MERICS CHINA MONITOR

June 24, 2021

THE CONNECTION OF EVERYTHING

China and the Internet of Things

John Lee

MAIN FINDINGS AND RECOMMENDATIONS

- **Massive growth in devices connected to the internet raises technical and policy challenges on a new scale.** This 'Internet of Things' (IoT) is diffusing power to a growing range of actors worldwide who build and operate connected devices and the underlying infrastructure, both physical and virtual.

- **The IoT is amplifying both rewards from technological leadership and risks from inter-connection across borders.** Sovereign governments are responding by imposing increasing control over the internet within their jurisdiction, leading to growing fragmentation of cyberspace governance on national lines.

- **China now plays a significant role in shaping the IoT, which is growing with the technological footprint of Chinese firms.** This is being driven by the incentives of private industry, and by the Chinese state's sustained policies to boost the role of Chinese actors in IoT development, including technical standardization.

- **Concerns about how China may exploit the IoT are driving moves to disconnect from Chinese networks, led by the US.** But the reluctance of other countries to join a "democratic" internet coalition excluding China means that instead, the IoT will likely continue fragmenting into a variety of distinct "cyber-spaces".

- **Europe must adopt measures to mitigate the growing risks from international connectivity, as well as to compete with China in shaping the IoT worldwide.** This implies adapting European "cyber diplomacy" to the growing role of non-Western countries, which have their own priorities and views towards Chinese influence, in shaping the IoT and the economic systems being built upon it.

- **The "public core of the internet" concept offers a baseline for compromise on these issues, focused on maintaining the internet's function as a global public good.** But while avoiding a stance of unmitigated confrontation with China, Europe must closely monitor Beijing's priorities for shaping the evolving IoT.

MERICS
Mercator Institute for China Studies

1. CHINA IS HELPING SHAPE THE WORLD'S TRANSITION TO THE INTERNET OF THINGS (IOT)

The rise of the Internet of Things (IoT) is transforming economic systems and social relations worldwide. China is a key actor shaping this transformation, thanks to the scale of its digital industries and state-led ambitions to lead in new technologies. Beijing committed early on to the IoT's development, using sustained state policy to leverage China's huge markets and central position in global manufacturing. Chinese actors, which before the late 1990s had little influence over design of the world's digital infrastructure, are becoming major players in shaping the international IoT, and by extension the power relations embedded within it.

The IoT's evolution will amplify the rewards accruing to those who wield influence over the design of the internet's architecture and constituent systems. For the transatlantic economies that historically dominated the design and governance of the global internet, China's role in the growing "interconnection of everything" represents a potentially profound shift in the international distribution of economic and technological power, which merits close attention.

1.1 What is the IoT?

The internet is no longer merely a communication medium among people. It now directly affects the physical world. An expanding range of "things" are being connected to the internet, resulting in a growing number of real-world functions being controlled through cyberspace.[1] The number and type of objects connected to the internet and which can be influenced through it is expanding massively, even as these objects increasingly interact with each other and with humans, often without human mediation. As a result, the world is becoming ever-more populated with inter-connected cyber-physical systems.

By one estimate, in 2020 the number of IoT connections (e.g., connected cars, smart home devices, connected industrial equipment) was approaching 12 billion worldwide, overtaking the number of non-IoT devices online (e.g., smartphones, laptops, computers). By 2030, this number could rise to 125 billion. US digital technology leader Qualcomm estimates that the global economic output of industrial 5G IoT technologies will be worth a trillion USD by 2035.[2]

The internet's penetration of the 'real world' means that relations among individuals, entities and societies will increasingly be embedded in the IoT. Those who influence the design, building and regulation of internet infrastructure will obtain gatekeeper and first-mover advantages. These advantages will be scaled up across emerging internet-connected technological ecosystems. Parties who hold these structural advantages will be able to shape other actors' choices across expanding fields of activity - often without actively exerting power. Increasingly, power will be implied in the structures of the evolving IoT.

Those who influence the design, building and regulation of internet infrastructure will obtain gatekeeper and firstmover advantages

1.2 The IoT presents challenges on a new scale, and China's role is growing

These changes are creating challenges much greater than those previously brought by the internet's expansion. Some of these challenges require more global cooperation, including with new and potentially non-"like minded" actors, to realize the IoT's potential. Others will present governments with hard choices between tolerating significant risks from international connections or sacrificing substantial benefits by disconnecting from the source of risk.

China's role in shaping the emerging IoT landscape will feature prominently for governments worldwide in addressing these challenges. Chinese firms are leading participants in both the development of IoT applications and of the internet's underlying infrastructure. China's cyberspace governance regime diverges significantly from the political values that have informed the internet's past evolution, although it also continues to be shaped by imperatives to maintain foreign connections. Security concerns around Chinese actors and the consequent responses by governments around the world are shaping the global evolution of IoT-enabling technologies, for example with fifth generation (5G) telecoms networks.

The IoT's growth compounds the security risks that are inherent in the internet's design to enable the free flow of information. Connection of vast numbers of devices with different functions and protocols complicates the task of securing the whole network. The expanding effects of internet-connected objects in the physical world are expanding the scope of harmful outcomes that could arise from manipulation across the internet.

IOT SECURITY DILEMMAS: CYBERATTACKS ON UKRAINE

The potential for "weaponization" of connected systems to produce real-world effects was seen in the 2015 cyberattacks on Ukraine's power grid, which disrupted electricity supply to 230,000 people in winter. In 2017, new attacks undermined the functioning of Ukraine's railroads, airports, hospitals and other critical infrastructure. These attacks had global flow-on effects that included a temporary 20 percent drop in shipping volume for Maersk, the global cargo handling group. In a world increasingly connected through the IoT, such events could produce cascading crises with costs orders of magnitude higher than previously seen.

These growing risks, together with imperatives to capture the IoT's potential rewards within national borders, are driving widespread and intrusive assertions of 'digital sovereignty'.[3] The universal architecture of the internet was designed for the seamless transfer of data. Yet governments worldwide have imposed growing constraints on use of the internet – China's "Great Firewall" is only the best-known example – to control data transfers and online activity within their jurisdiction.

This growing administrative fragmentation of the internet along political lines means that the global IoT will likely evolve as a federation of networks, which differ significantly within national borders in their governance arrangements, and possibly in their technical design. Basic functionality and systemic resilience will increasingly require cooperation among governments with distinct approaches to cyberspace, driven by divergent political priorities and underlying values. One example is the contrast between the 'European values' that nominally guide the European Union's cyberspace regulation and diplomacy, and the central role that China's cyber-governance regime gives the Communist Party's leadership.

Because the internet was designed to operate seamlessly, this fragmentation across borders threatens to undermine its efficient operation on a global scale. The recent controversy over Chinese firms' role in developing network protocols for the future internet shows how politics can influence the internet's international interoperability and performance at fundamental levels.[4] These problems will be amplified by the expanding complexity inherent in the IoT.

This complexity reflects the growing multitude of systems connected to the internet, most of which are being designed by private firms. The IoT's growth therefore implies the rising influence of a growing range of non-state actors. Business entities already wield significant influence over the security of networks, and over public equities such as free speech and non-discriminatory internet access ("net neutrality"). Cyber-physical device ecosystems controlled by private firms, increasingly including Chinese companies, are expanding rapidly.

Furthermore, many new applications touted as benefits of the IoT may require re-design of the underlying internet infrastructure to deliver the necessary performance. For example, self-driving connected vehicles and other time-sensitive applications require fast (low latency) data transmission that may be unachievable with legacy network architectures.[5]

Unlike the legacy "stack" of internet technologies, development of which was dominated by US and European actors, these new IoT applications are evolving through transnational collaboration and on a global scale. Many important developments are now taking place outside the jurisdiction of Western governments, with Chinese actors featuring prominently.

Important developments are now taking place outside the jurisdiction of Western governments, with Chinese actors featuring prominently

2. CHINA IS SHAPING THE IOT AT HOME AND ABROAD

China's government has driven development of a domestic IoT ecosystem by combining centralized direction and incentivization with decentralized implementation. The growing capacity of Chinese businesses to deploy IoT technologies, capture market share and attract international partnerships is bolstering the ability of the Chinese state and China's corporate champions to shape the internet's governance, design and implementation on a global scale.

2.1 China's footprint in the global IoT is growing

The concentration of electronics manufacturing in China has provided a foundation for the rapid development of IoT products and services, which has been further stimulated by massive domestic consumer demand. By one estimate, China accounted for three quarters of cellular IoT connections worldwide at the end of 2020. The US network technology leader Cisco projects that by 2023 China will lead globally in 5G connections.[6]

Although the overall level of digitalization in China's manufacturing sector remains low, more firms are moving towards automation and industrial IoT applications, with a few becoming global leaders.[7] Haier for example, the world's largest white goods-maker, in 2020 completed a "proof of concept" case study for IoT-enhanced manufacturing in cooperation with China Mobile, Huawei and the global mobile networking standards association GSMA. Two of Haier's factories are on the World Economic Forum's "Lighthouse" list of global leaders in the deployment of IoT manufacturing technologies with demonstrated benefits.[8]

China's private digital technology firms have turned to the IoT for new revenue streams, given the saturation of existing product and service markets. Xiaomi for example generated over 30 percent of its revenue from the IoT and lifestyle product sector in 2019 and says that over half its revenue now comes from markets outside China. Xiaomi claims that its IoT platform connected 325 million smart home appliances (excluding laptops and handsets) by end 2020.[9] Alibaba and Huawei have also developed large-scale consumer IoT platforms.

These firms are leveraging strengths in networking and artificial intelligence (AI) to enter new sectors, notably intelligent connected vehicles (ICVs). Baidu's Apollo, the world's first open-source ICV platform, has over 130 corporate partners, including foreign industry leaders like Volkswagen and Toyota. Huawei is a founding member of the international 5G Automotive Association and is extensively involved in international development of ICV systems. Xiaomi recently announced its own project to build a "best-in-class" ICV ecosystem for customers worldwide.

The performance demands of these emerging IoT ecosystems are in turn driving Chinese firms to become global leaders in enabling technologies. For example, in 2020, Alibaba introduced a leading-edge computer processor based on open-source RISC-V architecture. Such developments have potential to reshape the global information and communications technology (ICT) industry landscape and give leading Chinese digital technology firms greater influence abroad, while stimulating economic development at home.

The IoT's development in China also benefits from massive state-led spending on enabling infrastructure. By mid-2021, Chinese authorities claimed that the nation had installed over 800,000 5G base stations, around 70 percent of the global total. China's state-owned telecoms operators are projected to invest more than 200 billion USD over 2020 - 2025 in network infrastructure.

In mid-2020 the city of Shenzhen announced that it had achieved comprehensive coverage with 5G 'standalone' networks, which will provide the foundation for the IoT's more transformative applications, such as ICVs. Shenzhen has installed 46,000 base stations, compared to 850 standalone 5G sites across Germany in early April 2021.[10] In late 2020 a Chinese state-owned enterprise completed the first phase of a dedicated satellite constellation to support IoT services, which is due to be fully operational by 2023.

Chinese cities were global pioneers in deploying "smart city" management systems and platforms for commercial services based on narrow-band-IoT (NB-IoT) technology, through projects delivered by China's state-owned telecoms operators and Huawei. These early deployments translated into international industry leadership, with China Unicom, China Telecom and Huawei recognized by GSMA as key players in NB-IoT development globally.[11]

Beijing's strategic technology plans have for many years promoted the development of new network infrastructure technologies, addressing the technical requirements of the emerging IoT. For example, the 12th Five Year Plan (2011-2015) included among its major science projects a program (CENI) to develop alternative network architecture for the future internet. This program's backbone network became operational for testing purposes in April 2021.[12]

The rising profile of Chinese entities in IoT technologies has led to growing foreign interest in collaboration, particularly from European actors (see Exhibit 1). For a decade, the IoT has featured in dialogues between China's Ministry of Industry and Information Technology (MIIT) and the European Commission. In 2016 the Commission's DG-CONNECT co-published an IoT development policy paper with the Chinese Academy of Information and Communications Technology (CAICT). The Commission-backed Future Internet Research and Experimentation (FIRE) project has institutionalized collaboration with Chinese researchers and will reportedly connect to China's newly operational CENI network.[13]

The rising profile of Chinese entities in IoT technologies has led to growing foreign interest in collaboration, particularly from European actors

Exhibit 1

Selected Europe-China IoT collaborations

PARTNERING INSTITUTIONS	FIELD OF COLLABORATION
German Corporation for International Cooperation (Giz) - China Academy of Information and Communications Technology (CAICT)	Sino-German Cooperation on Industrie 4.0: strengthening industrial cooperation in intelligent manufacturing
SAP - Huawei	Cloud Partnership
SAP - Nanjing	Utilization of SAP IoT to analyze traffic movement patterns in real time
Dassault Systèmes - Huawei	Dassault Systèmes' 3DEXPERIENCE platform provided through Huawei Cloud
Siemens - Alibaba	Siemens' MindSphere operating system provided through Alibaba Cloud
Bosch - Huawei	Bosch IoT Suite services provided through Huawei Cloud
Ministry of Science and Technology of China - Innovation Fund Denmark	Research and innovation collaboration on green urban development (AI & IoT named as a priority)
Irootech - Putzmeister, Munich Reinsurance Company, Telenor Connexion	Irootech's RootCloud IIOT platform provided in European markets
Lenovo - Schneider Electric	Smart green manufacturing solutions for the Chinese manufacturing sector
ABB - Huawei	ABB Ability digital solutions provided through Huawei Cloud
1NCE - China Telecom	Partnership for the commercial launch of China Telecom's NB-IoT roaming SIM

Source: MERICS

© MERICS

The Alliance for Internet of Things Innovation, launched in 2015 to drive growth of a European IoT ecosystem, has signed a memorandum of understanding (MoU) with its Chinese counterpart the Alliance for Industrial Internet (AII). The AII counts among its members the German industry leaders SAP, Siemens and Schneider Electric.[14] The three-year EXCITING project, backed by a consortium of European and Chinese firms and research institutes, studied China's innovation ecosystem for 5G and IoT technologies to better promote Sino-European collaboration.[15]

Europe-China IoT-related collaborations have continued despite growing political tensions with Beijing, US pressure for technological 'decoupling' and growing European concerns about China's 'uneven playing field' for foreign firms. The German government is negotiating a new (MoU) to succeed the 2015 MoU with MIIT on intelligent manufacturing, reportedly with greater focus on the IoT.

Commercially, European firms continue to work with Chinese Technology providers. This is happening despite increased focus on security risks associated with Chinese firms and the Commission's goal of achieving European global leadership in 5G and 6G technologies. Last year, Nokia partnered with China Mobile IoT (CMIoT) to deliver IoT connectivity and services to CMIoT's customers in China and abroad. Ericsson is assisting China Telecom to develop commercial standalone 5G services.[16]

2.2 The Chinese state helps drive IoT development

The IoT is the next step in the pervasive application of ICT ("informatization") that China's top leadership identified two decades ago as a universal trend, that must be mastered to succeed in a competitive world. The implications were recognized in the 2016 guidance on "informatization" issued by the State Council, the highest executive agency of China's government. "New technologies... drive the evolution of cyberspace from interconnection of everyone to interconnection of everything, and digital, networked and intelligent services will be ubiquitous. The real world and digital world are increasingly... integrated."[17]

China's top-level focus on building the IoT goes back to 2009, when it was included in Premier Wen Jiabao's work report to the national legislature as one of five "strategic emerging industries." In 2010, the State Council issued a decision on strategic new emerging industries that included promoting the IoT. In 2012, MIIT identified the IoT as technological "strategic high ground", and alongside another powerful ministry, the National Development and Reform Commission, articulated basic tasks and priorities that have guided IoT development in China over the past decade. These policies drove establishment of industrial clusters and demonstration zones to concentrate R&D and implementation efforts.

China's top-level focus on building the IoT goes back to 2009

National and regional state agencies have continued churning out directives to stimulate IoT development. More than two dozen policies and plans were issued at national level alone from 2010 to 2020. For example, the Industrial Internet Development Action Plan issued by MIIT in January 2021 includes goals such as establishing 30 factories fully connected by 5G services and developing industrial internet platforms 'with international influence'.[18]

The State Council's 2015 "Made in China 2025" action program for building China into a manufacturing superpower called for accelerating IoT research and applications, with multiple IoT-related technologies listed in the associated "priority technical fields" roadmap. The State Council also in 2015 issued guidance on an 'Internet Plus' approach aimed at "deep integration" of the internet across China's economy and society.

In 2016, the State Council assessed that the 13th Five Year Plan (2016-2020) would coincide with critical technological changes worldwide, transitioning "from accumulation of potential to the collective efflorescence" of new technologies, led by the IoT.[19] Accordingly, the State Council and MIIT directed that a foundational infrastructure for the industrial internet be established by end 2020. MIIT issued an IoT development plan for this period, and in September 2020 commenced assessment of the results. These efforts' outcomes will shape the extent which China can achieve "deep integration" of the internet across multiple industries, a key goal over the period of the 14th Five Year Plan adopted in March 2021.

Public-private partnerships have also been utilized to drive development of China's IoT ecosystem, including enabling technologies like 5G infrastructure. For example, the IMT-2020 5G Promotion Group was established by three national ministries in 2013 to coordinate efforts by government, state-owned enterprises, private businesses and research institutes. The Alliance of the Industrial internet (AII) was set up in 2016 with similar goals.

China's leading digital technology firms have partnered with governments and state-owned telecoms operators on specific IoT projects. Alibaba, for instance, collaborated with the Wuxi city government on a "smart city" management platform, which combined Alibaba's big data analytics with Wuxi's advantages as a demonstration zone for IoT sensing devices.[20] Another example is the co-operation between CAICT, China Telecom and Huawei on the industrial internet testbed MQM to assist Haier in improving manufacturing quality control.

Sector-specific policies are also employed to stimulate IoT development. China's state-endorsed National Innovation Centre for Intelligent Connected Vehicles has set a goal for more than half of new vehicles sold nationwide to incorporate self-driving technology by 2025. As of December 2020, Shanghai's government had opened almost 600 kilometers of roads for testing of ICVs and integrated traffic infrastructure.

By 2016-17, CAICT's assessment was that China had developed a relatively complete IoT supply chain, albeit with "bottlenecks and deep-seated problems." CAICT's annual IoT White Papers have repeatedly highlighted systemic problems such as supply chain decentralization and inadequate product scalability, drawing unfavorable comparisons with an American IoT development ecosystem perceived as more streamlined and mature. The AII assessed in its 2019 Industrial Internet white paper that most Chinese enterprises are still struggling with basic levels of digitalization, and not yet able to generate income from internet platforms.

To address these obstacles, Chinese actors have sought partnerships with foreign industry leaders and IoT industry alliances. In this, they have enjoyed considerable success – in February 2021, Huawei alone had at least 38 IoT partnerships with non-Chinese actors.

So far, China's state-led IoT industrial policy has produced the most notable tangible results within China itself, which by one estimate accounted for around 90 percent of global NB-IoT connections in December 2019.[21] Even with these numbers, it appeared that China would fall short of MIIT's target of 600 million NB-IoT connections nationwide by end 2020.[22] Nonetheless, this progress shows how the Chinese state's promotion of R&D capabilities and market creation drives the IoT sector's development. By contrast, Japanese telecoms firm NTT shut down its NB-IoT service in 2020, apparently due to lack of take-up.

China's IoT connections now represent 30 percent of the global total , according to CAICT's most recent assessment in its white paper of December 2020. It assessed that China's total IoT sector had maintained an average annual growth rate of 20 percent in the 2016-2020 period. This growth helps explain why global leaders such as European auto-majors are now locating R&D operations inside China and entering partnerships with Chinese industry leaders in IoT-related fields such as connected vehicles. Examples include Huawei's partnership with Stellantis and Alibaba's with BMW and Ford Motors. Volkswagen is investing EUR 15 billion into electric vehicle development in China over the next four years.

China's IoT connections now represent 30 percent of the global total

US government 'decoupling' pressures present a challenge to this progress. China's IoT ecosystem is now faced with the threat of losing access to "core technologies" such as high-performance semiconductors, as well as to export markets and foreign industry partnerships. The Chinese state has responded by doubling down on the goal of increased national technological and economic self-reliance. The new 'dual circulation' slogan stresses development of self-sustaining domestic economies by leveraging new technologies such as the IoT. In January 2021, Xi Jinping described the digital transformation of infrastructure as China's economic "booster and gas pedal", despite "technological blockade by the US".[23]

A critical piece of the strategy to move Chinese firms up the technological ladder is to play a greater role in shaping the standards that guide ICT development. Standards-setting is becoming an increasingly contentious issue in advanced economies' relations with China. In the EU-China Comprehensive Agreement on Investment (CAI), provisionally signed in December 2020, Beijing agreed to provide equal access to China's domestic standards-setting bodies. How China pursues standardization domestically and abroad has particularly significant implications for evolution of the IoT, as a globally connected 'system of systems.'

2.3 China aims to shape standards for the IoT

IoT-related standardization in China takes place under the auspices of MIIT and the Standardization Administration of China (SAC). Much of this work is done by technical standardization committees that are nominally independent, though in reality they have close links to Chinese state agencies. For example, TC-260, which works on national information security standards, is headed by the Deputy Director of the Cyberspace Administration of China. Foreign firms are allowed limited participation in such bodies, but it appears that foreign contributions are only facilitated when consistent with Chinese policy goals.

Standards-setting within China is a multi-stakeholder process: China's leading technology firms are among the most influential actors and have had a prominent role in developing standards linked to the IoT. However the closed nature of China's technical standardization processes has led to significant divergence with standards abroad; by one estimate, only 15 percent of standards issued by TC-260 are currently aligned with international standards.[24]

China is seeking to internationalize its domestic standards by promoting them abroad

State recognition that Chinese firms are at a competitive disadvantage abroad if subject to parallel Chinese and foreign standards has led to attempts to rationalize domestic standards and harmonize them with international ones. At the same time, China is seeking to internationalize its domestic standards by promoting them abroad. In 2019, SAC published policy objectives that included enhancing standards cooperation and integration with countries participating in China's 'Belt and Road' infrastructure-building initiatives.

The revised draft of China's "Administrative Measures for National Standards," issued by China's market regulator in December 2020, directs that "development of national standards shall be based on adoption of international standards, in line with China's national conditions." Where Chinese standards have not yet incorporated international ones, it directs that foreign-language editions of extant Chinese standards be issued. Additionally, SAC issued "Guidelines on Adoption of International Standards", promoting "simultaneous initiation of international standardization projects proposed by China and of Chinese national standardization projects" and prioritizing their adoption in "key sectors" including the IoT.[25]

Nonetheless, China has yet to achieve a unified approach to IoT technical standardization. In 2019, SAC established a national coordinating body (SAC/TC28/SC41) with a mandate for comprehensive IoT standardization, which was expressly nominated to be a direct counterpart to the international standardization body responsible for the IoT and related technologies.[26] However this body's membership does not include the organization (CCSA) responsible for networking communication and security, which continues to develop standards issued by MIIT relevant to communication aspects of the IoT's.

This has apparently resulted in some "siloing" of IoT technical standardization work between ecosystems led by MIIT and SAC. However, it would be inaccurate to view all aspects of China's IoT standardization ecosystems as fragmented. MIIT and SAC jointly issued guidelines for standardizing the industrial internet in 2019, which appear to reflect input from the AII. The AII is also involved in regulating deployment of China's new industrial internet identification resolution system that will operate in parallel with the global internet's addressing system, which was developed by CAICT and is being trialled nationwide.

Standards development organizations (SDOs) within China have also pursued standards development by industry sector in tandem with real-world implementations. The pace of IoT-related standardization therefore responds to market forces, and not only the Chinese state's declared priorities. The SAC's webpage indexing "IoT standards" in January 2021 listed 76 national standards; 30 industrial standards; and 62 local, province-level standards. This probably results in some overlap and inconsistency. However, it also reflects the general challenge in standardizing the IoT that stems from the diversity of systems constituting it.

Overall, Chinese actors are having a notable impact on global IoT standardization processes. Ten out of 18 IoT-related standards adopted by late 2020 by two transnational SDOs – the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) – were proposed by Chinese actors. Development of the reference architecture (ISO/IEC 30141) for IoT standards – which the European Commission is committed to propagating under its rolling plan for IoT standardization – was led by China's Wuxi IoT Research Institute. Its director observed that this standard "will be universally accepted in the IoT industry like a 'constitutional law'."[27]

Chinese actors are having a notable impact on global IoT standardization processes

3. WILL THE IOT ACCELERATE THE WORLD'S DIGITAL DIVISION INTO A 'SPLINTERNET'?

As China's influence over the IoT grows, other nations are being forced to assess the risks of connections to Chinese networks. In many liberal democracies, concerns are increasingly being raised about the CCP's political values and methods. These are reflected in debates over involvement by Chinese firms in 5G networks and the role of Chinese actors in technical standardization. Concerns about alleged Chinese state-sponsored cyber-espionage and purported state control over firms like Huawei has spilled over into debates on the IoT.

Some experts question whether the emerging "Internet of Everything" can ever be acceptably secured, if it is populated with Chinese-made devices and connected to Chinese networks. This has led to increasingly urgent arguments for complete disconnection from Chinese networks, and from those of countries that refuse to do so.[28]

Such thinking likely informed the Trump administration's 'Clean Network Program', which encouraged other countries to exclude Chinese actors from their digital ecosystems, and other recent US government initiatives such as the US telecom regulator's termination of licenses for Chinese operators.

The Biden administration is continuing this general approach in a more calibrated manner. In March 2021, the US government served subpoenas on multiple unnamed Chinese firms that provide ICT services within the US, utilizing President Trump's 2019 Executive Order on securing the ICT supply chain. The US government recently completed reviews of the supply chains for semiconductors, large capacity batteries and critical minerals and materials – which are all foundational elements of the IoT – and is conducting a review into the US ICT industrial base as a whole, while the Secretary of state is promoting international cooperation "to foster a secure and trustworthy alternative" to Chinese digital technologies.[29]

In June 2021 the US Senate passed a bill, supported by President Biden, that includes a range of measures directed at competition with China in digital technologies and their implementations worldwide. And while in early 2021, President Biden pledged to "work with Beijing when it's in America's interest to do so", his words also reflected the perceived imperative in the US policy establishment for "some degree of technological bifurcation" with China.[30]

However, in pursuing selective decoupling, the US faces not just significant costs from eroding the global economies of scale that have supported ICT advances for decades, but also resistance in many nations to excluding Chinese technology.

Many developing nations prioritize economic and technological development, and already have an extensive Chinese presence in their digital infrastructure and technology collaborations. This influences their choices about the future internet and the involvement of Chinese actors. Indonesia and Malaysia for example recently signed agreements with Beijing on cybersecurity and capacity building, and they are implementing 'smart city' projects with Chinese firms like Huawei. Other large emerging economies like Brazil and South Africa are allowing Chinese firms to participate in their next-generation telecoms networks.

This means that even if countries within a politically "trusted community" commit to purging their digital networks of Chinese technology, they can still expect to face its presence across large areas of the world. For example, foreign transport markets might still be populated with vehicles made in China and operated by AI platforms designed by Chinese firms, using networking standards co-developed with Chinese actors and telecoms infrastructure built by Chinese firms. And within such a trusted community, the cost of developing 'China-free' technological ecosystems would rise significantly, due to reduced economies of scale.

Furthermore, technologically advanced liberal democracies disagree among themselves over the extent and type of state control to be imposed on the internet. Divergence between the US and EU over regulation of data storage and transfers, platform businesses and other internet-based activities seems to be widening, despite continuing efforts to reconcile these differences. Leading technology firms from countries like Germany, Japan and South Korea are continuing to invest in China and work with Chinese partners.

The prospect of the global internet 'splintering' cleanly is unlikely

Despite much talk of coordinating technology and industry policy vis-a-vis China, in most countries there appears to be little appetite for extensive 'decoupling'. And so far, governments are not providing resources sufficient to substitute for the opportunities offered by China's emerging IoT ecosystem. At the same time, competition is rising between advanced economies for dominance of future technologies and markets. This can be seen in the EU's growing flurry of policies directed at achieving 'digital sovereignty', at the expense of US business interests.

The prospect of the global internet 'splintering' cleanly, into a "liberal democratic" internet on the one side and a Chinese-dominated cyberspace on the other, is unlikely. The world will instead probably see a continued and messy evolution towards a 'federation' of networks, interconnected but increasingly divergent. The US continues to pursue technological 'decoupling' with China, which for its part seeks reduced reliance on the US and its 'like-minded partners' for "core technologies." Third parties will likely continue pursuing their own paths in between these two poles, choosing elements and connections that suit them.

4. EUROPE NEEDS TO TAKE ACTION TO COMPETE IN A CONTESTED IOT WORLD

The European Commission has taken various measures to promote European innovation and a single market for the IoT, including establishing the Alliance for Internet of Things Innovation, investing almost EUR 500 million over 2014 to 2020 and managing a rolling plan for IoT standardization.[31] The Commission's 'Digital Compass' roadmap announced in March 2021 sets ambitious targets for European digital transformation by 2030, and has at its core enabling technologies like the IoT. In parallel, the EU's cybersecurity process is addressing the IoT's implications for the security of European networks.[32]

The EU should double down on such measures to compete with the growing influence of 'China Inc.' over global markets for IoT applications and the underlying infrastructure. As challenges inevitably arise, European leaders may be tempted to fall back on the so-called 'Brussels effect', relying on the single market's global importance to ensure that EU regulations and standards are propagated worldwide by non-European actors. But shaping technology adoption requires more than simply specifying standards: "referees do not win the game".[33] Pooling Europe's advantages to build competitive products and services across the IoT ecosystem is necessary to compete.

European leaders should also focus on adjusting diplomatic objectives to the expanding community of actors shaping the global IoT. An informal proposal for the future of EU cyber diplomacy developed in 2020 by several member-states calls for European governments to "shape the [global] digital environment" and "build trust and dependable relationships," but does not address how to tackle the conflicting interests that are increasingly apparent.[34]

European leaders should also focus on adjusting diplomatic objectives to the expanding community of actors shaping the global IoT

For example, the European Commission's new "Digital Compass" emphasizes growing European digital connections with Africa. The African Union will be the first regional partner in the EU's recently launched Digital4Development Hub, aimed at "promoting a comprehensive values-based rulebook for a digital economy and society worldwide".[35] Yet South Africa and Kenya, two of the continent's most important economies, have chosen Huawei for their 5G infrastructure rollouts.

As of mid-2020, Huawei – which by one, admittedly controversial, estimate has equipped 70 percent of Africa's wireless broadband networks – had not lost any contracts from Africa governments due to security concerns, let alone concerns about "use of digital tools by authoritarian states ... contrary to the idea of a free, open and global internet."[36]

Addressing such divergent attitudes outside Europe towards Chinese "digital authoritarianism" is crucial. The IoT will increasingly be shaped by the developing world. The global South now accounts for the vast majority of internet users and the lion's share of economic growth worldwide. As developing nations increasingly contribute to digital technological development, their preferences on design and governance of the IoT, and the systems built upon it, will need to be accommodated in an integrated global economy.

One metric for this trend is provided by the collaborative software development platform GitHub, which estimates that by 2025 the US share of its users will halve compared to 2015, with an equivalent increase from developing nations.[37] Many of these countries are now engaged in infrastructure and logistics projects involving Chinese actors and branded under Beijing's 'digital silk road'. This promotes integrated digital infrastructure solutions that build-in emerging technologies like AI and digital currencies, in which China is striving to lead.

If Europe is to remain integrated in an internet-based economy global in scale, rather than confined to a relatively small group of "like-minded" states, it must find common ground with China and other emerging actors on the IoT's design and regulation. This requires grappling with approaches to internet architecture and management that go beyond those inherited from the 1990s-2000s. At the same time, connection with Chinese networks implies significant risks that will expand in tandem with the IoT, requiring potentially costly mitigation measures and likely placing limits on the desirable extent of international connectivity.

Connection with Chinese networks implies significant risks that will expand with the IoT

One potential approach is to focus on global cooperation to protect the internet's "public core", meaning elements that facilitate international data transfers (such as the domain name system and networking protocols). Supporting the security and stability of this essential function "as a global public good" is already mandated by the EU's Cybersecurity Act. The "public core" concept is also referenced in the Commission's December 2020 Cybersecurity Strategy and proposal to update the EU's Network and Information Systems (NIS) Directive, which if accepted would require member-states to adopt policies "related to sustaining the general availability and integrity of the public core of the open internet."[38]

This approach implies prioritizing international cooperation to maintain shared systems of common interest, potentially at some expense to propagation of political values. Western governments are already engaging in such limited compromises with greater frequency, as they diverge in regulatory practice from the widest conceptions of 'internet freedom.'

Prioritizing internet infrastructure also implies moving beyond the focus on content regulation, human rights and malicious cyber activity that still dominates debates over "internet governance." Shared interests in the internet's functionality as a global public good are readily identified. For example, managing network congestion requires international coordination; the alternative would be for each party to massively expand its own infrastructure and incur significant increases in costs.[39]

A focus on common-interest cooperation further implies keeping the challenges presented by Chinese actors in perspective, and not overreacting to their involvement in global infrastructure development or standardization processes. As an example, the negative reaction to the Huawei-led "New IP" proposal at the International Telecommunications Union was disproportionate to the proposal's content and its potential political significance.[40] Sustaining the internet as a global public good requires some adaptation to the role of politically non-trusted actors, reflected in Beijing's adjustment of its own "cyber sovereignty" concept to accommodate the "multi-stakeholder model| of global internet governance.

Ultimately, much depends on Beijing's own choices. So far, China's leaders have sought to strike a balance between "cyberspace sovereignty" and exchanges with the outside world. Even as technical advances augment the capacity of China's cyberspace governance regime for surveillance and political repression, this regime is still being calibrated to facilitate cross-border connectivity through the internet. This provides, for example, some prospect for convergence with China on regulation of international data transfers.

European decision makers need to closely follow China's evolving approach to the IoT's development on a global scale, and how this is shaping the politics of the "interconnection of everything".

ENDNOTES

[1] See generally DeNardis, Laura (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press.

[2] Lueth, Knud Lasse (2020). 'State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time'. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/; Wilson, Dave (2020). 'IoT is Creating Massive Growth Opportunities'. https://blogs.cisco.com/internet-of-things/iot-is-creating-massive-growth-opportunities; Mobile World Live (2019). 'Qualcomm tips Germany to lead on 5G industrial IoT'. https://www.mobileworldlive.com/featured-content/top-three/qualcomm-tips-germany-to-lead-5g-industrial-iot. Accessed: May 12, 2021.

[3] For an overview of this term's usage, see Pohle, Julia and Thiel, Thorsten (2020). "Digital Sovereignty." Internet Policy Review 9(4).

[4] Lee, John (2020). "Will China reinvent the Internet?" https://www.thechinastory.org/will-china-reinvent-the-internet/. Accessed: May 12, 2021. (Hereafter 'Lee, Will China Reinvent the Internet?" (2020)').

[5] Panwar, Shivendra (2020). "Breaking the Latency Barrier." https://spectrum.ieee.org/telecom/wireless/breaking-the-latency-barrier. Accessed: May 12, 2021.

[6] Cisco Annual Internet Report (2018–2023) White Paper (2020). https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed: May 12, 2021.

[7] Platform Industrie 4.0 (2020). "I4.0 x Industrial Internet: Practices and Findings" https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/China/i4-0-x-industrial-internet-practices-and-findings.html. Accessed: May 12, 2021.

[8] Onag, Gigi (2020). 'Haier gets its second "lighthouse" for advanced manufacturing https://futureiot.tech/haier-gets-its-second-lighthouse-for-advanced-manufacturing/

[9] Tang, Flora (2020). 'Xiaomi's IoT Move: Strategy, Investment Philosophy, Challenges and Success Drivers'. https://www.counterpointresearch.com/xiaomis-iot-move-strategy-investment-philosophy-challenges-success-drivers/; Onawole, Habeeb (2020). "Xiaomi Q3 2020 financial report reveals it recorded 46.6 million shipments". https://www.gizmochina.com/2020/11/25/xiaomi-q3-2020-financial-report-reveals-it-recorded-46-6-million-shipments/; Shen, Jill (2021). "Xiaomi invests $1.5 billion in fully owned EV business". https://technode.com/2021/03/31/xiaomi-invests-1-5-billion-in-fully-owned-ev-business.Accessed: May 12, 2021.

[10] Handelsblatt (2021). "Why Shenzhen has more 5G stations than all of Europe" (in German). https://www.handelsblatt.com/technik/it-internet/kolumne-asia-techonomics-warum-shenzhen-mehr-5g-stationen-als-ganz-europa-hat/27045968.html. Accessed: May 12, 2021.

[11] Chen, John; Walz, Emily; Lafferty, Brian; McReynolds, Joe; Green, Kieran; Ray, Jonathan; and Mulvenon, James (2018). "China's Internet of Things: Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission", 91-92.

[12] South China Morning Post (2021). "China starts large-scale testing of its internet of the future". China starts large-scale testing of its internet of the future | South China Morning Post (scmp.com). Accessed: May 12, 2021.

[13] SIGMA-ORIONIS (2015). "EU-China FIRE announces exciting final outcomes supporting EU-China cooperation on FIRE and IPv6". EU-China FIRE announces exciting final outcomes supporting EU-China cooperation on FIRE and IPv6 | News | CORDIS | European Commission (europa.eu). Accessed: May 12, 2021.

[14] Wessling, Claudia; Shi-Kupfer, Kristin; von Carnap, Kai; Arcesati, Rebecca; and Holzmann, Anna (2020). "China's digital platform economy: Assessing developments towards Industry 4.0", 9. https://merics.org/en/report/chinas-digital-platform-economy-assessing-developments-towards-industry-40. Accessed: May 12, 2021.

[15] EXCITDING, The EU-China Study on IoT and 5G (2019). https://www.euchina-iot5g.eu/. Accessed: May 12, 2021.

[16] Nokia (2020). "Nokia enables China Mobile with enterprise IoT connectivity globally". https://www.nokia.com/about-us/news/releases/2020/11/23/nokia-enables-china-mobile-with-enterprise-iot-connectivity-globally/; Ericsson (2020). "Ericsson and China Telecom achieve 5G Standalone data call with Ericsson Spectrum Sharing". https://www.ericsson.com/en/press-releases/2020/10/ericsson-and-china-telecom-achieve-5g-standalone-data-call-with-ericsson-spectrum-sharing. Accessed: May 12, 2021.

[17] State Council (2016). "13th Five Year Plan: National Informatization Plan" (in Chinese). http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm. Accessed: May 12, 2021.

18 | Ministry of Industry and Information Technology (2021). “Industrial Internet Innovation Development Action Plan” (in Chinese). http://www.gov.cn/zhengce/zhengceku/2021-01/13/content_5579519.htm. Accessed: May 12, 2021.

19 | State Council (2016). “National Development Plan for Strategic New Type Industries” (in Chinese). http://www.gov.cn/zhengce/content/2016-12/19/content_5150090.htm. Accessed: May 12, 2021.

20 | China Daily (2018). “Public-private collaboration drives China’s industrial IoT innovation”. http://www.chinadaily.com.cn/a/201809/07/WS5b95d1c8a31033b4f46551d5.html. Accessed: May 12, 2021.

21 | Clark, Robert (2020). “China crosses 100M NB-IoT connections but still short of target.” https://www.lightreading.com/iot/china-crosses-100m-nb-iot-connections-but-still-short-of-target/d/d-id/759145. Accessed: May 12, 2021.

22 | Ministry of Industry and Information Technology (2017). “Comprehensively Promote the Construction and Development of the Mobile Internet (NB-IoT)”. https://www.miit.gov.cn/jgsj/txs/wlfz/art/2020/art_3f73a956a16940b18a7e753df44a9a58.html. Accessed: May 12, 2021.

23 | Study Times (2021). “Grasp the Focal Point of Building Domestic Circulation” (in Chinese). http://theory.people.com.cn/n1/2021/0125/c40531-32010386.html. Accessed: May 12, 2021.

24 | Wang, Clara (2021). ‘Here’s who has the ear of China’s most active cyber regulator [TC-260]’ (Jan 2021) https://www.protocol.com/china/tc260-china-cyber-regulator-companies; Sacks, Samm and Li, Manyi Kathy. ‘How Chinese Cybersecurity Standards Impact Doing Business in China’. https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china. Accessed: May 12, 2021.

25 | State Administration for Market Regulation (2020). "Measures for the Administration of National Standards (Draft for Comments)” (in Chinese). http://www.moj.gov.cn/government_public/content/2020-12/19/657_3262142.html; Standardization Administration of China (2020). "Guidelines for the Adoption of International Standards in National Standards (2020 Edition)” (in Chinese). http://www.sac.gov.cn/sbgs/sytz/202101/t20210111_347021.htm. Accessed: May 12, 2021.

26 | Standardization Administration of China (2019). ‘Announcement of the Proposed National Information Technology Standardization Technical Committee on the Internet of Things Sub-Technical Committee’ (in Chinese). http://org.sacinfo.org.cn:8088/tcrm/recruit-index/notice/1672.do. Accessed: May 12, 2021.

27 | 2020 Rolling Plan for ICT Standardisation – Internet of Things’ (‘Action 5: Promote the development and foster the adoption of the international Reference Architecture for IoT developed in ISO/IEC JTC 1 SC41) https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/internet-things; http://www.chinadaily.com.cn/m/jiangsu/wuxi/2018-07/11/content_36556927.htm

28 | See for example Demchak, Chris (2018). ”Three Futures for a Post-Western Cybered World”. Military Cyber Affairs 3(1); Clarke, Richard and Knake, Rob (2019). “The Internet Freedom League: How to Push Back Against the Authoritarian Assault on the Web”. Foreign Affairs (Sep/Oct); Cohen, Jared, and Fontaine, Richard (2020). “Uniting the Techno-Democracies: How to Build Digital Cooperation”. Foreign Affairs (Nov/Dec).

29 | The White House (2021). “Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities.” https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/. Accessed: June 9, 2021. Bloomberg (2021). “Blinken Says U.S. Won’t Force ‘Us-or-Them’ Choice With China”. https://www.bloomberg.com/news/articles/2021-03-24/blinken-says-biden-won-t-force-us-or-them-choice-with-china. Accessed: May 12, 2021.

30 | The White House (2021). “Remarks by President Biden on America's Place in the World”. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/; China Strategy Group (2020). “Asymmetric Competition: A Strategy for China & Technology”. https://beta.documentcloud.org/documents/20463382-final-memo-china-strategy-group-axios-1. Accessed: May 12, 2021.

31 | European Commission (2021). “Europe's Internet of Things Policy”. https://ec.europa.eu/digital-single-market/en/internet-of-things; European Commission (2020); European Commission (2021). “Rolling Plan for ICT Standardisation 2021”. https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2021. Accessed: May 12, 2021.

32 | European Union Agency for Cybersecurity (2021). “Internet of Things”. “ https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot. Accessed: May 12, 2021.

33 | European Council on Foreign Relations (2020). “Europe’s digital sovereignty: From rulemaker to superpower in the age of US-China rivalry”. https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/. Accessed: May 12, 2021.

34 | “Non-Paper on EU Cyber Diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia”. EU Cyber Diplomacy – working together for a free and secure cyberspace - Federal Foreign Office (auswaertiges-amt.de). Accessed: May 12, 2021. (Hereafter “Non-Paper on EU Cyber Diplomacy (2020)”).

35 | European Commission (2020). “Team Europe: Digital4Development Hub launched to help shape a fair digital future across the globe”. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2321. Accessed: May 12, 2021.

36 | Bloomberg (2020). “Huawei Strengthens Its Hold on Africa Despite U.S.-Led Boycott”. https://www.bloomberg.com/news/articles/2020-08-19/china-s-huawei-prospers-in-africa-even-as-europe-asia-join-trump-s-ban; Non-Paper on EU Cyber Diplomacy (2020). Accessed: May 12, 2021.

37 | Github (2020). “The 2020 State of the Octoverse”. https://octoverse.github.com/. Accessed: May 12, 2021.

38 | European Commission (2020). “Revised Directive on Security of Network and Information Systems (NIS2)”. https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2. Accessed: May 12, 2021.

39 | Rauscher, Karl Frederick (2019). “US–China Collaboration on the Internet of Things Safety: WHAT NEXT?”. https://www.atlanticcouncil.org/wp-content/uploads/2019/12/US-China-Collaboration-on-IoT-Report-web.pdf. Accessed: May 12, 2021.

40 | Lee, “Will China Reinvent the Internet?” (2020); ICANN Office of the Chief Technology Officer (2020). “New IP”. New IP (icann.org) Accessed: May 12, 2021.

ACKNOWLEDGEMENTS

The author would like to thank MERICS colleagues and external peer reviewers who engaged with this report through substantive input, suggestions and feedback, in addition to reviewing previous drafts of the text. In particular, the author would like to thank Valentina Vengust for providing research support.

CONTACT
John Lee
Senior Analyst, MERICS
john.lee@merics.de

EDITORIAL TEAM
Claudia Wessling
Director Communications
and Publications, MERICS
claudia.wessling@merics.de

GRAPHICS AND LAYOUT
Alexandra Hinrichs
Graphic Designer, MERICS

PUBLISHER
MERICS | Mercator Institute for China Studies
Klosterstraße 64 | 10179 Berlin
Tel.: +49 30 3440 999 0
Mail: info@merics.de
www.merics.org