Testimony of

Mark P. Dallas, PhD

Associate Professor of Political Science & Asian Studies, Union College, NY
Director of Asian Studies, Union College, NY
Council on Foreign Relations, IAF-TIRS

Before the
U.S.-China Economic and Security Review Commission

Hearing on
"U.S.-China Competition in Global Supply Chains"

June 9th, 2022

Washington, DC

Table of Contents

1. Executive Summary

Supply chains raise thorny policy challenges for all countries. Not only are they complex, but they vary enormously across industries, with each product and production process having unique features. Furthermore, many of these features change rapidly. As such, it is often impossible to discuss 'supply chains' in generic terms, and impossible to create one-size-fits-all frameworks or policy solutions.

Supply chains also force countries to confront new vulnerabilities that have arisen as both innovation and production have become more globalized. Most fundamentally, these new realities compel us to seriously re-think some foundational concepts, including our understanding of 'economic and national security,' 'critical infrastructure,' 'dual-use,' and other commonly used policy concepts. As one small example, consider just one 'link' in the mobile telecommunications supply chain – mobile applications. Are the mobile apps installed on every American's smartphone a matter of national security? Are they a new form of critical infrastructure? These are new questions that remain unanswered, even as they regularly, and often unexpectedly, rise to the level of policy relevance.[1]

Obviously, China is deeply integrated with global supply chains, and this creates interdependencies between countries and new vulnerabilities. Our key task, as I see it, is not to cut China out of global supply chains that intersect with the United States, but to understand which circumstances create unacceptable risk, and which create tolerable or benign risk. For example, interdependency with China should not automatically be interpreted as vulnerability, even when Chinese companies possess large market shares in a particular link in a supply chain. We should worry about *asymmetric* interdependence, not all forms of interdependency. The best way to illustrate this is through data. As such, Section 2 of this testimony offers a brief, non-technical but deep-dive into one slice of the mobile telecommunications supply chain, based on very detailed studies I have carried out with many research collaborators.[2]

The purpose of this empirical deep-dive is, first, to demonstrate the complex trade-offs between benign interdependence and vulnerability. It is hard to fully appreciate the degrees of supply chain complexity and flexibility without engaging with their industry-specific idiosyncrasies through data. Second, the data also demonstrate the challenges of any future government efforts to monitor, regulate, let alone positively shape supply chains. Nevertheless, for critical supply chains, there still are many pragmatic actions governments can take to enhance economic and national security, as discussed in Section 4.

The empirical deep-dive also helps us to better understand China, the topic of Section 3. For China, information-communication technologies (ICTs) are somewhat paradoxical: it arguably is the sector about which the Chinese government feels the most vulnerability (based on policy documents and industrial policies), even when Chinese firms play important roles in the global industry, with Huawei as just one leading example. The reason is simple to state, but challenging to unravel empirically: China's leading firms, like Huawei, are substantially dependent on a host of technologies, machinery, hardware and

[1] For instance, the August 6, 2020 "Executive Order on the Threat Posed by TikTok" stated that "the spread in the United States of mobile applications developed an d owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States." This assessment was based on perceived risks to data collection, disinformation and censorship because the app had been "downloaded over 175 million times in the United States and over one billion times globally." Tiktok is a video-sharing mobile app owned by the Chinese company, ByteDance. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

[2] Most of the data in Section 2 consist of statistics based on large-scale proprietary databases and are the result of two years of collaboration with Timothy Sturgeon (MIT), Daria Taglioni (World Bank) and Eric Thun (Oxford University). Additional open-source data was analyzed in conjunction with Jing-Ming Shiu (National Cheng Kung University in Taiwan). Detailed data in Section 3 on Chinese news media derive from collaborations with Yeling Tan (University of Oregon), Abraham Newman (Georgetown University) and Henry Farrell (Johns Hopkins University). This report would have been impossible to write without these collaborations, although the views expressed in them are solely my own.

software components, and standard-setting processes that they do not control, and which have their center of gravity firmly set, for now at least, in OECD countries. Understanding the structure and dynamic of the ICT sector helps explain this paradox. Thus, by examining the ICT sector, we can see where China's and America's sense of vulnerability through interdependency intersect and clash.

One conclusion from the empirical deep-dive is to illustrate that while China possesses some key capabilities that expose America (and our allies) to vulnerabilities, China's dependency on the US and US-allied countries is far greater. As such, China's sense of vulnerability and insecurity is substantially elevated. This is confirmed in Section 3 which offers some insights into China's *perceptions* of technological and supply chain vulnerability, as well as China's concrete *policy* actions. These include both longer term trends in Chinese industrial policies (since early 2000s), as well as more recent reactions to American policy and world events (since 2018).

Broadly speaking, Chinese policy should be interpreted as 'defensive' and 'reactive,' and derived from their perceptions of vulnerability. While mostly harmful, China's long-standing industrial policies are aimed as much at reducing vulnerabilities from dependency on foreign technology in critical supply chain links (e.g. semiconductors), as they are aimed at enhancing China's overall economic development, or solving particular political goals (stability) or social challenges (e.g. demographic, epidemiological or environmental). Of course, they also sometimes aim at very disturbing goals, like state surveillance which have human rights implications for China and other countries. Nevertheless, China's long-standing goal of 'catching up' in critical technologies, and even their more recent aims of technological 'leap frogging,' are driven by deep-seated insecurities around foreign control over technology-intensive supply chains.

Furthermore, China's insecurities have intensified since trade and technology frictions became elevated in 2018, followed by the massive supply chain disruptions of COVID-19 and interminable lockdowns in China, which have raised alarms in the United States about inflation and dependence on China's export manufacturing sector. Most recently, these have further heightened with the unprecedented coordination among allied countries to impose economic sanctions on Russia and Belarus. These events have reaffirmed China's sense of vulnerability, offered positive affirmation to the policy perspectives of security-oriented bureaucrats in China, and will likely lead China to double down on its already extensive industrial policies to achieve 'self-reliance' in key technologies and critical links in supply chains. While China certainly creates and amplifies these worries to the point of paranoia, the fact of the matter is that there is a deep sense of insecurity in China, which crosses over into techno-nationalism, and other forms of nationalism. Predictably, China's nationalism only makes their circumstances worse, but it can also distort America's foreign policy reactions.

The data on ICTs (Section 2) and analysis of Chinese policies and perceptions (Section 3) lead to another conclusion: China's more aggressive and autarkic industrial policies are likely to fail, though not without inflicting damage on its own economy, and more importantly, on America and our allies. Thus, it is in our own national interest to find a way to reduce China's sense of insecurity, while also enhancing overall US security. Unequivocally, the goal of the American government is always to achieve American national security goals. However, America's sense of security is partly a function of China's sense of security. If China feels insecure, its policy choices will be reactive and harmful to US interests, such as many of its value-destroying industrial policies. In turn, Chinese policies and political rhetoric will enflame American perceptions of China's policy goals. If, in reaction, American policy also becomes knee-jerk and unnecessarily bellicose, then we will all be worse off. In a word, we are interdependent with a rising power and we need to get our policies right. As Dr. Joseph Nye sagely writes, "Thucydides famously attributed the Peloponnesian war to two causes: the rise of a new power and the fear that an established power creates. Most analysts focus on the first half of his statement, but the second is more

within our control."[3] While supply chains are incredibly complex and increasingly geopolitical, with appropriate policy nuance, there are positive-sum outcomes that can be accomplished by building institutions to promote transparency and confidence-building within critical supply chains. These will require the US to employ both carrots and sticks, both bilaterally with China as well as with our allies, as outlined in Section 4 on policy recommendations.

While I propose five specific policy recommendations, as a general rule, our supply chain goals should aim to achieve security *and* openness *and* prosperity. There is no law of nature which says that we must choose between them, and so policy making should at least attempt at a trifecta. Furthermore, to achieve this, we must eschew counterproductive labels that brand policies as 'hawkish' or 'dovish' towards China, such as the debate over maintaining or removing Trump era tariffs. We should acknowledge that the CCP and Chinese leadership will pursue what is in their perceived interests. Thus, US policy should work hard, along with our allies, to shape China's external environment and mold China's perceptions, so that they naturally and willingly behave in ways that are in America's national interests. Both hawk-like and dove-like policies will be needed to achieve this broader strategy.

2. Vulnerability, Security and the Supply Chain Challenge

Supply chains have become increasingly important objects of analysis for businesses, NGOs, governments and academics. However, there is no single definition or way to characterize them, and there is no common nomenclature, with even the term 'supply chain' itself contested.[4] While every analyst has their own research goal (and hence definition), broadly speaking, *supply chains are all of the activities performed by firms and workers in bringing a product from initial conception to final end-use.* This includes research and development (R&D), design, production, distribution, marketing, retail and even recycling. While this definition and the metaphor of a 'chain' may imply that they are always 'linear,' in fact, this is purely an artifact of the very high level of abstraction of this definition.[5] Others prefer 'network' metaphors,[6] and in the ICT sector, my collaborators prefer 'ecosystems.'[7] Below, I introduce the concept of 'massive modular ecosystems' which we developed to analyze ICTs, one focus of my testimony.

It is now clichéd to state that 'supply chains are complex.' What matters more is that each supply chain is complex *in its own way*, and so there is no one-size-fits-all way to analyze them or recommend policy. While there may be some broad similarities between supply chains at the sector-level (food, mining, transportation equipment, business services), it is usually more productive and insightful to dig deeper to the industry-level (wheat, copper, automobiles, legal services). Ultimately, however, each product is organized in its own way. This became evident during the COVID-19 pandemic when shortages of each type of PPE (medical masks, gowns, gloves, ventilators, etc.) had to be managed in different ways by hospitals and governments due to their unique supply chain structures.[8] Even within products, each 'lead'

[3] Nye Jr, J. S. (2020). Power and interdependence with China. *The Washington Quarterly*, *43*(1), 7-21, p. 14.
[4] For instance, 'supply chains' is often the term used in management and operations literatures that offer advice and analysis for companies to enhance efficiencies through improved 'supply chain management.' The term 'global value chains,' by contrast, is more expansive and more political in that it includes the strategic interactions between firms that determine how the division of labor between firms is constructed, and who creates and captures 'value.' For GVCs, see Gereffi, Humphrey and Sturgeon 2005.
[5] Given the sheer complexities of supply chains, this sort of abstraction and simplification is a necessity for insightful research.
[6] Coe, Neil M., and Henry Wai-Chung Yeung. *Global production networks: Theorizing economic development in an interconnected world*. Oxford University Press, 2015.
[7] Thun, Taglioni, Sturgeon and Dallas, "Massive Modularity: Understanding Industry Organization in a Digital Age," 2022.
[8] Dallas, Mark P., Rory Horner, and Lantian Li. "The mutual constraints of states and global value chains during COVID-19: The case of personal protective equipment." *World Development* 139 (2021); Gereffi, Gary. "What does the COVID-19 pandemic teach us about global value chains? The case of medical supplies." *Journal of International Business Policy* 3, no. 3 (2020): 287-301.

firm that manages a supply chain will vary in its size, organization, and business and governance practices. In a word, the closer to the ground that one looks, the more accurate one's understanding of supply chains and the more effective policy will be. However, this will require upgrading of government expertise.

Furthermore, many supply chains change fast, due to market forces, technology changes, government policy, and even the media (e.g. forced labor in Xinjiang cotton). The sheer diversity, complexity and speed of supply chains pose further problems for policy-makers, as discussed in the final section.

The remainder of this section briefly offers a non-technical but deep-dive into one segment of the ICT sector. There are three main takeaways:

(i) Supply chains have multiple and complex layers and links, each layer has its own distinct organization and they interlink with each other in varied ways. These details matter.

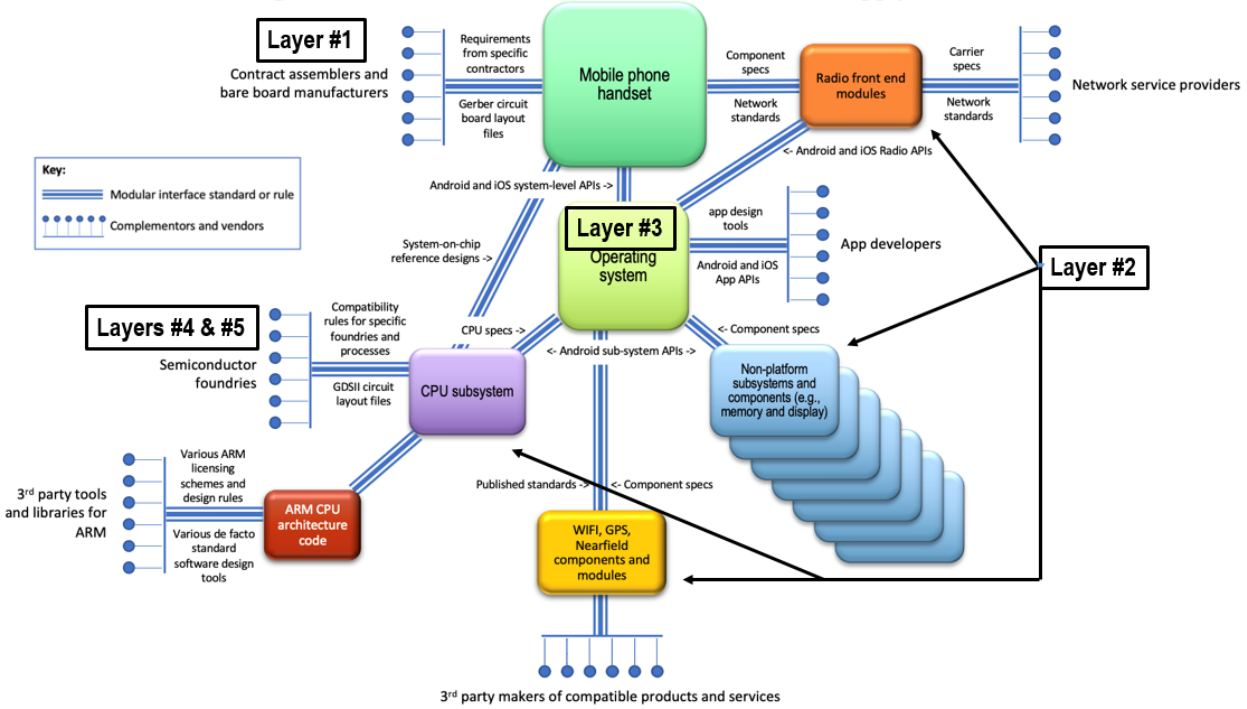
(ii) There can be extreme levels of country-level (and firm-level) specialization which generates interdependencies between countries and companies. Thus, the US is dependent on and possesses vulnerabilities with many countries and companies, not just Chinese ones.

(iii) China's position in supply chains is highly uneven, but in most ICT supply chains and layers, China's position is weak. This matches China's own sense of vulnerability in ICTs, which drives forward their industrial policies. But it is also paradoxical because this is the sector in which the US perceives China to be strongest, with Huawei as a prime example. The paradox is resolved because it depends on which layer and which 'link' within the layer one chooses to look. A strong argument can be made for Chinese strengths or weaknesses, depending on where one wishes to look. Again, the details matter.

Figure 1 is a simplified abstraction of a smartphone supply chain. For the purposes of this testimony, I will briefly focus on only five 'layers' in the ICT stack (labelled #1 to #5 in Figure 1), as well as the double-band links that connect the various boxes. On the outer edges of Figure 1, each 'branch' links to other dimensions and layers in the ever-expanding ICT ecosystem. Furthermore, Figure 1 represents only one device (smartphone), which itself is embedded within much larger systems, some of which consist of critical infrastructure. In other words, many more layers and links would need to be added to understand the full complexity of mobile telecommunications, something which my research collaborators call a 'massive modular system' (MME).[9] A very short list of additional layers might include telecommunications equipment and infrastructure, internet infrastructure, cloud computing (increasingly important in 5G era), among others, each of which would require their own simplified abstraction similar to Figure 1. Some fork-shaped branches also link to consumer platforms such as the Apple or Google app stores where everyone downloads apps, and innovation platforms, such as those offered by semiconductor foundries, like TSMC. These are massive modular ecosystems onto themselves, and not covered here.

[9] Thun, Taglioni, Sturgeon & Dallas, "Massive modularity: Understanding industrial organization in a digital age," 2022.

Figure 1: An Abstraction of a Mobile Phone Handset Supply Chain



Source: Thun, Taglioni, Sturgeon & Dallas, "Massive Modularity: Understanding Industry Organization in a Digital Age," 2022.

Very briefly, *modularity is the partial decomposability of a complex system into distinct sub-systems which interoperate through standard interfaces, and thereby maintains system-level coherence and functionality.* It is especially prevalent in ICTs due to digitization, and it can occur in large-scale systems (e.g. internet) and micro-systems (e.g. semiconductors). In terms of supply chains, massive modularity generates three paradoxes: (i) products can be both extremely complex *and* produced at scale; (ii) they create extreme market concentration *and* also fragmentation; (iii) they combine geographic agglomeration *and* dispersion. All of these characteristics are illustrated in the data below.

Since smartphones are familiar to everyone, it is as good a 'layer' to start as any. I will briefly 'descend' layer by layer into the phone following Figure 1, and I will only focus on one dimension – the distribution of *market share by country*, because of its clear policy relevance and to highlight China's position in the MME. The country-level data are constructed by aggregating together firm-level data, in most cases based on the location of the firm's headquarters. [10]

Two brief observations before our deep-dive. First, in general, hardware is much easier to monitor and quantify and so there is a hardware-bias to this exercise. Nevertheless, it should be kept in mind that various types of software interpenetrate every 'box' in Figure 1 and often bind boxes together. Below, we only offer evidence of software for mobile operating system. Second, as briefly discussed below, the double-band lines between boxes consist of interoperability standards which also serve as critical 'glue' holding the industry together. The important point to remember is that most standards extend far beyond the smartphone itself, whether telecommunications standards (e.g. 3GPP) or internet standards (e.g.

[10] This has implications for geopolitics as well because governments have authority over the headquarters of companies. Of course, policy tools like the direct product rule extends American law beyond US-headquartered and US-located companies. In terms of business capabilities, most companies have a large share of their key assets and resources in the country where they are headquartered. Furthermore, company headquarter also serves as a proxy for a range of critical supply chain activities, often including product design, R&D, supply chain management, and core governance decisions concerning what, how, where and to whom to outsource, among other key activities.

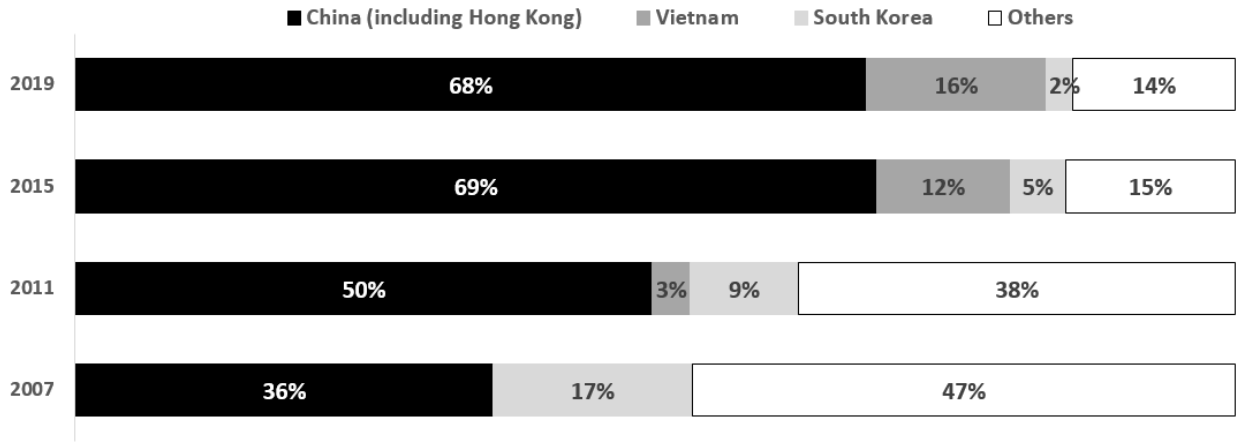
W3C). These are created in global, voluntary, consensus-based and industry-led organizations. But, other standards are created by dominant firms and thus are proprietary or semi-proprietary, such as Google Android operating system or ARM, the UK-based semiconductor IP company. Thus, standards are the invisible webs that not only tie the smartphone together, but ties the smartphone into many other ecosystems of equal complexity, and thus the following only scratches the surface. Interoperability standards are numerous and proliferating, and there is a risk they will become increasingly politicized.

Layer #1: Smartphone (system-level)

Figure 2 offers data on the locations where smartphones are manufactured and exported (2007-2019). That is, the countries where the smartphone assembly factories are located. I start with this layer because it is the perspective that is most commonly associated with China – a manufacturing and export powerhouse. Indeed, Figure 2 confirms this perspective: China's share of global mobile handset exports rose from 36% in 2007 to 68% in 2019. However Figure 2 does not represent the headquarters of the firms who own and manage the factories (such as Foxconn in Taiwan), nor the headquarters of the companies whose phones are being assembled (such as Apple in US). These data points would offer quite different perspectives on China's position in the supply chain.

Nevertheless, this still represents a significant vulnerability for firms (like Apple) who heavily rely on China-*located* factories. That said, due to interdependency, China is also vulnerable because the livelihood of millions of Chinese workers are reliant on assembly factories like these.

Figure 2: Layer #1 – Top mobile handset export shares by country, 2007-2019



Notes: China includes Hong Kong based on the assumption that most handsets exported from Hong Kong are imported from the Mainland and re-exported, even though they are not reported as such. Export values are calculated are made by summing imports from all trade partners of each reporter.
Source: UN Comtrade, HS 851712 (Telephones for cellular networks or for other wireless networks), from Thun, Taglioni, Sturgeon & Dallas "Massive Modularity: Understanding Industry Organization in a Digital Age," 2022

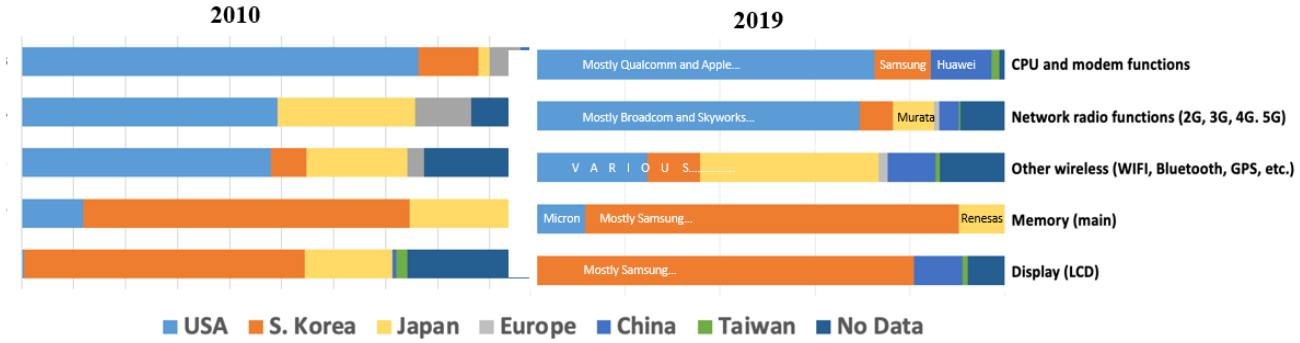
Layer #2: Major Sub-systems (Modules)

If one were to open the outer casing of the smartphone, there would appear a hodge-podge of very tightly packed hardware components. For instance, the Apple iPhone XS Max (2018) has about 1,745 distinct components depending on how one counts them, but 94% of them cost less than US$0.10. By contrast, Samsung sold Apple the expensive touchscreen display for $110.40. These components are grouped together into major sub-systems or 'modules,' each of which does one major function (like the touchscreen). Figure 3 contains only a few of the most expensive and critical modules, such as the apps

processor (main CPU), touchscreen display, memory, the radio frequency front-end module (that connects to the telecommunication system) and various other wireless connectivity.[11]

Figure 3 contains several noteworthy observations. First, most sub-systems are heavily concentrated in a single country, and the level of concentration has increased between 2010 and 2019. For instance, in 2019, 72% of CPUs and 69% of radio frequency module chips come from US-headquartered firms (e.g. Qualcomm and Qorvo, respectively), while 81% of displays and 79% of memory chips come from South Korea firms, such as Samsung and SK Hynix. Since a sub-system is essentially worthless unless it is integrated into a smartphone, these figures reflect a very high level of country specialization and global interdependence – something that every smartphone company (from Layer #1) must deal with. Second, by 2019, China has made a small amount of headway into these major sub-system, with 10% in displays and 13% in CPUs, which in the case of CPUs is almost completely driven by Huawei's fabless IC design subsidiary, HiSilicon. Huawei has followed in the footsteps of Apple and Samsung by bringing CPU design in-house over the past decade. Finally, Japanese and European companies have seen a diminished presence in Layer #2.

Figure 3: Layer #2 – Mobile phone sub-systems value and share by country, 2010 and 2019



Source: IHS Markit based on teardown reports of 456 handsets (average 38 reports per year)
From Thun, Taglioni, Sturgeon & Dallas, "Massive Modularity: Understanding Industry Organization in a Digital Age," 2022.

Layer #3: Operating Systems

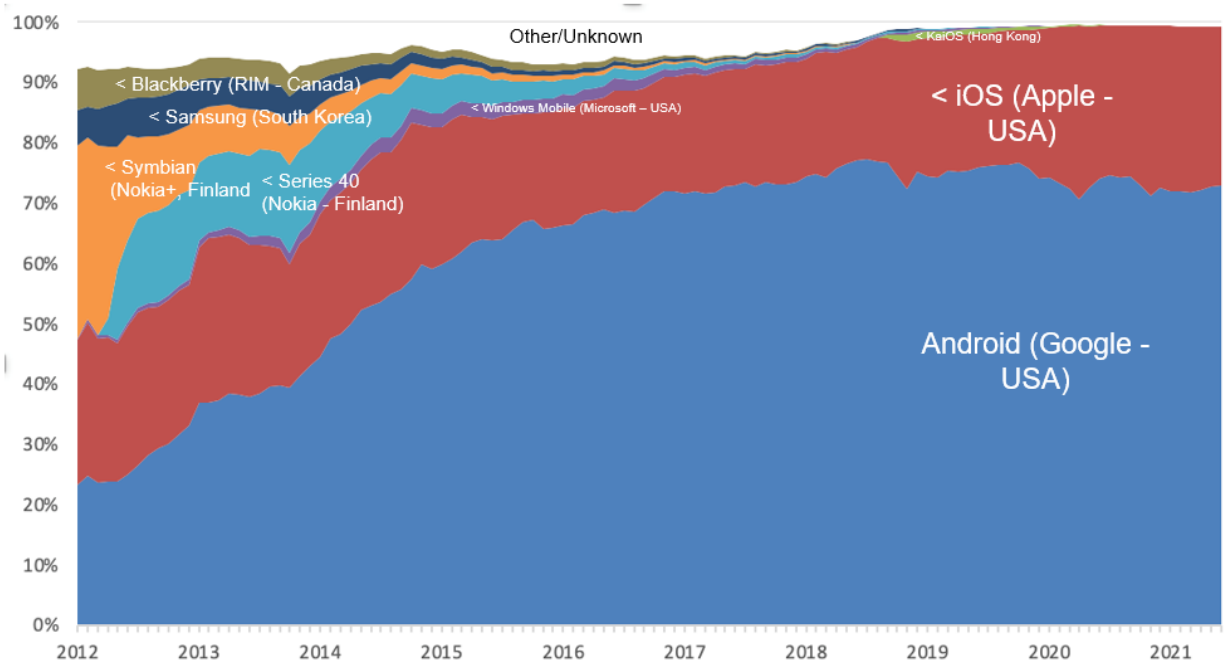
Figure 4 turns to the operating system of smartphones, which is our only insight into software, even though software interpenetrates all layers and components. Operating systems are platforms which contain standardized interfaces (called APIs) which are partially open and through which other companies interconnect with the platform (and with each other) to create and optimize their product. For instance, all of the companies supplying sub-systems in Layer #2 engage with the operating system. And the innumerable app developers all over the world who create the millions of apps that exist on Apple's App Store and Google Play (their respective app stores) must abide by a variety of standards, and go through a rigorous set of testing and verifications through the OS platforms.

Figure 4a shows that the period before 2014 exhibited diversity and competitiveness between mobile operating systems, with Finland's Nokia, Samsung's Tizen and Canada's RIM taking sizeable market shares. However, ultimately Apple and Google created a global duopoly of operating systems, due to the powerful network effects of their platforms. However, Apple iOS and Google's Android differ

[11] Mobile cameras are also very expensive modules which we have not included here, because the IHS Market dataset only gives the firm names of the assembler of the camera module (a layer), which is only a small fraction of the value-added of the camera. By contrast, the image sensors (a component of a lower layer) are some of the core components inside the camera module, and many of these are Japanese headquartered firms, like Sony.

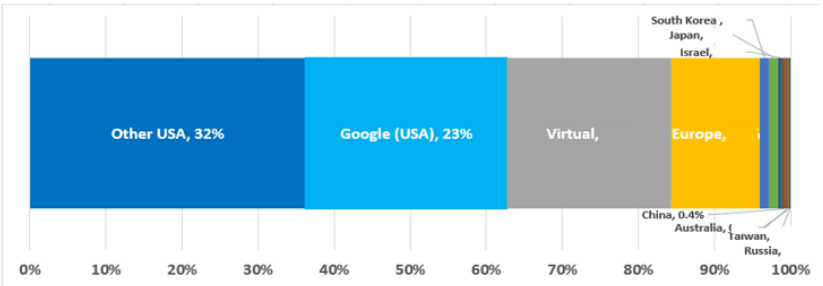
dramatically. While iOS is mostly proprietary, Google has constructed a very complex open-source software platform which allows any company in the world to participate in, contribute to, download and use, and even modify and customize the Android OS – completely for free. To illustrate the very different world of open-source software, Figure 4b reflects the country origin of the companies, non-profits and individual programmers who have contributed to Android's open-source software. While Google predictably contributed the most (23%), US-based software programmer contributed another 33%, with Europeans the only other significant regional contributor. Chinese organizations contributed only 0.4%.

Figure 4a. Layer #3 – Global Mobile handset OS market share, January 2012 – April 2021



Source: Statista based on StatCounter, which calculates OS data based on more than 1.7 billion page views per month worldwide. StatCounter defines a mobile device as a pocket-sized computing device - tablets are not included.
From Thun, Taglioni, Sturgeon & Dallas "Massive Modularity: Understanding Industry Organization in a Digital Age," 2022

Figure 4b: Layer #3 – Contributions (software code "commits") to Google's Android Open-Source Project (about 10 million commits since 2008)



Note: 'Virtual' includes private individuals and individuals who contribute to open-source organizations, but who do not have a formal employment relationship with the organization, such as Linux contributors.
Source: Android Open-Source Project (https://source.android.com/). Courtesy of Jing-Ming Shiu (National Cheng Kung University, Taiwan)

The significance of Android's open-source framework is not widely appreciated. For instance, the operating systems of China's largest smartphone companies (like Oppo, Vivo, Xiaomi and even Huawei) are all customizations (called 'skins') that derive from Android OS. In May 2019, Huawei was put on the US entities list and Google was prohibited from pushing OS updates and patches to Huawei, which over time slowly degraded all existing Huawei phones. In June 2021 and to much fanfare in China, Huawei released its own operating system, HarmonyOS, triumphantly announcing that it was "a milestone," with Huawei's head of software, Wang Chenglu, declaring that it was "neither a copy of Android nor [Apple's] iOS;" even Huawei founder and CEO, Ren Zhengfei declared, "in the software domain, the US will have very little control over our future development, and we have much more autonomy."[12] However, software engineers who explored Harmony OS after its release concluded that "HarmonyOS was identical to what Huawei ships on its Android phones, save for a few changes to the 'about' screen that swapped out the words 'Android' and 'EMUI (Huawei's Android skin) for 'HarmonyOS.'"[13] From a broader perspective, this means that 78% of China's smartphones have a (free, open-source) Google product at their heart, while Apple iOS has a 21% market share in China.[14] While Google's proprietary products exited from China in 2010, its open-source OS is ubiquitous there.

Layer #4: Semiconductors

Semiconductors are ubiquitous in smartphones (and all ICT devices), and they sit at the core of most of the critical components in the sub-systems of Layer #2, including the camera module, and the network and other wireless chips that communicate with the telecommunications system, the internet and other network infrastructures. Figure 5 contains data on all types of semiconductors (not just mobile chips), and it is very roughly organized as a linear supply chain. That is, the chain starts at the top of Figure 5 where the most upstream EDA software and IP cores provide critical inputs for fabless design houses,[15] which then design the myriad varieties of chips (logic, memory, OSD, etc.). Once the designs are set, they are passed off to be physically manufactured, which in Figure 5 encompasses 'semiconductor equipment,' 'materials' and ultimately the 'wafer fabrication' (or foundry). The final stage is 'assembly, packaging and testing.' Figure 5 shows that US firms are dominant in the upstream R&D, design and software-intensive segments, like EDA & IP (74%), logic designs (67%) and semiconductor equipment (41%). By contrast, with a 38% market share, China has entered the industry most significantly in the very last stage, which is capital and labor-intensive. They also have a foothold (16%) in the fabrication segment (e.g. SMIC). However, their leading foundries are two generations behind the leading-edge technology. For instance, in 2020, Taiwan's TSMC dominated 85% of the foundry manufacturing for the most advanced semiconductors (10-5 nm), with Samsung taking the remaining 15%. By contrast, China's leading semiconductor foundry, SMIC, just barely eked out 2 to 3% in the next (less advanced) tranche of semiconductor manufacturing (32-12 nm).[16]

[12] Celia Chen, "Huawei to roll out self-developed Harmony OS for smartphones next month, ending its reliance on Google's Android," South China Morning Post, May 25, 2021. https://www.scmp.com/tech/big-tech/article/3134783/huawei-roll-out-self-developed-harmony-os-smartphones-next-month

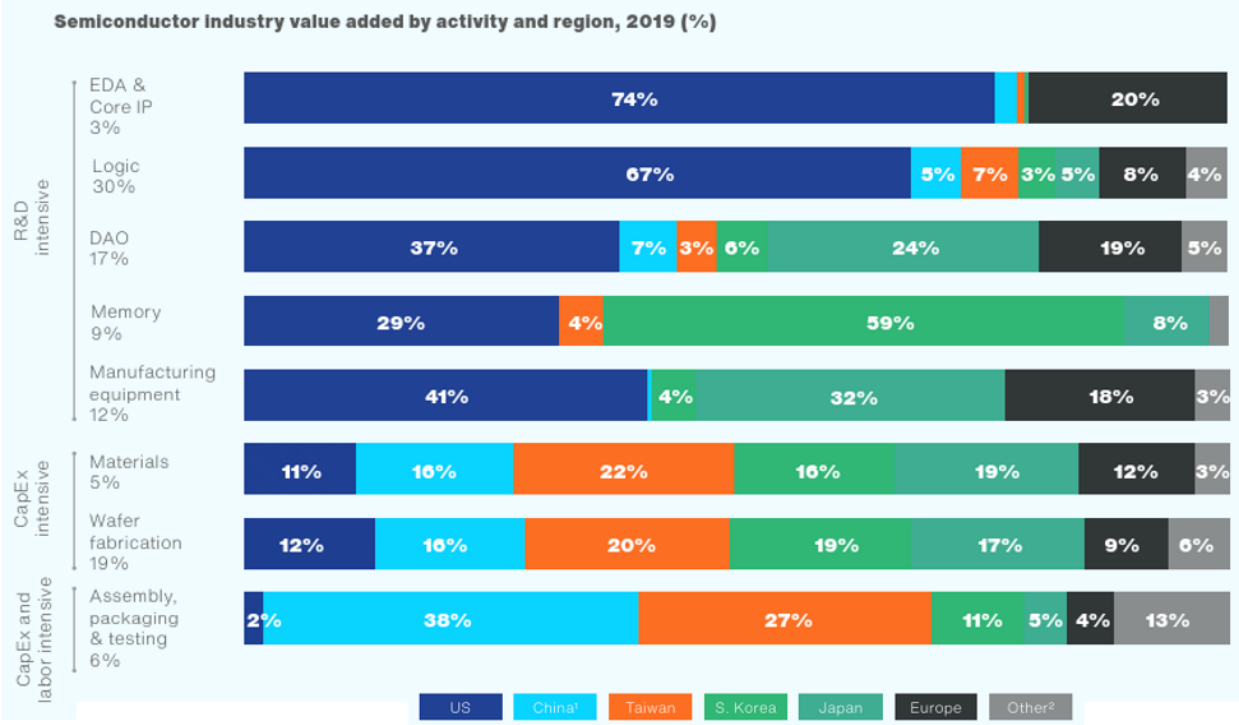
[13] Ron Amadeo, "Huawei officially replaces Android with HarmonyOS, which is also Android," Ars Technica, June 2, 2021. https://arstechnica.com/gadgets/2021/06/huaweis-harmonyos-will-rollout-to-100-android-models-over-the-next-year/

[14] Statista, "Market share of mobile operating systems in China from January 2013 to December 2021

[15] Fabless means they lack manufacturing facilities.

[16] Kathrin Hille, "TSMC: how a Taiwanese chipmaker became a linchpin of the global economy," FT, March 24, 2021.

Figure 5: Layer #4 – Semiconductor Supply Chain



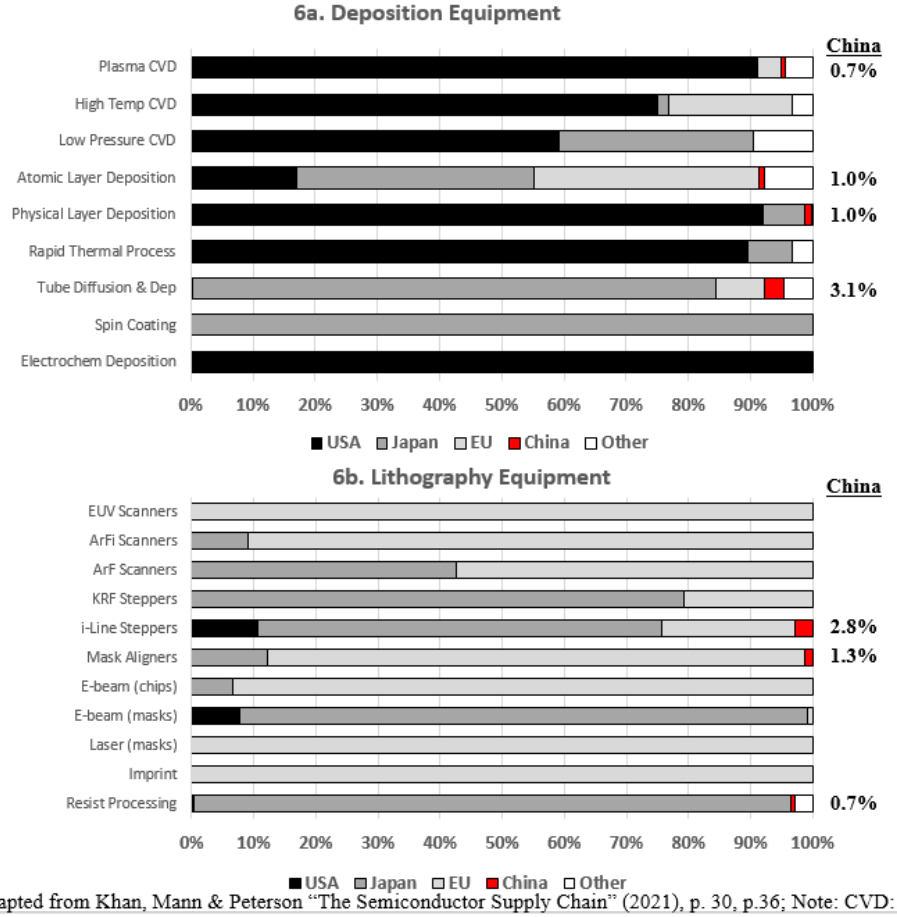
Source: Boston Consulting Group & Semiconductor Industry Association, "Strengthening the Global Semiconductor Supply Chain in an Uncertain Era," 2021.

Layer #5: Semiconductor Equipment

As mentioned, in Figure 5, each 'bar' roughly corresponds to a 'link' in the semiconductor supply chain. Of course, each link can be further disaggregated in various ways. For instance, 'manufacturing equipment' contains a large basket of various machines through which silicon wafers pass through their long journey to become finished chips. Figure 6 offers just a small flavor, using only two categories of semiconductor machinery as examples. Figure 6a shows the country market shares of various 'deposition' machines and Figure 6b shows 'lithography' machines, which are two sequential tasks in the semiconductor manufacturing process. The point of this exercise is not to understand the technology,[17] but to appreciate the complexity and layering of the technology and to understand China's position in these different layers.

[17] Very briefly, however, semiconductor fabrication consists of creating many ultra-thin layers on a silicon wafer to create various miniscule electrical devices (like transistors) and then create a pattern of interconnects between them, forming a circuit. Deposition and lithography machines are some of the most advanced in this process. While there are many steps and types of machines, the rough division of labor is that deposition machines 'deposit' a thin layer of material, while lithography machines draw a pre-designed circuit pattern onto the layer.

Figure 6: Layer #5 – Semiconductor Manufacturing Equipment



Source: Adapted from Khan, Mann & Peterson "The Semiconductor Supply Chain" (2021), p. 30, p.36; Note: CVD: chemical vapor deposition

Figures 6a and 6b (Layer #5) have noteworthy features. US firms (like Applied Materials and Lam Research) are dominant across a range of deposition machines, but Japanese and especially European firms dominate in lithography (like ASML in Netherlands, or Nikon and Canon in Japan). Once again, the degree of country (and firm) concentration is very stark and hence the inter-country and inter-firm interdependencies are profound. Furthermore, China has almost no representation in the market shares, and in fact has less than 5% market share across *nearly all* semiconductor machinery categories, except for some assembly, packaging and test equipment segments.[18] It should be kept in mind that each machine in Figure 6 can be disaggregated further into component and parts (forming Layer #6, etc.). For instance, ASML (Netherlands) has a global monopoly on the most advanced photolithography machines (called EUV or extreme ultraviolet), which are used to fabricate the currently most advanced chips. Those machines alone contain over 100,000 parts, coming from 5,000 suppliers and cost $120 million each.[19] In a word, the layering and supply chains goes deeper and deeper.

Standard-setting: The glue that makes it stick.

As mentioned, standard-setting is the glue that holds many industries together. But, they are particularly important in ICTs because they ensure interoperability (such as allowing the billions of smartphones and

[18] Khan, Mann, & Peterson "The Semiconductor Supply Chain: Assessing National Competitiveness," Center for Security and Emerging Technologies, 2021.
[19] Carrick Flynn, "The chip-making machine at the center of Chinese dual-use concerns," June 20, 2020.

millions of mobile apps to communicate with each other) and they allow for modularity. Each layer of the mobile telecom (and general ICT) stack contains many standards. One careful study estimated there are between 250 and 500 distinct technical standards that go into a typical laptop computer[20] – in some ways, a less sophisticated product than a smartphone. These are created by a variety of organizations. For instance, one online repository contains over 1,100 distinct standard-setting organizations (SSOs) and standards consortia, most of them voluntary, consensus-based, industry-led, and many of them global. However, standards can also be set by dominant firms, like the Android and Apple operating systems, discussed earlier.

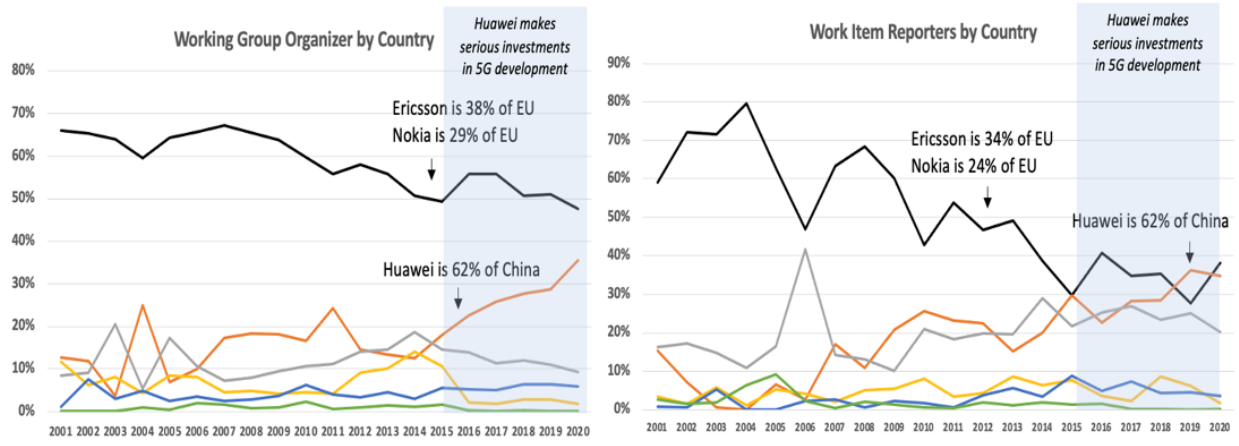
Standard-setting is a complex and diverse world unto itself, and so again, there is no one-size-fits all way to describe it. Nevertheless, one common tension in SSOs is that rival firms (e.g. Huawei, Nokia and Ericsson in telecom equipment) must find a way to agree on the most efficient standards. However, once a standard is finalized, some firms may possess an advantage because the standard may be based on technologies developed and most likely patented by a particular firm. In fact, in most SSOs, firms are required to declare when they have a patent which could later be infringed, which is called a standard essential patent (SEP). Given the potential of monopoly rents from SEPs, most SSOs also require that companies commit to offering their SEPs to other companies on "fair, reasonable and non-discriminatory" (FRAND) basis, which has legal weight in all major patent courts worldwide.

In the area of standard-setting in the mobile telecommunications industry, the central SSO is The Third Generational Partnership Project (3GPP). As Figure 7 shows, European firms have traditionally been leaders in mobile telecom standard-setting. But in recent years, Chinese firms (led by Huawei, but also including China Mobile, ZTE and others), have become increasingly important players in standard-setting, especially since around 2015. Chinese firms are now 'lead' sponsors in about one-third of work items (which turn into technical specifications and eventually national standards), and they hold leadership positions in about one-third of the work item committees. While beyond the scope of this testimony, it is important not to overly politicize one's conclusion from Figure 7. The conclusion is *not* that China or Huawei will soon dominate telecommunications standards and hence the industry; rather, the conclusion should be that Chinese firms have become important participants and collaborators in coming to international consensus over standards.[21] That said, there is always a risk that SSOs could become focal points of geopolitical struggle and thus lose their voluntary, consensus-based and industry-led approach. It boils down to *how SSOs are governed*, as discussed in Section 4. However, some government engagement may be helpful to ensure that profit-seeking companies are setting standards in the public interest.

[20] Biddle, Brad, Andrew White, and Sean Woods. "How many standards in a laptop? (And other empirical questions)." In *2010 ITU-T Kaleidoscope: Beyond the Internet?-Innovations for Future Networks and Services*, pp. 1-7. IEEE, 2010.

[21] As just one illustration of this, 3GPP requires a supermajority of participants (71%) to agree to a technical specification before it is finalized. So, Huawei standards cannot be imposed onto 3GPP, they must be effective. Most SSOs have a variety of institutionalized mechanisms to generate broad-based consensus.

Figure 7: Standards – Participation in mobile telecom interconnect standard setting by country (3GPP)



Courtesy of Jing-Ming Shiu (National Cheng Kung University, Taiwan)

Summary

This section offers a simplified but deep-dive into one ICT supply chain and it will be referenced later in this testimony. The key takeaways are:

(i) Supply chains are very intricately balanced, but more importantly, each supply chain is somewhat unique

(ii) There is substantial global specialization at nearly every layer in the ICT stack and this creates extreme interdependencies between companies and countries

(iii) With important exceptions, China's standing in the supply chain varies widely but overall, it is far more dependent on foreign and US capabilities than the reverse. As discussed next, this drives China's deep-seated insecurities regarding technological dependency on foreign countries, and pushes them towards a logic of 'self-reliance.'

These are important insights first because it demonstrates the policy challenges *for all countries*. It raises difficult questions for policy-makers with few concrete answers, such as:

(i) How and where can governments intervene in the supply chain to enhance security or for other worthy goals, without generating unintended consequences that excessively damage domestic constituents either upstream or downstream?

(ii) Will intervening in one link in the chain increase or decrease aggregate vulnerabilities? For instance, it is possible that reshoring in one link will reduce vulnerability in that segment, but then increase *aggregate* vulnerability since that link will have to create new supply chain links in order to remain commercially viable.

(iii) Does government have the necessary expertise to determine the cost-benefit analysis on a supply chain-by-supply chain basis? If not, what expertise and agency organization are needed to get supply chain policy right? Some of these are discussed in Section 4.

China equally is faced with these hard questions. However, despite China's important role in some supply chains, their rhetoric, perceptions and policies do not necessarily match a world organized by supply chains. This will have implications for China and its foreign economic relations.

3. Chinese Perceptions & Policies: Supply Chains, Critical Technologies and Interdependence

This section argues that indeed, there seem to be serious discontinuities between the reality of supply chain interdependence and China's perceptions and policies, such as its declared aspirations for 'self-reliance,' its techno-nationalism, as well as its concrete industrial policies. Furthermore, Chinese rhetoric can diverge from policy. But, before we turn to this, it is important to clarify a few points. First, it is difficult to separate out China's industrial policies and supply chains. Although Chinese policies generally do not explicitly declare a policy to be for 'supply chain security,' many of their stated goals for 'self-reliance,' 'self-strengthening,' or 'indigenous innovation,' all have important supply chain implications, particularly industrial policies with specific targets. Thus, many Chinese policies are *de facto* supply chain policies, without naming them as such.

Second and related, China's political rhetoric and its accompanying industrial policies should not always be interpreted through the lens that China's goal is invariably 'autarky,' or to achieve 'absolute advantage' in competition with foreign countries. For instance, some version of 'self-reliance' has been in the Chinese political lexicon since at least the Mao era (*zili gengsheng*, self-reliance), and continued into the Deng era (post-1978). More recently, it became focused on innovation in the Hu-Wen era (*zizhu changxin*, indigenous innovation), Made in China 2025 (*zizhu baozhang*, indigenous guarantees) and most recently (*zili ziqiang*, self-reliance, self-strengthening). Thus, it has been a common theme through CCP history, despite the epochal changes in China's policies, politics and economy over these eras. Since the Deng reforms in 1978, the same can be said about China's optimistic sloganeering towards 'international cooperation and collaboration,' which may appear in many leadership speeches and policy documents, even when reality may differ on the ground. Thus, much nuance must be applied to differentiate Chinese political rhetoric and sloganeering, and its underlying policy approach which not only continues to evolve but can be self-contradictory.

Together, both of these ideas highlight that it is important to differentiate general and high-level political and policy objectives from the details of Chinese policy and practices. Chinese policies can be incredibly detailed (when they want them to be), for instance targeting very narrowly defined industries or even products and technologies. But, at other times, they can appear very broad and vague, lacking clear, stated purposes. Clearly, the specific and targeted policies are more relevant to supply chains and easier to interpret than broader rhetoric and goals. However, they both matter, and may not always be aligned.

It is impossible to reflect in any summary way the views of the Chinese party-state over time, given bureaucratic and regional differences, and changes over time. The concept 'fragmented authoritarianism' has been perhaps the most enduring metaphor in the study of Chinese politics, and for good reason.[22] As such, any selection of quotes is unsystematic and cannot represent China as a whole, partly because China is not monolithic. Nevertheless, statements by Chinese leadership hold special importance and should be taken seriously, even if local realities diverge from central pronouncements. However, in this section, I report on research with my research collaborators, [23] which use systematic data from Chinese newspapers. Drawing from half a million media articles from over 650 Chinese newspapers between 2005 and 2021, systematic media data offer a birds-eye perspective to complement perceptions of leadership through their speeches or bureaucracies through policy documents.

[22] Lieberthal, Kenneth, and Michel Oksenberg. *Policy Making in China*. Princeton University Press, 1988; Mertha, Andrew. "'Fragmented authoritarianism 2.0": Political pluralization in the Chinese policy process." *The China Quarterly* 200 (2009): 995-1012; Tan, Yeling. *Disaggregating China, Inc.* Cornell University Press, 2022.

[23] Yeling Tan (University of Oregon), Abraham Newman (Georgetown University) and Henry Farrell (Johns Hopkins University).

There are four high-level conclusions from this section:

(i) Chinese anxiety concerning "technological security" and "economic decoupling" have clearly become more salient in recent years. In addition, there seems to be a lasting step-change, particularly after key events, such as the Snowden revelations in 2013, the various post-2018 denial orders placed on ZTE and Huawei, and finally COVID-19. Almost certainly, the Russian sanctions have reinforced this trend, though we have not collected new data.

(ii) Many of China's foundational economic and technological security concerns pre-date these events and even pre-date Xi Jinping. Thus, we have to be careful not to overemphasis events of the more recent past (5 to 10 years), and thereby forget important continuities concerning China's sense of economic and technological insecurity from prior periods, that predate Xi and even predate the global financial crisis when China's economy and industrial policy took a dramatic turn.

One way to square the circle is that China's insecurities regarding foreign relations and foreign influence have long existed below the surface (hence the perpetual CCP rhetoric of 'self-reliance' since Mao). But more recent events have tapped into China's long-standing insecurities and Xi has given greater voice to them (for instance concerning technological dependency and information security), thereby empowering security-oriented voices in China.

(iii) Despite China long harboring dreams of self-reliance and breaking from foreign dependencies in technology, in recent years, there do seem to be identifiable changes in their industrial policies, starting in 2006 and evolving since then. These changes include: 1) more resources allocations for industrial policies, 2) greater precision in their industrial targeting, and 3) a greater focus on upstream or infrastructural ICT sectors (5G, internet, AI, semiconductors, data) which are perceived to allow China to 'leapfrog' into the technological frontier. The policy precision can also be seen in newer instruments of Chinese economic coercion.

(iv) Chinese industrial policies have disturbing implications, and can distort technological innovation, however, our deep-dive in ICTs suggests even a partially autarkic approach will likely fail. That is, there is a fundamental conflict between China's policy goals and the structure of global supply chains. Unfortunately, China perceives its security as assured through 'self-reliance' and internalizing supply chains through industrial policies. But global innovation is so modularized, decentralized and interdependent, that China's two goals clash. China will likely have to choose between self-reliance and catching up to the global leading edge in most technologies.

3.1 Chinese Perceptions: Mass Media and Leadership

Based on research with my collaborators, we show that China's perceptions (through news media and through leadership and other speeches) have fundamentally shifted in recent years, often in response to unexpected, external events, including the Snowden revelations, the Trump administration's denial orders against ZTE and Huawei, and COVID-19, all of which caught China by surprise. The two figures in this section contain data on over 500,000 news articles from over 650 Chinese newspapers of varying types between 2005 and 2021.[24] The news corpus includes only news articles with at least one of three

[24] Most of the corpus is state-run media (with a small amount of private news), but we differentiate newspapers according to central government, provincial/local government and quasi-governmental (e.g. industry association) newspapers, as well as newspapers that focus on economy and industry, science and technology, security, general readership and specialized topics.

"technology" keywords[25] in the title, which ensures that we only select technology-focused articles. Finally, we focus on the prevalence in the news of two themes: "technology security" and "economic decoupling."[26] The figures are not simply absolute word counts, since there almost certainly has been a great increase in the number of newspapers and news produced over the fifteen year period. Rather, they are word ratios that count the words occurring in each theme *as a percentage of the total number of words* in all articles for the same month, which thereby standardizes the occurrence of keywords over time. Of course, there is always a gap between state-run media and Chinese leadership, so despite the systematic nature of our data collection, this should not be interpreted as reflective of universal agreement on the part of the Chinese central government, the CCP, let alone society at large.

China's "Technology Security": Snowden Revelations and China's Changing Perceptions (2013-)

Figure 8 shows the prevalence of "technology security" issues over time, and benchmarks the changes relative to the Snowden revelations that hit the global media in June 2013, as well as relevant policy and administrative changes in China. Clearly, the Snowden revelations triggered a heightened focus on 'technology security.' However, the heightened attention to technology security is not temporary. It continues to persist for many years afterwards, creating a semi-permanent change in perspective. Notably, this step-change occurs *over half a year after* Xi Jinping became General Secretary of the CCP. Furthermore, it appears that the Snowden revelations set in motion a flurry of policy and institutional changes. Soon after the Snowden revelations, the CCP formed the Leading Small Group on Network Security and Informatization, chaired by General Secretary Xi Jinping himself. The creation of this high-level body is indicative of the importance attributed to technology policy by the Party, and allows the leadership to overcome bureaucratic competition over network security issues and streamlines policy-making.[27] In August 2013, at a national work conference on propaganda thought, Xi portrayed the issue as an inter-civilizational struggle, stating: "Anti-Chinese forces in the West have always endeavored to take down China with the internet. … From America's PRISM and the XKeyscore surveillance plans, it's clear that their internet activity ability and scale have far exceeded people's imagination."[28]

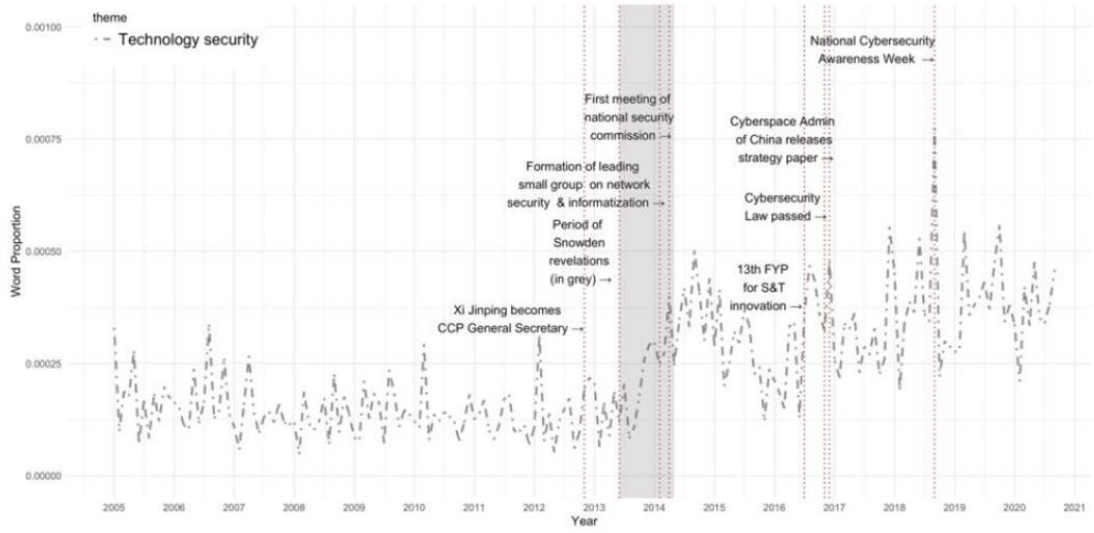
[25] These are 'innovation,' 'science & technology,' and 'technology.'

[26] For "technology security," we count instances in the body of the article for: "information security" (信 息 安 全), "network security" (网 络 安 全), "data sovereignty" (数据主权). For "decoupling," we count for: "chokehold" (卡脖子), "self-reliance" (自力更生), "domestic circulation" (国内大循环) "indigenous research" (自研) and "technology self-sufficiency" (科技自立).

[27] Segal, Adam. "China's New Small Leading Group on Cybersecurity and Internet Management." *Forbes Asia, February* 27, 2014.

[28] Wang chuan Xi Jinping 8•19 jianghua quanwen: Yanlun fangmian yao gan zhua gan guan ganyu liangjian, *China Digital Times*, Nov 4, 2013.

Figure 8: Chinese media reporting on "technology security" and the Snowden effects



Note: These record word ratios, or the share of words associated with "technology security" as a share of total words in the media corpus, by month.
Source: Tan, Dallas, Newman & Farrell, "Driven to Self-Reliance," 2022.

Soon thereafter and in quick succession, the Cybersecurity Administration of China (CAC) was created (2014), the State Council authorized the reestablishment of the State Internet Information Office (2014), the National Security Law was passed (2015), the Cybersecurity Law was passed (2016) and CAC issued a cybersecurity strategy (2016). Foreign supply chains were also singled out. Former PLA colonel Liu Jinghua argued, "what we read from the Snowden files showed that almost all the big companies in China were actually collaborating with the American intelligence agencies…That made China feel really insecure using all these components from American companies."[29]

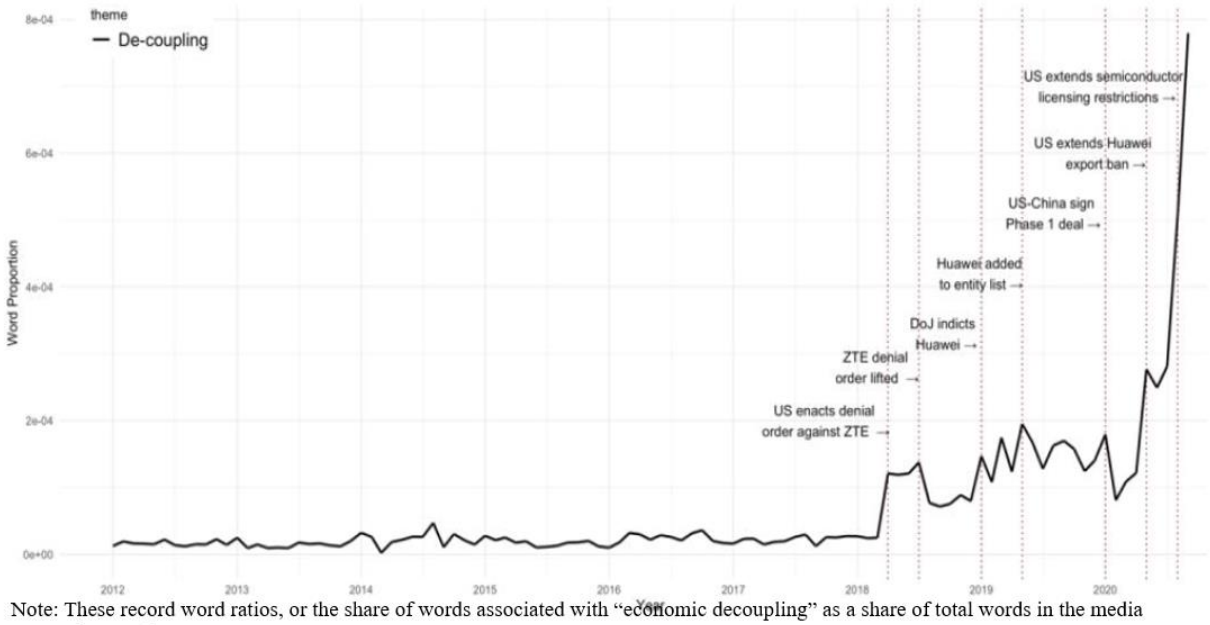
Despite all this, one should not jump to the too easy conclusion that the Snowden revelations "caused" this flurry of activity, in that China would have done none of this, save for Snowden. After all, it may very well be true that in 2013, Xi was at heart a strong advocate of enhancing Chinese security and intended or eventually would have deepened government cybersecurity oversight. Nevertheless, the policy and organizational outcomes arguably could have been different. As former US Ambassador to China, Max Baucus, concluded, "The Snowden leaks dramatically changed Chinese policy towards the internet, its own people, the United States, and the world, with respect to the internet and cybersecurity...It was a watershed development."[30]

"Economic Decoupling": Denial Orders against Huawei and ZTE and Chinese Perceptions (2018-)

A second major set of shocks and one at the heart of supply chain security came in quick succession with a denial order on the sales of US technology to Chinese telecommunications company ZTE (April 2018), the addition of Huawei to the entity list (May 2019) and the application of the direct product rule to Huawei (May 2020). In all cases, Chinese media surrounding "economic decoupling" (including terms like "chokeholds" and "self-reliance") all become elevated and remain elevated.

[29] Eli Binder and Katrina Northrop, 2020, "The Snowden Effect," The Wire China, December 6.
[30] Eli Binder and Katrina Northrop, 2020, "The Snowden Effect," The Wire China, December 6

Figure 9: Chinese media reporting on "economic decoupling" and the ZTE and Huawei Incidents



Note: These record word ratios, or the share of words associated with "economic decoupling" as a share of total words in the media corpus, by month.
Source: Tan, Dallas, Newman & Farrell, "Driven to Self-Reliance," 2022.

A whole slew of articles in April 2018 highlight the conundrum of being "choked" through technology dependence on US firms. One example is an article in *Science and Technology Daily* entitled "We cannot access core technology through begging for alms," which is a phrase previously used by Xi Jinping, in which Xi concludes that "we need self-reliance." China's *People's Daily* pinpoints particular vulnerable links in China's supply chain, stating, "(w)e urgently need to open a new wave of indigenous innovation in a global perspective, so that chips, operating systems, high-end manufacturing equipment and other core areas are no longer subject to the hidden concerns of being 'choked.'"[31] Other articles even from economically liberal leaning perspectives are worth quoting in full, since they question China's own long-held policy of reform, openness and integration into supply chains, arguing now for technological self-reliance:

> "In the past, some views held that with the current state of globalization, the world economy is already a highly integrated industrial chain - and that with the division of labor between countries, a country does not need have mastery over all the key core technologies. In other words, as the saying goes, "it's better to buy than to build, and it's better to rent than to buy." However, harsh reality tells us that with today's rampant trade protectionism and anti-globalization, if a large country does not hold the key technologies of important industries in its own hands, it will often be subject to "targeted attacks" by others, leading the relevant industries and enterprises to face a crisis of survival." … "Lessons from reality have repeatedly shown that technology involving the core competitiveness of a country cannot be bought by money, and the path of exchanging market for technology is also not feasible. We have to abandon such illusory thinking. Only by mastering key core technologies can we truly become an industrial and economic powerhouse."[32]

Of course, the rhetoric of self-reliance skyrockets once COVID-19 hits global supply chains. This is true even though we removed all articles referencing COVID-19 from our dataset in an attempt to neutralize its influence. But, clearly, the Chinese media had already been primed to frame issues as "self-reliance" and "decoupling," and COVID-19 strongly reinforced their prior beliefs. After the start of COVID-19 and during the direct product rule imposed on Huawei, Xi announced a broader strategy centered on the domestic market which incorporates ideas of both a consumption-led economy and self-reliance,

[31] http://opinion.people.com.cn/n1/2018/0425/c1003-29947992.html
[32] *Yi zizhu chuangxin shixian guanjian lingyu zhanlue xing tupo, Jingji cankaobao*, May 21, 2019.

encapsulated in the concept of "dual circulation." This concept was enshrined in Chapter 4 of China's 14th five-year plan in 2021, and can be seen as a continuation of a very long line of policies focused on 'self-reliance,' which will be discussed in the next section. Dual circulation is considered to be a "new development pattern" in which the domestic market is dominant and is supported by the external market.

China's continued lock-downs, most recently in Shanghai and Beijing, the closure of its border and even Xi Jinping's halting of his own in-person international diplomacy all reinforce an inward turn in China and shift towards self-reliance.

3.2 Chinese Industrial Policies and Supply Chains

News media and speeches by Chinese leaders may simply be an intricate dance between the pronouncements of elite leaders, mass propaganda and Chinese nationalism. Policies offer different insights into the intentions and goals of the Chinese party-state, though they too are not fool-proof insights. This final section focuses on Chinese industrial policies. Since that is a very large topic, it will largely focus on issues relevant to supply chains. Of course, the main link between Chinese industrial policy and supply chains is the key theme of this testimony – China's insecurities concerning dependency on foreign technologies drive their goals for self-reliance, which have implications for both technology and supply chains.

A primary conclusion is that although China has long harbored dreams of self-reliance, there has been a distinct shifted in its industrial policies over the past 10 to 15 years, and these changes have supply chain implications. In particular, the section highlights that: Chinese industrial policies have very substantial financial backing, they are more 'precise' in their targeting and they are aimed at 'leapfrogging' into emerging technologies, rather than the more typical and modest industrial policy goal of 'catching up,' which was the Japanese and South Korean strategy in the 20th century.

There are two further implications of this. First, even though Chinese industrial policies have evolved over time, these changes pre-date Xi Jinping (2012) and pre-date the 'Made in China 2025' program (2015), which received a lot of attention in the US and Europe. Second, the enhanced funding, improved targeting and focus on emerging technologies does not mean China will be successful. As Section 2 demonstrates, the geographic and organizational nature of critical supply chains suggest that China will have *to choose* between self-reliance and reaching the technological frontier. While costly, it is possible for China to achieve relative technological security through self-reliance, but they will likely trail the technological cutting-edge. At least in ICTs, the technological ecosystems are just too complex, too layered, too modular, and too dynamic for any country to try to internalize even one 'complete' supply chains, let alone the whole (and expanding) ICT stack.

It is impossible to do justice to Chinese industrial policy in a few paragraphs, but luckily, there is broad agreement about the basic contours.[33] First, industrial policy can have multiple meanings, but a narrow definition is: "measures and programs undertaken by governments to **shape the sectoral structure of the economy through channeling resources** into selected "pillar", "strategic" or "emerging" industries while

[33] The following offer excellent insights into China's most recent industrial policies (and S&T) policies since 2006: Heilmann, Sebastian, and Lea Shih. "The rise of industrial policy in China, 1978–2012." *Harvard-Yenching Institute Working Paper Series* 17, no. 7 (2013): 1-24; Heilmann, Sebastian, and Oliver Melton. "The reinvention of development planning in China, 1993–2012." *Modern China* 39, no. 6 (2013): 580-628; Chen, Ling, and Barry Naughton. "An institutionalized policy-making mechanism: China's return to techno-industrial policy." *Research Policy* 45, no. 10 (2016): 2138-2152; Naughton, Barry. *The Rise of China's Industrial Policy, 1978 to 2020*. Universidad Nacional Autónomica de México, Facultad de Economía, 2021; Sun, Yutao, and Cong Cao. "Planning for science: China's "grand experiment" and global implications." *Humanities and Social Sciences Communications* 8, no. 1 (2021): 1-9.

– ideally or purportedly – preserving market competition and firm-level decision autonomy in the targeted sectors." [34] Of course, within this definition, there can be much variation. Thus, it excludes resources that improve public goods that are shared broadly across industries, such as education, basic and public R&D, most infrastructure, among others.

Even though China's 'reform and opening' policies were the driving forces of the post-1978 Deng era, proponents of industrial policy were still active.[35] As China entered the WTO (2001) and with the transfer of power to the Hu-Wen administration (2002), the green shoots of industrial policy began to appear, which came to fruition with the Medium and Long-term Plan (MLP) in 2006. The centerpiece of the MLP consisted of 16 Mega-projects and 6 Mega-science programs,[36] and it introduced the concept of 'indigenous innovation,' which spurred a whole slew of 'indigenous innovation' policies on government procurement, taxes, accreditation, IPR, cyber, etc. But, it was not until the global financial crisis that China really opened the funding floodgates for the Megaprojects, and thus industrial policy took root.[37] By 2010, China had developed the Strategic Emerging Industries plan (which fed into China's 12th five year plan, 2011) which was better funded than MLP, had many detailed sectoral plans associated with it and attempted to attract private capital. Then, starting in 2015, a series of plans and strategies (timed around the 13th five-year plan, 2016) centered on targeting new emerging technologies. These included the well-known Made in China 2025 (2015), but also Internet Plus (2015), and specialized plans on Artificial Intelligence (2017) and Military-Civil Fusion (2017) and semiconductors (2014). At the heart of these is the 13th five-year plan and the Innovation-Driven Development Strategy (2016).

However, plans are only pieces of paper. What differs since 2006 is the sheer quantity of resources that are being pooled, especially since the global financial crisis. It is not easy to find or properly interpret data on industrial policy funding. A recent effort by CSIS tries to calculate the size of Chinese industrial policy funding and compare it to other countries (South Korea, France, Japan, Germany, US).[38] While it is extremely difficult for anyone to estimate, they carefully classify industrial policy funding into ten distinct channels and find that China's funding far exceeds any other country in the world. In 2019, as a share of GDP, China's industrial policy funding was 1.73% of GDP, while the next highest spender was South Korea at 0.67%, using their methodology. The United States was 0.39%. Looking at just one of these channels (government guidance funds, GGFs), Dr. Barry Naughton finds that they skyrocketed from 2015 to 2018, and that by 2020, 11 trillion RMB (US$1.6 trillion) was committed, however only about half of that was funded, and even less actually invested. Still, the sums are enormous. GGFs carry on the tradition in China of combining state guidance with market incentives. In essence, they try to replicate venture capital funds by investing in start-ups (but more patiently), and in theory are supposed to be profit-seeking with managerial incentives. However, the funds overwhelmingly derive from government or government-directed entities (including state banks and SOEs) and are guided by government objectives, such as industrial policy in strategic industries (but not exclusively them).

[34] Emphasis added, from Heilmann and Shih 2013, p.1. The second half, concerning 'preserving market competition and firm-level decision autonomy' differentiates it from a planned economy. The degree to which firms are autonomous in China and their investment sources is what differentiates China's recent industrial policies from the classic cases of industrial policy in Japan and South Korea.

[35] Heilmann, Sebastian, and Lea Shih. "The rise of industrial policy in China, 1978–2012." *Harvard-Yenching Institute Working Paper Series* 17, no. 7 (2013): 1-24.; Heilmann, Sebastian, and Oliver Melton. "The reinvention of development planning in China, 1993–2012." *Modern China* 39, no. 6 (2013): 580-628.

[36] Sun, Yutao, and Cong Cao. "Planning for science: China's "grand experiment" and global implications." *Humanities and Social Sciences Communications* 8, no. 1 (2021): 1-9..

[37] Naughton, Barry. *The Rise of China's Industrial Policy, 1978 to 2020*. Universidad Nacional Autónomica de México, Facultad de Economía, 2021..

[38] DiPippo, Mazzacco and Kennedy (2022), "Red Ink: Estimating Chinese Industrial Policy Spending in Comparative Perspective," Center for Strategic & International Studies, 2022.

Finally, there seems to be greater precision in Chinese industrial policies. This does not mean more accuracy in government support (i.e. success in outcomes), but rather a shift from more generic concerns about foreign economic and technological dependency to a greater attempt to identify and direct investments across multiple weak links in supply chains, and to identify 'strangleholds' (*qia bozi*) in supply chains. The GGFs are good examples of this. Only about 12% have a narrow industry focus (semiconductors, optoelectronics, etc.), but the venture capital model combined with government guidance is intended to narrow investments to government priorities, but then use more market-oriented assessments to more precisely identify weak points in China's supply chain. Furthermore, some major high-tech markets are also being 'made' by government-directed funding, such as large advanced infrastructure projects like 5G telecom, smart cities, smart grids, state surveillance, and even Industry 4.0 objectives laid out in Made in China 2025. Thus, rather than government itself locating and funding all of the weak points in China's supply chains, China may be combining a demand-side strategy through smart infrastructure, with a supply-side strategy through various industrial policy funding channels, but then hoping to introduce market incentives to pinpoint the actual weak points in China's supply chains in between. I should mention that no government document states this as a strategy, but examining Chinese policy and institutions as a whole, it could be seen as a rough system for rapid technological advancement and self-reliance.

Beyond industrial policies, China has also begun to build a more robust and institutionalized set of economic controls on their relationship with foreign countries and companies, including for purposes of economic coercion. Traditionally, China has used largely informal and imprecise mechanisms to exert selective coercion on targets. These generally centered on informal ways to make access to their domestic market more difficult for their targets, such as withholding domestic licenses, fomenting or encouraging product boycotts, or restricting certain imports based on WTO-permitted reasons, like trumped up phyto-sanitary issues. There was generally no direct legal justification and sometimes the intended target and the product were imprecisely linked, or the action was not comprehensive. This seems to be changing since the 2018 US-China trade and technology conflicts. China has recently expanded its export controls, created an unreliable entities list (which would be a *formalized* mechanism to deprive foreign companies access to the domestic market) as well as the new Measures for Security Review of Foreign Investments. The parallels to the US entity list and CFIUS are obvious. But more importantly, they formalize and add precision, compared to prior methods.

4. Policy Recommendations:

Apart from specific policy recommendations, this final section makes two additional key points:

(i) Supply chains are complex, diverse, malleable and opaque, and thus easily disrupted through unintended consequences. Thus, government agencies must be crystal clear on their precise goals and do proper due diligence to ensure the goals are in the public interest, government believes it has the proper capabilities to achieve them and has done a transparent and public cost-benefit analysis. Otherwise, unintended consequences are very likely.

(ii) There are two key underlying principles in terms of China. First, while easier said than done, the ultimate goal of supply chain policies should always be to achieve security *and* openness *and* prosperity. There is nothing compelling us to make these tradeoffs and we should never assume they cannot be combined. Second, as discussed below, it is deeply counterproductive to brand US policies as more 'hawkish' or more 'dovish' towards China (such as whether to remove Trump era tariffs). This lens is damaging not only because it is overly simplistic, but because they artificially narrow our strategic policy choices, because they imply mutual exclusivity. Rather, we need to acknowledge that the CCP and its leadership will do what is

> in their interests and so we must work hard to shape China's external environment and mold its perceptions to get China to behave in ways that are in our national interests. Both dove-like and hawk-like policies will contribute to this strategy, and they will contribute to our ultimate triple goals of security and openness and prosperity.

I first elaborate on these two points, and then turn to five specific policy recommendations.

Supply chain complexity and matching means to ends

It is worth recalling from the empirical deep-dive that even in the case of the homely smartphone, there are innumerable potential vulnerabilities due to extreme levels of global specialization and concentration, as well as the many interdependencies between layers and links. Furthermore, the supply chain of each product differs, and each can change and evolve over time. Governments who wish to engage with supply chains face a vast and uncertain landscape, filled with potential unintended consequences. What to do?

To begin, it is crucial for government to clarify means and ends for any policy interventions. The Biden administration's Executive Order 14017 (that launched the 100-day supply chain reviews and the full reports) was enormously ambition, filled with many worthy goals.[39] These included not only goals concerning reducing supply chain vulnerability and enhancing security, but job creation, revitalizing American manufacturing, environmental and sustainability goals, social justice, among others. In a word, supply chains were deputized to solve many of America's perceived problems.

On the other hand, there are a variety of means to achieve these goals. A slew of new terminology has been popularized, such as near-shoring, friend-shoring, reshoring, stockpiling, diversifying, trusted partnerships, sustainable domestic production, and ecosystem-building, among others. All of these means and ends can and should be on the table for a worthy reason that is in the public interest and that government believes it can positively contribute in solving (cost-benefit analysis).

However, in between the means and the ends, are the supply chains. Given the complexity and opacity of many supply chains, it is not completely clear how means and ends can or should be matched. For advocates of revitalizing American manufacturing, tax breaks may work in some links of certain supply chain, while fostering automation may work in others. For national supply assurances, government stockpiling and national reserves may work, for instance for primary inputs that will not depreciate in value quickly. By contrast, Moore's law dictates that semiconductors should not be stockpiled and thus other means would be required to ensure supplies, if that is the goal. As mentioned previously, there is no one-size-fits all solution. My fifth recommendation on bolstering supply chain data, knowledge and expertise inside and outside government specifically applies here. But each recommendation aims to a certain goal or end.

Two principles for policy making: No Hawks, No Doves & Shaping China's External Environment

Some of the recommendations below are more generic and can be applied across supply chains, such as enhancing knowledge and expertise. Others are more oriented towards China, geopolitics and technology issues, like a new multilateral export control regime. For these latter issues, however, economics and security are particularly intertwined in complex ways, and thus, there will invariably be struggles between

[39] Executive Order 14017, "Securing America's Supply Chains," Feb 24, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

objectives that are more security-oriented, more trade-oriented, more employment-oriented, among others.

Nevertheless, I believe there are two general principles that everyone can agree to. First, as a general principle and even in the case of China, the goal should be to achieve security *and* openness *and* prosperity. There is no reason that America should not attempt to have its cake and eat it too. For instance, many of our core agencies that deal with supply chain issues, such as BIS in the Commerce Department and CFIUS, are already designed to keep most economic exchanges open, while *selectively* applying security oversight, even with our rivals. Of course, stating the principle is easy. But, where to draw this line is much harder. The following recommendations do not assist in drawing that line. Rather, they assist in thinking through governance mechanisms by which that line can be drawn, re-drawn and then re-drawn again over time, as supply chains, technologies and our allies and adversaries move and change. Policy-making also needs to be resilient to change.

Second, a China 'hawk' vs China 'dove' mentality is overly simplistic and harmful because it artificially narrows our strategic maneuverability. Maintaining every Trump era tariff on China is not 'more hawkish' or tough on China, if they are harmful to overall American interests; equally, removing the Trump era tariffs is not 'more dovish' or soft on China, if we forego a bargaining chip by unilaterally reducing the tariffs. We can disagree on which is best, but the hawk-dove dichotomy is a self-imposed political constraint on our policy options, and is absolutely harmful. In fact, the best option is to eradicate the political labelling and consider how to creatively *mix ideas* together. For instance, a new Section 301 investigation could lead to the removal of some harmful tariffs, while also imposing new restrictions, given that China has not fulfilled its Phase 1 agreement obligations.

Below, there are recommendations that may appear more hawkish or more dovish towards China. But that is always the wrong lens, because there is a deeper principle at play. On the one hand, we must recognize that China is a continent-sized country with vast resources, a complex and fragmented domestic political system, with an obsession with stability, and that it is facing plenty of domestic and international challenges. Thus, we should not expect to be able to *directly* get China to do what we want, unless the party-state and Chinese leadership find it in their interests. Instead, we should work hard, along with our allies, to shape China's external environment and to mold China's perceptions in ways that naturally and willingly lead them to act towards achieving our ultimate desired goal. And in supply chains that ultimate goal is *security and openness and prosperity*, not choosing one or the other. This is easier said than done, but here are some specific recommendations.

1) Bilateral and Multilateral Free-Trade Agreements….excluding China

Diversification of supply chains is a worthy goal and so is revitalizing American manufacturing. However, companies will make sourcing and production decisions that are in their best interests, not the national interest. As a general rule, and outside of national security concerns, it is best for government to err on the side of not trying to unilaterally pinpoint critical links and directly reshape supply chains, given many unintended consequences and the capacity of supply chains to react flexibly to policy. It is also difficult directly to incentivize companies to diversify specific supply chains, even with light-touch tax incentives or other methods. Again, because supply chains vary widely and change over time, it is very hard to know exactly how or when to dial up or dial down incentives to get specific supply chains to diversify in the ways that government deems in the national interest (itself difficult to define). And this will be a moving target.

While pinpointing specific supply chains for diversification is difficult, one clearer goal is to diversify supply chains that are overly concentrated in China, though the same logic applies to other countries too.

The recently announced Indo-Pacific Economic Framework (IPEF) does exclude China, but there does not appear to be a lowering of tariffs. Thus, it is not likely to incentivize Indo-Pacific countries to negotiate on core concerns of the US, nor likely to shift overly concentrated manufacturing away from China.

By contrast, FTAs can create broad incentives across industries and firms to move operations and thus help diversify supply chains, even if it is hard to pinpoint which ones. Unlike unilateral tariffs, new FTAs would be pro-market, pro-trade, non-discriminatory, would not violate WTO obligations and are not likely to create unintended consequences at the supply chain level, which tariffs often do. By excluding China, some firms in some industries would be incentivized to shift production or outsourcing away from China and to countries within the FTA. Of course, if the incentives of the new FTA were so great, concentrated supply chains in China may simply become concentrated supply chains in Vietnam or India, thus reducing the value of the diversification goal (but perhaps still achieving other goals, like reducing the chances of supply chain weaponization). In fact, diversification of supply chains would prove to be beneficial for many countries. As new countries within the FTA gain a foothold in new supply chains, they will have a chance to learn and upgrade, which over time can create new clusters of specialized capabilities that could then compete even in export markets outside of the FTA. Furthermore, new FTAs would offer opportunities to experiment in a range of other issues areas, like digital trade, labor rights and sustainability.

2) Create a fifth *multilateral* export control regime…and possibly investment regime

As discussed, emerging technologies produced largely for commercial use are transforming our definitions of 'security,' 'critical infrastructure,' 'dual-use,' among others. However, as recently argued by Kevin Wolf and Emily Weinstein,[40] there is an inherent tension in our policy toolbox for export controls when it comes to non-military emerging and foundational technologies. On the one hand, our four existing multilateral export control regimes[41] are narrowly focused on traditional military applications, such as nonproliferation of WMDs, chemical and biological agents, and conventional military and dual-use technologies with clear military usages. Furthermore, the regimes often require consensus to make changes and updates. Thus, new technologies that pose non-military security threats or emergent issues that have non-military but strategic importance cannot be dealt with on a formal multilateral basis.

On the other hand, the US export control regime, especially after its substantial expansion with the introduction of ECRA reforms, provides wide latitude and substantial authorities to the Commerce department to target particular end-users, end-uses and products, and for objectives well-beyond military ones. However, they are strictly unilateral and thus do economic damage to and alienate our closest allies. The patience of our allies will have limits to abiding by the extraterritoriality of US laws, such as the direct product rule. Even if the US were to 'go it alone,' US unilateral export controls are likely only to have a short-term impact before quickly weakening, as ECRA itself admits. Multilateralism achieves longer-term buy-in and durability.

A carefully sculpted multilateral regime, starting with only a small handful of key high-tech allies, could potentially combine the virtues of multilateralism with the effectiveness and precision (end-user, end-uses and product lists) of US controls. It also could be applied to any future strategic objectives, such as threats to supply chain resiliency, unacceptable Chinese industrial policies or misuse of technologies. The seeds of broadly similar approaches to supply chains and emerging technologies are already planted, for

[40] Kevin Wolf and Emily Weinstein, "COCOM's daughter?," WorldECR, 2022.
[41] The Missile Technology Control Regime, the Australia Group, the Nuclear Suppliers Group, and the Wassenaar Arrangement.

instance with the US-EU Trade and Technology Council's Export Control Working Group, the Quad Security Dialogue and the Export Controls and Human Rights Initiative.

Undoubtedly, China would consider this a threat and vehemently and vocally oppose it as yet another example of 'the West' constraining China's rise. Indeed, it would create a unified, clear and multilateral voice. Surprisingly, these facets of a new regime would provide China with many unexpected (and unintended) benefits relative to a US unilateral alternative. For instance, it would create a higher bar to achieve multilateral agreement which would narrow the scope of export controls to truly critical ones. It would also institutionalize the process which indirectly benefits China through greater transparency and stability over time.

For US and member allies it greatly reduces commercial tensions through joint agreement, information sharing, joint enforcement, and could free up trade between member countries even on controlled items. Furthermore, China would be unable to incentivize and peel off our allies on a bilateral basis, such as brow-beating the Netherlands into selling them ASML produced photolithography semiconductor equipment (see Layer #5, above), which China has attempted to do. Finally, with a technological and multilateral sword of Damocles hanging over its own technological and industrial ambitions, China would be incentivized to join additional institutional settings to engage in dialogue over supply chains, cybersecurity and emerging technology issues (Recommendation #3).

Some of these ideas could also migrate to cooperative, multilateral investment security reviews between CFIUS and the growing and strengthening array of CFIUS-like equivalents in Europe (2020), UK (2022) and Australia (2020). Similar to multilateralism in export controls, the goal is to create a united front towards China, generate consensus, information-sharing and joint enforcement among core, technologically-advanced allies, and reduce acrimony among competing and interdependent firms. It would also avoid investment reviews from potentially slipping through the cracks (e.g. the sale of the robotics company Kuka to Midea, a Chinese company), and shed light on undisclosed coordination among Chinese companies, as was the case with Aixtron, a semiconductor company.

3) Weaponized Interdependence and the Road to an International Regime: Baby Steps

The ultimate goal of creating a fifth multilateral export regime or a joint investment review regime is not to isolate China, nor to coerce China. While it would create clear red lines, the real purpose is to shape China's external environment to lead it toward the ends we desire, and in my opinion, a better equilibrium for China too. Ultimately, China will make its own decisions, but we can shape the context within which they make decisions. Thus, if China's external incentives are correctly aligned, such as through a fifth multilateral export regime, it may be possible to coax China into other organizational formats, which may lead to achieving some deeper goals. .

Similar to cybersecurity and finance,[42] supply chains are becoming increasingly weaponized, potentially in devastating ways. While the stakes are much lower compared to nuclear war, we need to work towards building an international regime with a similar set of norms, redlines, formalized lines of communication, procedures and common frameworks of understanding to avoid escalation. This will be a long, drawn out and dynamic process, again because technology and supply chains are not stationary.

An international regime is clearly very complex and beyond this recommendation. However, some initial baby steps in that direction would entail a new forum to foster dialogue on China's and our own security

[42] Farrell, Henry, and Abraham L. Newman. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44, no. 1 (2019): 42-79.

concerns. This might exhume a forum akin to the prior US-China Security and Economic Dialogues, and its predecessors under the Bush and Obama administrations. Such a forum should add 'security' back in to the dormant Trump administration's Comprehensive Economic Dialogues. In addition, there should be a third 'technology' track. Or, if there is sufficient demand, a distinct and specialized dialogue on just security and technology with cybersecurity. Clearly, it would be best to sculpt these dialogues so that they can be more substantive than the prior history of US-China dialogues. But, ultimately, the goal is not dialogue itself, but to allow dialogue to lead to the slow, arduous building of a new international regime that handles threats from supply chains, commercial technologies and cybersecurity.

4) Encourage modularity in telecommunications equipment: Open RAN and O-RAN Alliance

One of the layers conspicuously missing from our deep-dive is telecommunications equipment – the layer that Huawei has become so competitive and which sparked much of the technology tensions with China. Indeed, in 2021, Huawei took about 35% of global markets in telecom network infrastructure equipment (the rough equivalent to Level #1 for smartphones but final-use telecom equipment). This was more than Nokia (16%) and Ericsson (11%), combined. While we lack the teardown data to dig deeper,[43] at this Layer #1, these three firms have dominated the industry for a long time and they are frequent collaborators in the standard-setting process (see Section 2). Given their long collaborations, it is likely that they are quite comfortable with the three-way competition and would find any attempt at modularization of their industry to be quite threatening. Traditional telecommunications equipment is more 'integrated' and telcos purchase integrated systems from these major vendors. There is limited interoperability between equipment, which benefits these telecom equipment giants.

While this is a highly technical field, to my knowledge, there are few technical reasons why telecommunications equipment could not be modularized through standard-setting that allows greater interoperability between more specialized modules. This has happened in many ICT products over many decades. For instance, a movement called 'Open RAN,' in principle, would allow telcos to mix vendor equipment and it would allow vendors to increasingly specialize, perhaps evolving into a full-blown massive modular ecosystem. Of course, as we saw in Section 2, modularity can still lead to high market concentrations and even the domination of chokepoints, such as with platforms or if system integration is a critical capability. Nevertheless, modular systems are inherently more flexible than integrated ones, and would introduce competition. Plus, the US innovation ecosystem generally competes quite well in modularized products, partly because of our strengths in software, relative to hardware. Thus far, however, it seems that Japan's NEC and Rakuten and South Korea's Samsung have the most ambitions in this space.

The US Congress appears poised to fund the Public Wireless Supply Chain Innovation Fund through a reconciled USICA and COMPETES Act which is intended to try to jumpstart Open RAN systems in the US. The bill's utility partly depends on its funding level. However, while funding is important, a major concern is how standards will be set. As discussed briefly in Section 2, standard-setting is critical to the development of interoperable systems like telecommunications or the internet. However, the governance of standard-setting organizations (SSOs) substantially influences the standards that are finalized. SSOs are generally voluntary, consensus-based and industry-led, but their governance can vary widely along different dimensions, including: transparency, openness and distribution of membership, patent obligations, degree of egalitarianism such as in voting rights, leadership positions, and the role of large and small firms, among other things. 3GPP, the central SSO for mobile telecom, is generally on the more

[43] Unfortunately, we do not have access to equivalent 'teardown' of each component contained within Huawei radio access network (RAN) base stations or other telecom equipment, to conduct the same multi-level analysis of Section 2. This is why it was neglected in Section 2.

open and egalitarian end of the spectrum. The O-RAN Alliance is less so, with privileges granted to its founding members, as well as a high share of Chinese firms due to its historical development. However, just like any international organization, public or private, Chinese participation should be welcomed. However, it must be within governance mechanisms that are fair, open, voluntary and robust, and which limit the power of any set of firms or countries. The ultimate goal of SSOs is to agree upon the most efficient overall standards. Properly structured governance of SSOs can achieve that, even when the participants are direct commercial rivals or even geopolitical competitors, as is the case in the well-run 3GPP. But vigilance is essential and so is participation. As such, the US government should try to encourage participation in SSOs, especially among small and medium enterprises who may not be able to afford the time or personnel to attend meetings and vote.

5) Bolstering information, data and expertise on supply chains in and outside government

While increasing information, knowledge and expertise may sound simple and straightforward, achieving the proper organization, incentives and flow of new knowledge through government is easier said than done. Furthermore, as discussed below, creating supply chain knowledge should not simply mimic the existing exercises of creating long lists of products (such as in dual-use arms control). This is because supply chain knowledge is fundamentally different.

Given the complexity, diversity and malleability of supply chains, there is a very good rationale to tap into *different types* of information sources and expertise, especially through public-private interactions. The Biden administration's proposal for a Supply Chain Resilience Program housed within the Commerce Department is broadly in this spirit, although it is not clear why supply chain expertise should be concentrated in a single agency.[44]

There is substantial expertise outside of government that already is utilized, and could be utilized more by diverse methods. For instance, the technical advisory committees (TACs) that rotate on a regular basis in Commerce department is one format, but specialized ones focused on supply chains would be needed, and they could be established across different agencies. However, it is important that they are filled with *diverse stakeholders* and not dominated by industry representatives. Currently, TACs are nearly costless to government, as TAC participants are unpaid and they are not even reimbursed for travel expenses. This unnecessarily limits the pool of willing candidates mostly to industry representatives.

Another possible model is even less formalized. Similar to the process of peer-review in academic publishing, government agencies could maintain long lists of experts who were willing on an *ad hoc* basis to offer expert reports on particular, pressing issues.

Since supply chains evolve and change, forecasting capabilities are also worthy additions in some areas of government, such as those dealing with emerging technologies and in the intelligence community. This was mentioned in the 100-Day Reports too, though implementation is unclear. The future is murky, but companies constantly try to forecast to survive. Attracting that talent into government may be difficult and expensive, but likely worth the cost in certain critical areas. Furthermore, with the internet, social media, increasing commercial surveillance and more powerful computing, there is enormous and growing potential to use open-source intelligence (OSINT), something which academics on shoe-string research budgets have learned to leverage well, including some of the data in this very testimony.

[44] White House, "Building Resilient Supply Chains, Revitalizing American Manufacturing and Fostering Broad-based Grown: 100-Day Reviews under Executive Order 14017," June 2021.

It is also encouraging that legislation is likely to enhance funding to the NSF and establish a technology directorate. However, research on supply chains is highly interdisciplinary, and thus it falls between the cracks of established academic disciplines. It would be encouraging if funding for research and data readily crossed disciplinary boundaries. For instance, small slices of funding under the broad NSF rubric of 'technology' could be hived off to researchers not directly contributing to the advancement of technology itself.

In terms of expertise within government, knowledgeable personnel should be spread across relevant government agencies where particular supply chains goals are sought. Again, the Biden administration's Executive Order targeted particular industries (ICTs, Pharma, etc.) and matched them to particular Departments (Commerce, HHS, etc.). So, why a supply chain taskforce should be housed only within Commerce is not clear. There are already deep expertise in each agency, which can be supplemented with experts that bring a supply chain perspective in certain critical areas. For critical supply chains, they may work to produce regular supply chain audits or identify supply chain vulnerabilities, using cutting-edge data. It seems some of these ideas are in the works, but how the information flows are organized and where data and information comes from and flows to, also matters.

As mentioned, creating 'lists' of technologies or products does not constitute generating supply chain knowledge. As Section 2's deep-dive demonstrated, supply chain research is principally about the technological, business, political and other *interdependencies* between products and production processes. Furthermore, this information collection and knowledge creation needs to be dynamic and evolving, because supply chains evolve. Apart from analysis of supply chains, this include potentially profound re-thinking of core concepts surrounding critical infrastructure, dual-use, strategic technologies, and other security issues, as the deep-dive hopefully illustrated.