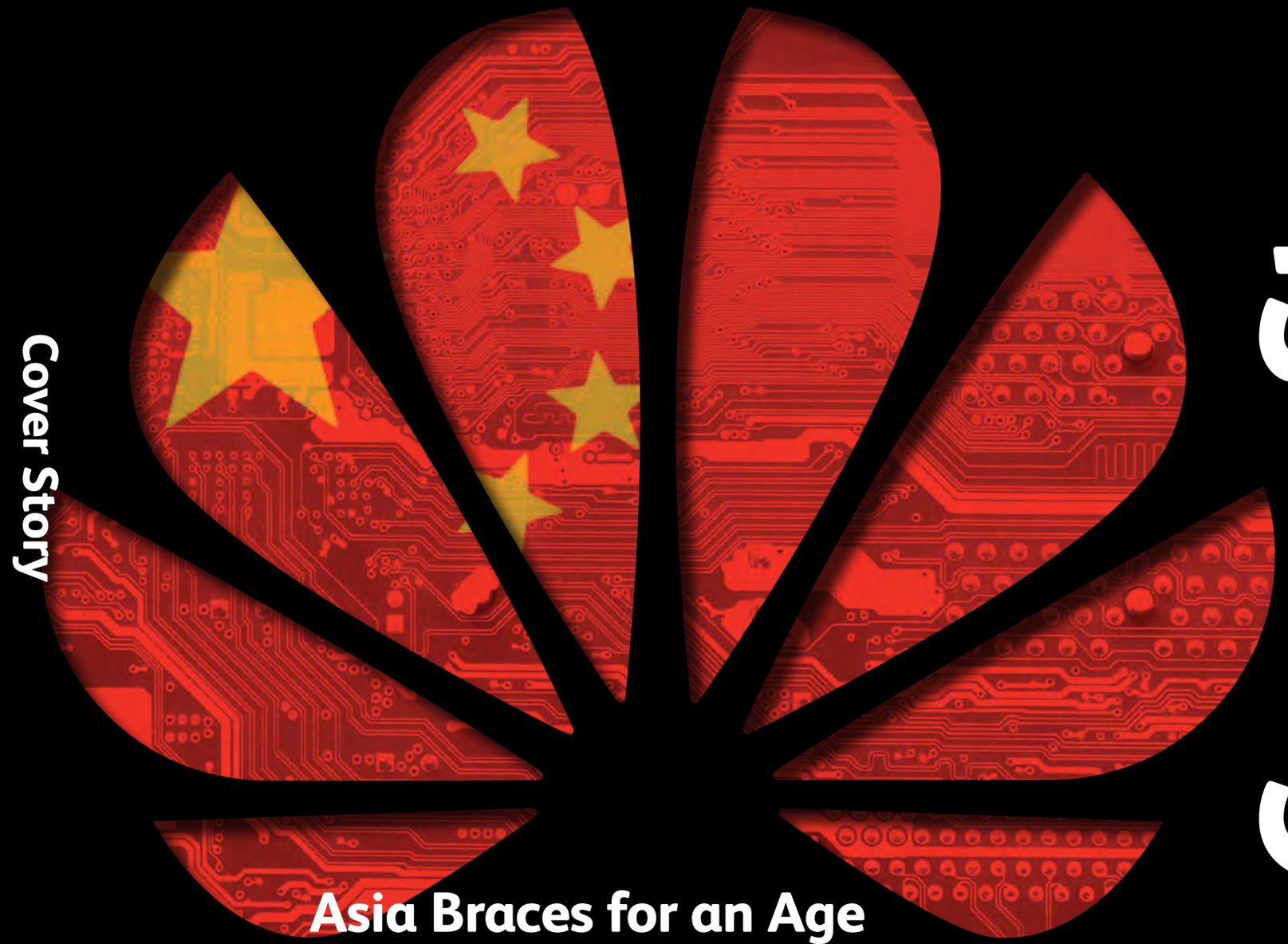
GLOBAL ASIA Vol. 14, No. 3, September 2019



Cover Story

Cover Story

Asia Braces for an Age of US-China Tech Rivalry

Huawei

The US-led campaign against the use of technology from the Chinese telecom giant Huawei — the world's largest provider of telecom technology — in the rollout of 5G mobile networks around the world is shaping up to be a major battle between Washington and Beijing over the future of emerging technologies. Asian countries are struggling not to be sucked into that geopolitical rivalry as they decide who will build their networks.

ESSAYS BY

Weaponized Globalization: Huawei and the Emerging Battle over 5G Networks

By Henry Farrell & Abraham Newman

The revelations in 2013 by former National Security Agency contractor Edward Snowden of widespread US electronic surveillance provoked shock at the revealed vulnerabilities of our interconnected world.

Now, the US is engaged in a global campaign to thwart China's ambitions to sit astride the world's telecom networks, particularly through the 5G technology the Chinese company Huawei hopes to supply around the world.

Henry Farrell and Abraham Newman examine how the campaign against Huawei illustrates an emerging battleground of US-China rivalry.

THE US AND CHINA are engaged in a bitter fight over Huawei, the Chinese telecommunications giant. The US has blocked Huawei from its markets and is restricting its access to US technologies and suppliers that have helped it become one of the great world companies. China has responded by threatening to introduce measures against US companies in retaliation, and accelerating its domestic program to build sophisticated semiconductors to ensure that its companies cannot be blackmailed or crippled in the future.

On the surface, this seems like another fight over trade. Yet it goes much deeper, and is a sign of a stark transformation in global politics. America's problems with Huawei have little to do with US President Donald Trump's obsession with the terms of trade. Long before Trump was elected, US officials were warning about Huawei, and trying to frustrate its rise.[1] Indeed, Trump's single-minded view of trade as the problem may lead him to swap a more free rein on Huawei for other concessions, frustrating his own national security officials.

WHY HUAWEI?

To understand the real, secret story of the Huawei fight, it is first necessary to understand how the nature of globalization has shifted. Economic networks once seemed to be a way of building global markets, crisscrossing the planet with new technologies that would smooth away the frictions of information exchange, trade and global finance. As Chinese companies such as Huawei began to build and participate in these networks, they would imbibe the spirit of entrepreneurial capitalism, and bring it back home, slowly transforming an authoritarian regime into something more open.

It hasn't worked out that way. Now, global networks seem less a harbinger of market efficiency than a plaything of nation states warring for strategic advantage. American officials see companies such as Huawei, with its obscure ownership structure and ambitions for global dominance, as threats to their national interest, and an effort to reverse their own past domination of global communications networks. The result is that a secret war has broken into the open, transforming fights over trade into a greater conflict to dominate the networks that are shaping the global economy.

In a recent research article in the academic journal *International Security*, we explain the logic of the shift toward what we call weaponized interdependence.[2] After 25 years of turbocharged globalization, most economies rely on common systems and networks. The Internet supports an endless hubbub of commercial exchange and exchanges of opinion. Financial networks such as the SWIFT messaging network and the dollar clearing system allow money to be transferred quickly and efficiently around the world. Logistics and communications networks have transformed national manufacturing systems into vast and intricate global supply chains, radically changing how products are made and conveyed to customers.

NETWORK VULNERABILITIES

The result is that most national economies are profoundly interdependent with each other. Businesses in one country rely on businesses in another to produce basic components. Banks have mostly stopped using the antiquated systems of communication and money transfer that they had to resort to in the days of nationalized economies, and instead rely on international networks to send and receive money even from local and national customers. The Internet has become nearly ubiquitous.

These networks offer vast economic efficiencies. Businesses and powerful states are now discovering, however, that they may also create enormous vulnerabilities. The mythology suggests that networks are endlessly fluid, and capable of rapid adaptation to avoid efforts to subvert or control them. The reality is very different. Many of the great networks of the world have grown in ways that make them increasingly centralized. The patterns of information and money flows, and the ways in which manufacturing is organized, mean that the networks are organized around central nodes. Payment systems such as Visa, or Internet providers such as Amazon Web Services, channel torrents of data or finance through a tiny number of companies. If those nodes are seized, and turned to strategic purposes, they offer potential control of the entire network.

This may have enormous repercussions. If a bank does not have access to the dollar clearing system, for example, it is not able to carry out ordinary financial transfers. A wave of fear may ripple through the network as banks that do have access are judged by their dealings with unscrupulous third parties, or judged by dealings that some state later decides were problematic.

Sometimes the vulnerabilities are more subtle. The Internet makes it easy to communicate, but if Internet communications are not encrypted, they can easily be intercepted and read by sophisticated national intelligence agencies. New technologies can transform telecommunications systems into vast ears, patiently listening for interesting and strategically valuable information.

The result is that the great business networks of globalization — the underpinnings of our interconnected and interdependent world — are increasingly being weaponized by states for stra-

1 www.wsj.com/articles/huawei-offensive-is-acceleration-of-yearslong-endeavor-1544274003

2 www.mitpressjournals.org/doi/full/10.1162/isec_a_00351

tegic purposes. Privileged states can take advantage of what we call the "chokepoint effect," the ability to deny other states or actors access to the networks that make globalization work. They also can use what we describe as the "Panopticon effect." The utilitarian philosopher Jeremy Bentham designed the original Panopticon, an ideal prison, in which it would be possible for a single central observer to watch what all the prisoners were doing. Control of the central nodes of the network allows states to do the same thing to the global economy, seeing who pays what to whom, who is talking to each other and what they are saying will be their next move.

The Huawei case is far from simply just another rift in US-China economic relations. It signals a new type of conflict, one in which global networks are the battlefield and global companies are strategic assets that may be deployed or destroyed.

ENTER THE PANOPTICON

The US fears that Huawei will turn the global telecommunications system into a vast distributed machinery of surveillance. It knows what it is talking about — after all, it did much the same thing itself.

The story of how the Internet was transformed into a version of Bentham's Panopticon can be pieced together from the Edward Snowden archives, which consist of leaked material from the US National Security Agency (NSA) and other intelligence agencies. Most of the material has still not been released, and some of it was difficult to interpret (and indeed, sometimes was misinterpreted). Yet, what we know tells us that the Internet and global telecommunications networks allowed the US to engage in global surveillance on an unparalleled scale. Spying agencies were no longer limited to expensive and chancy operations against high value targets. They could instead scoop up the phone traffic of an entire country.

This began with counter-terrorism programs in the wake of the Sept. 11, 2001 attacks. Secret programs with cryptic names like STELLARWIND and PRISM provided the NSA with access to domestic and global Internet traffic. This was far easier because the Internet's network was heavily centered on the US. As then NSA Director Michael Hayden described the new politics of spying, "This is a home game for us. Are we not going to take advantage that so much of it goes through Redmond, Washington? Why would we not turn the most powerful telecommunications and computing management structure on the planet to our use?"

Now, the US fears that China may do to it what it did to the rest of the world, gaining general access to the communications of the US and its allies. Huawei is building out the 5G infrastructure for many countries, perhaps offering the Chinese government access to vulnerabilities in the systems it is connecting. FBI Director Chris Wray warned in congressional testimony that he is "deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks."[3]

It is possible that the degree of access will be even greater in a world where nearly everything is connected to the Internet. 5G networks will connect an "Internet of Things," where everything from pacemakers to home thermostats to industrial robots will have embedded interconnected, mobile computers, and many devices will have microphones or cameras, with always-on connections. The Panopticon would no longer be confined to a prison building, or even phone calls and web surfing, but an intricate root system tapping into our homes and workplaces. What the US security establishment fears is that these underground tendrils would emanate from a taproot located in Shenzhen rather than Redmond or suburban Virginia.

PLAYING THE CHOKEPOINTS

The US is using chokepoints to prevent this new Panopticon from emerging (or perhaps to reshape it so that it accords better with US strategic priorities). This explains the Trump administration's sanctions against Huawei. In May 2019, the US Department of Commerce placed Huawei on its "Entities List." This list identifies companies and individuals that the US government deems are a threat to national security. As well as effectively banning US companies from doing business with Huawei, unless they receive a specific government license, the US flagged Huawei as a risky customer and provider.

The hubs in the global technology supply network have been turned against Huawei. Huawei consumer products run on the Android operating system, which is developed and maintained by Google. The day after Huawei was placed on the Entities List, Google announced that it would no longer update Huawei products. US pressure also limits Huawei's access to the Android app marketplace. Huawei's access to physical components is also threatened, including its ability to purchase advanced semiconductor chips produced by US firms including Broadcom, Qualcomm and Xilinx.

These actions strike fear into the heart of companies outside the US as well. Now that Huawei is on the Entities List, non-US companies face compliance risks if they continue to supply to Huawei. Much of the basic design information that goes into the manufacture of semiconductors has its origins in the US, providing US authorities with a hook for action against companies that use this data in their products. Both ARM, which is a UK-based semiconductor design firm, and Panasonic, the Japanese electronics conglomerate, have restricted sales to Huawei.

Trump signaled his willingness to ease restrictions during the G-20 meeting in June 2019 as

3 www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears

4 www.reuters.com/article/us-usa-trade-china-huawei-tech/trump-us-does-not-want-to-discuss-huawei-with-china-idUSKCN1VP2DZ

part of a larger trade deal. However, as of this writing, Huawei has not been removed from the Entities List. It seems as though national security interests have precedence over economic problems. Trump has verbally rejected efforts to bundle Huawei into renewed trade talks, saying "Huawei is a big concern of our military, of our intelligence agencies, and we are not doing business with Huawei … Huawei has been not a player that we want to discuss, we want to talk about right now." [4]

Even if Chinese negotiators manage to roll Trump, Huawei's ambitions have been frustrated. US suppliers have scrambled to remove Chinese firms from their production networks. Political attacks on Huawei's 5G rollout have undermined its sales efforts across the globe. The Chinese government has redoubled its domestic program to build highly advanced semiconductors.

The US government was able to act because it deployed its influence over key nodes in manufacturing networks to stymie Huawei's 5G rollout and efforts to achieve market dominance in global telecommunications networks. America's security officials used the choke point effect to thwart what it saw as a Chinese initiative to seize advantage from the Panopticon effect.

A NEW TYPE OF CONFLICT

The Huawei case, then, is far from simply just another rift in US-China economic relations. It signals a new type of conflict, one in which global networks are the battlefield and global companies are strategic assets that may be deployed or destroyed.

Powerful states now understand that the networks of globalization can be turned into powerful tools of coercion and surveillance, gaining advantage over their adversaries. Huawei demonstrates both US fears that another state may deploy the Panopticon effect against it, as it has used it in the past, and the use of the choke point effect to prevent these fears from being realized.

The Huawei fight will likely be a key case as the weaponization of interdependence continues. It shows how different effects may be deployed against each other across the numerous and overlapping networks that make up our globalized world. Networks for information, finance and production have distinct characteristics and sites of control, but they overlap, and effects on one field of combat may have consequences for another, as demonstrated by the US effort to use manufacturing networks to undermine Huawei's dominance of communications. This creates a new and vastly complex terrain of battle, which we have not even begun to map.

The consequences for US-China relations are stark. Policy-makers and companies on both sides are beginning to grasp the fact that they are in a new and unpredictable world, but do not yet understand their options. Nor do they necessarily agree on them, as internal Trump administration debates over implementing the Entities List suggest. Over the next few years, we will likely see many miscalculations, as policy-makers fail to predict the likely consequences of their actions. Escalation and tit-for-tat retaliations are entirely possible, increasing tensions, and hurting bystanders on both sides.

Henry Farrell is Professor of Political Science and International Affairs at George Washington University. Abraham Newman is Professor at the Edmund A. Walsh School of Foreign Service and Government Department at Georgetown University.
Support for this research was provided by the Georgetown University Initiative for U.S.-China Dialogue on Global Issues.