PRESS CONFERENCE BY NATO SECRETARY GENERAL JENS STOLTENBERG FOLLOWING THE MEETINGS OF NATO DEFENCE MINISTERS

4 october 2018

Good afternoon.

We have just finished a meeting of NATO Defence Ministers.

And in an unpredictable world, we are strengthening NATO's deterrence and defence. Fairer burden-sharing underpins this. There is a renewed sense of urgency for all Allies to invest more in defence. To move forward on all aspects of burden-sharing: cash, capabilities and contributions to NATO missions and operations.

This was the focus of our discussions last night. It is clear we are making progress. This will be the fourth consecutive year of rising defence spending. But we still have a long way to go. Allies have committed to have credible national plans. I would expect these to show real increases in defence spending year on year. And a realistic path to 2% of GDP on defence. Allies will report on the national plans before the end of this year, and we intend to discuss them at our meeting of defence ministers in February. Allies should also invest in new capabilities.

And make contributions to our missions and operations. This is about fairness. But more importantly, it's about our security in a more unpredictable world.

Our deterrence and defence includes conventional capabilities, cyber defence, missile defence, and the nuclear dimension.

So today we held a meeting of the Nuclear Planning Group. This is part of our work to ensure we have the right tools and procedures in place. So NATO nuclear forces remain safe, secure and effective.

We also addressed concerns about the Intermediate-Range Nuclear Forces Treaty.

A landmark agreement that abolishes a whole category of weapons. We believe this treaty is in danger because of Russia's actions. After years of denials, Russia recently acknowledged the existence of a new missile system, called 9M729. This system is destabilising. It is a serious risk to our security. Allies agree that Russia has not been transparent. And refuses to provide any credible answers. The most plausible assessment is that Russia is in violation of the INF Treaty.

We call on Russia to address our serious concerns.

What is more concerning is that this is part of a pattern of behaviour of many years. Today's announcements by the Dutch and British governments have exposed Russia's indiscriminate campaign of cyber attacks around the world. The Netherlands briefed the NATO Defence Ministers on the targeting of the offices of the Organisation for the Prohibition of Chemical Weapons in The Hague by a hostile cyber operation. This operation was carried out by the GRU, the Russian military intelligence services. But it was disrupted by the Dutch intelligence services in partnership with the UK. Moreover, the UK has identified the GRU as being behind a number of other cyber-attacks around the world. These have affected citizens in many countries, including Russia. And caused enormous economic costs.

NATO Allies expressed their solidarity with the decision by the Dutch and the British governments to call out Russia on its blatant attempt to undermine international law and international institutions.

Russia must stop this reckless pattern of behaviour. Including the use of force against its neighbours, attempted interference in election processes, and widespread disinformation and campaigns. In response, NATO will continue to strengthen its defence and deterrence in the cyber domain. We are making significant progress. Setting up a new Cyber Operations Centre. Bolstering our cyber resilience. And integrating national cyber capabilities into NATO missions and operations. Some Allies have successfully used their cyber capabilities against ISIS in Iraq and Syria: to suppress terrorist propaganda, hinder their ability to coordinate attacks, and to protect forces on the battlefield.

Today, several more Allies have offered their cyber capabilities to NATO. I thank them. This is a big step forward. These cyber capabilities will make us as strong in cyberspace as we are on land, at sea and in the air. Of course, we remain a defensive alliance. Acting proportionately. And in line with international law. We are also making progress in setting up new Counter Hybrid Support Teams. These teams will provide tailored assistance to our nations. To prepare for, and to respond to hybrid attacks. This too is about Alliance solidarity.

At the same time, NATO is responding to the instability on our southern borders.

Our new training mission in Iraq will help local forces to secure their country. And we continue to support other partners – Jordan and Tunisia – to improve their defence and security capabilities. Our Hub for the South in Naples is also working to monitor and understand regional threats, like terrorism and failing states.

Today, we were joined by EU High Representative Federica Mogherini and our partners Finland and Sweden. We are stepping up our cooperation with the EU on cyber defence, military mobility, and in countering hybrid threats. We also heard about the EU's efforts on defence, and how they can complement NATO's work.

This has the potential to contribute to the enhanced security of Europe and North America.

And with that, I'm ready to take your questions.

QUESTION: Thank you, Secretary General, given the attacks in The Hague and given that you are acquiring these new cyber capabilities will you respond in any way, will you respond to Russia's cyber-attacks?

JENS STOLTENBERG [NATO SECRETARY GENERAL]: We are responding every day. And just the fact that this this attack by Russia on the international Organisation for the Prohibition of Chemical Weapons was disrupted shows that we are getting better at reacting to this kind of … or responding to this kind of cyber-attacks. Getting better at providing the necessary attribution and what happened today was that UK and the Netherlands has exposed what Russia … their military intelligence services are actually responsible for doing in many places in the world. So, we are responding also by the ongoing strengthening of our cyber defences with the decision that we will integrate national cyber capabilities into NATO missions and operations by the fact that we have actually decided that cyber can trigger Article 5 and also by the fact that as part of the new command structure we are establishing a new cyber operation centre. So, we are doing many things at the same time and not least increasing the awareness around in the capitals when it comes to reacting to these kind of cyber-attacks.

QUESTION: Thank you very much Secretary General, Johnathan Marcus from the BBC. Two questions on this cyber issue. One, I think you referred to strengthening NATO's capacity to both defend and deter cyber-attack, deterrence implies having an offensive capability of your own, surely an essential element of deterrence is having that capability and being able to deploy it. Could you comment on that? And secondly, you referred again to the idea that a cyber-attack could trigger Article 5 – well, beyond a form of words, we've got documentary evidence from a number of countries in NATO that such attacks have been carried out. So, what is the actual value of this Article 5 in a statement, I mean, where does it take us beyond what is being done at the moment?

JENS STOLTENBERG: So, we will always act and react in a proportionate way. And in accordance with international law. So, we decide based on the situation, based on the character of what we see the way we respond. Partly as different individual national Allies which are reacting, and partly as an alliance when we act together. What we have seen is that we are significantly stepping up and we have to remember that the attack they tried to launch against OPCW actually failed, they didn't succeed. So, I think that shows that NATO Allies and NATO have become stronger in reacting to these kinds of attacks. Better intelligence, better at coordinating our intelligence. This was UK and the Alliance working together. NATO has established a new intelligence division - also to be able to coordinate even better the way we collect, understand and analyse intelligence. And also, the fact that we are helping Allies with sharing best practices, technology. We have large exercises increasing awareness. All that helps to react. And then just the fact that we work together and also now have more and more Allies who provide national cyber capabilities – all of that fits into this broader pattern of how NATO is adapting. And we also decided at our summit to establish cyber as a domain - military domain alongside land, sea and air. So, how we react will be determined from case to case. The

thing is that I think what we have seen is that we have been better at defending our systems, disrupting attacks, exposing attacks and also being able to collect the necessary intelligence to disrupt attacks against our cyber networks.

QUESTION: Dan Michaels, Wall Street Journal. Could you clarify on that, though – do you see NATO as having offensive cyber capabilities? Thank you.

JENS STOLTENBRG: We have integrated national cyber capabilities. And I described what they can do. Because we have seen how national cyber capabilities have been used against, for instance, Daesh. We have been able to disrupt the cyber networks of Daesh to reduce their ability to recruit, to fund, to communicate. And these capabilities have been used by NATO Allies against Daesh and these are the same kind of capabilities we now are creating the framework to integrate into NATO missions and operations. So, we call them national cyber capabilities. They have been used very effectively against Daesh and I think it is important that we have those capabilities in NATO missions and operations when needed because it's impossible to imagine any kind of military conflict in the future without a cyber dimension. And then of course we need many different kinds of cyber capabilities to have effective defences and the right capabilities.

QUESTION: Secretary General, I would like to ask you if there are steps forward with the Mediterranean hub. And if these steps were forward, open to the possibility of having trainings of security trainings in the Mediterranean and, for example, in the future with Libya? And also, I would like to ask you since you discussed about burden-sharing if you've seen the plans of Italy to reach the target of two percent and if NATO deems that they are okay? Thank you.

JENS STOLTENBERG: The hub for the south is important to coordinate, to analyse, to improve our understanding of the threats and the challenges emanating from the south and I welcome very much that we have been able to establish this now and I think the work of the hub in Naples is very important for the whole Alliance. NATO provides training. We do training and capacity-building in Afghanistan because we strongly believe that one of the best weapons we have in the fight against terrorism is the train local forces and enable them to stabilise their own country and to fight terrorism themselves. We are also now scaling up our presence in Iraq and we are launching a training mission there. All of this is relevant for the challenges we face from the south. We are in dialogue with Libya, we are ready to provide help. We are not there discussing a military training mission, but we are looking into the possibilities of providing Libya with help to build their security and defence institutions - Minister of Defence, military commands and so on because you need that kind of military institutions to stabilise the country.

QUESTION: Thanks very much, Michael Birnbaum from the Washington Post. Do the Russian cyber efforts that have been outlined today rise to the level of taking offensive cyber action in response to them? You've talked about the ways that NATO Allies have responded, but you haven't talked about cyber offensive action and what kind of cyber offence operations are NATO and NATO Allies prepared to take to respond to what Russia is doing? Thank you.

JENS STOLTENBERG: From what we have seen today is that NATO Allies are able to disrupt to stop cyber-attacks and the best thing we can do is to strengthen our cyber resilience, our cyber defence so we are able to prevent, stop, disrupt cyber-attacks and that was what we saw today. We have seen how UK; the Netherlands have exposed the Russian GRU cyber-attacks against important international institutions and how they were able to do that by using intelligence and their own cyber capabilities. So, the best response is, of course, to be able to disrupt, stop these kinds of attacks and provide attribution and expose those who are behind these kind of cyber-attacks and that's what we have seen today. To strengthen that we need to further improve our intelligence. We have established a new intelligence division and we have become better in how we analyse and understand and work when it comes to intelligence both as individual NATO Allies and as alliance, as a whole. When and if and how we will use our national cyber capabilities in NATO missions and operations I think it will be very wrong if I started to speculate now about that. That will only create unnecessary uncertainty, so we will decide when we use that in the different missions and operations depending on the circumstances.

QUESTION: Just a very quick one, on the same subject. Lorne Cook, Associated Press. Did any Ally brief of a cyber-attack on any military installation or was it just these other ones that we've heard about, the more civilian, more organisational?

JENS STOLTENBERG: Today we were briefed by the UK and the Netherlands on the cyber-attacks which they have briefed us publicly about today and which they were able to expose. But, earlier, of course, we have been briefed about cyber-attacks against the military networks and military installations. That's actually something which is happening quite frequently and that is one of the reasons why the main focus of NATO has been to strengthen the defences of our own cyber networks to be able to defend our forces out in Afghanistan or elsewhere in the world we're operating because we need to protect our operations and missions and the cyber networks we are using there. So, we have increased our ability to defend our own networks and we have also established what we would call cyber teams, which can be deployed out to different missions and operations - NATO forces - to help them strengthen their cyber networks and protection if needed.

QUESTION: After the attacks in Salisbury NATO responded by kicking out a few Russian diplomats and denying accreditation. Will there be a similar response this time after these attacks?

JENS STOLTENBERG: The main response has been, as I said, that the NATO Allies - UK and Netherlands - have been able to disrupt and stop these attacks. The Russian military intelligence GRU did not succeed, they failed in their attack and that I think shows we have strengthened our ability to attribute and to defend ourselves. And there is an ongoing adaptation, ongoing strengthening of our cyber networks, our cyber defences, our cyber resilience with exercises, with higher awareness, with better technology and all that and that will continue and then we will establish cyber as a military domain and we are also establishing the new cyber operation centre.

Source: https://www.nato.int/cps/en/natohq/opinions_158705.htm?selectedLocale=en