Digital threats in the 21st Century

Louis Einthoven, the first head of the Security Service was responsible for our agency's motto and shield. As Mr. Einthoven once observed, 'Only dead fish float along with the current.' He believed that citizens in a democracy like ours should play an active role in society and not just passively drift along on the waves of history. As should the Service! At AIVD we still take that mission to swim against the current very serious.

For an Intelligence and Security Service, swimming against the current, amongst other things, means telling the inconvenient truth whenever that is necessary. And yes, much of our work is cloaked in silence. With good reason! Because we can only be effective when we can conceal our modus operandi and protect our sources. But if we want to speak truth to power, we need to share what we can of our intelligence-based analyses.

So thank you very much for giving me this opportunity to talk on cyber as the AIVD sees it, to share some of our intelligence based insights.

For me personally, the age of cyber began when I bought my first computer in 1987. With 512 KB RAM, two floppy drives, a 20 MB Hard Disk, and a 620x200 pixel monochrome display, I felt ready for the future. Only twenty years later, in 2007, the iPhone was introduced in Europe, bringing together phone, internet and photography in a single item. I am not sure that we fully grasped what was about to happen. But today, another ten years later, we interact on line, we plan our holidays on line, we book our trips on line, we shop and buy our food and non-food items on line, we date, study, work on line, we control the appliances in our homes on line. Even our cars are controlled on line. Whether at home or on the road, through cyberspace we have instant access to everything that is important in our lives.

We have come to appreciate all the benefits of our digitalized world, while at the same time overlooking the fact that we have become fully dependent.

Of course, there is the enormous economic and commercial potential of our digital age. The Netherlands has long been a trading country, going back to the Golden Age of the 17th century, when our merchants sailed the seas to find new economic opportunities.
The port of Rotterdam still is an important point of transit for shipping goods between the Netherlands and other parts of the world. Traditionally we are an open economy, and we consider trading with other countries of utmost importance.

Today, we continue that tradition of trade on line. The Netherlands is one of the most IT-intensive economies of the world. Just think of AMS-IX, the Amsterdam Internet Exchange, probably the world's largest. Or take a look at our high-speed, broadband telecom networks with an almost 100% coverage of the Netherlands. Because of this sophisticated infrastructure and our favorable business climate, dozens of companies are based in our country. It generates jobs and economic growth.

But we should be aware that not a single day goes by without a new cyber incident.
And since everything is connected to the internet, everything is also a potential target.

Over the past few years, we've seen a worrying increase in the number of cyber incidents. I would like to touch on four digital threats that my organization has identified as risks to our national security and democratic society.

First of all, economic espionage. In recent years we have witnessed an increase in economic cyber espionage. The Netherlands has a number of world-class economic sectors: agriculture and food, the creative industries, chemicals, energy, high tech, logistics, water, life sciences and health. In itself that is good news. But at the same time it causes the Netherlands to be a top target for economic espionage and of great interest to certain state actors. We have made numerous companies and partner services aware of unwanted cyber activities. We have investigated attacks on firms in the IT, maritime technology, biotechnology and aerospace sectors. These investigations often revealed long-term malware infections in the international defense and other industries. We have seen the theft of highly sensitive and advanced maritime, IT, energy and defense technologies, as well as personal data. These developments endanger our economic potential and competitiveness. To be more precise, when companies are digitally robbed of their research, products and technology, the result will most likely be the loss of jobs and in some cases a company went bankrupt.

Sometimes, the affected parties were not even aware that they had been targeted. In fact, we concluded that two-thirds of them had no idea they had been compromised.
What we also realize, is that the attacks we have identified, most probably are only the tip of the iceberg. The total number of cases of economic cyber espionage will be much higher. We simply don't see everything. And this is troubling.

The second serious risk is the increase in **political interference** via cyberspace**.**

In 2015, a group of hackers attacked the German parliament, the Bundestag. It seems that the attackers stole sensitive political and personal information with the intent to leak it in the run-up to the German elections later this year.

More recently, in France, presidential candidate Emmanuel Macron was apparently also a target of cyber attacks during the presidential election.

It would be naive to assume this is different in the Netherlands. The Dutch government is under continuous, systematic attack by state actors. Foreign intelligence services are active on Dutch soil. After all, the Netherlands is a respected member of the EU and NATO, which makes us very attractive for political espionage. The attackers' probable objective is to acquire information about political decision-making and on official positions, the agenda of political meetings, or the preferred strategy on a range of national and international subjects.

We've seen highly professional phishing and spear-phishing attacks on government institutions. Messages that appear to be from a trusted source are used to infect the computer of the unsuspecting victim with malicious code to obtain confidential information. Technology-based information gathering is becoming more and more important in our digital age. On top of that, by the way, the classical modus operandi in espionage, -via human sources – remains very useful. Most of the time, adversaries indeed use human and technology-based intelligence in a complementary fashion.

Next to espionage, there is another form of political interference that is becoming more and more popular. It is a digital form of covert political influence, involving disinformation and propaganda. The use of false stories and fake news is not a new phenomenon. However, this practice has acquired a new dimension through the internet. The internet has made it far easier to extend the reach of disinformation, it is relatively cheap and the impact can be substantial. Fake news circulates very quickly on social media. It is used to influence public debates on sensitive political issues and to stir up emotions within society.

There is the spread of disinformation on the 2016 Ukraine referendum and other political issues in the Netherlands via a forged version of the website of the Dutch embassy in Moscow. In 2016, in the run-up to the Ukraine referendum, a video was posted on YouTube that showed alleged members of the Azov Battalion, a Ukrainian militant group, burning the Dutch flag and threatening terrorist attacks if Dutch voters did not support the Association Agreement between Ukraine and the EU.

We have seen the unfounded criticism of the Dutch-led investigation into the downing of MH17.

Shortly before Election Day on the 15th of March, the Dutch government decided to count the ballots by hand, because of fears about vulnerabilities in the system. It was felt that any attempt to interfere in elections undermines the credibility and trust we have in the processes that safeguard our democracy and democratic values.

The decision was also prompted by developments in the US, where the FBI, as well as the House and Senate Permanent Select Committees on Intelligence seem to have good reason to investigate Russian interference in the 2016 presidential elections.

As a final example, in Germany, stories appeared about a Russian-German girl, who had reportedly been raped by Arab migrants. Although false, it triggered a heated public debate. The ‘Lisa case’ showed once more how disinformation and fake news in the digital domain literally can jeopardize our democracies.

The third risk I want to point out is **digital sabotage.** When state actors, terrorists or others use the digital domain to sabotage our critical infrastructure or any of the other systems that have become so important to us. It is the kind of thing that can keep a person up at night.

Our critical infrastructure is already more and more dependent on digital technologies, whether in healthcare, transportation, water management, telecommunications, electricity or energy. And again, the use of the internet in our critical infrastructure has numerous advantages. But it also brings new vulnerabilities.

Sabotage in one of these sectors could have major social repercussions, causing public unrest, chaos and disorder. Imagine what would happen if an entire banking system were sabotaged. Or if there was a breakdown in our transportation network. Or if air traffic controllers faced cyber attacks while directing flights. The consequences could be catastrophic.

A striking example of a cyber attack on critical infrastructure happened to electric companies in Ukraine in December 2015. The attackers hacked into the systems of the electric companies and disrupted the operation of the system. It caused a major power outage and a blackout that lasted several hours. Hundreds of thousands of consumers were affected by the attack.

Another example occurred in Saudi Arabia. In 2012, Saudi's largest oil company was hit by a huge cyber attack that targeted thousands of computers. Several other government agencies and private companies fell victim to a destructive virus as well. Imagine the impact on our global economy if one of the largest oil companies in the world were to be stopped for a longer period of time from producing oil due to a cyber attack.

And, since last week we witness a worldwide ransom ware attack. I will not elaborate on that one; others will definitely do so.

The examples give you a sense of the digital threats facing us today. They're not imaginary. They're everywhere around us. Cyber attacks are cheap. Failure poses only limited risks, and success can be highly profitable. There are no geographical limitations to carrying out cyber attacks. They can be

launched from any part of the world. Some cyber attacks are massive in scale and can leave many victims.

Also, even though they're not entirely anonymous, cyber attacks make it easy to dodge responsibility, because they offer plausible deniability. So a cyber attack can be an attractive business model for any malicious actor.

In my opinion, we might be closer to a serious act of digital sabotage than a lot of people can imagine. Some actors do have the intention to mount an attack, but lack the capabilities to do so for now.

Which brings me to **the fourth** risk, a **terrorist attack using cyberspace.**
Attacks in Europe in 2016 and 2017 have shown that the terrorist threat to the West can take a variety of forms. Brussels, Berlin, Nice, Paris, and Stockholm: all these cities were struck by terrorist attacks.

Organizations like ISIS and Al Qaida already use the internet to spread their ideas, recruit new members, raise funds and gather information. At this point in time, however, the threat posed by cyber terrorism is limited. The level of technical expertise available to jihadist groups is still insufficient to inflict significant damage or personal injury through digital sabotage. They may not yet have the capability, but they definitely have the intent. Jihadist hackers, acting alone or in groups, have published lists of potential targets, including dozens of Dutch citizens. In most cases the personal details released were obtained from open sources rather than hacks, but the leaks did generate considerable public concern.

In July 2015, for the first time an ISIS propaganda video was released in which a child beheads a prisoner. We saw footage of four-year-old British child detonating a bomb that killed three prisoners. We have seen numerous chilling propaganda movies from ISIS since the foundation of the so-called caliphate.
And the online spread of jihadist propaganda – sometimes accompanied by gruesome videos of beheadings – can definitely lead to radicalization. Or worse, it can inspire groups or individuals to plan or carry out a terrorist attack.

Ladies and gentlemen, as the Head of the Intelligence and Security Service, the threat and risks that come with the use of cyberspace is only a part of my concern. The imminent threat of jihadist inspired terrorism is the number one priority in my organization right now. And yes, we are apprehensive of the accelerated geopolitical developments in the world. At the same time, I am convinced that it is the threat in the digital domain that we have to prepare ourselves for in the foreseeable future.

To do so, the AIVD operates in a network. We work hand in glove with the Public Prosecutor, the National Police, the National Coordinator for Security and Counterterrorism, the National Cyber Security Centre as well as with other government institutions. And we deem concerted action by the public and the private sector absolutely crucial.

In the digital domain, all the other threats will be supported or facilitated; it is also where our societies have become most vulnerable.