“How safe are we really?” was the question posed at TU Delft’s 172th Dies Natalis celebration. New technologies offer opportunities, but they also pose threats. This is certainly true with regard to internet safety, Cyber-Security Professor Jan van den Berg (EEMC/TPM) tells us. “The days of a happy-go-lucky attitude are in the past.”
‘We have built a highly complex society in which we no longer know exactly what is going on’

LAST YEAR WAS AN ACTIVE YEAR FOR LESS PLEASANT INTERNET ACTIVITIES. EXAMPLES INCLUDE THE HACKING OF KPN, THE CONAKRY BREAK-INS AND THE NSA REVELATIONS. IS IT JUST SELECTIVE OBSERVATION, OR ARE MORE INCIDENTS OCCURRING ON THE INTERNET EACH YEAR?

“I think that more is going on, and I don’t think that it’s going to stop. In the late 1990s, nobody was talking about cyber-security. At that time, we were only talking about information security. It was all about information. Cyberspace as we know it today had not yet been created. In the space of fifteen years, we have made ourselves completely dependent on IT. We have made a world in which three billion people are permanently connected to each other and in which we use the internet for all kinds of activities with each other. In addition to exchanging information, which was how it all started, they can conduct financial transactions, find friends and, in some cases, partners. Companies work with them. You name it. Everything that we do in reality, we have also placed in the virtual world, which has made it a world with real effects, where the same things happen that take place in the ordinary world: theft, deception, robberies, bullying – you name it. Don’t forget: real criminal organisations are behind this: the internet mafia and dark market. Truly shocking accounts have been written of these practices.”

CAN YOU NAME AN EXAMPLE?

“Well, people who are paid to do these things. You can get a botnet to carry out a DDoS attack. For a certain price you can rent these for a few hours or a few days. You are even told how to carry out the financial transaction in such a way that you cannot be traced. You can do this via a ransomware server, where you can then purchase zero-days.”

SO ARE THERE A BUNCH OF SMART GUYS FIGURING ALL OF THIS OUT FOR DUBIOUS BUSINESSES?

“Yes. They are paid to do this. It is a very smart network of people who do not know each other. This obviously involves complex relationships of trust. They communicate with each other anonymously, but only once you order something and pay to have it delivered, this obviously creates a network you can work with. In the real-world mafia, the boss is also unknown to the people on the ground. I’m no expert, but I know that’s approximately how it works. Our dependence on IT is only increasing, and my greatest fear is that the major infrastructures will become increasingly tied to each other: electricity, energy, ports, water works and industries. We have built a highly complex society in which we no longer know exactly what is going on.”

IT IS APPARENTLY ALSO NOT SUCH A GOOD IDEA TO CONNECT ALLO THE ELECTRONICS IN YOUR HOME TO THE INTERNET, INCLUDING YOUR THERMOSTAT, YOUR SECURITY SYSTEM AND YOUR REFRIGERATOR?

“Yes. Vulnerability is increasing, and problems of responsibility are emerging. I recently paid a visit to an internet service provider. They tell us, ‘In the past, our responsibility extended to the first box in the home’. That was connected to a TV and maybe a laptop. Now there are likely to be 10–15 appliances connected to it. Any of those systems could become infected with malware and start to behave inappropriately. The provider would actually prefer to disconnect that one device, but the privacy watchdogs will not allow this. This is an interesting dilemma, and we have not actually determined what responsibilities lie with the user. The user says, ‘Yeah, right. Security. I bought a PC. It should be able to keep itself free of viruses. I’m not going to pay for that. Why not, actually?’ We are also required to have our cars inspected periodically. Everyone now considers it perfectly normal to contribute to the overall safety of the highways. This realisation has yet to dawn within the digital realm. Farmers have to clean their ditches every autumn in order to maintain proper water management for the common good.”

WHAT TYPE OF USER RESPONSIBILITY ARE YOU TALKING ABOUT?

“The general idea is that, next to highways, water, air and space, the internet is a new domain in which all kinds of traffic rules apply. This is already quite different from the former happy-go-lucky attitude. It would mean that software or the use of devices could be subject to responsibilities. For example, annual PC inspections could become required. Why not?”

IN YOUR INAUGURAL ADDRESS, YOU SAID THAT THERE IS NO SUCH THING AS JOHN SECURITY, AND THAT IT IS UP TO POLITICIANS TO DECIDE ACCEPTABLE LEVELS OF RISK. BUT WHAT DO POLITICIANS KNOW ABOUT THIS?

“If you formulate the problem in that way, it’s difficult to solve, because it’s too big. My proposal would be to chart internet dependency within each domain and establish risk levels based on this information.”

WHICH DOMAINS ARE YOU THINKING OF?

“Through its ‘top-sector policy’, the Netherlands has defined nine top sectors. They are important to the country, and they have all been made dependent on information technology. We could start there. Chart the IT risks for these sectors and use this information to develop policy and design measures. This could serve a preventative as well as a detective purpose – the latter being my own discipline. I would like for us to be much more transparent about what happens on the internet. In effect, we should do what the NSA is doing, but with a clear, transparent objective.”

SHOULD WE ARRANGE A TYPE OF TRAFFIC CONTROL ROOM?

“We will do this with the other domains when the first plane took to the air and the first automobiles took to the roads. We suddenly had to start driving on the right. Hey! Can’t I drive wherever I like? I still remember when we had to start driving on the right. Hey! Can’t I drive

Last year was an active year for less pleasant internet activities. Examples include the hacking of KPN, the Conakry break-ins and the NSA revelations. Is it just selective observation, or are more incidents occurring on the internet each year?

“I think that more is going on, and I don’t think that it’s going to stop. In the late 1990s, nobody was talking about cyber-security. At that time, we were only talking about information security. It was all about information. Cyberspace as we know it today had not yet been created. In the space of fifteen years, we have made ourselves completely dependent on IT. We have made a world in which three billion people are permanently connected to each other and in which we use the internet for all kinds of activities with each other. In addition to exchanging information, which was how it all started, they can conduct financial transactions, find friends and, in some cases, partners. Companies work with them. You name it. Everything that we do in reality, we have also placed in the virtual world, which has made it a world with real effects, where the same things happen that take place in the ordinary world: theft, deception, robberies, bullying – you name it. Don’t forget: real criminal organisations are behind this: the internet mafia and dark markets. Truly shocking accounts have been written of these practices.”

Can you name an example?

“Well, people who are paid to do these things. You can get a botnet to carry out a DDoS attack. For a certain price you can rent these for a few hours or a few days. You are even told how to carry out the financial transaction in such a way that you cannot be traced. You can do this via an anonymous server, where you can then purchase zero-days.”

So are there a bunch of smart guys figuring all of this out for dubious businesses?

“Yes. They are paid to do this. It is a very smart network of people who do not know each other. This obviously involves complex relationships of trust. They communicate with each other anonymously, but only once you order something and pay to have it delivered, this obviously creates a network you can work with. In the real-world mafia, the boss is also unknown to the people on the ground. I’m no expert, but I know that’s approximately how it works. Our dependence on IT is only increasing, and my greatest fear is that the major infrastructures will become increasingly tied to each other: electricity, energy, ports, water works and industries. We have built a highly complex society in which we no longer know exactly what is going on.”

It is apparently also not such a good idea to connect all of the electronics in your home to the internet, including your thermostat, your security system and your refrigerator?

“Yes. Vulnerability is increasing, and problems of responsibility are emerging. I recently paid a visit to an internet service provider. They tell us, ‘In the past, our responsibility extended to the first box in the home’. That was connected to a TV and maybe a laptop. Now there are likely to be 10–15 appliances connected to it. Any of those systems could become infected with malware and start to behave inappropriately. The provider would actually prefer to disconnect that one device, but the privacy watchdogs will not allow this. This is an interesting dilemma, and we have not actually determined what responsibilities lie with the user. The user says, ‘Yeah, right. Security. I bought a PC. It should be able to keep itself free of viruses. I’m not going to pay for that. Why not, actually?’ We are also required to have our cars inspected periodically. Everyone now considers it perfectly normal to contribute to the overall safety of the highways. This realisation has yet to dawn within the digital realm. Farmers have to clean their ditches every autumn in order to maintain proper water management for the common good.”

What type of user responsibility are you talking about?

“The general idea is that, next to highways, water, air and space, the internet is a new domain in which all kinds of traffic rules apply. This is already quite different from the former happy-go-lucky attitude. It would mean that software or the use of devices could be subject to responsibilities. For example, annual PC inspections could become required. Why not?”

In your inaugural address, you said that there is no such thing as John security, and that it is up to politicians to decide acceptable levels of risk. But what do politicians know about this?

“If you formulate the problem in that way, it’s difficult to solve, because it’s too big. My proposal would be to chart internet dependency within each domain and establish risk levels based on this information.”

Which domains are you thinking of?

“Through its ‘top-sector policy’, the Netherlands has defined nine top sectors. They are important to the country, and they have all been made dependent on information technology. We could start there. Chart the IT risks for these sectors and use this information to develop policy and design measures. This could serve a preventative as well as a detective purpose – the latter being my own discipline. I would like for us to be much more transparent about what happens on the internet. In effect, we should do what the NSA is doing, but with a clear, transparent objective.”

Should we arrange a type of traffic control room?

“We will do this with the other domains when the first plane took to the air and the first automobiles took to the roads. We suddenly had to start driving on the right. Hey! Can’t I drive wherever I like? I still remember when we had to start driving on the right. Hey! Can’t I drive...”