Speech: Foreign Secretary speech at the NATO cyber pledge conference

Welcome to the National Cyber Security Centre.

Two centuries ago, the seminal military theorist Carl von Clausewitz described what he called the “fog of greater or lesser uncertainty” that surrounds decision-making in times of conflict.

He wrote: “A sensitive and discriminating judgement is called for; a skilled intelligence to scent out the truth.”

Clausewitz was writing in the era of swords and muskets, and yet his warning also applies to the cyber age, when sabotage, theft and disruption can be carried out in seconds by an invisible adversary.

At first, the impact of any such attack – along with who did it and how – will be shrouded in a fog of uncertainty.

It takes the most sensitive and discriminating assessment to piece together the evidence and discover the guilty party.

This Centre seeks to perform that task and allow the British Government to take appropriate counter-measures.

In the first two years of its existence, it dealt with over 1,000 cases of malicious cyber activity in the UK – or about 10 incidents every week – mostly perpetrated by hostile states.

In 2017, hackers in North Korea infected thousands of computers with the Wannacry ransomware, inflicting damage across the world.

In France, several Renault factories were brought to a halt.

Here in Britain, 48 NHS hospitals were infected, something that made a particular impression on me because I was Health Secretary at the time.

Russian cyber activity

This Centre shares its world-leading expertise with Britain’s NATO allies and other friendly countries to strengthen our collective response to common threats.

Today, we judge that Russia’s intelligence services are targeting the critical national infrastructure of many countries in order to look for vulnerabilities.

This global campaign also seeks to compromise central government networks.

I can disclose that in the last 18 months, the National Cyber Security Centre has shared information and assessments with 16 NATO Allies – and even more nations outside the Alliance – of Russian cyber activity in their countries.

We have regularly provided technical knowledge to help our partners to counter the threat.

Deterrence in cyber age

Together, NATO countries have become better at defending themselves against dangers in cyber space.

But we should not be content with just making ourselves tougher targets – crucial though that is. Our primary goal must be to deter this kind of behaviour from happening in the first place.

NATO is the most successful military alliance in history precisely because of our collective power of deterrence, and that prevented nuclear war and helped to keep the peace for 70 years.

Our profound insight is that strength is the surest guarantee of peace – and when we stand together, no aggressor can hope to win a war so it never makes sense to start one.

The challenge today is therefore to apply the eternal verities at the heart of NATO’s success to the Alliance’s newest operational domain.

And that means deterrence – strengthening our joint ability to deter those who would harm our citizens in cyberspace.

We have already made important progress.

In 2014 the Allies agreed that a cyber attack could result in the invoking of Article V of the Washington Treaty, meaning that the incident would then be treated as an attack on every member of NATO.

The North Atlantic Council would take any such decision on a case-by-case basis.
Britain was the first ally to offer our offensive cyber capabilities to NATO. Another eight countries have since done the same.

Then in 2016, NATO leaders endorsed the Cyber Defence Pledge, recognising the “new realities of cyber threats”.

But we can and must do more to improve our response.

In particular, we should be more emphatic about what we consider to be unacceptable behaviour and the consequences for any breach of international law.

Interference in free elections

At particular risk are the democratic processes in all of our countries.

In the cyber age, authoritarian states possess ways of undermining free societies that dictators of earlier times would have envied.

Time and again, we have seen attempts by states to interfere in democratic elections, often through the use of proxies.

In 2014, Russian hackers calling themselves “CyberBerkut” sought to disrupt the presidential election in Ukraine, including by tampering with the voting system and delaying the final result.

In 2016, the Russian state interfered in the presidential election in the United States with the aim of damaging one party’s candidate.

Free elections are at the heart of our way of life.

The leaders and ministers of NATO countries have been raised up by the decisions of millions of voters, expressed through the ballot box. We can all be cast down in the same way.

But recent events demonstrate that our adversaries regard democratic elections as a key vulnerability of an open society.

If cyber interference were to become commonplace, the danger is that authoritarian states would damage public confidence in the very fabric of democracy.

We cannot afford to wait until one of our adversaries succeeds in changing the result of an election.

We must be crystal clear that any cyber operations designed to manipulate another country’s electoral system and alter the result would breach international law – and justify a proportionate response.

Together, we possess options for responding to any attacks that fall below the threshold for Article V.

We should be prepared to use them.

Deciding to do nothing would be an important decision in itself – and the consequences could be escalatory.

The more we communicate our resolve to act, the more we lower the risk of miscalculation.

The more we work together to develop an array of appropriate response options – and signal our willingness to employ them – the greater our power of deterrence.

As always, we need to balance clarity about our determination to act with constructive ambiguity about exactly what we would do in specific circumstances.

The EU gained one further option last week when we adopted a new sanctions regime, allowing the imposition of travel bans and asset freezes on those who carry out “cyber attacks with a significant effect”.

In conclusion let us remember that throughout history, every new technology has created risks and hazards.

The problems have often seemed daunting; the responses costly or uncertain. Yet so far, despite such challenges, we have always been equal to dealing with every advance.

So it must prove this time as we strengthen and adapt NATO’s power of deterrence – our priceless asset – to meet the challenge of the cyber age.