Speech TALLINN MANUAL 2.0 – Minister Koenders

The Hague, 13 February 2017

Thank you, Professor Hirsch-Ballin, for your kind words of welcome.

Thank you also, Mr Sakkov, for your introduction.

Ladies and gentlemen,

These are exciting times. The digital revolution is proceeding at breakneck speed, bringing growth and prosperity to many. Just look at this country. The Dutch digital gateway to Europe is now more important to our economy than Amsterdam's Schiphol Airport and the Port of Rotterdam combined. So, for the Netherlands, bits and bytes outweigh Boeings and boats. And it's the same story for more and more countries.

But our digital dependency also leaves us vulnerable.

To criminals who prey on our citizens and companies.

To states that use cyber operations for espionage, disinformation campaigns and military gain.

There are plenty of recent examples I could cite. Take the cyberattacks against the power grid of one of our eastern neighbours. They left entire cities and provinces literally 'in the dark'.

Or take the attack that wiped computer drives at several government ministries in a Middle Eastern country. Public services were severely disrupted. I shudder to think what would happen if the 3,500 civil servants at my ministry turned up to work tomorrow and found they couldn't log into their accounts.

When attacks like these happen, a lot of technical questions get asked.

- What malicious software did the attackers use to gain entry into our systems?
- What made our systems vulnerable to outside interference?
- What action should we take to prevent such intrusions in the future?

And these are all important questions. But technical questions don't deal with *behaviour*. To understand and change behaviour, we need to think about rules and laws. That's why my country hosted the Global Conference on Cyberspace in 2015. And why, today, I'm sending the government's International Cyber Strategy to parliament.

The strategy describes where we need reinforcements to help us meet tomorrow's threats. It aims to keep cyberspace free, open and safe by strengthening international cooperation and diplomacy.

The cyberspace we value and rely on needs protecting. The sooner we recognise cyberattacks and disinformation, the better we can prevent harm. The strategy helps prepare possible diplomatic responses to such threats.

Because cyberspace spans so many borders and involves so many private parties, we need to protect it by working together: with other countries, with the technical community, with companies, with non-governmental organisations and with academics.

The last thing we need is an arms race in cyberspace. The Dutch government plans to launch a network for 'cyber diplomats', who will help to build trust so that countries can agree on norms for online conduct.

When cyberattacks are launched, international law helps determine how we can and should respond. The law on state responsibility, for example, has a lot to say about when a state can be held responsible for the conduct of a proxy. It also allows a state to take measures that would normally be in breach of international law, in order to address a prior breach by another state.

Or consider attempts to influence the outcome of an election – remember, this year there will be national elections in the Netherlands, France and Germany. We've already seen attempts to spread disinformation, with lies about the presidential candidates in France.

Such disinformation campaigns mostly fall outside the scope of the Tallinn Manual. They don't require a legal response – they require a robust democracy in which citizens know how to separate facts from fiction.

But we mustn't be naïve. Cyber operations against institutions, political parties and individuals underline why we need the international legal principles of sovereignty and non-intervention in the affairs of other states.

We know that international law applies to cyber operations. But applying international law to them is not always straightforward. And that's where the Tallinn Manual comes in. Today we celebrate the updated manual, version 2.0. I'm proud that the Netherlands was able to contribute through what's known as the Hague Process.

Over a century ago, major powers and smaller powers convened in the Hague to discuss matters of war and peace. The Hague Conventions led to agreements about the laws of war and the peaceful settlement of disputes. They brought us the Permanent Court of Arbitration, which exists to this day. The Conventions helped turn the Hague into the international city of peace and justice.

Today, cyber operations are becoming a weapon of choice. Matters of war and peace have entered the digital age. So it felt only natural for the Netherlands to arrange a series of consultations between the authors of the new manual and the legal advisers of states all over the world. We've also been facilitating further discussion in other countries and at other events.

We've done so because we think it's important to discuss this issue not just with great powers or groups of academics, but with a broader group of countries. After all, any country in the world can suffer the effects of malicious cyber operations. So every country has an interest in the stability that only international law can provide.

That's especially true now that the geopolitical party is over. We've reached the end of a twenty-five-year period of strategic stability and relative peace in large parts of the world. Today, international relations are entering a time of increasing uncertainty.

It won't be another Cold War - the world is too interconnected for that. Nor will it be World War Three. We're looking at something altogether different from what we've seen before. The digital revolution provides new ways to destabilise a country or to claim one's place in the world order. Conflict will take on new, more hybrid and ambiguous forms.

Again: cyber operations are not simply a technical issue. The use of cyber operations by states is highly political. States can exercise power through them. How they do so is determined by their broader interests, their national strategies, and their assessment of the costs and benefits.

In short, this is about behaviour, not about the technology itself.

The good news is: we can influence states' behaviour. By engaging in cyber diplomacy and digital conflict prevention. And by promoting an international normative framework for regulating cyber operations.

That is why on Saturday, during the Munich Security Conference, I will be launching the Global Commission on the Stability of Cyberspace. I like to call it the Club of Rome for cyberspace. It should achieve for cybersecurity what the Club of Rome achieved for climate and the environment. And it will do so by suggesting voluntary norms for responsible state behaviour.

Such measures, essential though they are, should only be an addition to the body of binding international law that already exists. I'll say it again: this is about behaviour rather than technology. International law is based on principles that apply regardless of technology.

It should come as no surprise that we want to promote the international legal order in cyberspace. The obligation to promote the international legal order is even enshrined in the Dutch Constitution. Fortunately, states have recognised that existing international law applies to the digital domain.

That said, many of these rules date from *before* the digital age. So it's not always clear *how* they apply to new technology.

Academic experts can help inform the debate among states, as the first Tallinn Manual demonstrated.

This newly updated version will prove even more useful. It deals not only with the relatively rare issues of the use of force and international humanitarian law. The new Manual also addresses cyber operations *below* that threshold. After all, it's not always helpful if the first legal question asked about a cyber operation is whether it is legally an 'armed attack'. In fact, that approach could escalate the situation.

Most cyber operations take place in peacetime, despite the often inflated rhetoric about cyber warfare and cyberattacks.

So it was a good idea for the NATO Cooperative Cyber Defence Centre of Excellence to invite the experts to update the manual.

But this cannot be something that only experts from NATO countries are concerned with. International law must rest on a globally shared understanding of its application.

I'm delighted to see that the International Group of Experts, which drafted the updated manual, was much more geographically diverse this time. As was the peer review team.

We felt that this was also an opportunity for a broader dialogue. Hence the Hague Process. By arranging a series of consultations, we sought to ensure that the updated manual would be more transparent, more representative, and therefore more legitimate.

I think we succeeded in that effort.

The Tallinn Manual provides guidance on the application of long-established legal principles in the cyber domain: sovereignty, non-intervention, due diligence, and state responsibility.

I find the discussion of countermeasures particularly useful. Countermeasures can provide a legal basis for a state to react to a malicious cyber operation ‘below the threshold’. We’re not left with our hands tied when a cyber-operation stays below the level of an armed attack that justifies self-defence. Given the risk of escalation, countermeasures are subject to conditions and limitations. The Manual describes them very clearly.

For example, countermeasures may only be directed at a state that is responsible for an ongoing breach of international law. And they have to be proportionate.

There’s also a chapter devoted to human rights. This is perhaps the longest chapter in the book, which reflects the importance of the subject. I’m glad to see that it starts by stating that human rights that apply offline also apply online. The Netherlands has always strongly supported that principle, and we will continue to do so.

But all this is only the start of a longer conversation.

The Tallinn Manual does not provide the answers to all the questions. It is not an official document, and the Netherlands does not necessarily agree with everything in it.

In fact, in many cases the manual describes more than one possible interpretation of a particular rule.

So the conversation must continue. With the legal advisers from over 50 states which participated in the Hague Process.

Let me reassure you, I say this only because I want to ensure we all remain ambitious. But in the meantime, we have every reason to celebrate! The Tallinn Manual reduces ambiguity and uncertainty. It reduces malicious actors' room for manoeuvre.

The manual shows that cyberspace is not simply a jungle, where the strong do what they want and the weak suffer what they must. The law applies there just as it does elsewhere. Especially in times of tension and conflict, the law should not be silent.

I'm proud that, together, we have been able to strengthen the voice of the law in this way.

Thank you.