British Embassy
Rome

Master in Cybersecurity,
Speech by H.E. Jill Morris CMG, HMA to Italy and San Marino delivered at La Sapienza University on 14/10/19

UK's cyber diplomacy: for a free, open, peaceful and secure cyberspace

Check Against delivery / liberamente illustrato

Good afternoon and thank you so much for the invitation to speak you about the UK's approach to cyber diplomacy and our efforts for a free, open, peaceful and secure cyberspace.

Cyber diplomacy is a relatively new concept. And its newness reflects our changing world – our new virtual world and how it relates to national interests. As such, cyber diplomacy covers everything from security to trade, from freedoms to governance. The big question is how do we conduct ourselves in cyberspace? What are the rules of diplomacy outside the traditional geopolitics that we know and understand so well?

The UK answer to this is simple: **cyber space is no different to any other domain**. Just as on land, at sea, in the air and in space, the same rules apply, so is true in cyber space. And, the same human rights apply online as they do offline. Essentially, the same tools we use for traditional diplomacy can be used to help maintain peace and build confidence between stakeholders in cyberspace.

As technological development offers increasing opportunities for economic and social development worldwide, it also increases reliance on networks that expand beyond national borders. We believe that a global network that is **free, open, peaceful and secure** best serves our security and prosperity.

What is more, we believe that the alternative - greater control of the internet by states or international organisations - risks stifling the dynamism that drives innovation on the internet and the platform for growth it provides, as well as impeding human rights such as freedom of expression.

So, perhaps for a moment, I can pause and spell out what we mean by free, open, peaceful and secure.

FREE means trusted by individuals who are able to act and enjoy rights online as they do offline, fostering economic and political stability. We want governments and corporations to adopt transparent, human rights compliant frameworks that give users freedom of expression whilst protecting them from abuses.

OPEN means interoperable across borders and accessible to all. Openness is central to the flows of goods, services, capital, data and skills that underpin our economy. Standards agreed by internet organisations should preserve interoperability, and data localisation trends should be resisted.

PEACEFUL means a clear understanding of acceptable state behaviour and the applicability of international law in cyberspace, fostering strategic stability and reducing cyber attacks. Norms of state behaviour in cyberspace should be widely agreed and promoted, and there should be a high cost to malicious state activity in cyberspace.

SECURE means software, hardware, and systems, which have been designed from the ground up, to be secure. We want global cyber security baselines, cooperation on incident management, threat sharing and upstream interventions via capacity building to help reduce incidence and impact to the UK and to all.

But of course, none of this is a given. The UK view is not shared universally and there are definitely areas where we are still working out the contours of our collective understanding, particularly in the 'peaceful' strand of our vision.

For example, what constitutes an 'attack' in cyber warfare and what is an effective and proportionate response? And this is where the diplomacy angle comes in.

The UK conducts cyber diplomacy in both traditional and new ways. We work **bilaterally**, with traditional allies like Italy, as well as new partners to establish and maintain strong, active political and operational relationships; creating the political conditions to build strong global alliances;

We work **multilaterally**, working effectively with our partners within multilateral organisations such as the United Nations, G7, G20, European Union, NATO, OSCE, and Council of Europe and within the global development community to protect the Rules Based International System (and I shall return to this in a moment); and

We also work **through multi-stakeholderism**, that is to say beyond the traditional remit of diplomacy – with various **non-state actors** from **industry**, **civil society**, **academia** and the **technical community**. These actors are crucial in informing and challenging international policy formulation, and strengthening political messages on a wide range of cyber issues.

This **multi-stakeholder approach** is fundamental to our vision for cyberspace. The UK believes that governments do not exercise exclusive control of the cyber domain, particularly when relevant infrastructure is largely owned and operated by the private sector, which also produces the products and services we use.

Rules Based International System

Whatever our approach, the UK's driving aim on cyber diplomacy is to protect the **Rules Based International System**, which is based on norms, rules and alliances. The RBIS has increased states' ability to resolve their differences peacefully, and provided a framework for the greatest sustained rise in prosperity which mankind has ever enjoyed.

Now, more than ever, the world needs the commitment of all to the system of rules that we collectively established. The current system is not perhaps perfect, but the UK is committed to working with others to ensure the Rules Based International System is relevant and effective to face 21st century challenges.

So will continue to encourage all states to take action to set out the rules of the road for cyberspace – including engaging constructively with the state-led, dual track process currently underway at the UN which are considering state behaviour in cyberspace, and we will assist others to uphold these rules and take collective action when these rules are broken.

As I hinted at earlier, central to achieving this is developing an agreement on the **application of existing international law and norms of state behaviour in cyberspace** and promoting deeper international understanding of these rules.

We believe the foundation for responsible state behaviour in cyberspace is our **mutual commitment to existing international law**, including the respect for human rights and fundamental freedoms, and the application of international humanitarian law to cyber operations in armed conflict.

The UK reaffirms that the **UN Charter applies in its entirety** to state actions in cyberspace, including the prohibition of the use of force; the peaceful settlement of disputes; and the inherent right of states to act in self-defence in response to an armed attack.

It is also our view that the **law of state responsibility applies to cyber operations in peacetime**, including the availability of the doctrine of countermeasures in response to internationally wrongful acts.

The former Attorney General set out UK views on the application of international law in cyberspace for the first time in his speech at Chatham House in May last year. Among other things, he said that **"*cyberspace is not – and must never be – a lawless world*"** and that **"*when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain.*"**

Of course, agreeing the rules is one thing, but we will only realise our shared objective of lasting stability in cyberspace if those rules are actively applied. That means developing Confidence Building Measures and the building of global capacity to put them into practice. These can be mutually reinforcing, helping to demonstrate trust and transparency between states in cyberspace, providing risk mitigation and helping reduce tensions. For example, the

Dinard Declaration on the Cyber Norm Initiative at this year's G7 provides the opportunity for us to set out how we adhere to the norms we have agreed.

Deterrence

Realising our vision for cyberspace means we must also impose a cost on malicious cyber activity, including interference in elections, sufficient to deter states that choose to engage in such activity. We won't always react identically to every individual incident and a cyber attack will not necessarily encounter a cyber response.

But, it is important that States have a toolbox of response options, including public attribution, economic and diplomatic counter measures, including sanctions where necessary. The EU has also recognised the importance of having a range of options available, and standing together, in implementing an EU cyber toolbox and a cyber sanctions regime.

Driving our prosperity

But it is not all doom and gloom… As I mentioned, cyber is a driver of prosperity as well as of peace and security. The UK has the highest percentage of individual internet usage of any G7 economy. We are among the world leaders on Digital Government. Digital accounts for a growing share of our economy and workforce.

But this means that cyber security is also a serious matter for UK business. Breaches are costly and disruptive issue. Just under half of all businesses in the UK identified one breach or attack in the last year.

So the UK's cyber diplomacy is also about demonstrating leadership and championing success and innovation. That is built on great efforts to build and sustain our own cyber capabilities.

Under the **cross-Government National Cyber Security Strategy**, we are working to maintain and enhance the UK's leading cyber security research capability, and enable innovation to improve the nation's cyber security and resilience, working with universities and research institutes to ensure we identify future challenges and opportunities created by developments in science and technology.

As part of a £1.9 billion transformative programme, in October 2016, we launched **the National Cyber Security Centre** to help make the UK the safest place to live and work online. Bringing together expertise from across the UK government and acting a single point of contact for the public sector, the private sector (including SMEs) and the general public, the National Cyber Security Centre helps to:

- understand cyber security, and distil this knowledge into practical guidance that is made available to all;
- respond to cyber security incidents to reduce the harm they cause to organisations and the wider UK;
- use industry and academic expertise to nurture the UK's cyber security capability;
- reduce risks to the UK by securing public and private sector networks.

The NCSC now deals with around 50 serious cyber attacks every month – not the total number, just those cases serious enough to warrant NCSC involvement. The majority of these incidents were, we believe, perpetrated from within nation states in some way hostile to the UK.

While nation state activity is the most acute threat, low-sophistication but high-volume cyber crime is the most chronic one. These amount to a strategic threat to our prosperity by undermining confidence in the digital economy. That is why the NCSC's active cyber defence (ACD) initiative – using automation to reduce some of the most common weaknesses in cyber security defences – is one of the the NCSC's most important pieces of work.

One example of how this initiative is having tangible results: since the programme started, the proportion of phishing sites in the world that are hosted in the UK has fallen from 5.3 per cent to 2.4 per cent.

The NCSC aspires to be a truly national centre, reflecting, and being present in, communities across the UK. We are particularly proud of the work the NCSC does in schools, particularly through the CyberFirst Girls Competition which this year attracted more than 4500 highly talented 12 and 13 year-old female students with an interest in cyber security.

So where next?

Among the conclusions we have already drawn from our first, comprehensive National Cyber Security Strategy, published in 2016, is that the scale and complexity of cyber means it cannot be addressed by Government alone, and requires a truly national and international response. In the long term, our ambition is that cyber security should become business as usual for the UK – a part of everything we do, including diplomacy.

We should also bear in mind that cyber security represents a significant opportunity, not simply a risk. Better security should go hand in hand with digital transformation, which has the potential to unlock growth and innovation for businesses and citizens around the world.

Finally, the Rules-Based International System is still the best means we have to respond to the significant global threats and challenges we face, but it needs all our support, especially when others try to challenge it, if it is to remain effective and relevant.

The UK is determined to stand up for shared interests and values through all diplomatic channels and means of influence. This means fighting to strengthen and defend the values that matter to us most: human rights, peaceful resolution of disputes and the rule of law. The UK's focus will be on positive practical measures that States could take to put voluntary norms into practice.

Given what is at stake for our prosperity and security, there may be no more vital mission for this and the next generation of diplomats. This is what cyber diplomacy means to the UK.