Prof.dr. Bibi van den Berg and Prof.dr. Aske Plaat

Safe connections: Security in the information society

Universiteit Leiden
The Netherlands

Safe connections:
Security in the information society

Dies lecture given by

Prof.dr. Bibi van den Berg

Professor Cybersecurity Governance

and

prof.dr. Aske Plaat

Professor of Data Science

during the 445th Dies Natalis

on Friday 7 February 2020 in the Pieterskerk

Universiteit
Leiden
The Netherlands

Plaat: Esteemed Rector Magnificus, thank you for your introduction.

Ladies and gentlemen,

The Dutch language recently acquired a new word: *Citrixfile* or Citrix traffic jam. This is what happens when people go to their offices en masse on a Monday morning because the software that they need to log to work from home has been switched off as a preventive measure. On Monday last week Twitter was full of tweets about how much fun it was to all be sitting together in a traffic jam. It's a good thing that we are able to put things in perspective because it's been one thing after the other: first the ransomware attack on Maastricht University at Christmas and now this.

The subject of this Dies lecture, as you have gathered, is cybersecurity. Of course, it's great when the subject of the Dies lecture is so topical, but this year it's a bit too much of a good thing.

Cybersecurity has become a hot topic in the last few years. Until recently, many of us could file it away as 'not my problem', but thanks to the vulnerabilities of Citrix and more frequent ransomware attacks on businesses, hospitals and universities, cybersecurity has become a real-life issue that affects our private and working lives. Cybersecurity is one of the major challenges of today, and will only become more urgent in the near future.

From the industrial to the information society

Today's world is increasingly governed by technology. Our hunger for knowledge and our thirst for understanding are what drive our prosperity. After the industrial revolution, there has been an information revolution; our society has become an information society and an increasing proportion of the things we do every day are made possible or are supported by digital, networked technology.

Computers control lifts, central heating and even our pacemakers; they make school timetables, determine our choice of films and decide which adverts and news reports we see; they help us communicate with our friends and choose our partners, and they help us track diseases and develop medicines. Matters of life and death are increasingly decided by self-reasoning systems.

In the 30 years since the internet became a public domain, much of our modern life has been influenced by the online world. This 'cyberisation' is happening because, whenever we have the choice, we consistently opt for the digital alternative as it's easier, better or cheaper, and thus contributes to our economic growth, prosperity and happiness.

At times we look back with some nostalgia at an earlier, more peaceful time when we weren't constantly looking at our phones, and when people really did have time for one another. And then we write a nice blogpost about it that will hopefully get a lot of likes. And anyway, if we **are** spending too much time on our phones, we can always install an app to wean us off it, can't we?

Whatever we may think about it, our society is filled with technology. But what happens when that technology stops working, or is misused by criminals?

A feature of security is that we only become aware of how important it is if it is under threat. In the physical world we can perceive danger with our senses. This is more difficult in the digital world. We can see and feel fire, for instance, but we can't see or feel bytes flying through the air. In cyberspace we often have no idea when our security is endangered.

What is cybersecurity?

Cybersecurity is about making information, networks and systems safe and keeping them safe. System failures and attacks from outside – and their consequences – need to be kept to

a minimum. Cybersecurity is a relatively new phenomenon; it only made its appearance after the Second World War, and has really taken off since the digitalisation of society. Unfortunately, this development has not gone unnoticed by people with less noble intentions. Cyberattacks are a fairly common occurrence and there is a kind of arms race between the smartest minds out there; it's big business. The impact of cyberattacks in 2019 was estimated to be between two and four trillion dollars (according to Juniper Research and Cyber Security Ventures respectively). Those are big sums, and this means an estimated loss of between 2 and 4% of the gross world product. The impact on the Netherlands in 2017 was estimated by Deloitte to be 10 billion euros, ten times as much as the impact of 'ordinary' crime. The consequences of cybercrime are clearly very considerable. When a Dutch university is affected, and when that's just before an exam period, it all feels a lot closer to home and the people at our own ICT Shared Service Centre have a very busy Christmas. And if you are then unable to work from home because Citrix has been disconnected, that's when you realise that the issue of security has penetrated the internet right to the very core.

But cybersecurity incidents are also becoming more common in our private lives. We understand how dependent we as a society have become on network technology when the pin machine at the supermarket stops working on Whit Sunday, when democratic elections are manipulated by a foreign power or when the alarm number 112 stops working. Cybersecurity then literally becomes a matter of life and death.

A multidisciplinary issue

Cybersecurity combines two fields: information technology and security science, the specialist fields of my colleague Van den Berg and myself. In a technical sense cybersecurity is about confidentiality, integrity and availability, in short CIA.

But cybersecurity is more than just a technical issue. It calls for an approach that offers both technical solutions and insight into social, legal, organisational and ethical aspects of our internet use. Only when we look at the problem from a multidisciplinary perspective do we really appreciate the full extent of it. This makes it important to look not only at the security of systems, networks and data, but also at the role of people, organisations, politics, government and law. This multidisciplinary approach is key to our Executive Master's in Cyber Security, in which our two institutes, the Leiden Institute of Advanced Computer Science and the Institute of Security and Global Affairs collaborate with Delft University of Technology and The Hague University of Applied Sciences.

Technical aspects of cybersecurity

If you want to understand the present, it's often helpful to take a look at the past. That also applies to cybersecurity, because secrets are as old as the human race, and secret codes or cryptography is as old as writing itself. The oldest known secret code comes from Egypt and dates from 1900 years before the start of our era. We also know that the Ancient Greeks and people from India and Persia used cryptography to keep secret information secure. They used such methods as transposition and substitution. However, this old form of technology did go wrong at times. Keys were copied, messages were intercepted, codes were broken and safes were cracked open.

The advent of the computer allowed cryptographic principles to really take off, and with the arrival of what are known as public-key methods we have gained codes that today's computers cannot crack. (And people are already researching post-quantum cryptography in preparation for if and when quantum computers are able to crack today's methods.)

The mathematics behind encryption methods is constantly being perfected, and the possibilities of fixing software errors are always improving, something that we in Leiden are contributing to. With modern technology, we can now store and send much more data and we can also make it more secure.

So why is cybersecurity one of the major issues of our information society? Why does so much go wrong in practice, and can we do anything about this?

This is the question we will be addressing here today, and my colleague Bibi van den Berg will tell you more.

Van den Berg: The role of technology is indeed increasing in modern life. We connect everything – and I do mean everything – to the internet. Aske Plaat has already mentioned a range of activities that we currently undertake in and through cyberspace, from making payments and sharing personal information through social media to purchasing products and reading books. At a higher societal level, we also see that physical reality and cyberspace are becoming increasingly intertwined. Critical infrastructures are so-called because they are critical to the functioning of society. If these infrastructures go down, that can result in enormous disruption. These days, more and more critical infrastructures are connected to the internet. Just think of how hospitals have digitised patient data in patient files, and how to an increasing extent their medical equipment, or sometimes even the whole operating theatre, is connected to the internet. And then there's Schiphol Airport, where the procedures, from checking in your suitcase and processing your ticket to the logistics of baggage handling and customs control, all rely on digital, networked technology. Rijkswaterstaat, part of the Dutch Ministry of Infrastructure and Water Management, is another case in point; in recent years Rijkswaterstaat has connected all the country's bridges, flood defences and waterworks to the internet, so they can be operated remotely. Under the motto of efficiency, almost all of the critical infrastructure of the Netherlands, from healthcare to traffic, and from finances to energy, has been connected to cyberspace.

But if Rijkswaterstaat's dike guard can open or close a barrier remotely because this is connected to cyberspace, so too can a hacker. And then a matter of digital vulnerability suddenly has the potential to result in physical damage (and possibly even death) in the offline world. This is the biggest concern facing governments in the area of cybersecurity. And take note: it is not only a hacker who can cause a flood, but also a system or human error. If an incident does occur, it doesn't really matter whether the damage was caused by a deliberate attack or by the failure of the systems on which we have come to depend. The issue is that cyberspace, as the backbone of so many of the systems on which we depend, has itself also become a critical infrastructure.

Four risk areas

Rapid advances in digitalisation have led to risks that we are only now, slowly but surely, starting to realise. How do we address these risks? And what should we be most concerned about? We will discuss four themes.

The first theme is how to protect critical infrastructures. These often run on large, infrastructural technology that has been specially designed for a specific complex, such as a complete factory. These systems were often built in the 1960s and 1970s, and were never designed with internet connectivity in mind. Now they are connected to cyberspace, one concern is that they have all kinds of inherent vulnerabilities that evildoers can exploit. These crucial technologies need to be made secure, and retroactively.

The second theme is cybercrime. Pretty soon after the advent of the internet, criminals discovered that cyberspace was well-suited to criminal activities. The anonymity and borderless nature of cyberspace enables criminals to reach a larger group of potential victims, with less likelihood of getting caught. Besides classic forms of crime that we all know from the offline world, such as fraud and the distribution of material showing child sexual abuse, with the advent of cyberspace, all kinds of new crimes have to be added to the Penal Code. Hacking and Distributed Denial of Service (DDOS) are just two examples. Before the existence of networked computers, these crimes did not exist – but unfortunately they do now.

The third theme relates to disinformation and fake news. After the presidential elections in the US in 2016 and the Brexit referendum that same year, it became apparent that we all need to be concerned not only about the integrity of data in cyberspace, but also about the manipulation of information. These two events demonstrated that state players increasingly use cyberspace to interfere in other countries. Concerns about democratic processes being influenced or undermined, or even freedom of information, are increasing hand over fist. The rise of Artificial Intelligence, and with this new technological possibilities such as 'deepfakes' also fall within this theme: it is becoming increasingly difficult to determine whether information is authentic, and whether or not it is true.

And finally the fourth theme relates to concerns about the rise of the Internet of Things. If in the near future we are going to add internet connectivity to more and more everyday objects, this will have major advantages (efficiency again, and ease of use) but unavoidable risks too. We link our bicycles, our coffee makers, our children's toys, our televisions and vacuum cleaners en masse to the internet. As a result, our privacy is under increasing pressure because more and more of our personal data is literally out in the public domain. And all these devices are access points for evildoers who are gaining a rapidly increasing 'attack surface'.

No major incidents

Meanwhile, digitalisation is advancing apace. Miraculously, there have been no truly disruptive incidents. There are occasional hacks, like the Sony hack in 2014, where data from employees at Sony Pictures was leaked and large parts of the company's systems were wiped out following the release of a satirical film about North Korean leader Kim Jong-un. And there was last month's ransomware attack on Maastricht University that we just mentioned, which shut down the whole university for several weeks. In the odd case, a discussion arises as to when a malware attack counts as a 'digital weapon', making it an 'act of war' (or not). One example is the Stuxnet incident in 2010, when malware caused damage to an Iranian nuclear facility. And sometimes attacks by state players go wrong and have a cascade effect worldwide. This was the case, for example, with the NotPetya attack in 2017. This was an attack by the Russians on Ukraine, but it spread like wildfire over the whole world. Large concerns such as the Maersk Shipping Company were paralysed and the damage ran up to 10 billion US dollars. On occasions we are shocked by an enormous data leak, like that of the Marriott hotel chain in 2017, when the personal data of around 500 million people was stolen. But on the whole, experts continue to say that the risks are great and governments continue to be concerned but the world just keeps on turning. Even the Citrix traffic jam made little difference to that.

So how should we look at the cybersecurity issue? And above all: what can we do to make cyberspace secure and keep it that way?

Plaat: Yes, the world keeps on turning and yes there have been no major catastrophes, but cyberattacks nonetheless cost us around four trillion dollars a year. We hear about the risk of viruses, ransomware and data theft. One vulnerability is discovered after another, with such terrifying names as Heartbleed and Spectre. Criminals, too, are experts at social engineering and phishing mails are hard to distinguish from legitimate ones. In a recent test at a Dutch university, no fewer than 20% of the employees clicked on the link in a fake phishing email.[1]

The question posed by Bibi van den Berg is therefore intriguing: if all computers can be tapped and attacked, and if people can be manipulated, why have we heard so little so far about successful attacks, and is our critical infrastructure still secure? Have there not been any attacks? To answer these questions, let us look at three reasons why there have been

1 https://www.erasmusmagazine.nl/2019/01/24/een-op-de-vijf-medewerkers-trapte-in-mail-virus/

no major cybersecurity incidents so far: the technology, the counterforces in society, and the knowledge required.

Segmented networks
The first reason why disruptive incidents have not occurred is a technical one. In practice, when one system fails this rarely causes a chain reaction because most systems are heterogeneous, and are only loosely connected with one another. Computers can communicate with one another (thanks to the internet) but company--critical systems are often not so closely linked that if one fails, the other does too. Let's take a power plant as an example, with its diverse generators and distribution system. The generator systems and the distribution system have been designed so that they can work independently of one another, and between these systems there is often also a human operator who can intervene. If a generator fails, the rest of the plant can carry on working.

A flu epidemic is a good analogy here. An illness will spread less quickly in a population (1) if the resistance of individuals to the disease is greater, (2) if these individuals have less contact with one another and (3) if the population is more heterogeneous. Diversity increases the population's resistance, and limits the spread of the disease, as research on complex networks has taught us. In the financial markets we have seen time and again that blindly replacing human intermediaries in a homogeneous environment can cause a chain reaction, This is something we need to learn from when developing our digital networked systems.

System diversity, such as a mix of different versions of Windows, Linux and Mac, is a good example: it means that if one system fails this does not cause all the other connected systems to fail. When designing systems, we have to resist the temptation to make everything the same and to connect everything without an intermediary or an intelligent firewall, even if it is more efficient and simpler. Instead, we should base our designs on a multiplicity of loose systems, we should segment access rights and we should use intermediaries or interfaces. Diversity may make systems less efficient, but it also makes them a lot more robust.

Response from society
The second reason why we are seeing few large-scale cyber disasters is that governments and other bodies are concerned about these issues and take appropriate measures. And that helps. On the whole, our critical infrastructure is more secure than that of individuals or the small and medium business sector. In the Netherlands we have the National Cyber Security Centre, people listen reasonably well to the advice of the Cyber Security Council (of which Bibi van den Berg is a member) and there is the national Cyber Security Agenda. Government, energy companies, the financial sector and large technology companies are aware of their societal role and the consequences of reputational damage, and they devote a lot of time and energy to making their systems secure, employing experts who are familiar with the latest developments.

Developments in the area of cybersecurity are very fast, and attackers and defenders are applying artificial intelligence to influence behaviour, and Bibi van den Berg has already mentioned deepfakes. Artificial intelligence can also be used to secure systems, for example self-learning firewalls that are better able to protect networks. From the viewpoint of cybersecurity, it is therefore important that we intensify our research on artificial intelligence. Having said that, we were very happy to hear the announcement at the recent Dies celebrations in Delft that the universities and medical centres that are part of the Leiden-Delft-Erasmus alliance will be collaborating on education and research in and with artificial intelligence.

Technical knowledge
The third reason why there have been no large-scale incidents so far is that cyberattacks require a certain level of technical knowledge, although it is becoming increasingly easy to buy

malware and exploit kits. If criminals or terrorists are set on achieving the most impact with the least effort, the obvious choice can be to ignore digital options because of the technical knowledge needed. Knowledge can therefore act as a barrier for large-scale disruptive incidents.

Unfortunately, not all disruptive incidents call for technical knowledge because fake news and disinformation can also be highly disruptive, as we have seen with the outcome of the Brexit referendum and the US elections. Anyone can send fake messages out into the world through social media and, as long as they know what they are doing, the power of the network will almost automatically ensure that the messages reaches a large audience. Social media propaganda calls for social knowledge rather than technical knowledge.

Various groups at our university are doing research into propaganda in cyberspace. For instance, *nieuwscheckers.nl* factchecks news and social media, different groups are conducting research on legal, administrative and network aspects of propaganda and this year the second Multidisciplinary International Symposium on Disinformation in Open Online Media conference, or MISDOOM as it is known, is being held in Leiden. This kind of research is not a minute too soon.

The weakest link

Evildoers look for the most lucrative place to attack, and they look for the weakest link. Banks and financial institutions are traditionally well protected, and the same applies for their cybersecurity. It is not surprising then that cybercrime often focuses on sectors that are less well protected. That often means private individuals, although there is less and less to be gained from us. For a cybercriminal it is more attractive to focus on sectors where the spoils are greater, such as the small and medium business sector, hospitals and, as we have seen recently, universities.

The foregoing reveals the considerations of evildoers when they want to launch an attack in or through cyberspace. First, it is easier and more effective to use cyber propaganda to disrupt society than to try to shut down well-secured power plants. And second, cybercrime is more lucrative when targeting poorly secured companies, universities and individuals than trying to enter a well-secured bank.

So what can we do with this knowledge? As a university, it is our role to expand knowledge and to foster the societal debate. If we are all the target of propaganda and cybercrime, we as a society have a task ahead of us. Cybersecurity has to be an integral part of digital skills education. If we want to understand how the digital world works, issues like computational thinking and digital resilience must be considered to be essential 21st-century skills. Universities have been advocating this for years, and the government now also recognises its role in the digitalisation agenda for primary and secondary schools. Will this be enough? I would say that there is still a long way to go with modernising school and university curricula. The LDE alliance for AI is a step in the right direction, and I welcome it wholeheartedly. Computational thinking is currently still a single, separate subject, but soon this way of thinking will become an integral part of many subjects and curricula.

Besides digital skills, there is of course a great need for specialised programmes in the area of digitalisation, artificial intelligence and cybersecurity. We mentioned earlier our own Executive Master's in Cyber Security as an excellent example of such programmes.

Your own digital resilience

We have seen how cybercrime is becoming a problem for individuals and small companies, which makes it extremely necessary to increase our awareness and knowledge. That is why I would like to end my part of this lecture with a brief lesson, especially for you, on how to increase your digital resilience. Here we go…

If you receive emails from your bank (or from your Rector) asking you to click on a link, don't do it. If you see a fantastic offer on eBay or get a text asking you to transfer money, don't do it. If you read a message on Instagram, Twitter or Facebook that confirms exactly what you think, don't get stuck in your own bubble: be critical! Don't connect USB sticks from people you don't know to your computer (and preferably not those of people you do know. Who knows what they have used their USB sticks for?). Only surf through secure connections: you know, that lock icon in the browser. Switch your firewall on, use a virus scanner and if you want to use wifi in the train or an internet café, use a Virtual Private Network (or VPN), particularly if you want to check your bank balance (if you don't know how to do that, ask someone you trust to help. You'd be surprised how many good friends you make along the way). Install security updates on your computer and phone as soon as they appear. Use two-factor authentication for all your important accounts, and if that's not possible, at least try to use different passwords for different accounts. Use cloud services from reputable IT companies for backups and collaborative work. (If a company's reputation is at stake, there's a bigger chance that their services will be in good order.) And, another thing, don't take any photos that you wouldn't like your neighbours to see. Consider using several different banks, different email addresses and, if you really want to be sure, different telephones. But if you have got to that point, you most likely work in security – on whichever side that might be…

We have looked at a few technical aspects that may explain why cybercrime is such a common occurrence, why there are so many phishing mails and fake news reports, and also why we have experienced few problems with our critical infrastructure. Cybercrime and propaganda are problems that affect us all. We, and our democracy, have become the weakest link. We have to forge ahead with teaching digital skills to all, and we have to cherish diversity, even in the digital world, even if that is at the expense of efficiency.

And now I am curious to hear how Bibi van den Berg sees this from the perspective of government and legislation.

Van den Berg: More and better knowledge of the use of digital technologies can certainly play a part in ensuring that fewer end users fall victim to cybercrime, fake news and other risks in and from cyberspace. Anyone who uses the internet needs to have at least a limited understanding of how it works and the dangers it can bring. Just as we expect pedestrians to know the rules of the road and to take the safety of others and themselves into consideration as they navigate traffic, we can equally expect end users to have a basic set of skills to ensure that they use networked technologies safely. Digital skills have become essential in an era when the internet, as we stated earlier, supports our everyday activities or make those activities possible.

Digital skills alone are not enough

Having said that, I also appreciate the limitations of relying on digital skills. In the first place, the security risks through cyberspace are increasing every year. The chances of becoming a victim are also increasing because more criminal activity is taking place and new vulnerabilities are coming to light, all of which bring new types of problems. Altogether, this means that digital skills will not be enough. You can try to learn Aske Plaat's lessons in digital resilience by heart, and they will certainly be a help, but they are no guarantee for the future. Just when you have remembered to be wary of clicking on links, you will fall for a deepfake. And just when you have grasped that you shouldn't transfer money to someone with a sob story on a dating site, you will fall victim to WhatsApp fraud. Digital technologies are developing at breakneck speed, and the risks are also evolving at an equal rate. This means that although we can expect citizens and consumers to practise a certain level of 'basic hygiene' on the internet, we can't expect much more than that.

A role for government
So what can we expect? Is it the government's job to make cyberspace safe? In my view, the answer is an absolute YES. But, you can be sure that this is no easy task. I will discuss two reasons why it is not easy for the government to influence cybersecurity.

Transcending national borders
The first reason is because cyberspace transcends national borders. It spans the whole world. Every time you visit a simple website in your browser, you are crossing at least three national borders as if they didn't exist at all. The internet might not stop at the Dutch border, but the sovereignty and legal jurisdiction of the Dutch state does. If countries want to make cyberspace safer, they will have to work together at an international level. This will mean enormous challenges, for example regarding the question of which norms should apply in cyberspace, and how to resolve the tension between, for example, freedom of expression and privacy, or national security and freedom of information. Setting standards, creating norms or drawing up legislation on all kinds of areas is by no means a short order. Much more research is needed on how such standards, norms and frameworks come about, or how they should come about. At this university we are contributing to this research by studying norms for state conduct in cyberspace in The Hague Program for Cyber Norms.

Although developing standards and frameworks will be a slow process, we are making excellent progress, particularly in Europe, in the area of international collaboration on cybersecurity and privacy. The General Data Protection Act (GDPR) that entered into force in Europe in 2018 is an example of legislation that helps make cyberspace safer for consumers and citizens. After years of tinkering away, European countries, companies and interest groups have succeeded in enshrining in this act how companies and organisations doing business in Europe should handle the data and privacy of end users.

The 'Brussels effect'
Unintentionally, this one act has also had a global effect. We call it the 'Brussels effect'. As international internet concerns like Google, Microsoft and Facebook want to continue to operate in the European consumer market, they have had to adapt to the demands of the GDPR. And once they have done that for European consumers, these modifications also apply to consumers in other parts of the world. Facebook, for example, will not be offering two services – one for Europe and another for the rest of the world. That would be both costly and inefficient. Although the Act was intended to protect the rights of European citizens, its implementation has had the unintended effect of improving the protection of the privacy and data of the whole world. The Brussels effect shows that the regulatory power of the European Union can ensure greater internet security worldwide. But what is the potential scope of this effect? Could we make conscious use of it to increase cybersecurity worldwide by means of regulation? In the meantime, we in Europe have taken the first steps to harmonise legislation and regulations in the field of critical infrastructures. If we make further progress along this path, the Brussels effect could also improve the protection of airports, hospitals, energy networks and so on.

A role for government?
Having heard this appeal, you may be left wondering whether government should play a role in security in cyberspace At all. Isn't it something that companies can do themselves, without the need for government involvement? Shouldn't the private sector take the lead here?

The private sector does not do enough
The answer to this question is yes and no. Getting cybersecurity in order will take a lot of time, money and manpower, and when companies have invested that money, the result that they achieve is for there to be no incidents. And worse, if there are no incidents after all that money has been spent, it may relate to the time and energy that organisations

have put into getting their data protection in good order. But that isn't necessarily the case. Investments in cybersecurity as still often regarded by organisations as a 'nice to have', an extra bonus on top of the primary process. That IT has now become part of that primary process, and that in the event of an IT failure or an attack, the primary process can also be affected, is not yet clear enough to many organisations. It will take years of frequent incidents before cybersecurity becomes an intrinsic part of the DNA of healthy organisations. At the moment, there are still too many distractions that can stop organisations investing in their own cybersecurity.

For large technology companies, it is not very likely that they will take action to make cyberspace safer. Apple has been saying for years that protecting your and my privacy is its 'unique selling point', and the it takes a firm stand in discussions with intelligence and security services about breaking cryptographic codes to gain access to Apple devices, and about building in loopholes that could be used by those services. But last year we saw how Mark Zuckerberg was unable to answer the questions of the American Congress about Facebook's role in combatting fake news and disinformation. Facebook does not want to be identified as a media company, with all the responsibilities and guarantees that that entails when it comes to the quality of the information offered through its platform. Rather, it would prefer to maintain its claim that it is simply a conduit for information that end users share with one another. With this claim, Facebook positions itself as powerless in the face of a phenomenon on which, with a technical, normative and social code, it could exert much more influence. The profit that Facebook makes from everything we share continues to be a stronger incentive than the moral and social duty to make cyberspace a safer place.

Internet as a basic need

In other words: although it is logical to claim that the private sector should be responsible for better cybersecurity for us all, there are countless reasons why it is unlikely that we can expect any improvements from this direction in the short term. The government therefore needs to take a take a leading role in the area of cybersecurity. I have to admit that this reason is somewhat negative in nature.

There is a second reason why the government should take on that task. As we saw earlier, the government is responsible for protecting critical infrastructure: those facilities in society where a failure could lead to societal disruption. We also saw earlier that the internet itself has become a critical infrastructure: all the more reason to make sure that the risks in and of cyberspace are kept to a minimum.

If the internet has indeed become a basic need, then citizens and consumers should be able to feel confident that the internet they use is safe, even if they themselves have no knowledge whatsoever about how it works or what the risks are. You can compare it to food safety. When I go to the supermarket in the Netherlands, I should be able to assume that the food I buy there is safe and will not make me ill. The government plays an important role in safeguarding food safety: legal requirements and rules are in place for producers and there are regulating agencies and quality labels. The whole chain involved in the production, transport and sale of food products is subject to very strict food safety rules. The government plays a key role in this by making rules, seeing that they are adhered to and exercising control over the food branch.

We have yet to develop such an approach for cyberspace, for our internet use. Cyberspace is but a few decades old, so it is not so surprising that such a regulatory system does not yet exist. But, given the importance of cyberspace to our society, it seems clear to me that we have to work on a system analogous to the system that is in place for food safety or safety at work or product safety, to mention just a few examples. That government should play a key role in this is inevitable.

Plaat: If there is one thing that this lecture has shown you today, it is that cybersecurity is a complex, multi-layered issue. It is a prime example of an issue that brings together technical, legal, social, political and ethical issues. A multidisciplinary or even interdisciplinary approach is the only sensible way to address this complex issue. At this university, technical and behavioural scientists work together on research projects, like the research on fake news, in which they put flesh on the bones of this multidisciplinary issue. They also teach, for example in the Minor in Cybersecurity that will start next year. We are proud of the fact that our university in Leiden and The Hague offers a place where scientists from various disciplines can work together on implementing all these perspectives. Together, Bibi van den Berg and I wish the University on this 445th Dies a Happy Birthday tomorrow.

We have spoken.

Prof.Dr. Bibi van den Berg

Bibi van den Berg is full professor of Cybersecurity Governance at Leiden University, and the head of the Cybersecurity Governance research group at the Institute of Security and Global Affairs of this university.
She is also a member of the Dutch Cyber Security Council, a Council that advises the Dutch cabinet on how to improve cybersecurity in The Netherlands.

Prof.Dr. Aske Plaat

Aske Plaat is professor of artificial intelligence at Leiden University, where he is scientific director of the Leiden institute of advanced computer science (LIACS).
He is also co-founder of the Leiden Center of Data Science and has initiated the program for Society, Artificial Intelligence, and Life Science (SAILS), the university wide program for artificial intelligence.

Universiteit Leiden
The Netherlands