



LUIS GRAÑENA

EXCERPT

Huawei Goes to Iraq

How the Chinese telecom giant built a global business by chasing contracts in the Middle East—and attracted U.S. regulation in the process.

EVA DOU – JANUARY 16, 2025

BUSINESS



Ed: This excerpt from Eva Dou's <u>House of Huawei</u> (Portfolio, 2025) was first published at our sibling site <u>The</u> <u>Wire China</u>, and is ungated here. Join us on January 21 at Asia Society in New York to hear Eva Dou talk with Dan Wang about Huawei, the Tiktok ban and more — register for your seat <u>here</u>.





n December 17, 1998, at 20 minutes after midnight, the eerie wail of air-raid sirens pierced the dark sky over Baghdad. The horizon exploded with bursts of light as Iraqianti-aircraft guns sprayed fire. American B-52H planes were bombing the Iraqi capital.



6

At the Chinese embassy earlier in the evening, the mood had been light. No one seriously expected the Americans to attack. Still, just in case, embassy staff had distributed bulletproof vests and helmets. Now, with sirens screaming, everyone rushed to the basement. According to a Huawei staffer's account, the embassy turned off the lights to avoid drawing fire. Since this was before the 1999 U.S. bombing of the Chinese embassy in Belgrade, some even wondered if it would be safer to declare themselves friendly bystanders by blazing the lights and flying China's red-and-yellow flag.

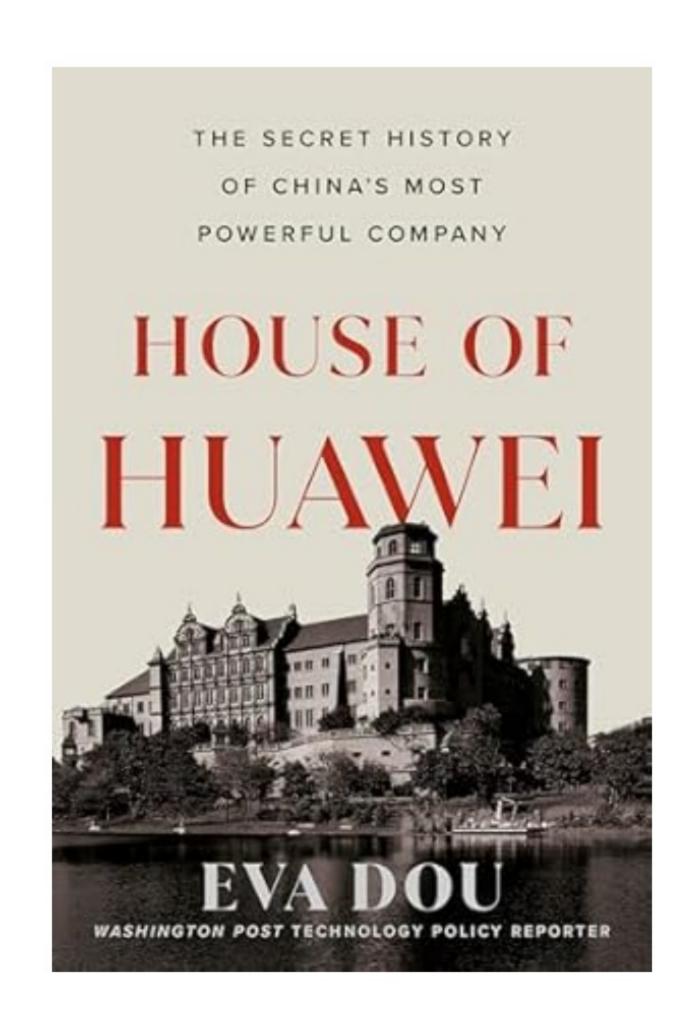
That night, some 200 U.S. Navy Tomahawk cruise missiles were fired into what the Americans called "sensitive targets," sites suspected of being associated with the development

of weapons of mass destruction.

In the morning, as the embassy's staff evacuated the city by car, a Huawei employee saw a group of Iraqi residents standing in the street, looking up at the sky. "I suddenly thought of the scenes from China during the Opium War, when foreigners used their foreign guns and cannons to confront Chinese people armed with traditional weapons like knives," he later wrote. "How terrifying it is to be a weak and small country. And as a citizen of such a weak nation, what kind of humiliation will they endure?"

Huawei, the Chinese telecoms behemoth, was only a year and a half into its international expansion. In April of 1997, it secured its first international joint venture, Beto-Huawei, in the Russian city of Ufa. But as the company looked out at the global telecommunications landscape, it saw a market dominated by the West. America's Lucent Technologies — a direct descendant of Alexander Graham Bell's Bell Telephone Company — was number one in the world, with Sweden's Ericsson, France's Alcatel, and Canada's Nortel rounding out the heavyweights. There were plenty of smaller contenders too, all jostling for space: Britain's Marconi, Germany's Siemens, Japan's Fujitsu, Finland's Nokia, and Motorola and Cisco in the US.

To thread its way into this competitive market, Huawei, which was founded in 1987, began working for "rogue regimes." Huawei founder and chief executive Ren Zhengfei made an overseas stint a requirement for promotion in 1998, and Huawei executives focused on distant, overlooked and sometimes dangerous corners of the earth.



Buy the book >

Ren, a former engineer in the People's Liberation Army and proud patriot, called his workers his "iron army." He called his managers "generals," his engineers "soldiers," his sales teams "guerillas," and their salaries "rations." He sent new employees through military-esque boot camps to build discipline and camaraderie. And he said Huawei's executives took their inspiration from the U.S. military in choosing which staffers to promote: "Has this person been in combat? Has this person been in a live firefight? Has this person been wounded?"

Huawei executives swapped stories as a rite of passage. One staffer posted to Burundi reported frequent power cuts, a T-shirt shortage due to the lack of a nearby market, and a close call with a hippopotamus. Another recalled sticking it out through an Ebola outbreak in Sierra Leone, including offering to take a customer's sick employee to the hospital. When civil war broke out in Libya, Huawei's staffers divided themselves into two teams so that they could keep the phones running on both sides.

But some staffers, like the ones in Iraq, were cloaked in secrecy and code names.

Iraq was tricky territory for a company like Huawei. The country had been under United Nations sanctions since the 1990 Iraqi invasion of Kuwait, which meant that sales of telecommunications equipment into the country were largely blocked, with any exceptions requiring a UN waiver.

Huawei was operating there but trying to keep a low-profile presence. A few years after the U.S. bombing, when asked by a Western journalist about the company's Iraq office, a Huawei executive said he was uncertain if it existed. When Huawei had brought a prospective Iraqi customer to visit its headquarters in Shenzhen, it had taken pains to go under the radar. "At that time, it was difficult to send formal invitation letters to them through normal channels," one Huawei employee working in Iraq recalled, saying that a colleague had used their connections to help them secure a visa to China.

The risk and maneuvering, however, were worth it. These controversial contracts would serve as the engine for the company's early global rise. By the 2010s, the Middle East was the beating heart of Huawei's global empire, with some 4,000 employees across the region.

But these early contracts would also put Huawei in Washington's crosshairs for the first time. For one thing, the National Security Agency (NSA), the signals-intelligence agency of the U.S., had relied on interception of radio communications to monitor countries like Iraq. As Huawei laid down fiber-optic cables to modernize the phone networks, the NSA found itself shut out from conversations it would have liked to hear.



6 Early contracts [in the Middle East] would also put Huawei in Washington's crosshairs for the first time.

> n February 16, 2001, Huawei found itself in a shocking predicament. Under the orders of President George W. Bush, the United States and Britain launched a joint air strike on five targets outside the Iraqi capital of Baghdad. When the dust cleared, the Pentagon announced that the target was a network of fiber-optic cables that Huawei was installing for Iraq's military.

> The Pentagon gave few details publicly at the time, except to say that the fiber-optic cables were a threat and helped Iraq target allied jets. Behind closed doors, U.S. officials acknowledged they were also trying to smoke out Iraqi troops by cutting off landline connections, which would force them to use radio communications that the NSA could intercept.

"If the Iraqi air-defense communications were shifted to fiber, then interception of communication would be impossible and there would be increased risk to patrols," Charles Duelfer, former special adviser to the director of central intelligence, later wrote. "The attacks forced the Iraqis to use radio links or none at all."

An earlier classified CIA memo about the technology had noted that "fiber is immune to unauthorized intercept by conventional means," calling this "a unique feature not available from other modes of communications." Matthew M. Aid, a former NSA analyst turned independent military historian, wrote that the NSA had persuaded U.S. military officials to carry out the air strike.

The controversy put Huawei in the diplomatic limelight at the highest levels in a way that

Ren and his team were wholly unprepared for. Huawei denied having made any sales in Iraq that violated sanctions, but this did little to quell the controversy. U.S. Secretary of State Colin Powell confronted China's ambassador to the United States, Yang Jiechi, directly.



Gary Milhollin criticizes export control for Huawei during a U.S. Congressional hearing in 2002. (*C-SPAN*)

The Washington Post reported that in 1999,
Chinese diplomats had twice applied to a UN
sanctions committee to obtain permission for
Huawei to supply Baghdad with telecom
equipment, reflecting that the Chinese
government was aware of, and supported,
Huawei's operations in Iraq. The Post also reported
that the Huawei contracts might have proceeded
clandestinely after Britain and the U.S. placed
"holds" on Huawei's application with the UN
sanctions committee. Pressed for comment, a

spokeswoman for China's mission to the UN told *The Post* that if a company was found in violation of UN Security Council resolutions on Iraq, the Chinese government would investigate and prosecute.

One former Huawei executive wrote that he'd only seen Ren scared out of his wits twice: "Once was when the central government's inspection group arrived, and the other was when Huawei exported equipment to Iraq and was facing U.S. sanctions."

The incident sparked broader scrutiny of Huawei in Washington, including calls for restriction of U.S. technology sales to the company. At a Senate committee hearing on weapons of mass destruction in November 2001, Gary Milhollin, director of the Wisconsin Project on Nuclear Arms Control, criticized the Commerce Department for granting Huawei licenses to purchase advanced U.S. components to build its products. He said that Huawei had been allowed to purchase half a million dollars' worth of telecom gear from U.S. tech giant Qualcomm, as well as high-performance computers from Digital Equipment Corporation, IBM, Hewlett-Packard, and Sun Microsystems. Milhollin argued that this U.S. technology had helped build Huawei "out of virtually nothing."

Yet Huawei ended up escaping from the Iraq incident more or less with a warning. Powell told reporters that China had ordered companies working on fiber-optic cable projects in Iraq to "cease and desist." Huawei's executives were perhaps left with the lesson that they could successfully work in countries sanctioned by the United States so long as they proceeded carefully.



Huawei ended up escaping from the Iraq incident more or less with a warning.

99

A fter Saddam Hussein was overthrown in April 2003, the global telecom industry went into a frenzy. Iraq would be able to build a mobile phone network for the first time

— a project worth up to \$900 million. "Wireless vendors around the world are clamoring for

a piece of this lucrative pie," one industry publication said. Another reported that vendors were "salivating" at the prospect.

After the Pentagon had bombed Huawei-built installations in Iraq in 2001 and accused it of violating sanctions, Huawei had pulled back. But when whispers of a U.S. invasion began circulating, Huawei quietly began sending employees back into Iraq. "At the start, we didn't have a clear mission in Iraq," recalled an employee who was sent in that January. "The task that the company's leadership gave us was to rebuild the cities after the war."

In March 2003, President George W. Bush gave Hussein an ultimatum to leave the country or face an imminent influx of U.S. troops. In hopes of sealing a contract, Huawei launched an urgent operation to whisk some employees from the Iraqi telecom operator Asiacell to Huawei-headquarters in Shenzhen, where they could attend a training session. The company scrambled to sort out visas for the Iraqi engineers.

"The war was about to break out," a Huawei manager overseeing Middle East sales later wrote. "If the customer's engineers are not pulled out to the company for training at this time, then they will not be able to come out after the war breaks out, and even contact with the outside world will be interrupted."

By the time a tender conference was held in Amman, Jordan, to pick the telecom operators who would get the licenses to set up Iraq's mobile networks, Huawei was ready. A Huawei engineer stationed in Iraq traveled to Amman for the tender, passing a bombed-out landscape along the way. "If not for war and tyranny, what a rich and happy land this nation would be," the engineer wrote.

Huawei's customer, Asiacell, emerged as one of the three winners.

By December 2003, streams of Huawei engineers in sturdy SUVs were making the 17-hour drive from Amman to Sulaymani-yah, in northern Iraq, to work on Asiacell's 2G wireless network. Meeting some friendly U.S. soldiers patrolling in Hummers, one managed to get an incongruous snapshot as a souvenir: a smiling Chinese man in a black suit and tie, hands clasped, standing amid a bunch of American troops toting machine guns.

Huawei's "iron army" was being rewarded for going where others shied away. And it only picked up steam from there.



Ren Zhengfei's profile in *Time*'s 100 list, 2005

In 2005, the China Development Bank, a Beijing-controlled policy bank, allocated a whopping \$10 billion to fund Huawei's overseas expansion. This was a staggering sum —twice Huawei's 2004 revenue. It meant that telecom operators around the globe could buy Huawei equipment with little cash down, paying back the loans bit by bit. It was clear encouragement from Beijing to go forth as quickly as possible. In quick succession, Huawei announced deals in South Africa, Jordan, Argentina, Thailand, and a string of other countries.

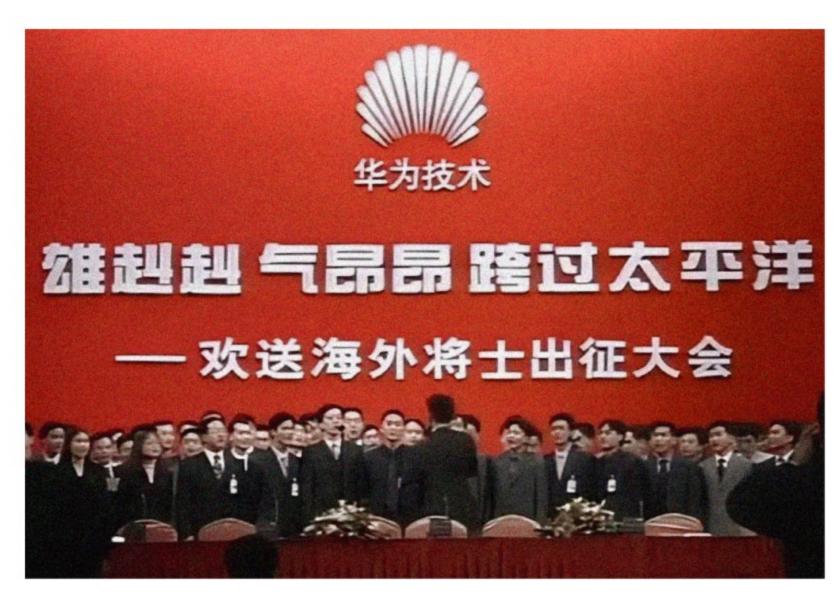
That year, Ren also appeared in the ranks of *Time* magazine's 100 Most Influential People of 2005. Ren was "a former soldier who fashions himself after Chairman Mao," *Time* said. "Like China's former leader, Ren Zheng-fei is known for spouting folk witticisms, purging associates and challenging U.S. power."

6 Meeting some friendly U.S. soldiers patrolling Iraq in Hummers, one Huawei engineer managed to get a snapshot as a souvenir.

Ithough few realized it at the time, the 2001 Iraq bombing proved to be a pivotal moment for Huawei. As one former Huawei executive put it, it was the first time Huawei had come onto the U.S. radar screen as a potential national security threat — and it would never be able to fall off. "The Iraq incident was very important," he said. "The U.S. strategy toward Huawei shifted. At that point, Huawei knew that something would happen eventually ... though perhaps no one could have predicted that thing would turn out to be Trump."

Indeed, it would take nearly 20 years before President Donald Trump moved to sanction Huawei, but with Huawei increasingly integrated into global networks, the company was being watched closely by spy agencies and government officials for years.

Several industry executives recalled Western intelligence officers reaching out with questions. In July 2007, FBI agents interviewed Ren at a New York hotel. Not much is known about the circumstances, except that Ren told them Huawei had not dealt directly with any Iranian company, having only sold some equipment to a third party, "possibly in Egypt."



A Huawei event in 2000, with the sign "Crossing the Pacific with great courage — Send-off ceremony for employees going overseas." (<u>梨视频</u>)

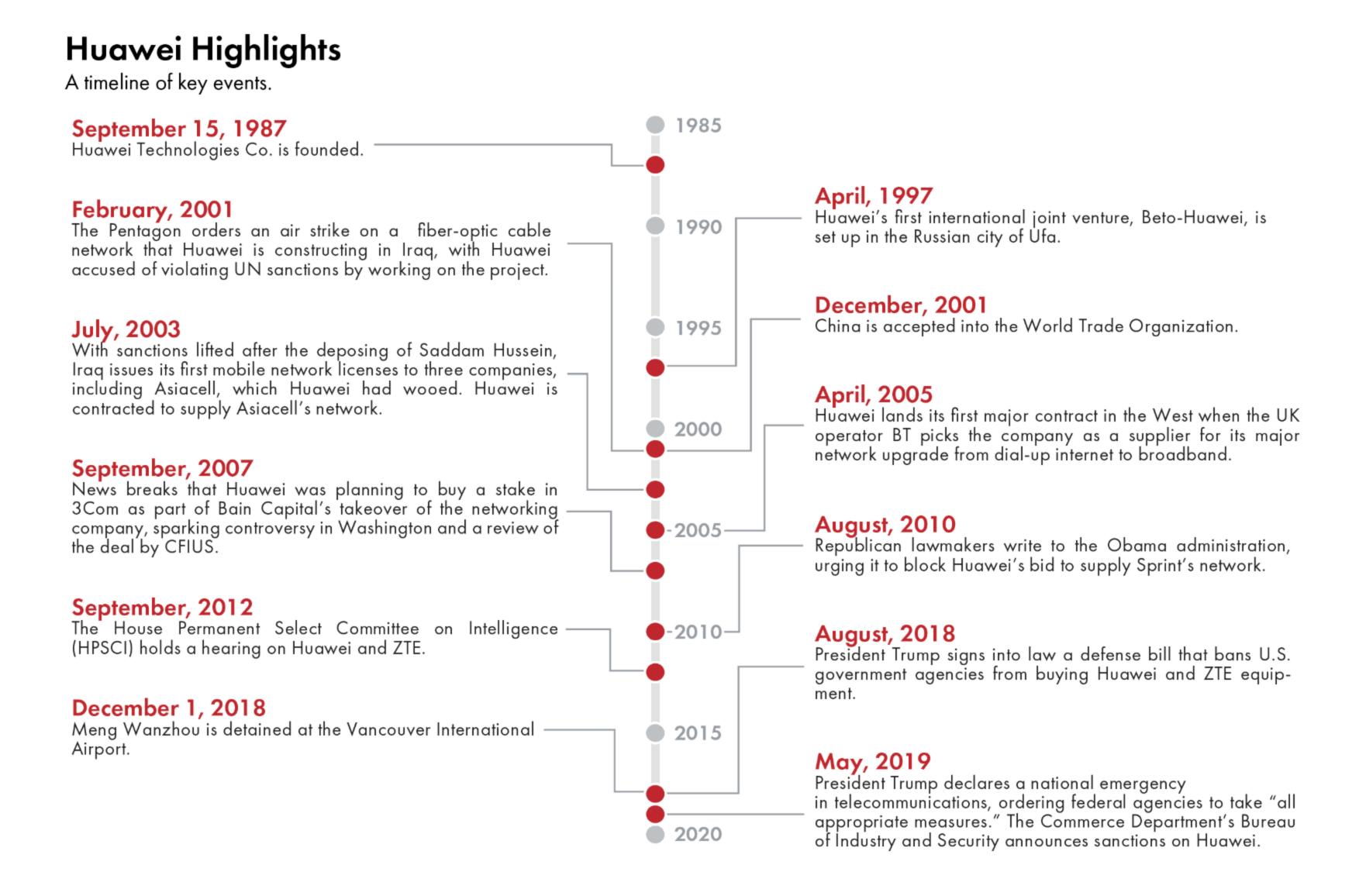
Charles Clancy, who was a research leader with the National Security Agency, recalled visiting Asiacell's headquarters in Sulay-maniyah, Iraq, in 2009 or 2010. He says he saw a lot of Huawei engineers posted there to support a managed services contract. "The Huawei engineers and the Asiacell engineers were playing soccer," he said. "They were the ones that were really running a lot of the infrastructure." Clancy later told a Senate committee that Huawei's managed services gave the company's employees broad access to overseas networks without any hacks having to take place. "A back door is not needed if

you already have a key to the front door," he explained to the committee.

Government officials were also meeting with domestic networking companies about Huawei. In November 2010, Dan Hesse, the CEO of Sprint Nextel, the third-largest wireless provider in the U.S. behind Verizon and AT&T, got a phone call from Gary Locke, the U.S. commerce secretary. Locke told Hesse that he and his colleagues knew Sprint was considering a bid from Huawei to expand its 4G network upgrade. He said they had concerns.

"It wasn't heavy-handed in any way — he actually made it clear this was Sprint's decision," Hesse recalled. "He wasn't telling me as a member of the government not to choose Huawei equipment. But they wanted to make sure I knew that they had security concerns with Huawei equipment going into our network."

Indeed, the prospect had raised alarms in Washington. "If Huawei builds the components for our cell towers in the U.S. 4G network, then every cell tower is a potential listening post for Beijing," Edward Timperlake, former director of technology assessment for the Pentagon, was quoted as saying in *The Washington Times*. (Sprint eventually rejected Huawei's bid.)



In the fall of 2012, concerns about "back doors" in Huawei's equipment had reached a fever pitch. The House Permanent Select Committee on Intelligence held a hearing about "the possible threat posed by telecommunication companies influenced by a foreign nation." Executives from ZTE, the Chinese state-owned telecoms company, and Huawei were grilled, and a month later, the committee released its report. It recommended that Huawei and ZTE be shut out of U.S. government systems, particularly sensitive ones, and that U.S. companies stop buying from Huawei and ZTE. It also suggested that U.S. regulators block the two companies from acquiring U.S. firms.

"Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems," it said.

The report would immediately become political fodder. President Barack Obama's reelection campaign seized on it the day it was published, using it to blast the incumbent's Republican challenger, Mitt Romney, by reminding voters that Romney's company, Bain Capital, had been a part of Huawei's ill-fated bid to purchase U.S.-based 3Com in 2007.

"The House Intelligence Committee concluded that a Chinese tech firm that previously partnered with Bain Capital on an attempted deal from which Romney stood to profit poses

such a threat to our national security that it should be banned from doing business in the United States," an Obama campaign spokesman told *Politico*. "But Romney refused, despite requests from his fellow Republicans, to oppose the deal that could have put our security at risk."

The committee's report would prove to have lasting influence beyond the political moment, and it would be cited repeatedly by U.S. officials and foreign governments over the years. "It was the first U.S. government entity to put on paper what a lot of folks already knew was happening in the national security space," said Andy Keiser, former chief of staff for Congressman Mike Rogers, chair of the House Permanent Select Committee on Intelligence. "This was an official report. It was no longer being conveyed in a hushed tone."

But while some, such as Australia, swiftly joined the anti-Huawei camp, it remained a decidedly small minority in the world for the foreseeable future.

As 2012 drew to a close, Huawei was the world's top telecom vendor, having deployed more than 500 mobile networks, including in 68 capital cities around the world. The company's-fixed-line switches and routers were being used by 45 of the 50 top carriers in the world. Its fledgling smartphone business was number three in the world in sales, just behind Samsung and Apple.

Thanks to Ren's "iron army," Huawei's products now reached three billion people: two-fifths of humanity. ■

Adapted from House of Huawei: The Secret History of China's Most Powerful Company by Eva Dou, published January 14, 2025, by Portfolio, an imprint of Penguin Publishing Group, a division of Penguin Random House LLC. Copyright (c) 2025 by Eva Dou.

Register now for Eva Dou's book talk on January 21, 6:30pm at Asia Society in New York. In conversation with tech specialist Dan Wang, Dou will talk about Huawei's story, as well as the TikTok ban, Tencent's military designation and other aspects of tech rivalry across the Pacific.



Eva Dou writes about technology policy for *The Washington Post*. She was previously a foreign correspondent for *The Wall Street Journal* in Beijing from 2015-20, and Taipei until 2022. Much of her work focuses on the intersection of technology and geopolitics. Dou is the author of *House of Huawei* (2025). She lives in Washington, D.C.