to U.S. IoT data is problematic for U.S. national security and economic competitiveness. In the short term, Chinese government and corporate access to U.S. data would be a huge opportunity for Chinese intelligence targeting operations. In the longer term, such access would provide a major edge to Chinese artificial intelligence (AI) development efforts, eventually culminating in a substantial Chinese economic advantage in another field that is expected to shape the economy of the future.

Existing U.S. data protections appear insufficient to protect U.S. data against harmful but authorized data access. The patchwork nature of U.S. laws and authorities leaves loopholes that could facilitate Chinese access to U.S. IoT data in bulk, an especially risky proposition given known Chinese motivations for accessing big data. To address these deficits, the U.S. government should:

- Enact a tiered disclosure regime for IoT products broad enough to cover multiple aspects of authorized IoT data collection;
- Mandate data expiration and de-identification of data where appropriate according to existing principles of data minimization, especially for information resellers;
- Codify existing U.S. data regulations and others in a single, comprehensive federal law governing data privacy;
- Require foreign IoT products to disclose affiliation with foreign entities that may pose a significant risk of harmful but authorized access to U.S. data;
- Refer corporate-level attempts to transfer U.S. data to foreign entities to CFIUS for approval; and
- Expedite passage of a unified federal data privacy statute applicable to both foreign and domestic IoT companies.

Conclusions

The United States can counter or blunt the challenge from China in many areas through sound policy. A comprehensive accounting of Chinese participation in key international standards bodies would identify areas that might require more U.S. involvement. More exhaustive studies of the effectiveness of European data privacy protections may help determine what model of data protection would be most effective in closing the front door to the IoT data of U.S. citizens. Some of these countermeasures require only U.S. action and do not depend upon Chinese cooperation.

In other areas of IoT development, however, the U.S. ability to protect its own interests and those of its citizens will be limited. For example, the one-party Chinese regime is simply more empowered to demand all data collected by Chinese IoT companies, including data from U.S. consumers. Although the U.S. government could theoretically prevent U.S. companies from turning over the data they hold to Chinese entities, there is little it can do to prevent the Chinese government from obtaining such information once it is in the hands of Chinese companies. This reality demands a clear-eyed understanding of these challenges and needs greater coordination between the resources of Washington, the innovative capacity of the U.S. private sector, and perhaps coordinated efforts with U.S. allies abroad. Participation in international standards bodies, long overdue data privacy legislation, and industry best practices for IoT security would benefit from such coordination and help mitigate the challenges from Beijing.