Speech by the Chief of Defence of the Armed Forces of the Netherlands, Admiral Rob Bauer, at the International Operational Cyber Symposium on October 26th 2017, Amsterdam

Note: check against delivery!

Ladies and gentlemen,

"It is not enough that we do our best. Sometimes we need to do what is required." This quote from Winston Churchill is very appropriate, as 26 October is the national day of the deployed. So today, we are thinking of the military men and women who are deployed across the globe. And I thank all of them for their service.

When Odysseus invented the Trojan horse, it was an act of brilliance.
He found the ideal way to enter enemy territory.

Unseen, unheard and unnoticed.

In order to cross the walls of the city, not a single act of violence was needed. All that was needed was the good faith and naivety of the enemy.

It was a "too good to be true" scenario.

In many ways, cyber operations can be seen as a "too good to be true" scenario. They are fast. They don't require boots on the ground. An enemy can enter a country – a society, without anyone noticing, while still being able to cause immense damage. And because of their lack of transparency and complex attribution, they often come with little chance of serious repercussions.

However, as is the case with all scenario's in life that seem too good to be true… they have their drawbacks.

Cyber operations require extensive preparation. They are always tailored to a specific target, at a specific time and under specific circumstances.

They are therefore difficult to repeat. While a piece of traditional weaponry can be used and re-used for years on end, a piece of malware has a limited shelf and operational life.

Due to the constant updating and upgrading of information systems, the cyberspace domain is always in motion. Windows of opportunity can come and go within months, weeks and sometimes days.

This means that executing a cyberattack will often be a costly, time consuming and complex task.

Now, if you're on the defensive side, that's great news. But otherwise… not so much…

Cyber technology presents both opportunities and risks for military operations.

Therefore, I am glad that we are discussing this issue more and more. Especially in conferences like the one you are having today. It is important we are realistic about the powers and pitfalls of cyber operations.

Because, whether we realize it or not – we have become utterly dependent on digital technology.

A large scale cyberattack could already have an enormous impact on society.

If we want to create a resilient society, we have to develop the skills to defend ourselves against cyberattacks.

This is not a responsibility of the Armed Forces alone. Far from it. But we do have an important role to play when it comes to developing the military ability to conduct cyber operations.

(…)

Over the last decade, more and more state actors and non-state actors have been developing cyber capabilities. This means that the likeliness of a cyberattack has increased and will continue to increase.

We are all familiar with the examples of Stuxnet in 2010 and the attack on the Ukraine power grid in 2015.

These examples show us some of the potential that cyber operations have. They also remind us that we need to act proactively if we don't want to be the victim of an attack.

We have to realise that cyber deterrence can also play a role in preventing cyber conflicts. We have to convince potential adversaries that the consequences of launching cyber-attacks against the Alliance will be severe. In other words: that the costs for them will be high.

Ladies and gentlemen,

The fact that NATO decided to recognize cyberspace as an operational domain was a major step. It is crucial that NATO sees cyberspace not just as an issue of network security, but also as an opportunity to develop and deploy operational capabilities.

So the following questions come to mind: how can we incorporate cyber capabilities into the larger framework of NATO operations?

How can we ensure that NATO makes the best use of the opportunities that are presented in the cyber domain?

And how can we use our respective cyber capabilities to help NATO in its task of conflict prevention?

These questions raise both technical, organizational, political, legal, and even ethical issues, which we are all dealing with on our respective national levels.

Defence organisations play an important role in the protection of the national security. But when it comes to cyber security, Defence organizations have to ask themselves the question: what does society expect from us and to what extent will we be able to live up to those expectations?

After all, the Armed Forces are not the national firewall. We don't have 'digital sandbags' that we can drag in to solve any cyber crisis...

In order to tackle the issue of cyber security, Defence organizations have to work together with other governmental organizations, as well as the private sector and research institutes. Together, we can work on awareness, capacity building and training.

This cooperation can also mean: inviting people from the cyber industry to work directly with or for the armed forces.

We have to make the best use of all the scarce talent that is available in our respective countries. In the Netherlands, we have therefore started to recruit cyber reservists. This is part of our Adaptive Armed Forces concept, and we are very positive about the possibilities of this programme.

However, recruiting the 'cyber savvy' is not enough.

We have to add cyber capabilities to the tool box of operational commanders. In order to maximise their impact and effectiveness, cyber operations must form an integral part of existing military capacities.

This means that we also have to make sure that the Defence cyber community and other non-cyber defence stakeholders understand each other.

All too often, there is a gap between the 'cyber-world' and the 'non-cyber world' in the Armed Forces.

In order to bring these two worlds together in the Netherlands Armed Forces, we have established the Defence Cyber Command.

General Hans Folmer will give you more details on the working of the Cyber Command, later on. But since this is a subject close to my heart, I'm sure he will allow me elaborate a little on this.

The Defence Cyber Command helps us to address the challenges that we face when we want to incorporate cyber capabilities into our operations. Those challenges are not necessarily operational.

For instance: is the Defence acquisition framework well-suited for the cyber terrain?

Can we buy the right equipment at the right moment?

Are we flexible enough to respond immediately to new threats and take advantage of new opportunities?

Can we optimize information sharing and capability development between the intelligence community and the military cyber defence organisation?

Can we educate our military men and women quickly in order to create cyber awareness?

These are all important questions, but it doesn't stop there. We also have to make sure that a commander in the field can make an informed decision between executing a kinetic attack or a cyberattack. Only then we can talk about fully integrating cyber operations with existing military capabilities.

Ladies and gentlemen,

As we all know, the cyber domain does not recognize our national borders. An email containing a dangerous virus doesn't pass any physical borders and can be delivered anywhere in the world in milliseconds.

This means that when we deal with this issue, we cannot afford to think in terms of national silo's.

The Netherlands is keen to work together with like-minded nations, not just to exchange knowledge but also to discover real ways in which we can cooperate.

In order to do that, we need to be realistic about both the powers and pitfalls of cyber operations.

When Odysseus placed the Trojan horse in front of the gates of the city, there was only one man, a Trojan priest, who saw it for what it was. He warned his fellow citizens, but his protests fell on deaf ears.

(And for those of you who know the story, you will know that things unfortunately did not end well for him…)

You may have heard this already, but the word '*cyber*' actually stems from the Greek word '*cybernetics*' which means '*steersman*'. And that is exactly what we should be doing. We have to steer the cyber domain, before it steers us.

In order to properly execute (or: steer) cyber operations we have to stay ahead of the curve and work together. That is what I believe this conference is about.

It is my sincere hope that you use this day of speeches and deliberations to work on this issue and learn from each other, so that we can improve our knowledge and skills of cyber operations which are becoming increasingly important.

Thank you.

-0-0-0-