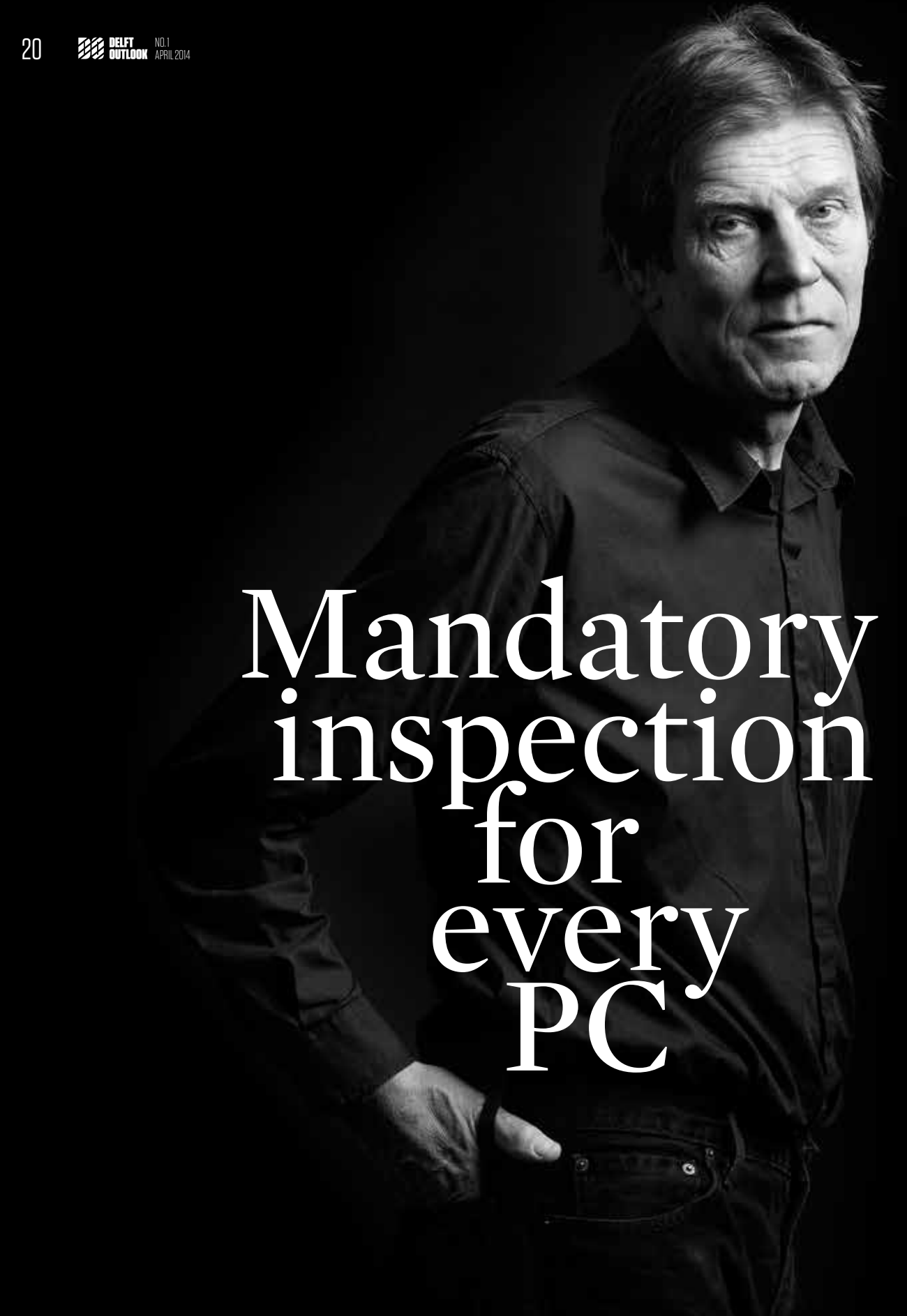
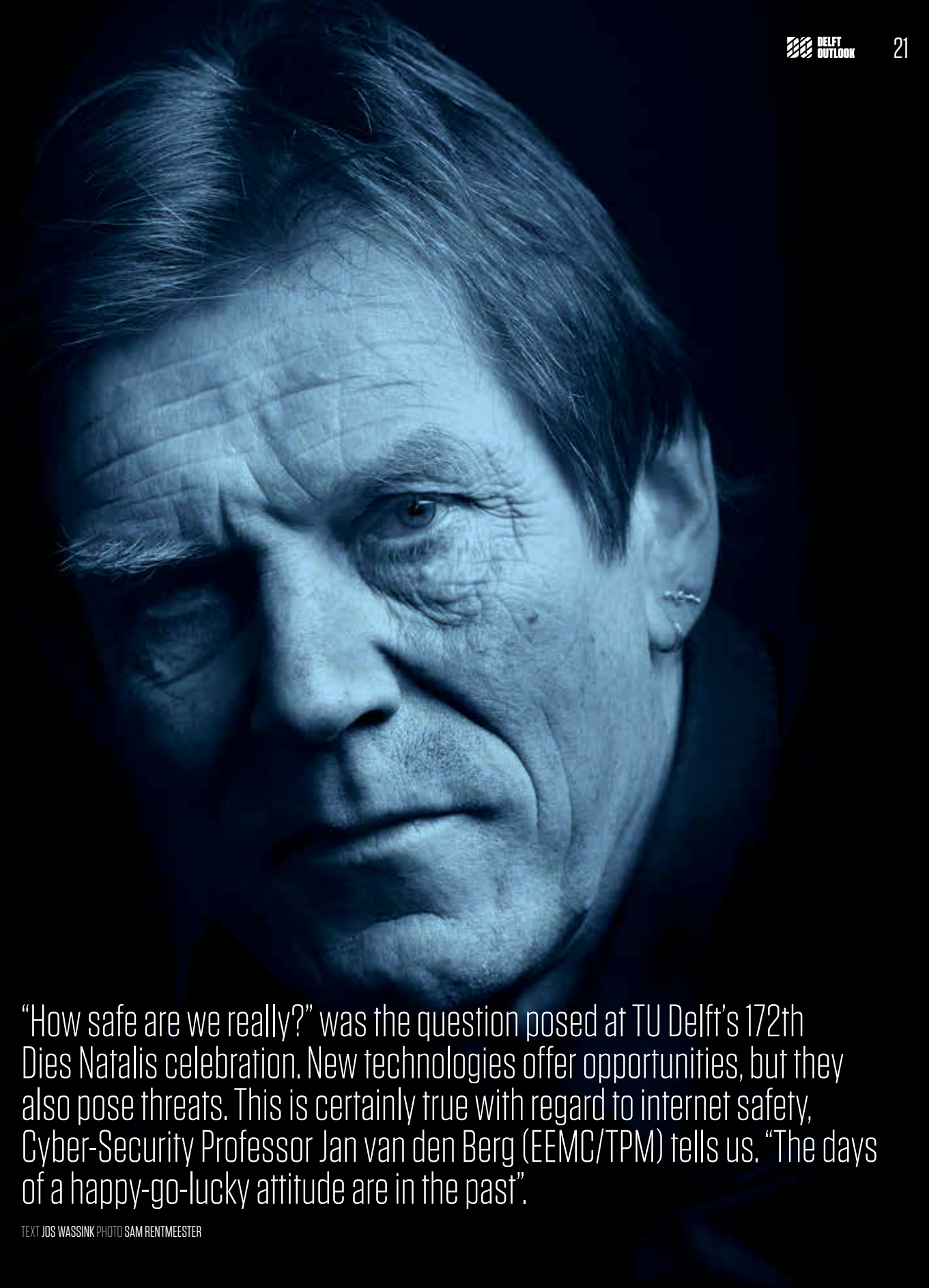




Mandatory inspection for every PC



“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”.

TEXT JOS WASSINK PHOTO SAM RENTMEESTER

YOU GRADUATED IN 1977, LONG BEFORE THE RISE OF THE INTERNET. HOW DID YOU END UP IN THE FIELD OF INTERNET SAFETY?

“For me, the breakthrough came in the late 1990s, with the advent of Web 2.0. We already had Web 1.0, which emerged in the mid-1990s. That was passive. Although there were websites, individual users – lay people – had no influence, because it was too complicated. With Web 2.0, however, it became very easy for users to post content to the web themselves. Companies started to engage in e-commerce with dynamic content on their own websites. Social network sites emerged rapidly as well. End users began to notice that they could do something on the web. Sometime in the past 14 years, since about 2000, criminal activity started to creep in.”

‘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, DDOS ATTACKS 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 they engage in 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 botnetⁱ to carry out a DDoSⁱⁱ 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 that via an anonymous server, where you can then purchase zero-daysⁱⁱⁱ.”

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

“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 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, highways, 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.

“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, a PC 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^{iv} 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 where the responsibilities lie. 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 could 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 100% 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^v. 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 precise in monitoring what happens on the internet. In effect, we should be doing what the NSA is doing, but with a clear, transparent objective.”

SHOULD WE ARRANGE A TYPE OF TRAFFIC-CONTROL ROOM?

“Yes, actually. A cyber-security control centre should ultimately be able to function in such a way that it would have an overview of what is going on. What the NCSC (National Cyber-Security Centre) currently does is to present an annual overview of cyber-security. If I ask them, ‘What is the situation in cyberspace now?’, they wouldn’t have any answers for me. At most, they could say something about the financial sector. In this sector companies like Fox-IT monitor all financial transactions in real time. They try to single out unusual patterns. If they have a feeling that something is not right – in most cases, they do not know exactly what is wrong; that would require domain-specific knowledge – they alert the bank and advise them to investigate. The banking world is perhaps the first to take an active approach to ‘cyber situation awareness’, as it is called.

DO YOU THINK THAT ANYONE WOULD SUPPORT SUCH A MONITORING PROGRAMME IN THE WAKE OF THE NSA SCANDAL?

“When I heard about it, I thought, ‘The most serious consequence will be mistrust of governments regarding this subject’. We all trust the government when it is transparent. This should be just as applicable to the internet as it is to the actions of the police. We should figure out how to develop a level of transparency for the new domains. But if we aren’t monitoring what is happening on the internet, we’re fighting a losing battle in terms of cyber-crime. We will always be behind the times. I don’t think there’s any way around it. If we want to have this digital world, and we all do, we must accept the consequences. If we wish to operate safely in this world, we must be able to monitor it. This is my message: We must learn how to cope with the new fifth domain. We did 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 wearing safety belts. You should have heard all the protests! Or wearing a helmet. Now it’s just second nature.”

ⁱ botnet - a collection of software robots (hacked computers) or bots, which operate automatically and independently.

ⁱⁱ DDoS - distributed denial of service - an attack in which a server becomes inaccessible when many hacked computers try to contact it at the same time.

ⁱⁱⁱ zero days - attacks that exploit vulnerabilities in operating systems that are not yet known and against which even the most current virus scanners thus offer no protection.

^{iv} malware - collective term for malignant and/or harmful software

^v The top sectors are as follows: Agriculture & Food; Chemicals; Creative Industries; Energy; High-tech; Logistics; Life Sciences & Health; Horticulture, and Water.

CV
Jan van den Berg (1951) studied mathematics and physics at TU Delft and was active in the national student movement. He graduated in 1977 and went to teach (mathematics, physics and IT) at schools of higher professional education. During this period he also spent two years teaching in Mozambique. In 1989, he joined the Econometric Institute at Erasmus University Rotterdam, teaching and conducting research in the areas of data analysis, complex systems, economics (and econometrics) and information security. He completed his PhD in 1996. Ten years later, he joined TU Delft, where he was appointed Professor of Cyber-Security in the Faculty of Electrical Engineering, Mathematics and Computer Science and the Faculty of Technology, Policy and Management in July 2013. On 13 December 2013, he held his inaugural address, which included a simulated hack.