NEWS

Huawei was able to eavesdrop on all calls from mobile KPN customers, including those of the prime minister

Image JeRoen Murré

Huawei had free access to KPN's mobile network. This is evident from a secret report by Capgemini from 2010 that the Volkskrant has in its hands. Among other things, the Chinese company was able to listen in with members of the cabinet and in a database of tapped lines.

Huib Modderkolk April 17, 2021 , 5:00 am

THE MAIN FINDINGS FROM THIS ARTICLE

had access to tapping information in violation of the law. Huawei thereby violated agreements with KPN. This is evident from a secret internal report from KPN from 2010, which is in the hands of *de Volkskrant* .

with tapped telephone numbers. This is contrary to the Telecommunications Act.

The findings of the internal report were so explosive that it was feared the fate of KPN Mobile if it were leaked. From the report: ' **The continued existence of KPN Mobile is in serious danger** because permits may be revoked or the government and the business community may give up their confidence in KPN if it becomes known that the Chinese government can eavesdrop on KPN mobile numbers and shut down the network.'

Before Guusje ter Horst takes a plane to Beijing for a five-day working visit in the autumn of 2009, the Minister of the Interior receives security training from the AIVD. At the ministry in the Wijnhavenkwartier, two AIVD employees talk about the risks of the visit to China. Ter Horst's travel company is also present at the training: her employee Jean Fransman, a policy officer and top civil servant Dick Schoof, who later became head of the AIVD.

It is not so much the nature of the working visit - the four of them travel to sign a bilateral agreement on police cooperation between the Netherlands and China - as the behavior of China that the company should pay attention to, say the AIVD. Jean Fransman: 'We were briefed extensively. They told us what to do with confidential documents and our telephones. ' At the end of each day, the official documents are taken with an embassy employee to a safe in the Dutch embassy.

Phones are a separate risk. Frenchman: "We were warned not to have conversations over the phone." The officials will receive a new SIM card, which will be destroyed afterwards. Minister Ter Horst receives a prepaid telephone from the AIVD, which she must hand in to the service after the trip. She is also advised not to share confidential information over the phone.

It is not surprising that the AIVD is concerned about China. In 2008, the intelligence service saw an increase in the number of digital attacks on the Dutch government and business from China. Ministries and high-tech companies are a favorite target. China is mentioned by name in the annual report that year. Responsible minister Ter Horst said about this later in the House of Representatives: 'There may sometimes be reasons to explicitly mention some countries in the annual report. This happens when the scale is such that the AIVD is of the opinion that it should be widely shared. '

Concerns about China are also growing in Germany in 2009. That country is under constant attack from Chinese state hackers, says Walter Opfermann, a counterintelligence expert for the state of Baden-Württemberg quoted in *The Guardian* . He estimates that the espionage activities cost the German economy tens of billions a year. China is in so many systems that it is capable of sabotaging entire parts of the German infrastructure.

Despite this presence, Chinese espionage appears to be difficult to discuss in Germany, says Opfermann. 'Companies do not want to admit that they are vulnerable and therefore lose customers. In addition, they do not want to waste business opportunities in China. That is why we only see the tip of the iceberg. '

That attitude is no different in the Netherlands. Because while the AIVD is concerned about Chinese espionage, Dutch telecom parties are investing heavily in equipment from the Chinese technology company Huawei. The reason: the Chinese company is much cheaper than competitors Nokia and Ericsson.

Only a few, especially in the security departments of the telecom companies, are concerned about data leakage to China.

If the customer and billing system is replaced at Telfort and different providers send a quotation, the Huawei offer turns out to be so much cheaper that employees wonder whether the Chinese company has entered the correct amount. Huawei asks 25 percent of the price from the other providers, according to a confidential document from parent company KPN that has been viewed by *de Volkskrant* . The British telecom company BT saves 1 billion dollars by opting for equipment from Huawei.

KPN also likes to use Huawei's technology. In 2009, the former state-owned company is the absolute leader in the mobile telephony market. KPN owns more than half of the market and leaves competitors Vodafone (25 percent) and T-Mobile (24 percent) far behind. In 2009 KPN has 6.5 million mobile subscribers who use the 3G network. The phone calls, text messages and e-mails of millions of Dutch people go through the KPN network thanks to Chinese equipment.

In order to further reduce costs - KPN, just like practically all large companies, suffered from the financial crisis in 2009 - KPN has devised a plan to place the management of the Chinese equipment completely in the hands of Huawei technicians. KPN therefore asks consultancy firm Capgemini to make a risk analysis in the autumn of 2009 in preparation for this step.

Capgemini's specialists are investigating the risks associated with Huawei and how the Chinese company behaves within KPN. The conclusions of that report are so alarming that the findings are declared secret. Ten years later, the report is in the hands of *de Volkskrant* and it becomes clear why it had to remain a secret.

Trustworthy partner

In the final version of the report it is plainly stated: Huawei personnel are able to eavesdrop on KPN mobile numbers both within KPN buildings and from China. Huawei knows which numbers are tapped and the company gains unauthorized access to the heart of the mobile network from China. The company is thereby violating the

There are fears for the continued existence of the mobile branch of KPN if the report is leaked. 'If the defects identified by the researchers become publicly known (...), account must be taken of the possibility that governments and the business community will switch en masse to another provider. The KPN Mobile business, which has an impact on KPN as a whole, will then be seriously endangered. '

In 2009, Chinese Huawei technicians have their own space at KPN's head office, right next to the A12 near The Hague. Six Chinese walk in and out and manage the equipment at the core of the mobile network. Huawei supplies *switches* to KPN, devices that link KPN numbers together. When person A calls person B, the data flow goes through a switch from Huawei. In addition to the six employees, part of the management of this equipment is provided from China. KPN apparently sees Huawei as a reliable partner, the Capgemini researchers conclude.

Still, there are concerns about that reliability. In 2008 and 2009, the AIVD had talks with KPN and told about digital attacks from China. The service also pointed out that the "Huawei management has close links with the Chinese government". The AIVD was unable to provide concrete information about Huawei's unreliability in those conversations with KPN. It turns out to be complicated to find out the precise operation of Huawei's devices.

Capgemini does find that concrete information.

The researchers are looking at the possibilities of Huawei to look into the heart of the network. The data streams pass through unencrypted and valuable *call detail records* (CDR) can be seen. The procedures for Huawei to access this sensitive part of the network from China are therefore strict. If Huawei wants to join, the company must request a security code from KPN's Network Operations Center. After that, KPN technicians prepare access. Only then can Huawei be at the heart of the network. A KPN source: 'Safety awareness was already well organized in 2009. It was seriously thought about. '

But it still goes wrong. Huawei appears to be outside the procedure to provide access to the core of the network from China. KPN security people know that this is happening, but they do nothing.
"Uncontrolled and unauthorized access from China actually occurred

Capgemini finds more.

KPN has a system for tapping telephone numbers, Lawful Intercept. When the provider receives a tap order, a copy of the call is sent to KPN in Groningen. An overview of tapped numbers is kept in an encrypted database. It is on a Huawei server. The researchers therefore ask the Chinese company who can access the data and how encryption is arranged. Huawei is only willing to "provide clarity" after much insistence. Huawei appears to use an extremely weak encryption and do the key management itself. Capgemini: 'That means numbers that are on tap are known at Huawei'.

The company's six Chinese employees can also access the call information, the content, of the calls being tapped. This is contrary to the Telecommunications Act. A former security manager at KPN: 'This really surprises me. Lawful Intercept belongs to the highest safety category, everything is boarded up there. I don't understand how this could have happened. '

According to the report, Huawei hardly discloses matters and contradicts the findings of the researchers. The company states that no indication is given anywhere when a number is tapped and that employees cannot see who is being tapped.

But that is incorrect. That notification is there and Huawei has a view of it. Capgemini: "Huawei is aware in detail how KPN realizes its taps, manages the equipment over which this call detail record is sent and has access to the database with numbers under the tap."

The researchers believe that Huawei is violating the agreements with KPN. "Huawei does not behave as a reliable partner in relation to KPN."

And they make another serious discovery. The six Chinese employees work with a program that enables them to listen in on every telephone call that goes through KPN. That too is contrary to agreements. This option means that Huawei employees can listen to KPN numbers anywhere in the world. This means that they can follow parts of the conversation or the entire conversation without the callers or anyone at KPN knowing.

Huawei contractually has the option to monitor a conversation briefly - a few seconds - for quality purposes, which is called listening in. Following the entire conversation - listening in - is prohibited. A source: "They could tap songs, they could listen in from anywhere in the world, KPN had no idea what Huawei was doing on the network."

Then the further implications also penetrate. If Huawei can access KPN numbers uncontrollably and without limit, it can also eavesdrop on communications from the Dutch government. Sources say that this option has been discussed within KPN. A former KPN digital security manager: 'Unbelievable. I would have liked to see these findings, but never got them. '

The team of ministers, including Minister Ter Horst, Minister of Defense Eimert van Middelkoop and Prime Minister Jan Peter Balkenende, are calling via KPN. The extra secure telephones of ministers also use the KPN network. A source: "The conclusion of the Capgemini report actually meant that Huawei could eavesdrop on the government or Chinese dissidents and no one would notice."

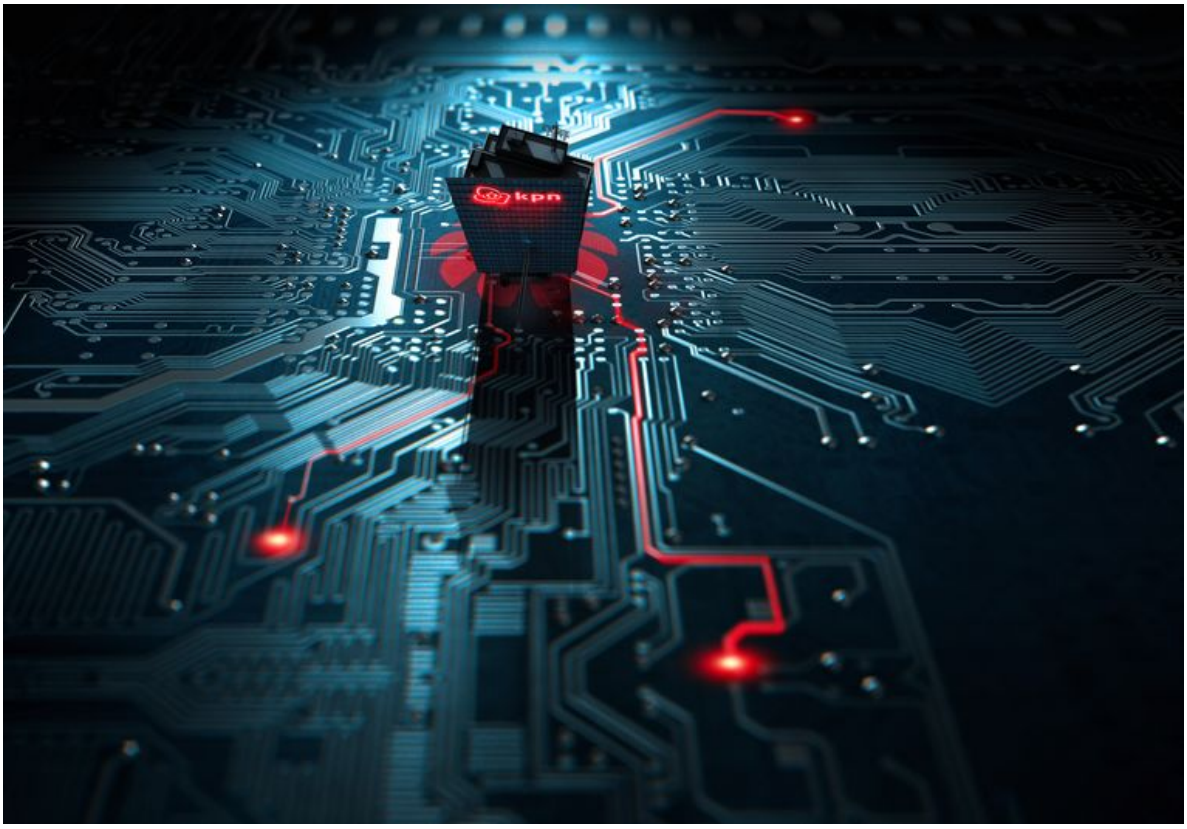

Image JeRoen Murré

The researchers cannot verify whether and how often Huawei is listening in on a conversation. The reason: if Huawei is listening in, it will not be registered and the program the company is using is in

Chinese. "Because the interface uses Chinese characters, it is unknown which actions are actually performed."

The researchers note that Huawei has quite a bit of power over the KPN network. If Huawei wants to, the company can cause serious damage to KPN and society. 'Dutch society is at risk because KPN's mobile network can (potentially) be switched off by Huawei.'

Capgemini's conclusions pose a dilemma for the researchers and KPN. The company has already invested heavily in equipment from the Chinese company. It is no longer possible to stop. 'The researchers are fully aware that the choice for Huawei, which was made by the board of directors a few years ago, cannot be reversed. A recommendation to refrain from the use of Huawei equipment and / or the maintenance of Huawei equipment by the Chinese is therefore not realistic. '

The researchers therefore recommend taking 'far-reaching management and control measures' to limit Huawei's access and to coordinate these with the government organization Agentschap Telecom. KPN is starting a follow-up study at sister company E-Plus in Germany, which uses technology from the Chinese ZTE. The conclusions are equally alarming according to insiders.

Sources tell *de Volkskrant* that Eric Kuisch, Manager Network Services at KPN, will have a meeting with the director of Huawei Netherlands in the spring of 2010. The purpose of that conversation is to reach clearer agreements. If Huawei does not adhere to this, KPN wants to be able to impose high fines, like BT, for example. Whether Huawei has agreed to this is unknown. Kuisch, who has since left KPN, does not want to answer any questions about the conversation. 'I don't respond to questions about former employers, they can do that very well themselves.'

KPN says that an improvement plan was drawn up and implemented in 2010 on the basis of the risk analysis. According to a spokesperson, this has also been discussed with the Telecom Agency. Partly on the basis of the report, it was decided at the time not to outsource (to Huawei, *ed.*). To this day, KPN maintains its mobile core network itself, with the support of experts from several parties. '

What else happened to the report's findings? Sources say that the conclusions from the Capgemini report have been shared with the AIVD. The service does not want to answer specific questions about the situation in 2010, nor whether the service has warned the government. Several former ministers of the Balkenende IV cabinet say they have not been informed. Minister Ter Horst, then responsible for the AIVD, did not respond to a request for comment.

From 2010, China will be given an increasingly prominent place in the annual reports of the intelligence service.

'The cyber capacity, knowledge and expertise of China is so great that the chance of success is also high that they can penetrate somewhere digitally', AIVD, MIVD and NCTV write in a joint publication at the beginning of this year. But it is not known whether China will use Huawei's access.

The intelligence position of the AIVD is not strong in the years from 2010 onwards. The service does see an increasing number of Dutch victims of China's digital espionage, but it is unable to build up a good position in China itself. This is partly due to the staffing, sources say. No more than three AIVD employees are involved with China in Digital Espionage. While the same team sometimes manages to penetrate deeply into Russian networks and espionage groups with minimal resources, China is a lot more complex. China is a black box.

From 2015, visibility will be slightly better. The AIVD sometimes succeeds in hacking a *command and control* server of a Chinese spy group. The AIVD also finds KPN customer files with a Chinese hacking group. And the AIVD and MIVD gain insight into the behavior of Chinese groups in Asia. A source: "Chinese spy groups are massively chasing telecom companies there." They are attractive for several reasons. Once inside, it is possible to bypass two-step verification at a target, tap a network or intercept communications, and find out the exact GPS locations of victims. In India, a large telecom provider was hacked by China. In 2015, the MIVD estimates that China will use more than 100,000 hackers to spy on the West.

Huawei in particular seems to be paying the price for the Chinese expansion drive. The company is accused by all sides of espionage and warm ties with the Chinese government. Partly on the advice of the

AIVD, the Dutch government has decided to ban Huawei from the core of the new 5G network.

Back to 2009. The five-day work trip from Ter Horst to China is going well. The company first flies to Beijing, has several agreements with Chinese delegations and eventually signs the treaty for police cooperation. In Shanghai, Ter Horst and Schoof will visit the Dutch pavilion for the World Expo, which will take place later in 2010. Prime Minister Balkenende will then travel to Shanghai and meet with Chinese President Hu Jintao. 'What was very striking', recalls Jean Fransman, 'is that we were accompanied everywhere by security officers. They even posted outside my hotel door, while I went along as a simple spokesperson. '

Afterwards, Ter Horst returns her phone to the AIVD. During the same period, Capgemini researchers discovered that Chinese employees of Huawei can eavesdrop on all KPN numbers. Also the number of the Minister for the Interior.

COMMENTS FROM EXPERTS

Ronald Prins, intelligence expert, founder of cybersecurity company Hunt & Hackett: 'Huawei has been able to see live who is putting the Netherlands under the tap and may have been able to see who is calling whom from all customers. That concerns everyone. Even if you are not a KPN customer. This case shows how China plays the game. Conquer a market position through (too) cheap technology.

'The knife then cuts both ways: they make the West dependent on Chinese technology and it offers them an easy way in, to do whatever they want within a telephone network.'

Bart Jacobs, professor of computer security at Radboud University in Nijmegen, member of the Cyber Security Council: 'This report shows that Huawei had deep access to KPN's systems. Huawei could listen in on every conversation and shut down KPN's mobile network. From China, Huawei employees could access everything, including the most sensitive information: who is under a telephone tap at KPN, on behalf of the Dutch police or intelligence services?

'That is a serious threat to national security and is a cause for great alarm. Obtaining such a position is a great espionage success for China. KPN apparently mainly looked at its own commercial advantages and hardly imposed any restrictions on the Chinese company. '

Michel van Eeten, professor of cyber security at TU Delft and member of the Cyber Security Council: 'The telecom market in 2010 was incredibly competitive. There was great economic pressure to outsource management. That's how cheap Huawei entered. At the time, safety was secondary. That way of working is now unacceptable. Part of the telecom industry is still relinquishing management, while it is now known which geopolitical complications are associated with this.

Huawei's behavior can be judged in two ways: in the face of the ongoing espionage threat - there are plenty of reasons to be very critical of China and the Chinese business community - or as the standard rumble of companies in the telecom sector. In both cases the behavior is bad. '

RESPONSE KPN

'No supplier of KPN has' unauthorized, uncontrolled and unlimited' access to the networks and systems, or is able to eavesdrop on KPN customers or view tapping information.

'In all years, we have never found that Huawei has stolen customer data from our networks or customer systems, or that eavesdropping has taken place. If that had been the case, we would certainly have informed the competent authorities and our customers about this and taken measures towards the supplier.

'Capgemini carried out a risk analysis on behalf of KPN more than eleven years ago, because KPN wanted to know whether there were security risks in certain systems and processes of KPN's mobile core network and what risks existed in the event of outsourcing the full maintenance of this network. to Huawei. Partly on the basis of this risk analysis, it was decided at the time not to outsource this. For the renewal and replacement of the mobile core network, we are now working with a Western supplier, Ericsson. '

REACTION HUAWEI

" *De Volkskrant* has Huawei Netherlands approached with questions about an internal report KPN that dates back to 2010. This document was commissioned by KPN and never shared with us. It is impossible for us to provide an informed, detailed response to questions about a KPN document that is not available to us.

'We distance ourselves from the situation outlined in the article. Huawei employees have not had unauthorized access to KPN's network and data, nor have data extracted from that network. Huawei has at all times worked under the explicit authorization of KPN. This applied to both employees of Huawei and the Huawei employees hired by KPN ('insourcing') to support its activities. The persons referred to in this article fell into this latter category to our understanding. In fact, these people worked for KPN, which puts the findings from the report in a different light.

'The government has strict legislation regarding access to data in telecommunication networks. The network administrators also constantly monitor our activities. Worldwide, Huawei is the most verified network supplier. Since our start in the Netherlands, 15 years ago, we have never been called to account by the government authorities about unauthorized acts. This while the report has apparently been in the possession of the intelligence services for more than ten years, as is endorsed in this article. Maintaining trust is of unprecedented importance to us, because it forms the basis of our right to exist. That is why Huawei has made cyber security and privacy protection a top priority worldwide. '

anonymously.

Also read

In search of the whistleblower who claims that tech giant Huawei is spying

Huawei had unlimited data access to millions of Telfort customers

Massively fake accounts used to influence the vote on Huawei

MORE ABOUT ECONOMICS, BUSINESS AND FINANCE COMPUTER AND INFORMATION TECHNOLOGY ECONOMIC SECTOR COMPANY INFORMATION KPN HUAWEI CHINA AIVD HUIB MODDERKOLK

News & Background

REPORT

This Groninger GP convinces her

patients one by one to get vaccinated

NEWS

MORE >

Live: 42 million euros in vouchers issued by bankrupt D-travels

Are eases coming soon? These are the numbers to keep an eye on

Wall Street Journal: 'Problems with electronics Boeing 737 MAX bigger than expected'

In Italy there is a big difference between an ice cream and a takeaway ice cream

It started as a joke, now crypto coin dogecoin is worth tens of billions

Liesbeth (65) receives a text message: you can receive a vaccine within half an hour. Why is that not possible in the Netherlands?

Weekend lockdown in Suriname, Denmark eases ahead of schedule

NEWS

Trust in Rutte gets a blow, but the voters see no major obstacle in him

ANALYSIS

Postpone school advice? That only

you do not comply, you will not receive any money

BEST READ MORE >

1 Huawei was able to eavesdrop on all calls from mobile KPN customers, including those of the prime minister

2 This Groningen GP convinces her patients one by one to get vaccinated

3 Fokko read the love letters from his father, a cruel SS man from Camp Amerfoort. This is his story

MORE NEWS & BACKGROUND

Would you like to share important information with de Volkskrant?

Tip our journalists here

General

Contact the editors

Contact customer service

Privacy statement

Subscription Terms

Terms of use

Cookie Policy

Cookie settings

Colophon

Service

Customer service

My account

Holiday service

Single sale

More de Volkskrant

Subscribe

Newsletters

Digital newspaper

Webshop

Including

RSS feeds

Facebook

Twitter

Android apps

iOS apps

Navigate

Columnists

Reviews

The Volkskeuken

Archive