Interview with Arjen Kamphuis, information technology specialist

Securing our information – we have the technology; we just have to have the will to do it

Author: Valentina Novak

"The hackers need you as much as you need them." That was the closing sentence by Arjen Kamphuis in a lecture about information security at this year's media festival Naprej/Forward in Slovenia. A Netherlander who spends most of his time warning people about the dangers of information spying, especially for investigative journalists, believes in collaboration between journalists and technology advisors. He is claiming that with a little interest and time people (and especially journalists) can secure themselves even from spying of the NSA. His lectures and workshops are well thought, thought provoking, justifiable and convincing, which makes it really hard for a person to not be interested more in what he has to say. He is calling out for a bigger engagement for the right to privacy: "With a little effort you can make your laptops not just secure, but extremely secure – to the level where this is the kind of stuff that Julian Assange and his crew use successfully to continuously invade a massive amount of surveillance against them. If it is good enough for them, then it should be good enough for you."

How did you decide to start working in your field with journalists? What drew you to it?
(longer reflection) I originally started working in IT security in general for companies and for different clients. Then I started getting questions from more and more journalists about how can they secure their information. Helping them seemed a very logical thing to do. And it was a lot of fun to do as well. It really felt like doing something that is genuinely important and relevant. Besides, a lot of the time when you are doing consulting work remotely, it is very abstract and it is hard to see the result of your work. But here you can actually see after, for example two days of training, that people can do encrypted email, when before it was a complete mystery to them. So you get immediate feedback – they are now a little bit safer because of the two days of training that they had, and I find that very satisfying. It is

very important that journalists are able to do journalism without the government being able to manipulate the process; that is what ultimately drew me to it. So far it has been interesting and significant and I was already doing it prior to Snowden, but because of Snowden it just became ten times bigger, so now it takes a big chunk of my time and gives a bigger sense of importance to my work.

Last summer you and your colleague Silkie Carlo wrote a book Information Security for Journalists about how we are getting spied on and how to protect ourselves from spying. Why did you decide to do that?

The main reason is that after Snowden's revelations there has been a lot of demand for this sort of knowledge. Even prior to Snowden I was already working with the Centre for investigative journalism in the UK on setting up education workshops about information security. As we were doing those, we noticed that they are extremely efficient but you have to work in a small group, with only six or eight people per day. Therefore we started talking about how to help people who cannot stop by our training sessions, so that they would be able to grab a piece of information and help themselves. Sit down with it over the weekend and go through it. The Centre for investigative journalism then decided to fund me and the co-author to write the book and we did it. The book is now available on the internet for free.

What is it mainly about and what is its purpose?

It is written in a way so that most people, not just journalists, can go almost through the entire book on their own without any help. It is designed for non-IT specialists, so anybody who has basic knowledge of using a computer in a non-technical sense is able to benefit from it – if you can read email, browse the web and use a word processor, that is all that is required. We are also constantly collecting all kinds of feedback from people who are using the book and currently we have the new version up, which includes all that feedback and some little changes to make it more usable. The main idea is that you can sit down with your laptop, internet connection, USB drive and the book, and just teach yourself email encryption, file encryption, installing a secure operating system on your laptop, using detailed system for USB drives, using secure chats and also get a general understanding of what info-security means and how you need to deal with it. There will be a few bits of software to install, but we described that in detail – 'click there', 'click there' and 'click

there'. You do not have to go through all of it – if you just want to do email encryption; you just go forward and check that. You can take what you want out of it.

You also write posts on your blog Gendo. What are those mainly about and where do you get ideas for them?

A lot of what I write is about my other work, which is technology policy. So I advise governments and large corporations on fundamental choices that they make, with respect to information technology. That means that this is about what kind of software do you buy long-term, how it is compatible with other systems, can you secure it, how can you organize your projects, things like that. So my blog posts tend to be fairly specialist and abstract, which means that some of them are really for a small news audience. But I always try to make it accessible for wider audience; sometimes that is easy, sometimes it is not. I also post all sorts of interviews and clips from television. I also try to question the way things are done now and give some alternatives about how you can do them differently.

What do you think about the European and worldwide reaction to Snowden's revelations?

I think it has been way too understated. I do not think most people fully comprehend the implications of this level of spying; what it means when your elected representatives have their phones taped all the time, so their position for negotiation on your behalf in relationship with a foreign power is completely destroyed. It touches the heart of your democracy, of your ability to be a country. I do not think people generally understand the implications of Snowden's revelations; they tend to have an individualistic perspective on it. They say "I have nothing to hide," as if this is only about them individually! The real problem is not at an individual level, but more on a societal level, ecosystem typed, structurally created, where nobody can keep secrets from one super powerful entity. And that powerful entity can do literally anything they want. They become unlimited in their ability to manipulate processes, other people and society.

What do you think is the reason for this individualistic perspective?

Part of it is surely a consequence of the failed education system; where we do not explain this context to children. The other part is the fact, that most of the media is not talking about it in this way. It should be about talking of this problem as a society-ecosystem

problem, instead of "*Oh they might know what I did yesterday*". Yeah, who cares? That is not relevant. This is also not about the personality of whistleblowers, although I wish all of them truly well and I'm happy to make some effort in helping them. In the end what happens to the whistleblowers is not relevant to the bigger societal question. I do think we should try and help the whistleblowers as much as we can, but to endlessly theorize their fate, it does not really help anything. I think we best honour the whistleblowers by using what they've shown us and doing something with it.

How can we do that?

Even small actions can contribute, like if more and more people start encrypting their emails. If everybody encrypts their email, then the people who need it most are not going to stand out. With encrypting your email – aside from having your privacy, which is your right anyway – you are also helping the next whistleblower, journalist, civil rights lawyer who operates in a difficult country, because their encrypted emails are now going to be part of a much bigger pile that is easier to hide.

In an interview for KeiserReport you also talked about the spying of NSA and said that the solution is to increase the cost of spying. Could you explain that?

The spying for NSA and other similar organisations right now is very cheap, because most people do not do anything to prevent it. They can have a lot of information about us without spending very much money on that process – they spend about a tenth of the dollar, something like that, for an internet user per day. By encrypting all your communications and using secret platforms you can increase that to much higher amount. You can increase it by something like a fracture of a million. If a lot of people do that, then the NSA can no longer – at their current budget – surveil the entire planet. They will start to make choices; will they go after the few people that are actually dangerous for some reason, like terrorists, or will they go after journalists? If enough of us just up the level, then they are going to burn resources on a limited number of people and run out of money. Again this is something that every individual person can do and make their contribution to protecting our (and theirs) privacy. Of course the NSA and other agencies' budgets are large, but they are not unlimited, right? We have the technology; we just have to have the will to do it.

How to bring the awareness of how important is information security closer to people? Most of them think it's very complicated and hard.

Well of course the technology is complex, but the reason why most of the people are not willing to try and understand it, is because they do not find it important. The general awareness of the people needs to be changed. There is a foreign government spying on your personal privacy, on the secrets of the company you may work for and therefore damaging that company – endangering your job –, they are spying on your elected representatives, making it harder for them to represent you in the world. You should not want that. It really is that simple. The Americans are not going stop with spying on their own, so we need to financially incentivise them. Stop buying some of their products, especially IT products – obviously –, stop buying Microsoft Windows, which is what we should be doing anyway because it is just way too expensive for what you get out of it. *(laughs)* If we can drop half of our software preferences as Europe from America, that is 60 billion Euros a year. Then you can be sure that some American lobbyists are going to be working very hard on our behalf in Washington to end the spying. It is very much a no-brainer, but it requires a political will to do it, which is the one thing that is lacking because of the US political pressure. It really comes down to the question of are we still a bunch of sovereign nations.

How do you compare the information security and spying in other countries – for example in China or Russia opposite to America?

We do not know a lot about it. It would be wonderful to have a Chinese Snowden and a Russian Snowden. We can safely assume that China uses a position as a manufacturing giant of the world to gain an intelligence advantage; it would be insane for them if they would not do it. Consequentially, that also means we have to question outsourcing everything to a country like China. We have to really think about what some of the fundamental consequences for our society are going to be long-term, if we cannot make anything ourselves anymore, if we just hand things over to a foreign country with whom we might not share all their values about how you organize your society.

How can Slovenian journalists secure themselves more?

Because Slovenia is a small country where most people know each other, I think Slovenian journalists should form little groups and get together. You should teach yourselves and each

other with the help of local technical people, who are surely willing to help, and just start with the basics. Start encrypting email, chats and files on USB drives – things like that. When you become a little more comfortable with it and you have practiced it a couple of weeks, move on to advanced methods which are a bit harder, but also a lot more secure, and just see how far you can go and become used to using those kinds of tools. So when the time comes, when you are actually going to need them for a really serious story, you are already proficient and practiced, and you can also explain that to your source. At some point there are going to be twenty or thirty journalists in Slovenia, who will publish their email encryption key on their website or on their business card, and will be known for being capable of encryption and securing the data they collect, because they have written a piece about it, or gave an interview, or did some work with the hacker space. You can bet that when an interesting source appears, he is going to go to one of those journalists. So in which group do you want to be?