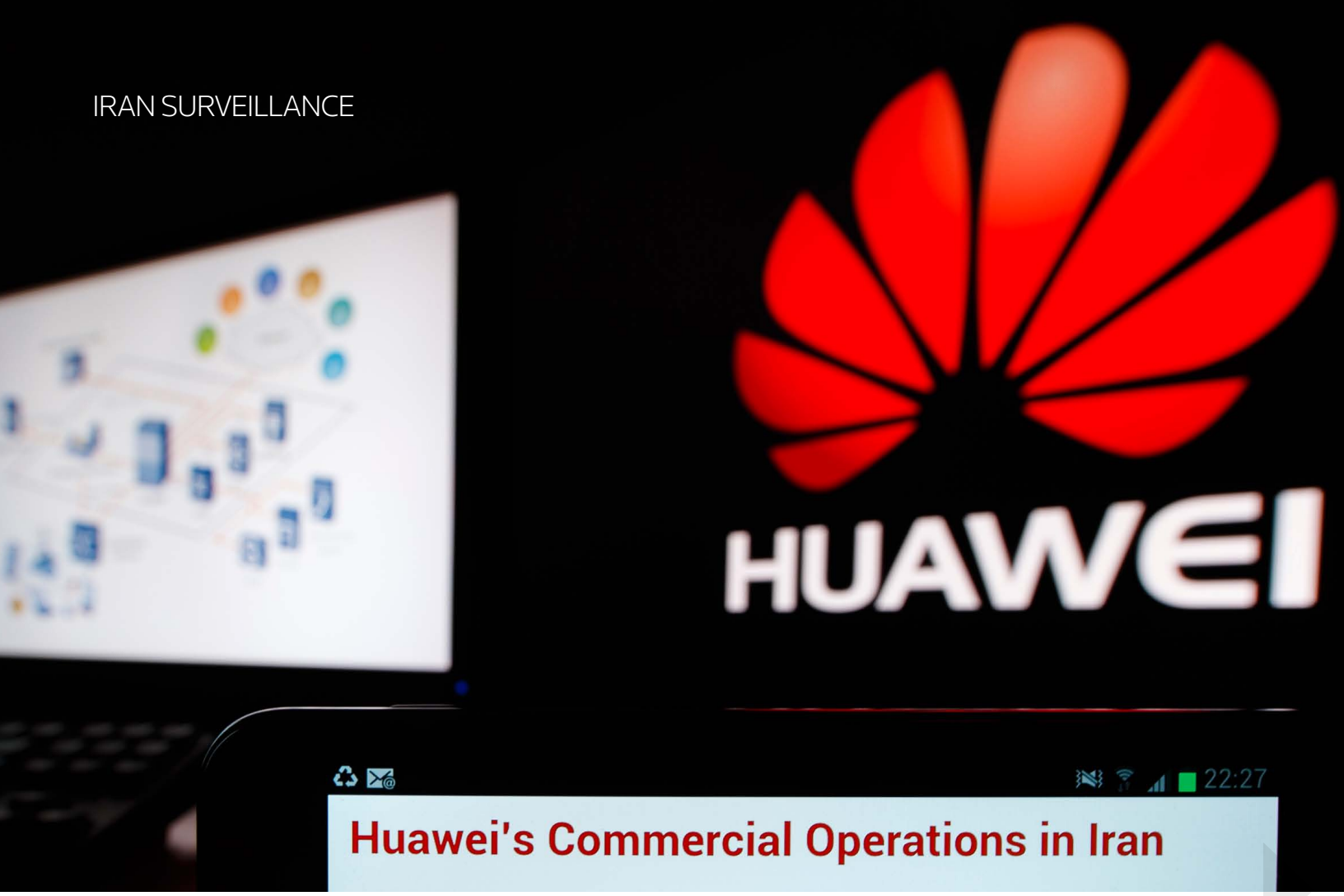


ON OFFER: An excerpt from a statement by Chinese telecom equipment maker Huawei, the firm's logo, and marketing material for a Huawei 'deep packet inspection' system. **REUTERS/VALENTIN FLAURAUD**

How foreign companies tried to sell surveillance technology to Iran

Monitoring Iran

BY STEVE STECKLOW

LONDON, DECEMBER 5, 2012

In the summer of 2008, Iranian security agents arrived at the family home of Saleh Hamid, who was visiting his parents during a break from his university studies.

The plain-clothes agents, he says, shackled him and drove him blindfolded to a local intelligence detention center. There, he says, they beat him with an iron bar, breaking bones and damaging his left ear and right eye.

Hamid says the authorities accused him of spreading propaganda against the regime and contacting opposition groups outside Iran. The

evidence? His own phone calls.

"They said, 'On this and this day you spoke to such and such person,'" says Hamid, now 30 and a human rights activist in Sweden. "They had both recorded it and later they also showed me the transcript."

Hamid was not the only one. The Iran Human Rights Documentation Center and other human rights groups say they have documented a number of cases in which the Iranian regime has used the country's communications networks to crack down on dissidents by monitoring their telephone calls or internet activities.

Now a Reuters investigation has uncovered new evidence of how willing some foreign companies were to assist Iran's state security network, and the regime's keenness to access as much information as possible.

Documents seen by Reuters show that a partner of China's Huawei Technologies Co Ltd offered to sell a Huawei-developed "Lawful Interception Solution" to MobinNet, Iran's first nationwide wireless broadband provider, just as MobinNet was preparing to launch in 2010.

The system's capabilities included "supporting the special requirements from security agencies to monitor in real time the communication traffic between subscribers," according to a proposal by Huawei's Chinese partner seen by Reuters.

Huawei also gave MobinNet a PowerPoint marketing presentation on a system that features "deep packet inspection" - a powerful and potentially intrusive technology that can read and analyse "packets" of data that travel across the Internet. Internet service providers use DPI to guard against cyber attacks and improve network efficiency, but it also can be used to block websites, track internet users and reconstruct email messages.

Huawei says it has never sold either system to MobinNet and doesn't sell DPI equipment in Iran. But a person familiar with the matter says MobinNet did obtain a Huawei DPI system before it began operating in 2010. The person does not know how MobinNet acquired it or if it is being used.

Asked to comment, Vic Guyang, a Huawei spokesman, said in a statement, "We think it's not for us to confirm or deny what systems other companies have." He later said, "It is our understanding that MobinNet does not have such equipment." An official with MobinNet declined to answer any questions, saying only, "So you know the answers. Why do you need confirmation?"

The relative ease with which Iran has been able to obtain technology that enables surveillance illustrates the cat-and-mouse nature of the American-European campaign to contain Iran's nuclear ambitions through crippling economic sanctions. It wasn't until this year that Europe and Washington – which primarily have focused on Iran's banks and oil industry - targeted the sale of monitoring gear to Iran. But even now, the ban is not global, and does not extend to Chinese companies.

> "So you know the answers. Why do you need confirmation?
>
> **MobinNet official**

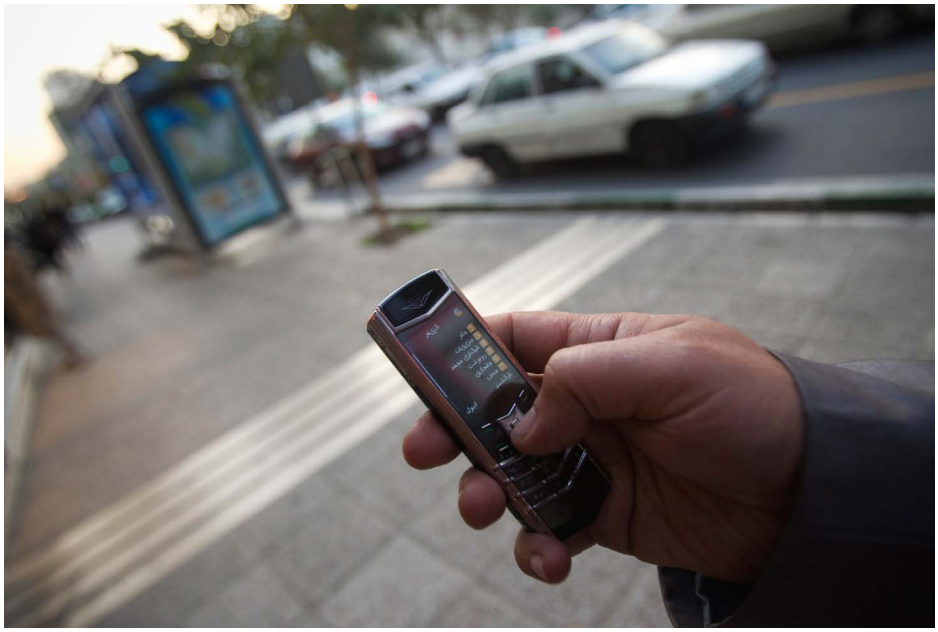
Reuters reported in March that China's ZTE Corp had recently sold Iran's largest telecom firm, Telecommunication Co of Iran, a DPI-based surveillance system that was capable of monitoring landline, mobile and internet communications.

ZTE later said it intends to reduce its business in Iran. Huawei made a similar announcement a year ago.

FIXING "THE PROBLEM OF YOUTH"

In the case of Huawei, the documents seen by Reuters challenge statements made by the company that it doesn't sell any internet monitoring or filtering equipment. In a statement still on its website that was posted last year, the Shenzhen-based firm says, "We have never been involved in and do not provide any services relating to monitoring or filtering technologies and equipment anywhere in the world."

But the documents' descriptions of the Huawei systems pitched to MobinNet emphasise their filtering capabilities and ability



SIGNAL: Human rights groups have alleged that Iran monitors phone calls to crack down on dissidents. **REUTERS/MORTEZA NIKOUBAZL**

to enable monitoring by security agencies.

For example, a proposal made to MobinNet dated April 2009 offers what it calls a Huawei "lawful interception" solution. The proposal was prepared by China's CMEC International Trading Co which states in the document that it had selected Huawei as its bid partner.

"As we know, lawful interception is mandatory and sensitive for the operators in Iran," the proposal states.

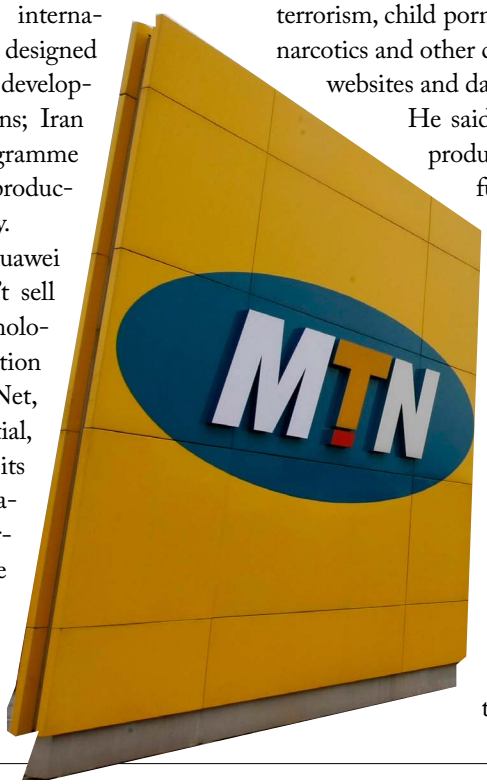
An accompanying diagram illustrates how the system can duplicate data streams and transmit the copies to multiple "monitoring" centers. It also states that more than 0.5 percent of all subscribers could be targeted and that individuals would not be aware their communications were "being intercepted."

The "lawful interception (LI) solution was developed by Huawei," the document states.

CMEC is a part of an engineering conglomerate that includes a unit that for years has been under U.S. sanctions for allegedly helping Iran and Iraq obtain weapons of mass destruction. CMEC didn't respond to a request for comment. Huawei says it no longer partners with CMEC.

U.S. and other international sanctions are designed to deter Iran from developing nuclear weapons; Iran says its nuclear programme is aimed purely at producing domestic energy.

Although Huawei maintains it doesn't sell any filtering technologies, its presentation given to MobinNet, marked confidential, repeatedly says its "DPI Solution" features "URL filtering," which can be used to block specific websites. The presentation also cites a number of



> "As we know, lawful interception is mandatory and sensitive for the operators in Iran.
>
> **Huawei partner's proposal**

customer "success" case studies - including in Britain, Russia, Colombia, and China - where it says telecommunication operators were using its system to filter websites.

For example, the presentation states that a Chinese telecoms firm was using the Huawei system "to settle the problem of youth getting secure and healthy access to websites, and the traffic should be controllable." The presentation also states that the system was used during the 2008 Beijing Olympic games to block "illegal" internet phone services, filter websites and to conduct "user behaviour analysis."

In a series of emailed statements, Guyang, the Huawei spokesman, did not address Huawei's claim that it doesn't "provide any services related to monitoring of filtering." But he says website filtering is used by many telecoms, including in the U.S., "as part of efforts to counter cyber terrorism, child pornography, smuggling of narcotics and other crimes, as well as illegal websites and data."

He said Huawei "did not sell products containing this function in Iran." He also said the Huawei system described in the proposal - the Quidway SIG9800 - can't access "content" in the telecommunications network.

But a former Huawei employee who has worked in Iran said the SIG9800 can be used to reconstruct email messages provided they are not encrypted. "This product has some special usage which Huawei customers do not like to share ... especially in Iran," this person said.

STORING EVERY TEXT MESSAGE

The proposal to MobinNet for the Huawei lawful-intercept system states that it includes technology from a German company called Utimaco Safeware AG. Utimaco says Huawei is one of its worldwide resellers but that neither MobinNet directly - nor Huawei on behalf of MobinNet - purchased or licensed its products.

The proposal also states that Huawei equipment at another Iranian telecom had "already successfully integrated with" an Utimaco product "and accumulated rich integration experience, which will be shared."

The other Iranian telecom isn't named but Malte Pollmann, Utimaco's chief executive officer, confirmed that in 2006, Nokia's German unit had purchased Utimaco software for MTN Irancell, Iran's second-largest mobile phone operator which has a major contract with Huawei. He said the product hadn't been maintained for several years and that Utimaco believes it no longer is being used.

MTN Irancell is 49 percent owned by South Africa's MTN Group, Africa's largest telecom carrier. It declined to comment about the Utimaco product.

Interviews and internal MTN documents reviewed by Reuters show that prior to MTN's launch, Iranian intelligence authorities took a keen interest in the capabilities of its lawful-intercept system, and pushed to make it more intrusive.

Like most countries, including the United States, Iran requires telephone operators to provide law enforcement authorities with access to communications. But people who have worked at Iranian telecoms say authorities sometimes abused their access, targeting certain individuals without a warrant or with little or no explanation.

In response, a spokesman for Iran's mission to the United Nations in New York

emailed a section of Iran's constitution which states that recording telephone calls, eavesdropping and censorship "are forbidden, except as provided by law."

The terms of MTN Irancell's licence agreement stipulated that Iran's security agency could record and monitor subscribers' communications, including voice, data, fax, text messaging and voicemail, the internal MTN documents show. "At least 1 percent of all subscribers" could be targeted, and authorities wanted access to their location – "within 10 to 20 meters" - as well as billing information, according to the documents.

According to a person familiar with the matter, prior to its launch, Iranian authorities pushed MTN Irancell to provide them with even more surveillance capabilities. The requests included copying and storing all text messages on the network for 30 days and providing 36 different monitoring centers with access to communications.

The authorities also wanted to be able to intercept every call handled by an individual mobile-phone tower. "They were not talking of a single tower, they were talking of a large number of towers," the person said. "That is not the norm."

MTN, which oversaw the telecom's launch, didn't express to the authorities any concern about potential abuse, according to this person. Rather, the company argued during a series of meetings that the new requirements weren't part of the scope of the licensing agreement. MTN offered to add other surveillance capabilities over time, this person said.

MTN declined to comment. In April, its chief executive, Sifiso Dabengwa, said that any allegations that MTN was complicit in human rights abuses in Iran "are both false and offensive."

The pressure on MTN Irancell by the Iranian authorities to enhance their surveillance capabilities is made clear in the internal MTN documents.

"The reality of the situation is that the

1%

Percentage of subscribers Iran wanted MTN Irancell to be able to monitor

LEA (law enforcement agency) has the authority to prevent Irancell from launching and even worse to stop our operations from continuing after launch if their requirements are not adequately met," MTN wrote to Nokia, its contractor for the lawful-intercept system, in September 2006. "We have verified this with our own research within the Iranian market with the other operators."

The Iranian intelligence authorities eventually agreed to hold off on their surveillance wish list – and allowed the telecom's launch. But they made clear they expected MTN Irancell would eventually install more capabilities, according to the person familiar with the situation. "Their view was ... it's not a negotiation, we just want to know when you're going to do it," the person said.

The extent to which MTN Irancell later added new surveillance capabilities to its network remains unclear. The network did add enhanced location-based services in 2011.

A British company, Creativity Software, announced in August 2009 that it had won a contract to supply the technology, which it said would allow MTN Irancell to offer its customers special rates at home. "Creativity Software has worked in partnership with Huawei, where they will provide first and second level support to the operator," the company said at the time.

An official with Creativity Software did not respond to requests for comment. In a statement last year, the company said its sale was legal and "any connection implied between the provision of commercial location-based services deployed by MTN Irancell in Iran and any possible human rights abuses is ... erroneous."

Hamid - the human rights activist who says Iranian security agents told him in 2008 they had listened to his telephone conversations - says he had been using a mobile phone he had purchased through MTN Irancell.

Then a student at a Syrian university, he said in an interview that he had returned to Iran to visit his family in Ahwaz, Khuzestan. The region is home to many Iranian Arabs who allege they have been subject to discrimination and economic deprivation by the Iranian government.

Now 30, Hamid said he eventually was released on bail and fled the country. But he said he was arrested in Iraq, jailed for three years and finally received refugee status in Sweden.

He said he was surprised that Iranian authorities had intercepted his phone calls. "I was completely taken aback," he said. "When I bought the Irancell mobile, I didn't even buy it in my name."

MTN declined to comment. The spokesman for Iran's U.N. mission said Hamid's allegations "are unfounded" and that Iran's constitution protects the rights of Iranian Arabs and other ethnic groups.

"Iran's constitution also bans any kind of torture and espionage," the spokesman added.

With additional reporting by Yeganeh Torbati in Dubai; Edited by Simon Robinson and Sara Ledwith

FOR MORE INFORMATION
Steve Stecklow
steve.stecklow@thomsonreuters.com
Simon Robinson, Enterprise Editor, Europe, Middle East and Africa
simon.robinson@thomsonreuters.com
Michael Williams, Global Enterprise Editor
michael.j.williams@thomsonreuters.com