# INVISIBLE THREATS

## THE DIGITAL DANGERS TO OUR REAL LIVES

AN INTERVIEW WITH
**JAN PHILIPP ALBRECHT** &
**RALF BENDRATH**

We live in an increasingly interconnected world, where new technology is racing forward at breakneck speed, ostensibly to make our lives easier and more convenient. Yet the unexpected consequences of these developments have led to the emergence of sinister new threats which not only put our privacy but also our immediate safety at risk.

**GREEN EUROPEAN JOURNAL: What are the real dangers and threats to EU citizens today when it comes to digital security?**

**JAN PHILIPP ALBRECHT:** The biggest dangers come from very insecure systems developed over the past years and from the fact that most of the technology we have today was not prepared to be constantly connected to the internet or equipped to face very sophisticated attacks. That makes every person and every system vulnerable today. There are many widely-used online products and systems that lack basic IT security safeguards and therefore could easily be hacked into with very damaging results today.

So, the biggest threats are invisible to us today. When dealing with banks or insurance companies, for example, individuals are aware that they run a risk of financial loss but often do not see the greater risk of what could be done with their data or with certain systems they use if they were to be compromised in the future. The point is that we just do not know all the possibilities yet, and that's the biggest danger.

**RALF BENDRATH:** I think the main threat at the moment goes beyond data processing – it's about connected systems that can now have physical effects. Recently, a hotel chain fell the victim to a hacker

attack that locked the doors of all its rooms. This is because they were electronic locks with a central control systems. The hackers then demanded a ransom from the hotel owners – which was paid. Similarly, hackers in the United States proved they could remotely hack into a car's engine control system and shut down its engine, driving at 70mph on the highway, just by using the Internet from their couches at home. That can kill people. This can get worse. Think of pacemakers. You can programme them using Bluetooth without any encryption or password security. You could kill somebody, via Bluetooth, from a couple of metres away. That's the real danger. We have not really thought about all these physical devices, which are now online.

**So that's a very tangible threat, especially given how we all want to have smart devices, from the smart car to the smart lock or vacuum clear. How do we regulate this 'Internet of Things'?**

**JAN PHILIPP ALBRECHT:** It's not that we don't have any regulation but it's not applied! New technological developments are being made without following basic safety standards and legal obligations. There are rules but it's not clear which ones apply to new technologies and how, so the first task is to check to which extent existing laws could apply. The second task is then to design new laws, for example on IT security.

There is today no general safety standard applicable to all these new tools – our phones, smart watches, or smart cars. We need a certain technical standard of security to make citizens safe in the 'internet of things'. But we also need to make designers and manufacturers liable, with fines and sanctions if they don't comply. Not only if something happens, but in general: if a loophole is detected, for example, just because of the high risk entailed.

**In other words, the current legislation is not fit for purpose. The problem is that legislation, often coming from the national level, takes a while to catch up with technology. How do we tackle this?**

**JAN PHILIPP ALBRECHT:** At the moment, many companies produce new technology and directly provide new services online. This is a problem since they don't stop to question which laws they should comply with and instead follow their own standards and wait to see if someone has a problem with it.

Many countries are weak in applying their own regulation and laws. Companies profit from this weakness of the regulator, and whenever a state complains, usually well after the facts or entry on the market, they then invoke the fact that citizens are already using their services and products. In Europe, we have not insisted enough on having our own standards, but the weak position also stems from the fact that

*YOU COULD KILL SOMEBODY VIA BLUETOOTH FROM A COUPLE OF METRES AWAY; THAT'S THE REAL DANGER – R. BENDRATH*

we don't have global standards. For any company, it would be close to impossible to produce and yet comply with hundreds of different national laws.

**Are there basic security standards at the EU level to protect citizens?**

**JAN PHILIPP ALBRECHT:** Currently there is a lack of basic security standards and of a basic idea of secure systems and environments. It's as if people were using the roads without a clear highway code, and without independent authorities checking the safety of cars or the functioning of traffic lights. That's the current situation, digitally. We are not talking about excessively burdensome security measures which impinge on the fundamental rights of people, but simple safety standards for the infrastructure provided. The problem here is that this infrastructure, in most cases, is built and organised by private companies. They don't have an incentive to apply basic safety standards, so the political level needs to urge them to do that – to create the legal environment in which everybody can trust that they can go out without getting harmed. That's the main challenge for the moment. Once you have safety standards, whether hackers can get into a system is a different question. We need to talk about proportionate action and proportionate measures when it comes to security.

**RALF BENDRATH:** In the non-digital, or analogue, world, security is often understood as protection from physical harm. But we also know we can't turn every house into a bunker to protect oneself from the outside world. In the digital world, this is different, because everything is based on computer code. Only if my computer code has security vulnerabilities can somebody throw a digital bomb on my house. In the digital world, if I want, I can actually fortify my systems and put my virtual house under a digital bunker by making sure there are no vulnerabilities or back doors. The defence is, theoretically, quite strong.

**So, how do we ensure and enforce security in the Internet of Things in Europe?**

**JAN PHILIPP ALBRECHT:** First you need to set basic limits and to then make sure that these are respected, to minimise the chance of attacks occurring. Then, regarding the enforcement part it is really not very different from the physical world: when there's a crime, you go after the criminal! That's also why it's important to exchange information on attackers to investigate into networks.

**RALF BENDRATH:** Maybe it's slightly different and more challenging than in the analogue world in the sense that it is always cross-border. Not even just within the EU – of course we have a certain level of European police cooperation and coordination, which could be improved – but we also need common rules with other countries.

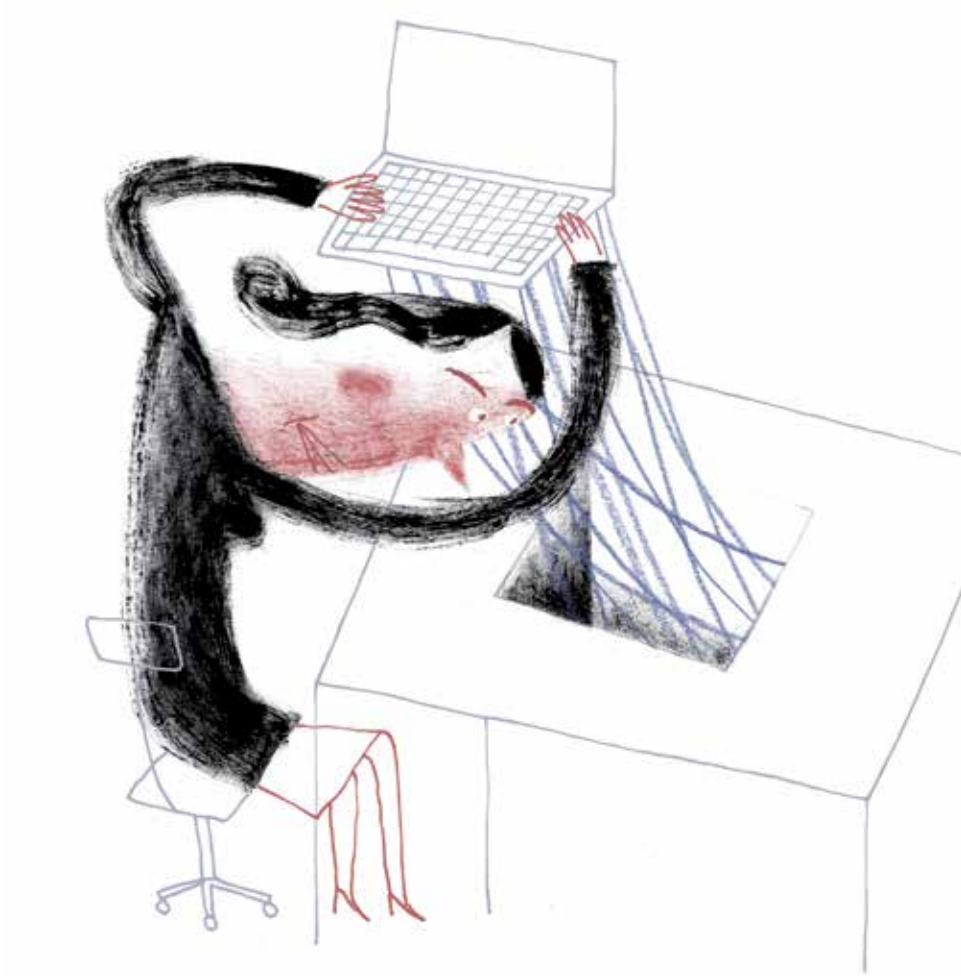
**JAN PHILIPP ALBRECHT:** There's a cyber-crime centre at Europol and there have been efforts to improve technical expertise and equipment in order to have cross-border digital legal enforcement. I think that investigations in the analogue world should increasingly go digital because when it comes to fighting organised crime or terrorism, the sphere of action is increasingly digital.

**RALF BENDRATH:** In addition to the safety standards and law enforcement issues, there's a third element that needs to be addressed: the immunity system of the Internet of Things. Well-meaning hackers – so-called 'white hat hackers' – must not be criminalised if they just happen to discover a previously unknown vulnerability. They don't do any damage if they tell the operator or software manufacturer. We should encourage that.

Manufacturers of hardened software can only fix their vulnerabilities if they are aware of them. If hackers don't tell them because there is, for example, a profitable black market where they can sell this knowledge – especially about vulnerabilities that nobody else has yet discovered, the so-called 'zero days'– then they may sell it to criminals or even to another frequent buyer on these markets: the national intelligence agencies! This also means security agencies make every one of us less secure, by increasing the profitability of selling these vulnerabilities.

**Surely safety standards are key but if that's the policy response, what's the difference that Greens and progressive forces can bring?**

**JAN PHILIPP ALBRECHT:** That is the difference! Of course, everybody is in favour of having a secure environment, but when it comes to really demanding that a company, for example, install basic safeguards, things are different. If a website should only use a secure connection, encrypted with 'https', which makes it slightly



slower than the normal connection, these companies will say that they cannot comply with such safety restrictions because it's a huge obstacle to business and therefore puts their competitors at an advantage since clients will turn elsewhere. Many political actors just accept that answer. It's like the fight for seatbelts in cars. For a long time, car producers were convinced that if they were obliged to put seatbelts in cars to protect drivers and passengers, the car industry would be dead. Politicians accepted this until Green and human rights activists pushed for this to be a mandatory requirement. We shouldn't underestimate how important even slight, minimal changes to this system would be for consumers or how hard the industry will fight them.

**RALF BENDRATH:** Maybe Greens are quite uniquely positioned here because we've always been very strong on digital civil liberties – against mass surveillance of our telecommunication, for example – and because of that, we have traditionally worked together with people who know this digital stuff much better than we do, such as the hacker community, like the Chaos Computer Club in Germany. That has enabled us to understand earlier than other political parties that we really have to go after the root causes. The approach from other political families usually either calls for more surveillance or sets up helpful but weak private-public partnerships.

*THERE IS A LACK OF BASIC SECURITY STANDARDS AND OF A BASIC IDEA OF SECURE SYSTEMS AND ENVIRON-MENTS; IT'S AS IF PEOPLE WERE USING THE ROADS WITHOUT A CLEAR HIGHWAY CODE – J. ALBRECHT*

**This discussion also brings us to very geopolitical and material questions that were asked after Merkel's phone was tapped and Brazil's NSA surveillance led to ideas of having 'independent' undersea optical fibre cables.**

**RALF BENDRATH:** If we make the systems more secure, it doesn't matter if a criminal or an intelligence service wants to attack me and break into my computer. If my computer is safer, then all of these threats, to a certain extent, are reduced.

**We would then need European computers, because if these products come from elsewhere then we cannot regulate the manufacturer.**

**RALF BENDRATH:** Yes, that's the point. If it's free and open source software, it's already easier. The European open source industry is like a sleeping giant with the companies and movement behind it. The Snowden revelations also indicate that we should think about regaining the capacity of producing hardware within Europe that we control, and not rely on China or the US, like we did with Airbus to overcome our dependence on and the monopoly of Boeing.

**JAN PHILIPP ALBRECHT:** Europe has been very naïve in that regard in the past. We've sort of accepted that devices coming from the US or China are ok and we didn't think that it was important to check on the telecommunications companies that installed software and manufactured our connected devices. If we really want to have a safe environment, then we need to control what's in those devices and software. That doesn't mean producing everything in Europe, but it means that if we buy something from somewhere else, where the rules – and also political interests – are different, we must check every little detail in the system.

*THE SNOWDEN REVELATIONS WERE A TURNING POINT BECAUSE IT MADE POLITICIANS IN EUROPE REALISE THE SCALE OF THE PROBLEM – J. ALBRECHT*

The Snowden revelations were a turning point because it made politicians in Europe realise the scale of the problem – and that authorities cannot assure citizens, one hundred percent, that what is happening in their name or on their systems is within the law. That questions the basic principles upon which our democracies are built. In order to make sure that authorities are acting in accordance with the law, they need the capacity to check their systems. If they use products, such as Microsoft systems, where they don't have access to the full source code, then maybe they should be forbidden to continue using them. They should be forced to buy an alternative. In my constituency, somebody is building an alternative to Microsoft systems already, which is open source, but it just isn't being bought. It's strange, because European authorities could be far better off and in better control of what's happening if they simply invested in a different alternative.

In Europe, there is still far too little awareness about these things, not only amongst the public, but especially within policy makers' circles. In particular, if you think two steps ahead and think of the intelligent machines which programme on their own, there will be a huge question of how to deal with this, politically, socially, and ethically. We have not yet grasped the extent to which this will affect our lives. I hope that we will be able to further develop and educate ourselves on this, quickly, and without the need for drastic, negative events or situations such as the Snowden revelations to make us realise that this is really important.

**Do you see evidence that momentum is building, at the political level or among grass-roots activists, for action to be taken in this area? Can we expect this to be one of the main issues in the next elections, in Germany or at theEuropean level?**

**JAN PHILIPP ALBRECHT:** Rather than digital security, the main questions coming up in the elections taking place in Europe this year will be security in terms of how to fight terrorism and deal with external borders and the refugee and migration question. This is, I think, a big mistake, because forward-looking questions on digital security really need public awareness and political debate. It's not a basic security question. In the future, we will be faced with the fact that many jobs, from insurance agents to investment bankers, will no longer be done by humans, but algorithms. Maybe there will even be automated, autonomous tanks going to war. We will certainly have to deal with the question of which ethical guidelines are necessary for such developments and what the consequences are for the humans who worked in those areas before. Along with the consequences for the social system we have to deal with the fact that all of this is vulnerable to digital attacks, technical mistakes, and insecurity. It impacts all areas.

**JAN PHILIPP ALBRECHT**
has been a Member of the European Parliament for the German Green Party since 2009. He is vice-chair of the Committee on Civil Liberties, Justice and Home Affairs. Before his election, he studied ICT law in Berlin, Brussels, Hannover and Oslo.

**RALF BENDRATH**
is senior policy advisor to Jan Philipp Albrecht, with a focus on digital civil liberties, including privacy and security. Before joining Jan's team in 2009, he did political science research in this area at universities in Berlin, Bremen, New York City, Washington D.C., and Delft.