News story: Defence Secretary to attend NATO meeting of Defence Ministers

From:
First published:
15 February 2017

Deputy UK Ambassador to NATO, Paul Johnston, announces that Defence Secretary, Michael Fallon, will meet new US Defence Secretary Mattis at NATO Defence Ministerial

This week's NATO Defence Ministerial is the first of the year and the first chance for Allies, including our Defence Secretary Michael Fallon, to meet collectively with the new US Defence Secretary Mattis.

Secretary Mattis knows NATO well from his time as Supreme Allied Commander for Transformation, a post he took up 10 years ago. But the security environment facing NATO has itself been transformed in the intervening decade. So this week's meeting is a chance for the 28 Allies to take stock on the challenges and opportunities we face, to the East and South of the Alliance, to reinforce the transatlantic bond and to affirm our commitment to deepening that link and our wider Allied engagement.

For the UK therefore, our priorities will be two-fold:

- to ensure the Alliance continues to make progress on taking forward the ambitious agenda agreed at Warsaw, in particular on modern defence and deterrence towards Russia. On that front (literally), the enhanced forward presence of NATO battlegroups is deploying this Spring to the Baltic States and Poland, with the UK proud to be leading the formation in Estonia, one of our most effective Allies in the Helmand campaign; and

- to take stock of what NATO has done since Warsaw to expand NATO's role in addressing instability on our Southern flank and beyond, including the new NATO Training and Capacity Building activity in Iraq, helping Iraqi security forces build their ability to secure the country after the defeat of Daesh.

All this requires resources and reform.

We are one of only four Allies other than the US currently meeting the NATO

target of spending 2% of GDP on defence. We support the new US Administration's focus on this burden-sharing issue.

But a more effective Alliance is not only about money. It's also about continuing to modernise our structures and ways of working to ensure the Alliance is capable of addressing simultaneously the complex and challenging world around us, including the scourge of terrorism.

So this week's Ministerial will help set this year's agenda. One where NATO builds on the achievements and decisions of the Wales and Warsaw Summits and, looking ahead to the next Summit later this year, shows it is gripping collectively the new challenges we will face together.

News story: Petunia Seaways and Peggotty report published

From:
First published:
15 February 2017

Collision between ro-ro freight ferry Petunia Seaways and historic motor launch Peggotty on the River Humber.

MAIB's report on the investigation of the collision between the ro-ro freight ferry Petunia Seaways and the historic motor launch Peggotty on the River Humber, UK on 19 May 2016 is now published.

The report contains details of what happened and the subsequent actions taken.

UN warns of civilian casualties in 'face to face' fighting in eastern Ukraine

14 February 2017 – Intensified fighting between Government and non-Government forces near densely populated areas in eastern Ukraine is endangering

civilians, the senior United Nations humanitarian representative in the country told reporters in Geneva today.

“The situation in eastern Ukraine is actually quite serious, you will be aware that between 21 January and 3 February the fighting intensity increased,” said Neal Walker, UN Resident Coordinator and Humanitarian Coordinator in Ukraine, citing frequent violations of the ceasefire and fighting near the towns of Avdiivka, Yasynuvata, Makiivka and Donetsk.

“There was extremely intense fighting from the 29th until the 3rd of February,” Mr. Walker recalled, noting that that the number of ceasefire violations exceeded 30,000 in a week or so, compared to less than 30,000 over the course of a month.

The conflict in eastern Ukraine erupted in March 2014. A ceasefire was eventually negotiated in Minsk, Belarus, in February 2015 but there have been frequent violations. The latest truce began on 23 December last year.

“The approximation of fighting forces, armed separatists in the east and Government troops, the distance separating them has narrowed, has narrowed incredibly,” Mr. Walker said. “And they are now face to face. You also have an increased presence of heavy weapons directly in violation of the Minsk accord.”

Mr. Walker also mentioned that the humanitarian situation is quite critical. “Let’s not forget temperatures in the past weeks have been between 10 and 20 below zero centigrade,” he said.

The UN Resident Coordinator also warned about environmental damage to critical civilian infrastructure due to shelling. “We have for instance a phenol chemical plant which has enormous potential to do severe environmental damage if the shelling is continued and it is damaged further,” he said.

“There are probably between 800,000 and one million IDPs (internally displaced persons) in government controlled areas of Ukraine,” Mr. Walker estimated. “We estimate another 200,000 have actually returned to non-government controlled areas from government controlled areas,” he added.

Since the beginning of the conflict, around 10,000 people have been killed in the violence, with civilian deaths on the rise.

Press release: PM call with US President Trump: 14 February 2017

From:
First published:

14 February 2017
Part of:

Prime Minister Theresa May spoke with US President Trump.

A Downing Street spokesperson said:

> The Prime Minister spoke to President Trump this afternoon, as part of their regular engagement. They discussed a range of issues, including trade and security and also discussed the President's upcoming state visit to the UK. The Prime Minister said she looks forward to welcoming him later this year.

Speech: Chancellor's speech at the National Cyber Security Centre opening

It is a pleasure to be here today at the launch of the National Cyber Security Centre, having been involved in this project, in various roles, since its inception.

In my current role, as Chancellor, I know how much the internet revolution has transformed our economy. And how much it holds the promise of future growth and prosperity for our country.

But as we enter the so-called 'Fourth Industrial Revolution', we have to be alive to the fact that this transformation is not without its challenges.

The development of artificial intelligence heralds a technological revolution that will fundamentally change our lives.

But it will also disrupt existing patterns of work, life, and society.

The fact is that the greater connectivity that will enable the development of the digital economy. Is also a source of vulnerability.

And those who want to exploit that vulnerability have not been idle.

The cyber attacks we are seeing are increasing in their frequency, their severity, and their sophistication. In the first three months of its existence, the NCSC has already mobilised to respond to attacks on 188 occasions.

And high-profile incidents with Sony, TalkTalk, and TV Monde have reminded us

of the scale of damage that a single successful cyber-attack can inflict.

So this new centre, and its work, is vitally important.

This is a unique institution.

Our overseas competitors can only dream of the level of interagency cooperation that underpins it.

And we in Britain can be extremely proud to be blazing a trail that others will surely follow.

There are three key points to make about the way the centre will approach its task.

First, it will not just focus on protecting against major attacks on critical national infrastructure, but also raising our security capability against day to day malicious cyber activity.

The most dramatic threats are the high-end sophisticated state-sponsored attacks.

But the most common threat that businesses and the general public face are the less sophisticated, mass targeted attacks, from phishing to email viruses.

83% of UK businesses are online.

The average British home has 8 devices connected to the internet.

This provides enormous potential for day to day attacks, from electronic data theft to online ransom.

The ONS estimate that there were two million such incidents in the past twelve months alone.

If these numbers were included in our crime figures, the UK’s crime rate would double.

So the NCSC will play a unique and crucial role bringing together the public and the business community on the one hand, and our intelligence and security agencies on the other.

Second, it will focus on partnership.

Our intelligence and security agencies are the best in the world. No question.

Our digital sector is also the best in the world – contributing a bigger proportion of our GDP every year than any other country in the G20.

And to prove it we have the highest proportion of online shoppers in Europe.

And what we are doing here is, bringing them together, this centre will work

hand in hand with industry to keep the UK safe.

65% of large businesses reported a cyber breach or attack in the past 12 months.

Yet nine out of ten businesses don’t even have an incident management plan in the event of a cyber breach. Business has to sharpen its approach as the scale of the threat from cyber increases and intensifies.

Just as you would expect a shop on the high street to fix its locks and burglar alarms, so businesses operating digitally need to fix their online security.

And this Centre stands ready to help them in doing that.

It can be as simple as providing guidance on things like ransomware and device security so that the public and businesses can protect themselves.

Or it could be drawing on our most sophisticated capabilities to road-test and make available safeguards against more sophisticated threats.

Or mobilising the resources of public and private sectors to intercept, defeat and mitigate the effects of a concerted cyber assault.

Either way, its success will rely on partnerships.

The third and final point I want to make is that we are prepared to invest the necessary resources to get this right.

We invested £860 million on enhancing our cyber defences in the last Parliament.

And we are investing another £1.9 billion to further bolster our armoury against cyber-attack in this Parliament, as well as developing our offensive cyber capability to deter, and if needs be, retaliate against, those who seek to do us harm in cyberspace, a new and critical domain of our defence.

And all this is set in the context of our commitment to meeting the NATO pledge to spend 2% of our national income on defence for every year of this decade.

At the beginning of this month, the UK signed the NATO Cyber Defence Memorandum of Understanding so that we can share our expertise with our international allies, and learn from their experiences.

And today I am delighted to announce a new kind of partnership, closer to home, here at this centre.

We will invite business to second up to 100 employees to come and work in the NCSC – allowing us to draw on the best and the brightest in industry – to test and to challenge the government’s thinking as we take this project forward.

And for these people to then return to the private sector and draw on their experience at NCSC to drive change within industry.

Because the government cannot protect businesses and the general public from the risks of cyber-attack on its own.

It has to be a team effort.

It is only in this way that we can stay one step ahead of the scale and pace of the threat we face. I want to thank the staff here at the Centre for their dedication, commitment, and skill.

And I want to thank our industry partners for teaming up with government, to ensure that the UK becomes truly, the safest and most secure space for digital business.

Thank you.