Speech: “Deterrence in the Cyber Age” speech by the Foreign Secretary

I’m delighted to be here at Glasgow University.

For centuries, this City and its University have been at the forefront of science, technology and medicine. The modern disciplines of physics and economics – and the Industrial Revolution itself – find their origins here. There could be no better setting for a speech about the challenges presented by the advance of new technology.

Just occasionally, even a Conservative Foreign Secretary should break with tradition, so I propose to begin by quoting the late Tony Benn.

In his book “Arguments for Democracy”, Benn wrote: “If one meets a powerful person ask them five questions: “What power have you got? Where did you get it from? In whose interests do you exercise it? To whom are you accountable? And how can we get rid of you’?”

And the final question is by far the most salient.

“If you cannot get rid of the people who govern you,” Benn wrote, “you do not live in a democratic system”. And he was right, of course.

The freedom to pass judgement on your leaders and change your government peacefully, through the ballot box, is the defining quality of a liberal democracy.

Millions of people have made immense sacrifices for the sake of that essential liberty.

Exactly three decades ago, the year 1989 saw the fastest advance of liberal democracy in history.

On 4th June, a free election in Poland triggered the fall of the Iron Curtain.

Within a decade, another 16 countries had broken the chains of dictatorship.

But what the Poles, Czechs and many others did not have to contend with in 1989 was the reality of cyber technology, a hugely powerful force for openness and transparency, but one that also possesses a dark side, capable of being used to subvert the very democratic processes we hold dear.

Threats to democracy in cyber age

So far, we’ve seen no successful interference in UK elections or referenda.

Yet in the cyber age, an authoritarian regime armed with nothing more ambitious than a laptop computer could try to manipulate our democracy.

In his book, The Perfect Weapon, David Sanger wrote that North Korea's leadership went from "viewing the internet as a threat to viewing it as a brilliant invention for levelling the playing field with the West".

Events have demonstrated how our adversaries regard free elections – and the very openness of a democratic system – as key vulnerabilities to be exploited.

In 2014, it was widely reported that Russian hackers calling themselves "CyberBerkut" tried to undermine the presidential election in Ukraine, including by tampering with the vote-counting system and delaying the final result. Last October, the British Government publicly confirmed that this group acts for Russia's GRU military intelligence service.

In 2016, the GRU targeted the United States, penetrating the email accounts of the national committee of the party that was then in control of the White House, before leaking information with the obvious aim of damaging its presidential candidate.

For every example of publicly attributed interference, there have been others that never saw the light of day. Whilst we cannot know for sure the effect of these operations, the material fact is that the Russian state has tried to subvert democracy.

And the implications are profoundly disturbing.

At a minimum, trust in the democratic process is seriously undermined.

But in a worst case scenario, elections could become tainted exercises, robbing the Governments they produce of legitimacy.

And the greatest risk of all is that a hostile state might succeed in casting a permanent cloud of doubt over an entire democratic system.

The uncomfortable truth of the cyber age is that authoritarian regimes possess ways of undermining free societies that yesterday's dictators would have envied.

During both World Wars – and despite the risk of invasion – British democratic institutions remained strong enough to remove Prime Ministers and change governments, in accordance with Tony Benn's rule. Through every year of conflict, Parliament continued to hold by-elections without fear of outside interference.

Yet in the cyber era, hostile states wouldn't need to fight wars or expend blood and treasure to subvert democracy. At long range and minimal cost – perhaps without even being discovered – their cyber experts could inject propaganda into an election campaign and target swing voters, in order to favour one party over another. In a country with an electronic voting system, they could potentially manipulate the result itself. Democracy can never be taken for granted but in the cyber age, the message is clear: Britain and other democracies need a strategic approach to safeguard the free institutions at the heart of our way of life.

Cyber deterrence

The UK is one of the leading cyber powers in the world and GCHQ possesses extraordinary expertise, benefiting every part of the country.

One of the reasons for that expertise is the great knowledge-base of our universities and I was very proud to visit the School of Computing Science here at Glasgow University.

Along with our allies, we have improved our collective ability to detect those responsible for malign actions in cyberspace, including election interference.

The Government has a £1.9 billion programme to protect British infrastructure and systems from cyber threats. The National Cyber Security Centre is doing excellent work to help safeguard British companies and institutions.

But we must go further.

Simply making it harder for our adversaries to inflict damage in cyberspace won't be sufficient on its own. Nor will verbal condemnation or written agreements create the taboo we should seek for the manipulation of democratic elections.

In 2013 and again in 2015, a UN Group of Governmental Experts affirmed that international law and the UN Charter applied to cyberspace, including the prohibition on interference in domestic affairs, which must cover elections.

Ironically, Russia was among the countries in the UN General Assembly that endorsed these reports. But treating the symptoms is never as effective as dealing with the cause.

We need a strategy that deters hostile states from intervening in free elections in the first place, a new doctrine of deterrence against cyber attacks in our democracies.

The very word "deterrence" summons images of nuclear-tipped confrontation between superpowers during the Cold War.

Henry Kissinger once wrote that a "new order of experience requires new ways of thinking" – and that is certainly true of the cyber age.

Today's tools are different from those of the Cold War and our responses must be different too.

The British Government's starting point is that we must impose a price on malicious cyber activity, including interference in elections, sufficient to deter authoritarian states. We won't always react identically to every individual incident and a cyber attack will not necessarily encounter a cyber response.

Instead, our approach to cyber deterrence has four principles.

First, we will always seek to discover which state or other actor was behind any malign cyber activity, overcoming any efforts to conceal their tracks.

Secondly, we will respond. That could include naming and shaming the perpetrator in public, in concert with our allies, exposing not only who carried out the action but, so far as possible, how it was done, thereby helping the cyber security industry to develop protective measures.

Thirdly, we will aim to prosecute those who conduct cyber crime, demonstrating they are not above the law.

And finally, with our allies we will consider further steps, consistent with international law, to make sure we don't just manage current cyber attacks but deter future ones as well.

Naming and shaming

Now one of the most powerful tools is the sunlight of transparency.

The British Government has already exposed a series of incidents, including the Russian cyber attacks in Ukraine, North Korea's infection of thousands of computers with ransomware – including the computers of 48 NHS Trusts – the targeting of 300 universities by an Iranian group, and the theft of commercial data by hackers acting for China's Ministry of State Security.

In every case, Britain made these attributions in the company of our allies. Fourteen countries joined us to expose China's actions; 19 publicised the operations of the GRU.

But a doctrine of deterrence will require us to go further.

The perpetrators must believe they run a credible risk of additional counter-measures – economic and diplomatic – over and above public embarrassment.

The European Union has agreed that economic sanctions, including travel bans and asset freezes, could be imposed to punish malicious action in cyber space.

Last October, Britain helped secure a decision by EU leaders to create a new sanctions regime for this express purpose. After Brexit, the UK will be able to impose cyber-related sanctions on a national basis.

As for diplomatic penalties, we won't hesitate to highlight any breaches of international agreements, such as when the operation by China's Ministry of State Security broke a bilateral agreement with the UK and a commitment from every G20 country not to conduct or support malicious activity of this kind.

Finally, Britain now has a National Offensive Cyber Programme, delivered by a Joint Mission between GCHQ and the Ministry of Defence.

The UK has already conducted offensive cyber operations against Daesh terrorists in the Middle East, designed to hinder their ability to carry out attacks, protect British and coalition forces, and cripple Daesh's online

propaganda.

The coalition to deter malign behaviour in cyber space and defend democracy needs to be as broad as possible. So the Foreign Office has 50 “Cyber Attaches” in British embassies around the world, charged with working alongside their host governments to raise the cost of malicious cyber activity and safeguard a free and secure internet.

We will increase their number by a further eight as we take forward the expansion of Britain’s diplomatic network. And today, we are helping over 100 countries to strengthen their cyber security, partially funded through our overseas aid budget. Among them are Commonwealth members, from Botswana to Jamaica, building on the Cyber Declaration agreed in London last year.

Conclusion

Gradually – and none too soon – the democracies of the world are joining forces to improve our response to the cyber manipulation of elections.

But after multiple recent attempts, we can no longer afford to wait until an authoritarian regime demonstrably succeeds in changing the outcome of an election and weakening trust in the integrity of democracy itself.

The risk is that after just a few cases, a pall of suspicion would descend over a democratic process – and once that happens, the damage would be difficult, perhaps impossible, to repair.

So now is the time for Britain and our allies to act together to protect democracy in the cyber age by deterring those who would do us harm.

Let me close with the words of a late Rector of this University, William Gladstone, who campaigned to extend the franchise with this phrase: “You cannot fight against the future. Time is on our side.”

We too cannot resist the future represented by the cyber age.

But we must safeguard the ability of the British people, secured by Gladstone and many others, to vote in a free and fair election safe from outside sabotage.