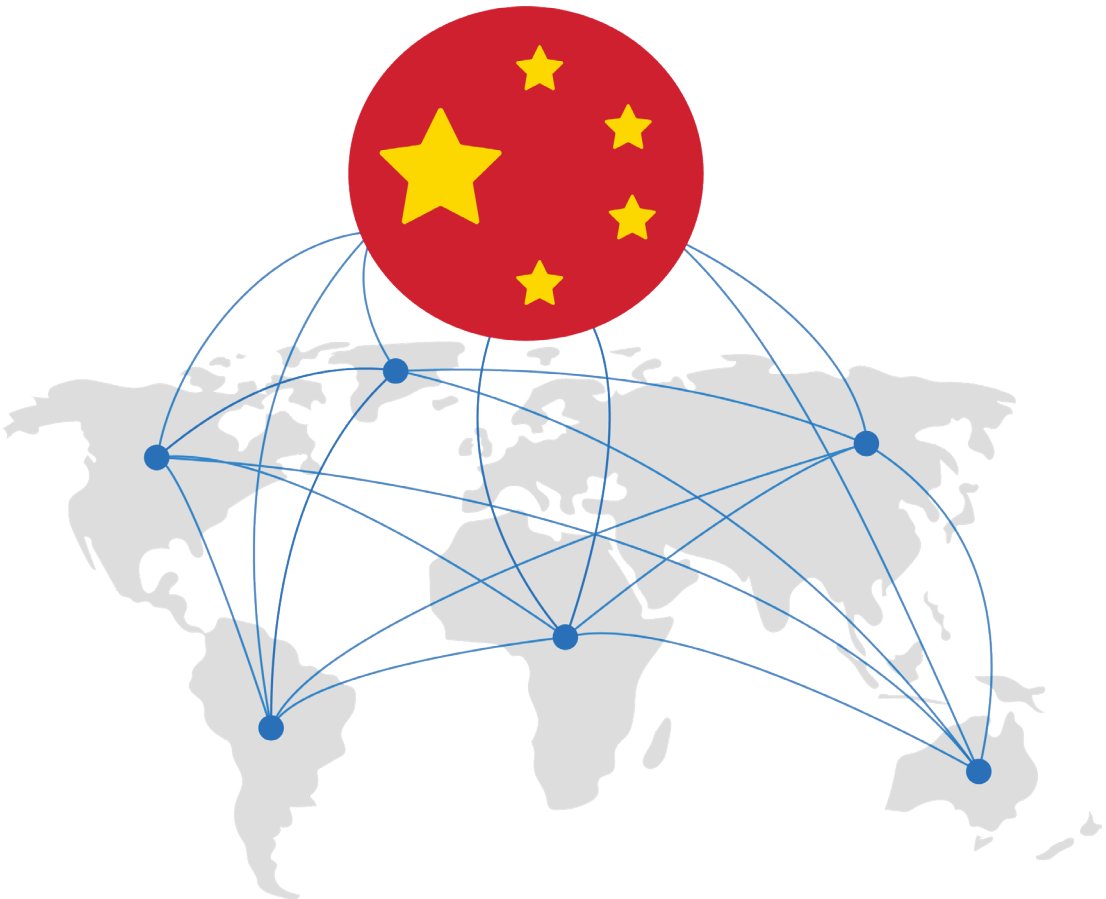
Recorded Future

The New Cyber Insecurity:

Geopolitical and Supply Chain Risks From the Huawei Monoculture

By Priscilla Moriuchi



2019-0610

Background

The real-world corporate and personal consumer risks in Huawei as a global technology conglomerate building next-generation (5G) cellular networks have been largely genericized and misunderstood. The breadth of technologies and services provided and global reach of the company are emblematic of an evolved and more comprehensive technology supply chain threat.

Assessing the corporate or personal implications of introducing Huawei products or services is impossible without examining its aggregate technological, strategic, and geopolitical elements. We believe corporations, consumers, and organizations should consider the potentially significant business and personal risks of operating Huawei technologies for the following reasons:

1. The enormous range of products and services offered by Huawei generates a nearly unimaginable amount of data for one company to possess. From the personal device level (smartphones and wearables), to the network level (routers, switches, and 5G base stations), to the global level (undersea cables, fiber optic lines, and "safe city" surveillance systems integration), we can only begin to imagine what a single company can do (whether benign or malign) with access to that scope of information on people, governments, and companies. Huawei offers a broader range of products and services than companies traditionally associated with the Western technology industry, including Facebook, Microsoft, and Apple. It is a perfect storm of unintended consequences waiting to happen.
2. Huawei does not just exist within an authoritarian state with a one-party system; as a company, it has benefitted from that system, supported that repressive rule, and is intertwined with the success of that government's policies. The position that Huawei occupies in China and its obligations under that government's laws and regulations cannot be minimized. As a 2018 Hoover Institution report aptly states, "not only are the values of China's authoritarian system anathema to those held by most Americans, but there is also a growing body of evidence that the Chinese Communist Party views the American ideals of freedom of speech, press, assembly,

religion, and association as direct challenges to its defense of its own form of one- party rule." This government-level hostility toward freedom and openness combined with a legal and extrajudicial regime that places the responsibility on individuals and companies to assist intelligence and security forces foists Huawei and its employees into an unwinnable situation. Huawei, as a Chinese company, is not inherently malign; however, the people that compose Huawei will at some point likely be forced into making decisions that could compromise the integrity or corporate ambitions of their customers.

3. The third-party supplier threat has quickly evolved beyond hardware and software supply chains. Today, most companies contract some substantial portion of their business operations (including cloud data services, video conferencing, remote desktops, cross-domain solutions, and more) to external providers. The breadth of products and services provided by Huawei places much of that technology supply chain within the domain of one company, and exposes its customers to cross-technology risks. Single points of convergence can also lead to single points of failure. While Geer and co-authors argued in their seminal 2003 essay, "CyberInsecurity: The Cost of Monopoly," that one singular operating system — referring to the Microsoft monoculture of the time — aggregated global cybersecurity risk, today, the monoculture is one of data ownership, where few companies own the personal and professional data of billions of people. The residence of this much of the global technology supply chain (and data) within one company, governed by an undemocratic authoritarian government that threatens basic human freedoms, could potentially pose a serious business and personal hazard.

In this analysis, we lay out the supporting data and analysis that has led us to these conclusions. We focus heavily on the number and breadth of technologies and services Huawei offers because of the evolution of the modern global supply chain threat.

The global economy has undergone a transition from pure hardware and software supply chain threats to a world of third-party risk. The panoply of services offered, purchased, run, and used outside of a company's network exposes each nation, company, and user to

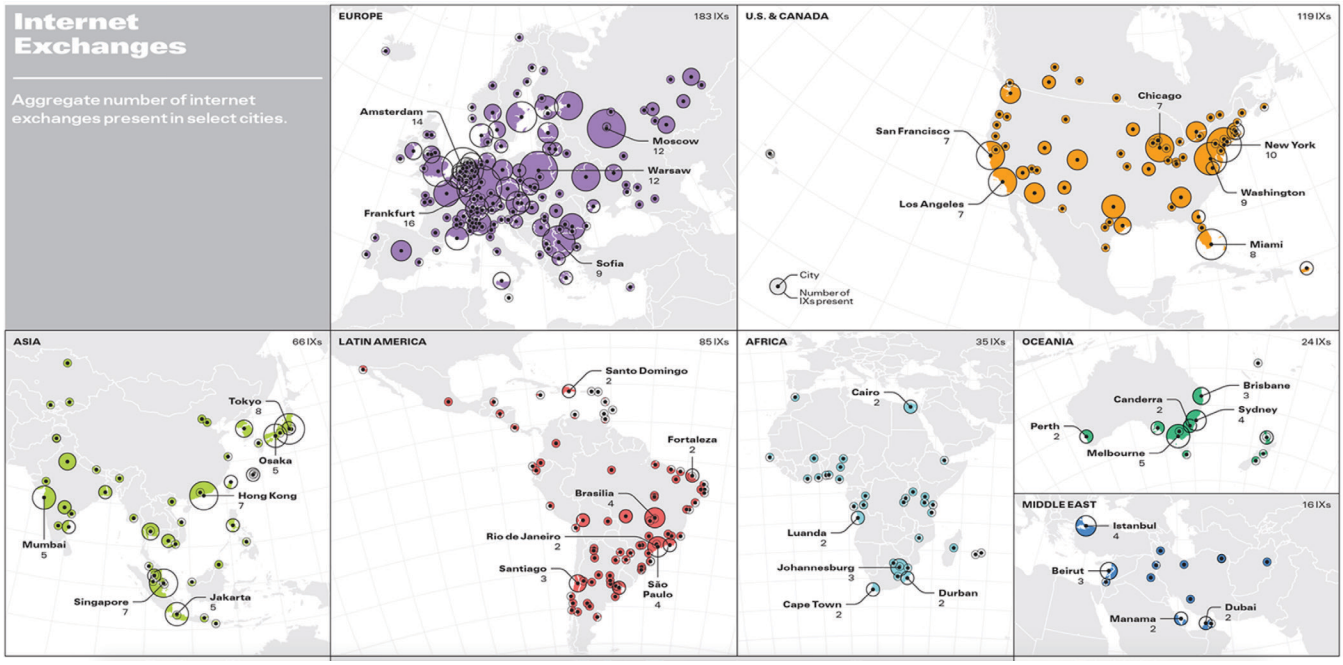
different levels of risk at each point. The reach and scope of Huawei is a perfect example of how security risks and threats multiply as the number of technologies used by a company and the "distance" each packet of information has to travel grows.

Analysis

Undersea Cables, Internet Devices, and Traffic Routing

The global internet in a physical sense is a complex system of cables and devices, made up of switches operated by ISP and home routers, satellite terminals, and undersea cables. These cables and devices are part of a larger system that is not holistically or strategically managed, but one that is cobbled together and functions based on a series of underlying principles.

The physical infrastructure that makes up the global internet is unevenly distributed and does not serve the world uniformly. An excellent example of physical hardware and infrastructure that compose the internet is compiled each year by a company called TeleGeography. The 2018 map below documents and lays out the world's 528 internet exchanges by geography.



Geographical distribution of internet exchanges according to TeleGeography.

As is evident from the graphic, the greatest density of internet exchanges is in Europe, while areas such as the Middle East and central Asia possess far fewer internet exchanges. Further, TeleGeography also determined that of the top ten internet hub cities in the world, six are in Europe, two are in the United States, and two are in Asia. These are not just interesting statistics, but critical data points in understanding global internet routing and the resultant risks.

Global internet routing is a largely random system. Traffic is routed across the globe based on which infrastructure nodes have available capacity, the lowest latency, the largest number of exchanges, and more. The real-world distance between the requester of a web service and its provider has little impact upon the route the packets take. Below are several examples of traceroutes, or the actual routes that packets take across the global internet infrastructure to get from source to destination.

- A user in New York City sent an email to a colleague in Germany, whose closest email server also resides in Germany.
    - Path: New York, to Colorado, to Germany
- A user in Turkey attempted to search for Chinese pop music on baidu[.]com.
    - Path: Istanbul, to Los Angeles, to Beijing
- A user in London streamed South Korean dramas.
    - Path: London, to New York, to Chicago, to Minneapolis, to Seattle, to Seoul

Every time a communication is initiated, the path that the packets travel from source to destination can be different. However, because the lowest latency and greatest capacity is typically in the areas with the most exchanges, traffic overwhelmingly tends to be routed through large hub cities and geographies, such as Europe and the U.S., as opposed to more geographically direct routes through low-capacity areas such as the Middle East or Central Asia.

Huawei's Role

Huawei has become part of this internet-routing infrastructure over the past decade for three reasons: China's Belt and Road Initiative (BRI), Huawei's own efforts to lay undersea cables, and the international purchases and deployments of Huawei "safe city" surveillance technology.

According to CSIS, the BRI is:

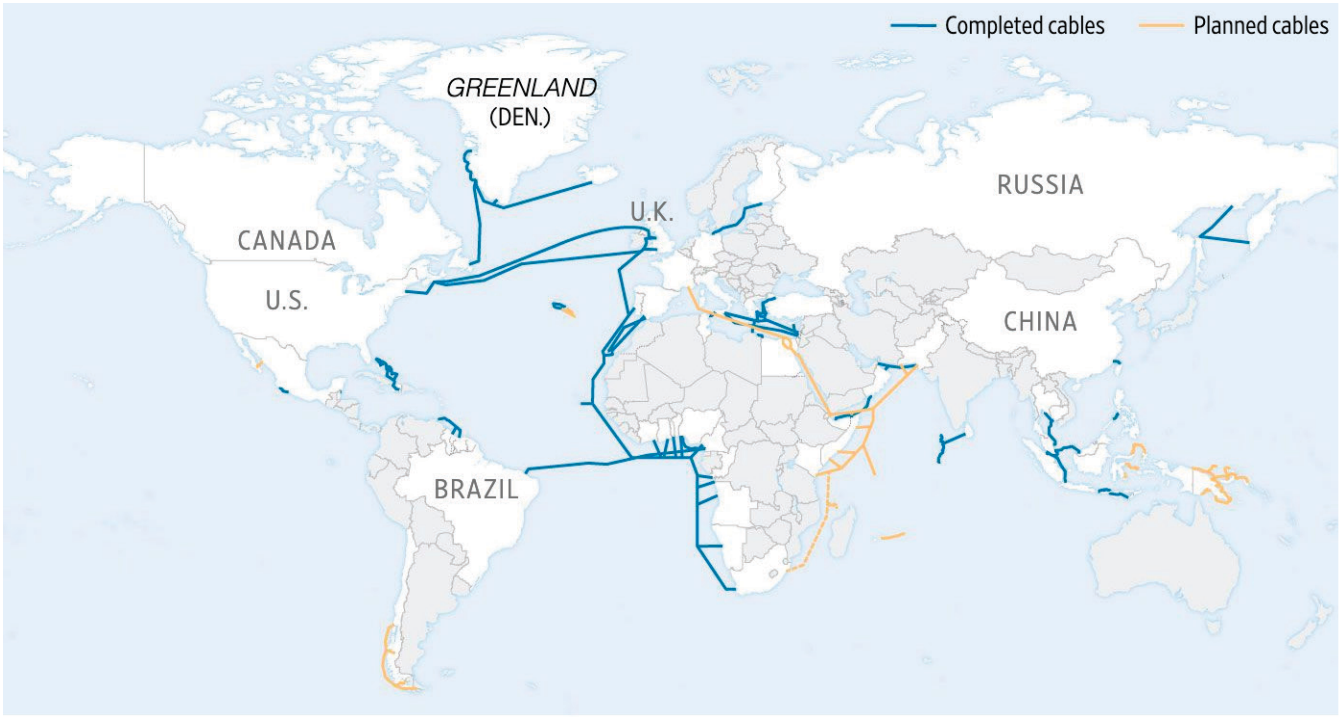
> "... a diverse array of initiatives that enhance connectivity throughout Eurasia and beyond [and] could serve to strengthen China's economic and security interests while bolstering overseas development. The BRI is an umbrella initiative which covers a multitude of investment projects designed to promote the flow of goods, investment, and people. The new connections fostered by the BRI could reconfigure relationships, reroute economic activity, and shift power within and between states."

Among the early success stories for the BRI is a flagship project called the China-Pakistan Economic Corridor (CPEC). China and Pakistan have long had a close political and economic relationship, and the CPEC is an ambitious project to connect the western Xinjiang province with Central Asia to counter violent extremism. The areas where BRI funds will be leveraged include:

- The construction of highways, railways, ports, and other transportation infrastructure
- Laying a cross-border fiber optic cable and updating Pakistan's internet infrastructure, including the national data center and a second submarine cable landing
- Major energy projects in the areas of oil and gas, hydropower, clean energy generation, enhanced power transmission, and more
- Industrial parks and the creation of Special Economic Zones (SEZ)
- Agricultural development, tourism promotion, and more

One of the earliest projects under the CPEC to reach completion was the laying of an 820-kilometer long fiber optic cable from the Khunjerab Pass on the China-Pakistan border all the way down to Rawalpindi. Both within the structure of BRI and CPEC and outside of it, Huawei has become deeply integrated into Pakistan and, as a result, Central Asia's telecommunications systems. Huawei built Pakistan's first data center to assist with e-government transformation in 2016, has begun work on the PEACE undersea cable connecting Pakistan to Central and Southern Africa, and has been awarded contracts to install its "safe city" surveillance, intelligence, and technology integration systems in Lahore, Islamabad, and Peshawar — all financed by concessional or preferential loans from the Chinese government.

However, Huawei's work to expand internet bandwidth has not been exclusive to Central Asia or Africa alone. Formed in a joint venture with British engineering and underwater services company Global Marine in 2009, Huawei Marine has worked on over 90 projects installing or upgrading undersea cables around the world.



Map compiled by the Wall Street Journal of Huawei Marine-constructed cables.

As seen in the map above, Huawei Marine has worked on undersea cables around the world and has expanded capacity in not only underserved areas such as Africa and the Middle East, but several North America to Europe projects as well. The Wall Street Journal article further quotes expert sources as qualifying the risk from Huawei cable development as both technological and geopolitical:

> "These officials say the company's knowledge of and access to undersea cables could allow China to attach devices that divert or monitor data traffic — or, in a conflict, to sever links to entire nations. Such interference could be done remotely, via Huawei network management software and other equipment at coastal landing stations, where submarine cables join land-based networks, these officials say."

How Development Links to Risk

What links these significant internet infrastructure upgrades in Pakistan and across the globe to the broader Huawei risk concern is regional latency and international traffic routing. When examining internet routing data and the subset of traceroutes performed above, what emerges is evidence of a virtual internet routing desert, with central Asia and the Middle East possessing marginal routing capacity. At the practical level, this means that much of the traffic (email, video streaming, messaging, chatting, etc.) that theoretically "should" transit Central Asia, because geographic proximity should enable faster packet transmission, is instead routed through exchanges in Europe and the United States.

This same routing behavior applies to sessions initiated in or destined for China as well. User traffic initiated in the Middle East or Central Asia and destined for China is more frequently routed through Europe and the U.S. than through Central Asia, despite the closer geographic proximity. This is a security concern for China because U.S. and European lawful intercept provisions allow intelligence services and law enforcement to collect data for national security purposes.

For example, in the U.K., under the Intelligence Services Act and the Regulation of Investigatory Powers Act, intelligence and security agencies are allowed to obtain warrants that authorize them to intercept communications transiting the U.K. in the interest of national security. As home to the second-largest internet hub in

the world, these laws could provide the British government insight into a wider swath of global communications than equivalent legal regimes and services in Saudi Arabia, for example. The U.S. has similar legal provisions through the Foreign Intelligence Surveillance Act of 1978. Both the U.K. and U.S. laws have well-defined legal limitations and face regular review by legislative and judicial authorities.

The Chinese government probably wants as few of its communications to traverse European and American exchanges as possible, and expanding and upgrading cables and exchanges in Central Asia, the Middle East, and Africa would provide additional latency and therefore routing options for Chinese internet communications.

For European and American governments, the inverse is true but with notable differences. These governments want as few of their communications to traverse Chinese or Chinese-operated exchanges and infrastructure as possible. This is because while European and American intelligence and security agencies' communication interception capabilities are governed by strict laws and stringent oversight, which is not the case for their Chinese equivalents.

The Challenge of Chinese Law

Chinese law gives the intelligence and security services vast powers over data collection and communications interception with few limitations and no checks or balances. The series of recently enacted laws that govern intelligence and security services include the 2017 National Intelligence Law. In a thorough analysis on Lawfare, one Chinese legal expert argued that Chinese citizens and corporations are obligated to assist the government in national security work and that the National Intelligence Law appeared to:

> "... shift the balance of these legal obligations from intelligence 'defense' to 'offense' — that is, by creating affirmative legal responsibilities for Chinese and, in some cases, foreign citizens, companies, or organizations operating in China to provide access, cooperation, or support for Beijing's intelligence-gathering activities."

In terms of the role of Chinese citizens or corporations in assisting the Chinese government with intelligence-gathering, many legal

experts outside the mainland agree that there is no legal recourse to refuse a national security request from the government. For Huawei in particular, legal analysts use the provisions in Chinese law to counter Huawei's arguments that the company has no duty to install backdoors or surveillance tools in their equipment, and that overseas employees and systems are not subject to Chinese laws.

Commentators and legal specialists in a Financial Times article on the Huawei legal defense sum up the company's legal obligations in this way:

> "Wang Congwei, a partner at Beijing Jingshi law firm, said: '[Huawei] cannot refuse, the law stipulates that companies have an obligation to cooperate for national security and investigation needs. National security laws, the anti-terrorism law and other laws all require companies to assist the judiciary. The National Intelligence Law mandates intelligence agents to do work 'within and outside of' China, and to compel organisations to assist them in their work. State security officials have in the past travelled to the US to harass practitioners of the Falun Gong spiritual group. 'I think the territoriality issue is a red herring,' said Paul Haswell, a partner at Pinsent Masons in Hong Kong. 'Regardless of what any law says, if the state asks you to do something, you'll face consequences if you don't, be they legal or more sinister. The [Communist] party is supreme and has the final say on everything.'"

These legal analyses mean that Chinese citizens and companies — even those operating outside of China — are obligated to assist in national security or intelligence work when requested by the government, and it also means that the Chinese legal system does not provide a means of recourse to refuse.

Our own research has also demonstrated how foundational the intelligence and security services have become to the Chinese national security legal structure. Both China's primary foreign intelligence (the Ministry of State Security) and domestic security (Ministry of Public Security) services have extensive investigation, enforcement, and operational authorities under China's recently updated national security legal framework.

Further, Huawei has purportedly received funding from the Chinese military and a branch of the intelligence services. Huawei was also the main supplier of hardware and software for a new headquarters building gifted to the African Union (AU) by China in 2012, where

a French investigation alleged that massive amounts of data from AU servers were covertly transferred to China every night.

After pulling all of the disparate threads of the Huawei legal defense together, it is evident that Huawei is in fact obligated to assist Chinese intelligence gathering and security operations. This commitment can be summarized with three points:

1. National security, cybersecurity, and intelligence law updates passed since 2016 require Chinese citizens, companies, and organizations to assist state intelligence gathering.
2. There is no legal mechanism in China for a company to challenge or contest a request by the intelligence and security services.
3. China has a demonstrated history of leveraging private organizations and individuals to conduct intelligence gathering. This is not simply installing intelligence officers into positions in existing organizations, but forcing private individuals (often referred to as co-optees) to use their positions at private organizations to gather information for the state.

From a technology supply chain risk perspective, any data that transits Chinese-owned or operated exchanges, cables, devices, or other infrastructure could be subject to requests from intelligence and security services. As Huawei's global footprint and number of services and technologies grows, that risk is amplified.

Huawei Technologies, Surveillance, and Data Integration

The technologies, services, and devices offered by Huawei to global consumers are exceptionally broad. Among the products and services offered by Huawei (from its own website) include:

- Switches
- Routers
- Mobile phones
- Laptops and tablets
- Wearables
- Broadband network elements

- Software for IT infrastructure management
- Cloud computing, storage, and data utilities (Huawei Cloud)
- Video surveillance
- “Safe city” intelligence and technology integration
- Undersea cables

A quick search on Shodan for one specific Huawei network device yields over 9,500 results spread across the globe.

Shodan results for Huawei Versatile Routing Platform (VRP) network devices globally. The red dots indicate devices’ approximate geolocations.

Clusters can be observed in China, Europe, Venezuela, and Brazil, and single devices already exist in the United States. Beyond the range of services and network devices that Huawei sells and administers are the integration technologies and services that compose the “safe city” program.

Using technology that was largely built for Chinese domestic surveillance and in preparation for the 2008 Beijing Olympics, Huawei and other Chinese companies have sold so-called “safe city” surveillance and big data technologies to countries around the world, often enabled by financial assistance and loans from the government in Beijing. A New York Times article places Huawei “safe city” technology currently in use in at least 18 countries globally, including Zimbabwe, Pakistan, Ecuador, Kenya, and the UAE.

Huawei's own advertising portrays a much broader and more integrated solution, with a promise of "omnipresent sensing" and big data solutions that focus on "prevention, management, and investigation." Huawei promises to integrate and make searchable in a "one-button search" so-called business, local, and social intelligence, which includes everything from flight reservations and social media monitoring to emergency calls, case management systems, and video surveillance.

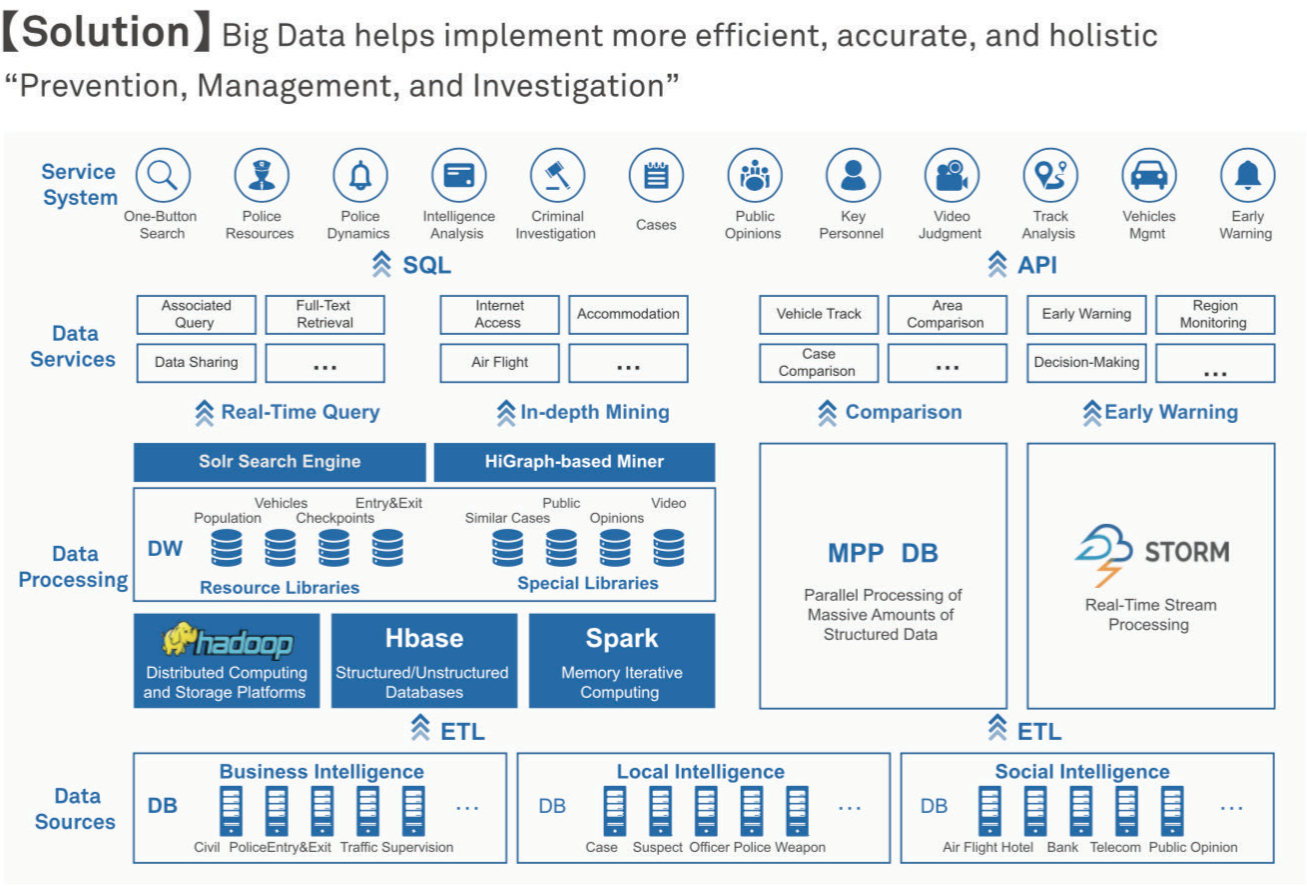
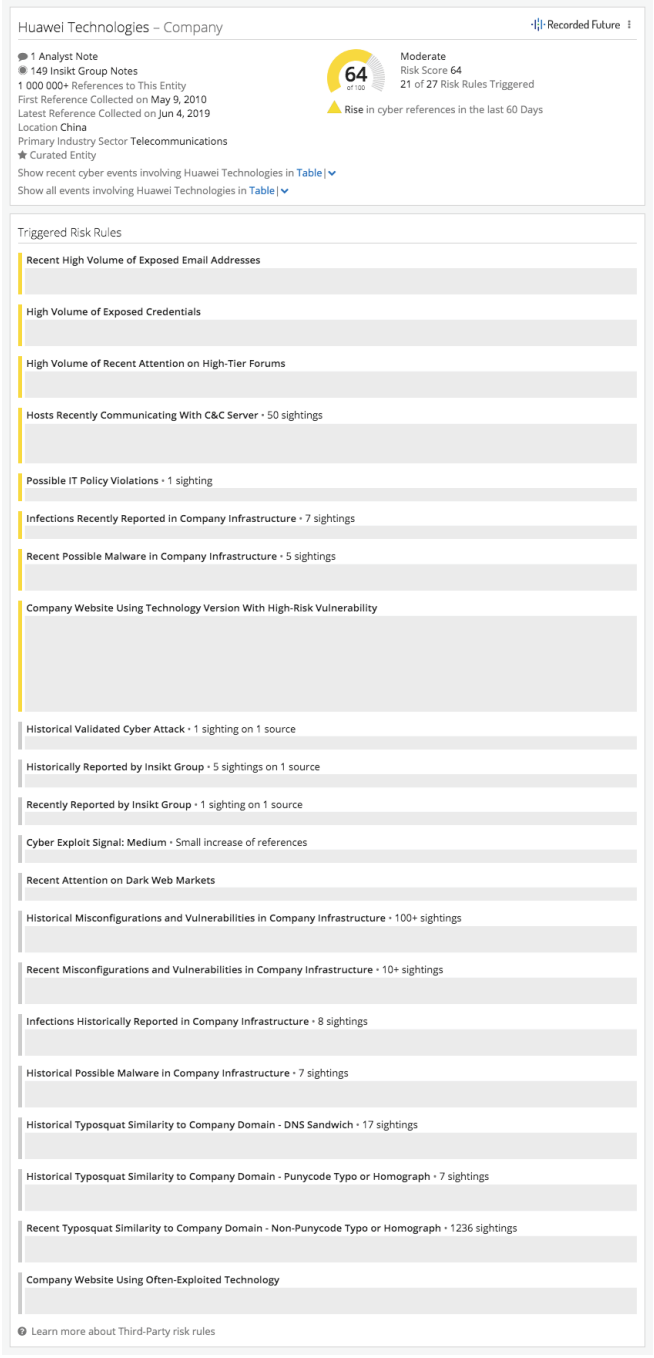


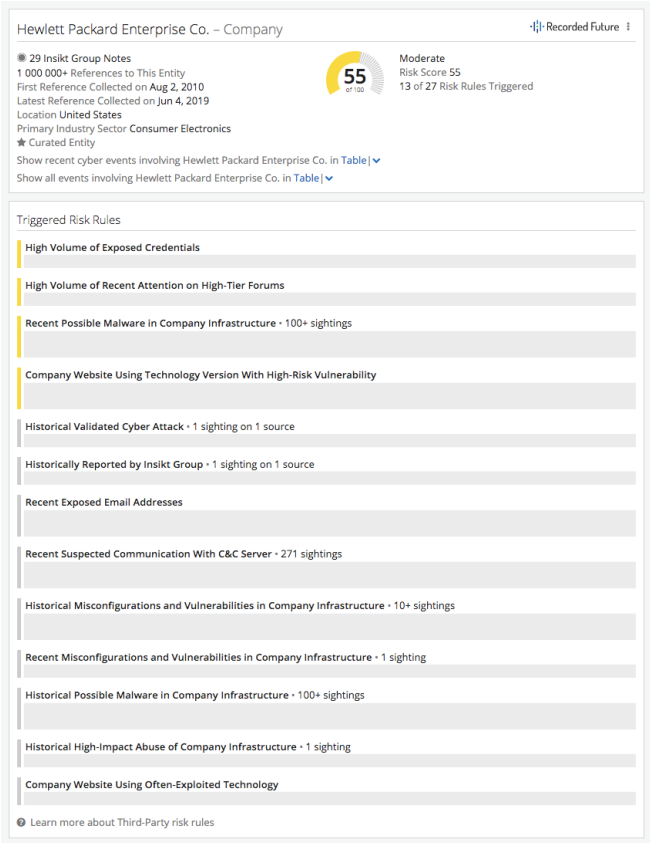
Image of the data sources, processing, and integration offered to governments and security services by Huawei.

It is not yet clear what role Huawei has in maintaining and administering these safe city systems. In video testimonials from customers in Punjab, Pakistan, Bandung, Indonesia, and Manilla, Philippines, users allude to the time, tailored support, and system upgrades that Huawei provided, suggesting that Huawei engineers and personnel maintain involvement in running these systems even after they are sold and deployed.

Putting These Elements of Risk Together

At the core of the 5G deployment debate is whether the risk from Huawei and Chinese telecommunications firms to European and American governments and companies can be managed. It is a question of both technology and geopolitics. From the technology perspective, Huawei's risk as a managed service provider (MSP) and hardware and software vendor can be quantified using the Recorded Future Third-Party Risk module.





In comparison with a similar company in the telecommunications industry, Hewlett Packard Enterprise, Huawei has a higher Recorded Future risk score as of May 28, 2019 because of the vulnerabilities in its hardware and software. Huawei's risk overview on its corresponding Intelligence Card indicates potentially severe infrastructure risks on both its industrial and consumer-facing websites associated with high-threat CVEs and use of unsupported PHP versions (5.2.x, 5.3.x) with known serious vulnerabilities, which may subject Huawei's websites to exploitation risk.

What risk scores and data-based calculations are unable to quantify, however, are the risks from Huawei in the geostrategic aggregate. In commentary on Huawei for a December 2018 Washington Post article, former Director of National Intelligence James R. Clapper Jr. stated that companies such as Huawei:

> "... represent a counterintelligence threat because the Chinese approach is to use them as intelligence gatherers. They not only permit it but encourage it. So if you buy their equipment or avail yourself of their services, you open yourself up to a potential counterintelligence vulnerability."

For private sector companies and individuals, the concept of a counterintelligence vulnerability can be distilled from the risk to data, networks, intellectual property, business data, personal information, and even long-term corporate viability. In other words, counterintelligence vulnerabilities pose an existential threat to corporations. What former DNI Clapper alluded to in his statement was that the government of Xi Jinping views national and economic security as "whole of country" issues. Consequently, his government has implemented a system of laws, regulations, extrajudicial levers, and personal and corporate accountability that raises the risk of doing business with Huawei.

We believe that the breadth of technologies and range of information that Huawei could have access to, including internet traffic transited on undersea cables, mobile and cellular devices, network switches, personal health information from wearables, and integrated video surveillance and communications networks in "safe cities," will likely be too great an opportunity for Chinese intelligence and security services to pass up. This does not mean that Huawei corporate executives would be complicit in, or even knowledgeable of, Chinese military or intelligence efforts to exploit these technologies and data. However, it does mean that Huawei is potentially subjected to a government-driven obligation to capitalize on its global network and consumer devices ecosystem to fulfill core national security and economic dominance objectives.

Repeated cases have demonstrated that Chinese intelligence and security services often use attractive or coercive means to co-opt individuals at lower levels in organizations — employees who can enable intelligence activities without prompting scrutiny. In our view, this is one of the more likely Chinese government assistance scenarios.

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.