Huib Modderkolk

THERE'S A WAR GOING ON BUT NO ONE CAN SEE IT

The shadow side of the internet: global intelligence, digital espionage and our privacy

Six years ago Huib Modderkolk began investigating the digital world. He gradually formed a picture of how systems built for free communication are exploited for espionage and manipulation, and unearthed secret operations by the Dutch, American and Russian intelligence services. His most important conclusion? We are vulnerable – computer systems control access to our most basic human needs.

Summer 2017: computer screens go blank in 150 countries. The British NHS is so affected that hospitals can only take in patients for the Casualty department. Ambulances are grounded. MRI scanners and blood refrigeration systems stop functioning. Computer screens turn on spontaneously and the words "Oops your important files are encrypted" appear. Employees who desperately pull the plugs on their computers are too late. Restarting is pointless, the computers are locked. And now the attackers ask each victim to pay them 300 dollars. This is hijack software. Those who transfer the money get nothing in return, their computer systems are in ruins.

A month later, an unknown virus strike on 27th June 2017 doesn't just shut down Rotterdam harbour but also systems in France, India, Great Britain, Poland and Germany, before spreading to 60 further countries. Modderkolk's research into this incident and the previous one lead him to the Ukraine, the apparent target of a Russian attack. Are the other victims just collateral damage?

Publishing details

Het is oorlog maar niemand die het ziet (2019), 272pp

This is just one example of how digital disruption in the Netherlands is inextricably connected with the rest of the world. Security systems installed by companies and governments are globally sourced. Israel, for example, is one of the cheapest producers. But internet security systems can also discreetly collect data. There are other weaknesses. Data storage companies can be based anywhere and fall outside of national jurisdiction – criminals can store illegally-gathered data undetected. And how infallible are the certificates obtained to ensure that internet users end up on the sites they believe they are accessing?

Building his explanation on the cases he has investigated, Modderkolk takes the reader on a tour of the shadowy corridors of the globalised digital world and its back doors. He shows how a seventeen-year-old misfit was able to hack the Dutch telecoms company KPN and access key data to practically the entire population. How the Dutch police tapped drug lord El Chapo for years at the request of the FBI. He reconstructs the British-American espionage operation on Belgium telecoms provider Belgacom and reveals how the power relationships between countries enable intelligence services to share and withhold data from each other.

The book focuses on key players such as NSA whistle-blower Edward Snowden, DigiNotar: the Dutch-based certification company with a global client base, Russian hackers Cozy Bear and Evgeniy Bogachev 'the Pablo Escobar of the digital era', and provides insights into military hackers, spies, saboteurs, malware and trolls.

The internet knows no national borders yet the Netherlands is at the frontline of an invisible digital war. The reason - it is one of the fastest digitalizing countries in the world. The Netherlands embraced the internet early on; it is a small country with fast connections and government subsidies that made the internet available everywhere. Widespread internet banking soon followed. An attractive proposition for criminals. And spies.

> 'In the old days, anyone wanting to understand the world read the bible. Anyone wanting to understand the world today should read this book.' - Arjan Lubach, writer and TV presenter
>
> 'Those who wanted to understand the world as it once was read the Bible. Those who want to understand the world as it is now is read this book' - Arjen Lubach, writer and TV presenter
>
> 'This is even better than John le Carré, because it's true' - Matthijs van Nieuwkerk
>
> 'Modderkolk's talent is shaping incomprehensible cyber jargon into a clear-cut narrative with heroes, villains, defeats and triumphs which is accessible to all'
> Beatrice de Graaf, *NRC Handelsblad*

'Huib Modderkolk is the perfect guide to this new world' - *De Correspondent*

'Modderkolk's book on war reads like a thriller' - Maxim Februari, *NRC Handelsblad*

'Het is oorlog... is a brilliant book. Modderlijk's skills as a journalist are out of this world' - *Follow the Money*

Huib Modderkolk (b.1982) is an investigative journalist for the Dutch national newspaper *De Volkskrant*. He is a frequent guest on the popular talkshow *De Wereld Draait Door* where he explains the complexities of the digital world in simple terms.

Modderkolk won the most prestigious journalistic award De Tegel in 2016 and was nominated for it on two other occasions. He also won the Dutch-Belgian investigative award De Loep in 2018. His reports have been taken up by *NY Times, Washington Post, Reuters, CNN, The Guardian, BBC, Der Spiegel, France24* and many other media sources. He has collaborated with *The Wall Street Journal, The Guardian, NY Times* and *The Intercept*.

Sample translation from

There's A War Going On But No One Can See It

by Huib Modderkolk

Translated by Scott Emblem-Jarrett
Amsterdam: Podium, 2019

Bomb on a SIM card

She was blonde, tall and was about to fly off to Spain. That was all the information I had as I stood at one of the red and white cubes at the arrivals halls at Schiphol Airport at 18:30. A woman had sent me an email about a strange incident in England and we had made arrangements to meet. She suddenly appeared in front of me: 'Huib, right? '.

As soon as we sat down in Café Rembrandt on Schiphol Plaza she began to tell all. She wanted to remain anonymous; let's call her Robin. A couple of years ago she was living in England looking for work when she searched online and saw an ad for translation jobs from the Australian company Appen. They were looking for freelance translators in a number of language combinations (including Dutch) in order to improve speech-to-text software.

Robin went to the website and filled in an application form online. She then received an email from a contact person by the name of Alan; she would first have to do a test and, if that went well, he promised she would start receiving assignments and would be paid per task via PayPal. The test involved listening to short audio clips and writing them out verbatim.

Robin passes. Whenever a new 'project' was ready, she would receive an email from Alan; 'You should now see the following project available.' She logged in, read the instructions and she went to project 'Dutch free speech transcription'. She saw a list of recordings, and when she clicked on them she heard people talking in Dutch. She had to transcribe word-for-word what she heard in the clips, which lasted ten, twenty or even thirty seconds in length.

She heard taxi drivers, but the clips were so short she didn't understand the context. Other people could also work on the same project at the same time. She hears people talking about private matters:, such as a man and woman talking about their holiday to Turkey. She translates the conversations and doesn't give much thought to it . She carries on like this for weeks, signing up for one project after another and getting more proficient at her job with every task. She translates thousands of clips and she's paid via PayPal.

She steadily began to establish a picture of the people she was listening to. The most remarkable thing was that the conversations were very recent, hearing discussions about political events and news from recent few weeks. Another interesting thing was that she heard many young men from Turkish or Moroccan backgrounds; most of them were taxi drivers, talking with the taxi company or with each other. The more clips she translated, the clearer it became whether the drivers were from The Hague or Amsterdam.

She began to wonder how this was possible. How had an Australian company got hold of their communications? She sometimes worked on a conversation that was clearly a text message: short messages read aloud by a computerised voice. This also concerne her: did these people know their conversations are being listened to?

●

My contact with Robin came about at the time where I was at a stumbling block as an investigative journalist. I understand how attractive the internet is for security services: you can spy on another country without physically crossing any borders and you can hide behind a false identity or VPN server without anyone seeing. The only difficulty is making clear what the consequences of this are: the articles I write about it are often abstract and theoretical.

Any taboos surrounding wiretapping have clearly disappeared. As of 2012 the NSA in the US had implants in more than 50,000 computer systems worldwide. The service's special hacking unit, Tailored Access Operations, enters an organisation's routers via the Internet and installs software on the computer network. This way the NSA always has access and can redirect data or paralyse an entire network. This method is becoming increasingly popular, or so it seems, according to leaked information from the NSA itself. Within a few years the number of infected computer networks could reach several million.

Technology offers further possibilities. Filtering data from fibre optic cables is more practical than placing a microphone somewhere out in the open. According to one of its own presentations (Current Volumes and

Limits) the NSA has stored 312 billion Internet details and 135 billion phone details. This makes 19 billion phone calls per month, or around 600 million per day.

The AIVD, the Dutch intelligence service, scans whole forums, including the details of people who are not threats. What applies to security services also applies to companies and government bodies: technology makes possible a new kind of background check that was once considered unthinkable. The Tax Office receives so many parking fines, payment details and number plate registration that its employees can follow motorists practically in real time. The police can predict crimes by combining all sorts of data. Online searches for the police have been automated thanks to the iColumbo programme. Now detectives only have to fill in one search term (an email address, number plate or user name) and the programme automatically gets to work.

In my newspaper articles I try to make clear why these subjects concern us all, but I doubt that I've managed to do so. This is also due to the fact that up until now the consequences have been hypothetical: the KPN hack by a 17-year old called Edwin received so much attention because he was able to access the data of millions of customers, and that he could have abused this access, but ultimately chose not to. Filling in a new Digital Patient Form is risky because it can lead to possible privacy violations (whether this is the case is not known). Facebook's purchase of WhatsApp means that Facebook now has access what data WhatsApp collects and uses (which we do not know). The collecting of data by Dutch security services is questionable because it is possibly in conflict with the law (yet this is also remains unclear). This all contributes towards explaining why people feel indifferent towards the risks.

My struggle is reinforced by the findings of an NRC Handelsblad study that shows the rise of so-called 'Snowden fatigue'. According to NRC head editor Peter Vandermeersch, readers are increasingly bored with stories about the NSA whistleblower who leaked hundreds of thousands of secret documents. Every day Vandermeersch fanatically sends the paper's editing team a list of the 25 most read articles, often with feedback on how they could have been improved. He has tracked long term trends on a chart and the conclusion is clear; put 'Snowden' in a headline and most readers will skip past it.

The reason for this is twofold. On the one hand, the Snowden story is, to a certain extent, media hype, and as with any media hype, interest begins to wane after a certain amount of time. Yet there is also something more significant at play: for many people, the reasons why articles about wiretapping and hacking are important are unclear, and so at some point they tune out. These articles often deal with laws, collaborations or incidents, and they deal very little with the systems behind it and the consequences for citizens. What does the fact that the NSA has infiltrated 50,000 computer systems mean if you have no concept of what this means? The consequences (such as 'possible privacy violations') are also often not tangible. Who are the consequences for, and how? What does this mean exactly?

It is time for the next stage. I have to go deeper. What does it mean for society if governments and security services have access to more and more data? Just at that moment I get an email from a woman who wants to 'share her experience'. Sometimes journalism is a matter of being lucky.

●

Robin ordered a Diet Coke and continued her story. She spent months working on the conversations of dozens of Dutch people who were unaware they were being listened to. Her discomfort began to grow. One day she listened to someone in a car recording a voicemail concerning a business deal. She was shocked. 'I was sure I heard my ex-boyfriend's voice'. For a moment she thought she was going mad , but then her suspicions were clearly confirmed; in one of the next clips he called a woman and calls her a pet name that he also once used for Robin. 'It's no ordinary pet name either. I almost fell off my chair'.

She called him up. She wanted to know if he was working on this project. 'I was so naïve apparently'. He was taken aback. At first he didn't believe her, but she told him the details of the conversations she had just been listening to, conversations that took place weeks ago. He didn't understand: he never gave permission for anyone to listen to him. He called Vodafone, but couldn't believe that his provider would go so far as to pass on confidential phone calls to an Australian company.

Following this experience, Robin stopped doing these translation tasks. She didn't feel comfortable with it. She had listened to thousands if not tens of thousands of confidential phone calls made by people who weren't aware they are being recorded. She began to rack her brains about how this was possible. She didn't dare talk to Appen about it; she didn't trust them one bit. Robin did some investigating of her own but didn't get very far, so she put it to one side for years but didn't forget about it. Once the NSA wiretapping scandal bega however, she felt she had to do something with the information.

When she saw me doing a piece on wiretapping on *De Wereld Draait Door*, a popular Dutch current affairs programme, she decided to send me an email. During our conversation I asked her for as many details as possible in order to prove she really did work for Appen and was also paid for this work. She showed me emails and bank statements, and also gave me her ex's phone number. When I called him he confirmed Robin's story: although it happened several years ago, it was still very clear in his mind. He had never had any idea why he was chosen to be listened to.

These are two educated people with good jobs. Not conspiracy theorists but normal, level-headed people who abide by the law. They have no intention to destroy the company; they have no grievances against Appen, they are just shocked. They talk about it because it left an impression on them. In the months following our meeting in Schiphol we kept in regularly contact. She sent me all kinds of information: her registration with the company, the translation tasks she did, new tasks that came in. I could look through all these and use them, provided that the two of them remain anonymous. What on earth is happening here?

•

This is usually how it works after receiving a tip: as a journalist you ask the source of the tip the ins and outs of it all, and then you get to work using this information. What do we know already? Who can tell me more about it? And how and where can one find confirmation of this news? But new technology has changed the investigative work carried out by journalists. Nowadays the correct interpretation of how technology works can make or break a story. When the NSA scandal broke, I tried to find out what foreign security services were listening in on us in the Netherlands. A logical place to start would be the AMS-IX, the Amsterdam Internet Exchange. Each person I speak to who has a different theory. 'You have to look just outside the data centres, that's the easiest place to tap' says one of them. 'I'd look at the server cabinets to see what connections are being made. That's where you want to be' says another.