What if they can do what we can do?

Ladies and gentlemen,

Thank you for inviting me to speak a few words here at the One Conference.

I have had the honour of standing here in the past, but that was in my capacity as National Counterterrorism Coordinator.

Now I am here on behalf of the AIVD, the Dutch General Intelligence and Security Service.

We all have our different roles to play in the world of cyber. This goes for the government, such as the NCTV or the AIVD , as well as for the corporate world.

But we all share a common goal: to ensure the cyber-security of the Netherlands.

As I mentioned just now, I am here on behalf of the AIVD. The purpose of an intelligence and security service like the AIVD is to reveal threats that no one else can see.

We inform our partners about threat developments. We often know just that little bit more because we are allowed to use special investigatory powers, such as wiretapping and hacking.

We try to describe phenomena and trends and occasionally we even attempt to say something sensible about the future. But we do not have a crystal ball, so do not expect clairvoyance.

Still, as the topic of this One Conference is the security of our future, I will try to deliver some remarks on the future we foresee.

What threats can we see now and perhaps predict? How can we protect ourselves against these threats? I would like to go over these with you from the viewpoint of the AIVD, one of the players in the cyber-security field.

When I look at the times in which we live, I notice most of all that digitalisation makes our lives a

great deal *easier*. And even more important is it for our economic development.

When we look at the future, digitalisation will not just make our lives *easier*, it will make it *possible.*

The digital realm will be 5G, the *Internet of Things*, artificial intelligence, and quantum computers. We will be living in smart cities, be driven around in self-driving cars, digital health care and get served by advanced robots.

The functioning of our society will come to depend more explicitly on digital technology.

Right now we often still have an analogue escape. Some still keep a road map in their car but this may not be possible anymore or would be of no use in the future.

More and more processes are exclusively digital, with no fallback option.

All this new technology is changing the way we live, work, even wage war. The best analogy with the past, perhaps, is the invention of the internal combustion engine and the automobile.

These, too, changed our way of life, our work. We had to do everything possible to make sure these changes were safe.

Today, we follow clear traffic rules, wear seat belts, and in case of a collision we are protected by airbags.

So how can we ensure that we remain safe with all this new technology? What are the threats to this digital society?

The role of the AIVD is to look at the activities of other countries or state actors that constitute a threat to the security of the Netherlands, or that pose a risk to our interests.

We have seen that internet technology helps states in their attempts to spy on our country, to sabotage us, to spread disinformation.

The AIVD also has other areas of interest, such as terrorism and extremism.

Where these are concerned, we see that social media is mostly used for propaganda purposes. We have not yet seen a serious terrorist or

extremist cyber-threat that could paralyse our society.

For us, cyber-attacks by states that have the aim of political and economic spying and sabotaging are the most important risk.

Compared to traditional espionage and sabotage tactics, the use of digital means greatly expands the impact and extent of an attack.

Given our growing dependency on the internet, this will only increase.

Let’s look a little bit closer.

In our investigations we also see that various state actors no longer limit their cyber-attacks to the users of digital products and services, but increasingly also go after the suppliers of these digital products and services; think of internet service providers, telecommunications providers, and managed services providers.

These suppliers can be themselves targets, but they can also be used as a springboard for the

infiltration of a particular target – a so-called supply chain attack.

This development worries us because these providers often have access to the networks or the sensitive information of their customers, which may be very interesting to hostile states.

Many companies and government organisations outsource various processes, such as payroll administration, marketing and increasingly also network administration, internet access, and sometimes security, including information security.

To provide their services, these providers often need to have access to the customer’s network.

Hostile states can exploit the provider’s legitimate access to their customers’ networks.

This makes prevention and detection of abuse much more difficult.

Supply chain attacks have also targeted Dutch businesses and government agencies.

Another thing we note is that these supply chain attacks not only facilitate espionage, but also the

creation of long-term covert presence in vital infrastructure with the aim of carrying out acts of sabotage when needed.

This could result in the disruption of vital internet-connected infrastructure, such as fresh water and electricity distribution or financial services.

Also the service providers themselves can also be targeted by hostile states, resulting in the theft of sensitive information.

Think, for example, of internet service and telecommunications providers that facilitate internet and telephone communications for companies and government organisations.

Potentially these service providers also have access to sensitive information.

By infiltrating such providers, a hostile state does not need to hack into the network of a company or government agency to gain access to this information.

We have seen in our investigations that states infiltrate telecom providers on a huge scale in

these so-called man-in-the-middle attacks, with the aim of intercepting their clients’ phone traffic.

This information will then be used to map and monitor targets and their contacts.

We have seen, for example, that senior military officials, politicians, and dissidents are being followed in this way.

Because we trust our service providers, supply chain attacks can create extensive, profound and structural access to a target’s network data streams.

They offer many possibilities for espionage and the collection of information: on technology, finance and economy, politics and policy, and of course personal data.

And from government institutions as well as private businesses.

The managed service providers, internet providers and telecom providers that are targeted in these supply chain and man-in-the-middle attacks are often companies that are

active nationally and sometimes even internationally, with thousands or even millions of customers.

Any hostile state with access to all this data can do a great deal of damage, potentially resulting in huge numbers of victims across the world.

This makes the increase of supply chain attacks and man-in-the-middle attacks using these kinds of service providers a very alarming development.

The risks of such attacks also increase when these providers use hardware or software from countries that run an offensive cyber programme against Dutch interests.

These companies can be obliged to collaborate with that country’s intelligence and security services.

We, the Netherlands, also use foreign hardware and software.

With today’s globalisation and international takeovers it is quite conceivable that an ICT

company could come into the sphere of influence of another country. This increases our vulnerability.

All these kinds of cyber-attacks present a risk to any company, organisation or institution.

They could result in the theft of company secrets from high-tech companies, or government policy documents falling into the wrong hands.

When it is our society that is at stake, when processes are involved that are crucial to our everyday existence, then the consequences of a cyber-attack can be even more disastrous.

I imagine there will be some of you who are thinking right now: yes, that is all very well, but is it not true that you do the very same thing?

Are you not being holier than the pope? It is true, we do do these things.

We hack and penetrate systems of others to find out what they are up to. And we use vulnerabilities in hardware and software, if necessary.

And if they can do what we can do, then that only worries me more. Because we do what we do in the interest of national security, to protect the Netherlands.

Yes, our operations are offensive, but always to a defensive purpose.

What’s more and even more important, we are subject to very strict control by an oversight committee and by Parliament. This kind of control is absent in the countries that are targeting us.

And there are quite a few countries with an offensive cyber-strategy that target Dutch interests.

It is with regard to these countries that we, the AIVD, believe it would be undesirable if we were to use hardware or software from those countries for processes that are of vital importance to our own country.

Using such equipment should only be permitted after a thorough risk assessment.

We carried out an assessment of this kind with regard to the security of 5G.

But what does this mean for the future, I hear you ask.

The arrival of 5G only boosts the vital position of information communication technology in our society, in addition to the fact that – let us not forget – it will make life more convenient.

The importance of ICT services in our daily lives will only grow.

But imagine if the current 4G network were to go down.

That would mean your phone would not work as it should, as you won’t have internet on your smartphone.

But if, in the future, the 5G network were to fail, that could result in systems shutting down – not only the fridge and the central heating with their internet connection, but also the operations of vital machinery and processes.

If our energy supply were disrupted, society would grind to a halt.

This implies risks for all of us. And when vital processes are involved, we need to be extra careful.

5G is a game changer and can provide an economic boost, but we must also look at the downside, that is part of my work.

What does the AIVD do to protect us from these threats?

What is our added value when it comes to cyber-security?

As I mentioned earlier: the AIVD investigates threats by state actors.

To do this we have more options than others.

We are allowed to talk to people who can provide us with information, we are allowed to wiretap, to hack into systems.

If necessary we also do this offensively, to find out what the interests of foreign services are.

We are only allowed to do this if there is no other way to get that information.

And there has to be a need, namely: to help us identify a threat against the Netherlands.

We also help private and public organisations detect intrusions and attacks.

With our National Detection Network we monitor the traffic of a large number of government organisations, together with the National Cyber Security Centre NCSC.

We scan for anomalous behaviour and traffic, using the knowledge we gained from our intelligence investigations.

This also provides us with new insights that we can use to identify other threats.

Only last week we encountered two alarming hits following probes with government organisations within this network.

We took the necessary steps in collaboration with these organisations to ensure that the government’s networks remain protected.

We not only investigate threats, we also provide the government and our partners in our national vital infrastructure with information on how to keep their information secure.

We see in our investigations how other countries operate. We use that knowledge to educate others and enable them to make their own assessments and then act.

As far as I am concerned, the days when the AIVD bluntly cried out how dangerous the world was and then shut the door, are behind us.

Of course, we are legally prohibited from divulging how we get our information, and it would be counterproductive if we were open about that.

However, we are not a secret service, we are a service who sometimes has secrets.

When we look at the commotion caused by concerns surrounding the security of the future 5G network, this has taught us how important it is that all parties understand what the threat is.

It is up to us to make that visible. It is for others to decide what has to be done.

An important advisory body for our government, the Netherlands Scientific Council for Government Policy, recently published a report on cyber-threats.

The council concluded that we are not yet adequately prepared for a cyber-attack.

We need cooperation and intensive sharing of knowledge.

Sometimes economic interests and the protection of national security overlap.

Sometimes they get in each other’s way and sometimes they even collide.

By being more open about our intelligence, we can create a stronger cooperative base.

The taskforce Economic Security, under guidance of the NCTV, of which the AIVD is a member together with several other government agencies, is a good example of this kind of cooperation.

This also helped us when we looked at the risks related to future developments, together with telecom companies.

We have been able to show in what way states can abuse the telecom sector.

And this works both ways. When you are a trusted conversation partner to the telecom sector, you also receive useful information.

In this way we can create a stronger network, together. The AIVD is a reliable partner of this network.

And that is the only way to ensure we can have actual progress in the digital world.

As we approach the third decade of the twenty-first century, we are on the threshold of a bright new technological future.

But this bright future also looms for our opponents.

That is why it is of the utmost importance that we stay vigilant, *stay alert*!

Thank you!