Conference on Law and Society in the Digital Era, 17 November 2016, Amsterdam

Speech by Rob Bertholee, Head of the General Intelligence and Security Service.

Ladies and gentlemen,

I'd like to thank the Centre for Law and Internet for inviting me to speak today on a very topical issue, Law and Society in the Digital Era, at this impressive historic venue. This building, West India House, was the headquarters of the Dutch West India Company. It was from here that the order went out to build Fort Manhattan, the seed from which the city of New York was to grow.

In the age of the West India Company, the Netherlands prospered. There is a dark side to that part of our history. We employed the colonial methods which were commonplace at the time, and which paid no regard to human values. Today, fortunately, we place a higher value on human rights. Many of them are guaranteed by our constitution. These fundamental rights exist to protect us from harmful external influences. They include freedom of expression and the right to privacy.

These are fundamental rights which my organisation, the AIVD, helps to protect every day.

After all, we are not the instrument of a dictatorial regime. We do not hunt or arrest innocent citizens. On the contrary. Our mission is to identify threat against our democracy before they materialize.

We are not a state within a state and no other intelligence and security service anywhere in the world is scrutinised so closely to ensure it complies with the law.

My 1,500 staff and I are committed to keeping the Netherlands safe. We need to be, because we live in an age marked by troubling developments on a number of fronts. These developments require my organisation to remain vigilant in many areas. Please be aware that our mission comprises responsibility not only for traditional intelligence and counterintelligence efforts, but also for cyber issues and cybersecurity. Actually, I think you don't need me to tell you how the Russian Federation is involved in a geopolitical power play – using the economy, energy and the military as its weapons. There is hardly a state in the Middle East that is not involved in an armed conflict with one or more other states in the region. In Africa, the situation is not much better. Algeria, Libya, Tunisia, Egypt, Somalia, Ethiopia and Eritrea – to name just a few – will cause us headaches for many years to come. Add in: failed economies, migration and refugee flows, and you have a very explosive mix. In short, we see an arc of instability that runs from Casablanca to Murmansk.

A bit further afield, we see that China is adopting a much more assertive role in the international arena. So relationships in the region and beyond are changing rapidly. And not always in the direction of more friendly or civilised interaction. I could go on. Needless to say, we have a tremendous amount of work ahead in the field of intelligence and counterintelligence.

The threat that lives and moves through our digital spaces is less clearly defined…
State actors are using cyberspace to gain insight into our political decision-making, steal all sorts of scientific and economic information and find out about innovations in our most important industries, especially our 'top sectors'. We've identified an increasing number of Advanced

Persistent Threats in the last couple of years. These APTs extend over a long period of time – we're talking about years. They can be very complex in design, and they target government, scientific institutions and industry alike. These are threats that cross national borders and against which virus scanners and firewalls often offer inadequate protection. Although finding their source is not easy, we have no doubt at all that these attacks are executed by state actors. And by the way, these attacks are not a substitute for the traditional methods of espionage – using human intelligence – which we come across every day as well. These cyberattacks come on top of all that.

Can we withstand these forms of espionage and terrorism? Can we cope with covert influence campaigns? The Cold War may seem a distant memory, but in some respects Russia's activities are back at that level.

The political instability in North Africa and the Middle East, which I mentioned, has created many safe havens where terrorist organisations can flourish. ISIS has capitalised on this like no other group.

And developments in these regions have repercussions for our security, here in the Netherlands...

ISIS and the conflict in Syria are a magnet for potential jihadists. And this phenomenon is often fuelled by the internet. Some 270 boys and girls, men and women, fathers and mothers have left the Netherlands – often young people, who are volunteering to be taken back to the seventh century. Young people who are joining an organisation that preaches not religion, but violence. Young people who have shown no hesitation in resorting to violence, both within the so-called caliphate and beyond. Young people who no longer embody future promise, but rather a direct threat to our security. Young people, each and every one of whom I have to keep track of, especially on the internet.

The threat is complex. Attacks are orchestrated from outside Europe, but are also the product of people here, acting on their own initiative, possibly inspired by calls from ISIS and al Qa'ida. They can be carefully planned professional operations, or relatively simple, small-scale acts of violence. The threat can come from organised groups and networks, but also from individuals or small groups.

Unfortunately, we live in a world where those with evil intent exploit the opportunities offered by the digital environment...

They pose a threat to the security of our society. State actors, criminals, terrorists and fraudsters are experts at harnessing the technologies available in 2016. We counter threats based on legislation that predates the era of the smartphone. Legislation that was made when we only phoned each other. Before chatrooms, Instagram and mobile email had been invented.

So we need the new legislation. But what does that mean?

Are we allowed to intercept all internet traffic?
Do we want to crack the encryption on everyone's digital messages?
Do we read everybody´s e-mail?

Let me say loud and clear: the answer to those questions is 'no'. I may have the technical means to read your emails or break into your digital systems. I have enough smart people to do it. But I have absolutely no wish to do so, and absolutely no right to do so. Not now and not in the future.

I have no wish to listen in on everyone or intercept all internet traffic. We don't want to read you e-mails.

But I need to be able to deal with the enormous amount of data. Be aware, most of the time we are looking for the unknown.

What we will do, when the new act comes into force, is look at flows of metadata if we suspect a targeted threat to the Netherlands.

Do I want to crack the encryption in general on everyone's digital messages? No, I do not. And I've never said I do. But in the event of a suspected threat, I do want to be able to read a message sent by a potential terrorist. After all, I need to know where and when they intend to strike.

More and more countries are realising that it's not difficult or expensive to get hold of information by mounting digital attacks. The costs are low, the rewards are high, and the risks are small. My organisation alerts government bodies and affected companies if we detect espionage activities. When we do, two-thirds of them are unaware that they are under attack. In that respect, we're still rather naive. We should not underestimate the risk of a digital attack. We all are a potential target for foreign powers.

I'm convinced that, pretty soon, the digital threat will be greater than the threat posed by jihadists...

If our society is to function securely, digital security is a must. The economic and geopolitical importance of our digital infrastructure is growing, and espionage and sabotage threats are increasing. But our resilience is lagging behind.

This brings us back to today's theme, 'Law and society in the digital era'. I see the law as providing the framework for all the work we do. But the society in which we live is changing so quickly that legislators can't keep up. So I'm calling for robust legal frameworks that are not dependent on the technology of the day.

Thank you.