

News story: Julie Lennard appointed Chief Executive of DVLA

Julie Lennard has been appointed as the new Chief Executive of the Driver Vehicle Licensing Agency (DVLA).

Ms Lennard will take up the post shortly and has been DVLA's interim Chief Executive since March. Prior to this she was DVLA's Director of Strategy, Policy and Communications, held since August 2014.

Department for Transport Permanent Secretary Bernadette Kelly said:

It is with great pleasure that I welcome Julie Lennard to the role, leading DVLA at such an important time as it develops into a digital hub for motorists. Julie is an experienced and talented leader and brings a wealth of experience to this crucial role.

Ms Lennard is the first woman to be appointed as DVLA's Chief Executive. In her previous role as Director of Strategy, Policy and Communications, Julie was responsible for delivering the organisation's business strategy and policy development, overseeing a directorate that also includes data protection, Parliamentary liaison and communications.

Prior to this, Julie worked at The National Archives where her responsibilities included developing strategic policy relationships with senior stakeholders and overseeing Parliamentary and legislative issues.

Julie has also worked for Which? one of the largest independent consumer organisations in Europe, in a range of roles including as a journalist and representing the campaigning organisation to government departments, agencies and other stakeholders at a national and international level.

Roads media enquiries

Media enquiries

020 7944 3021

Out of hours media enquiries

020 7944 4292

Switchboard

0300 330 3000

[Press release: Plant nurseries will remain exempt from business rates](#)

Owners of plant nurseries will continue to benefit from a business rates exemption thanks to government legislation introduced today (Wednesday 23 May) by Local Government Minister Rishi Sunak MP.

For nearly a century, land and buildings at plant nursery grounds enjoyed an agricultural exemption from business rates to support the rural economy.

However, following a recent Court of Appeal decision, the Valuation Office Agency has begun to assess buildings at plant nurseries, including structures such as poly-tunnels.

Local Government Minister, Rishi Sunak MP, said:

Plant nurseries are an essential part of the rural economy and it is vital they are protected.

This legislation will put a stop to this unreasonable burden on businesses and will help maintain a productive, competitive and sustainable agricultural sector.

Under the legislation, plant nursery owners who have been paying rates since the Court of Appeal decision will be able to apply for a backdated refund.

Further information

Read the [Non Domestic Rates \(Nursery Grounds\) Bill](#) introduced today.

Plant nurseries are establishments where plants or trees are grown in the initial stages of their lives. The bill does not extend to garden centres where plants are displayed and sold to the public (including garden centres sometimes called “nurseries”). Garden centres are rateable and will continue to pay rates after the Bill.

The Bill will amend the Local Government Finance Act 1988 to ensure both agricultural land and buildings at plant nursery grounds are exempt from business rates.

The legislation will be amended retrospectively, with effect from 1 April 2015. Any plant nurseries charged business rates from this date will be eligible to apply for a refund.

We have also published a [factsheet](#) on the Bill.

Office address and general enquiries

2 Marsham Street

London
SW1P 4DF

Contact form

<http://forms.communiti...>

General enquiries: please use this number if you are a member of the public
030 3444 0000

Media enquiries

Email

newsdesk@communities.gsi.gov.uk

Please use this number if you are a journalist wishing to speak to Press
Office
0303 444 1209

Social media – MHCLG

Twitter – <https://twitter.com/mhclg>

Flickr – <http://www.flickr.com/photos/mhclg>

LinkedIn – <http://www.linkedin.com/company/mhclg>

[News story: New Chair of the Social Mobility Commission recommended](#)

Education Secretary Damian Hinds has today (23 May) recommended Dame Martina Milburn as the preferred candidate for the position of Chair of the Social Mobility Commission.

Dame Martina has been put forward as the preferred candidate after showing that she had the skills and experience to drive forward the work of improving equality of opportunities for disadvantaged young people. She has spent 14 years as Chief Executive of the Prince's Trust, supporting more than 450,000 disadvantaged young people across the country in that time, with three in four of these going on to work, education or training.

Since 2004 she has led work to remove the barriers too many young people still face, including more than 100,000 through 'Achieve' – an education programme that helps those at risk of exclusion from school – and projects that improve young people's emotional wellbeing and resilience. Dame Martina also oversaw the charity's expansion by integrating the Fairbridge personal development programme and Mosaic, a mentoring initiative, extending links with young people from deprived inner-city areas and those from Muslim communities.

She is also a non-executive director of the National Citizen Service and the Capital City College Group, and was previously Chief Executive of BBC Children in Need and of the Association of Spinal Injury Research, Rehabilitation and Reintegration.

Education Secretary Damian Hinds said:

Dame Martina has spent her career as a tireless champion for underprivileged children, young people and their families, providing better opportunities for them to fulfil their potential. Her leadership of the Prince's Trust has improved the education, skills and self-esteem of thousands of young people, and will be key in progressing our social mobility agenda.

I am grateful to her predecessor Alan Milburn, whose work as Chair of the Commission over five years shone a light on the injustices that still exist too frequently in this country. I look forward to working with Dame Martina as she works with us to eliminate them.

The recommendation comes as the Department for Education publishes its [response](#) to the Education Select Committee's report on the future of the Social Mobility Commission.

Dame Martina was chosen out of a competitive field of applicants, and demonstrated strong commitment to the values of the Commission during the assessment process.

Dame Martina Milburn said:

It is a privilege to be put forward to Chair the Social Mobility Commission. I hope my experience of working closely with and listening to young people from different backgrounds will help make a difference.

The Chair of the Social Mobility Commission will hold the government and Ministers to account on its work to spread opportunity evenly across the country.

The Secretary of State for Education will now ask Robert Halfon MP, Chair of the Education Select Committee, to arrange for the committee to meet Dame

Martina. He will consider the committee's conclusions before deciding whether to proceed with the appointment.

Press release: UK to lead global challenge to clean up carbon

- UK to lead global challenge to reduce the cost of innovative new carbon capture technology
- UK strategy to reduce costs and capture global export opportunities
- £21.5 million of UK funding for ground-breaking projects to capture CO₂ emissions

Energy Minister Claire Perry has today (Wednesday 23 May) announced the UK is to lead an international challenge with Saudi Arabia and Mexico to remove carbon from emissions. It will be a unique opportunity to enable an up and coming technology to scale up by working together with other countries.

It is one of 7 Mission Innovation challenges announced in 2015 at COP21 with the UK setting out £21.5 million of funding for innovative new Carbon Capture, Utilisation and Storage (CCUS) technologies.

The aim of the funding is to invest in innovation that could reduce the cost of the technology by supporting its development so that CCUS can become commercially viable at scale.

CCUS is where carbon from power stations or industry is captured then either used for industrial applications or transported to be stored safely underground, reducing pollution from the air we breathe.

While there are currently 22 plants in operation or construction, the UK has the opportunity to become a world leader in this field.

There is a global consensus that carbon capture will be critical in meeting the aims of the Paris Agreement and supporting clean growth. This technology can capture carbon dioxide emissions from industry or power generation as well as support low carbon hydrogen production.

Energy and Clean Growth Minister, Claire Perry said:

My ambition is for the UK to become a global technology leader in carbon capture, working with international partners to reduce its costs. As the UK has led the debate globally on tackling climate change and pioneering clean growth, we are leading this global challenge with an initial £21.5 million investment in CCUS innovation – a key part of our [modern Industrial Strategy](#).

UK companies are already involved in some of the most innovative CCUS projects internationally, and just this week a ground-breaking negative emissions [bio-energy project at Drax Power Station in Yorkshire was launched](#).

The [Clean Growth Strategy](#) sets out the new Government approach to CCUS in the UK, highlighting the important role of innovation in supporting cost reduction. Government has committed to spend up to £162 million to improve CCUS and industrial energy efficiency.

As well as the potential to help us reduce our emissions in industries through the manufacture of concrete, chemicals, steel, there are also opportunities to maximise economic opportunities for the UK through new technologies and the supply chain.

Government is working with industry to adopt CCUS in the UK by reducing its costs and capturing the export opportunities, and a CCUS Cost Challenge Taskforce will report to government in July this year. Energy Minister Claire Perry will host an international CCUS summit with the International Energy Agency, in Edinburgh later this year.

The UK's modern Industrial Strategy is a long-term plan to build a Britain fit for the future through a stronger, fairer economy. Through this we will help businesses to create better, higher-paying jobs – setting a path for Britain to lead in the high-tech, highly-skilled industries of the future.

As part of this, the modern Industrial Strategy sets out 4 Grand Challenges, including Clean Growth – Ensuring the UK is at the forefront of innovation and maximising the advantages for UK industry in the global shift to clean growth.

Notes to editors

1. The [Carbon Capture Challenge](#) is one of 7 Mission Innovation challenges announced in 2015 at COP21. The Carbon Capture Challenge is focused on addressing the innovation challenges CCUS presents, for example enhancing innovation for carbon capture technologies to reduce the cost of the technology and support the technology's development.
2. A call for CCUS innovation will offer £15 million of grant funding for projects up to 28 months and will be available to 31 March 2021. BEIS will consider grants of up to £5 million for a single project. Both projects that are UK-led or that involve collaboration with an international partner will be considered.
3. BEIS and UKRI has committed £6.5 million to the [2nd call of the Accelerating Carbon Technologies \(ACT\) Research Programme](#). This research and development programme is made up of 10 European countries (5 of which are involved in the CCUS Mission Innovation Challenge – Norway, The Netherlands, Germany, France and UK). The overall grant available from all the countries involved amounts to approximately €25 million.
4. Further information is available on [how to apply for funding and about the programmes](#).

Speech: Cyber and International Law in the 21st Century

CHECK AGAINST DELIVERY

I am particularly pleased to be speaking here, at Chatham House Royal Institute for International affairs, which has a longstanding record of engaging governments, the private sector and civil society in debate about the most significant and pressing developments in international affairs.

Today I want to talk about the importance of international law in cyber space and to emphasise that cyber space is an integral part of the rules based international order. That being so, it is the UK's view that there are boundaries of acceptable state behaviour in cyberspace, just as there are everywhere else.

One of the biggest challenges for international law is ensuring it keeps pace as the world changes. International law must remain relevant to the challenges of modern conflicts if it is to be respected, and as a result, play its critical role in ensuring certainty, peace and stability in the international order. If it is seen as irrelevant it will be ignored and that makes the world less safe.

Whilst the need to adapt to changing times is true of all law, international law is unusual – other types of law are found in statutes and in court judgments – but there are few of either in international law, instead there are treaties, and customary international law formed from the general and consistent practice of states acting out of a sense of obligation.

The necessity of international law keeping pace with the modern world underpinned my speech at the International Institute for Strategic Studies on the modern law of self- defence in January 2017. In that speech, I set out how the law of self-defence must adapt to meet the particular demands of a world in which an armed attack is as likely to be inspired by something on the internet as it is to be instructed by someone in direct contact with the perpetrator, and where we can't see such an attack coming in the way we once could.

I made that speech last year because I believe that a nation like ours should be open and clear in setting out the rules it feels bound by. In doing so, we demonstrate not just our commitment to the rules based international order, but also our leadership in its development.

I am here today in pursuit of the same goal.

There are few areas in which the world has moved faster than in the development of cyber technology. Cyber has become a noun and a prefix meaning

anything including or relating to computers, especially the internet.

And cyber is everywhere – in the light transmitted along millions on miles of optical fibre cables crossing the deep ocean floor, from our homes to the battlefield and on the display screens of stock markets across the world. It is increasingly the means by which we communicate in every sphere of our lives, locally and globally.

Right now, the impact of the internet is near universal. Even those not online themselves are using public or private sector services whose operations depend on interconnectivity via cyberspace. We have moved from a country and a world operating in analogue, to one where almost every aspect of daily life is affected by cyber activity.

In addition to the enormous opportunities for further freedom, understanding, advancement, global connectivity and prosperity, the cyber domain is now one of the primary means through which states conduct their international relations, both in peacetime and in times of conflict. It features in the risk assessments of Ministers, diplomats, intelligence officials and military leaders. The growth of cyber technology has also meant that the threats we face as nations have never been as widespread or as complex. And this complexity is easily exploited.

Yet, despite this ubiquity, until a few years ago, the international community had yet to agree whether there were any applicable rules in cyber space at all. The academic community has been quick to fill the gap and academics have made valuable contributions to the debate, but states have remained relatively quiet.

This is in part due to the fact that cyber technologies develop at an unprecedented pace. It is also no doubt due to the fact that these technologies are uniquely accessible to a wide range of state and non- state actors, crossing a number of legal and practical boundaries and frameworks and resulting in unparalleled complexity. The development and use of these technologies can also stray into highly sensitive areas that governments have been traditionally unwilling to publicly comment on or to debate.

But the truth is, as authors and subjects of international law, states have a responsibility here. A responsibility to be clear about how our international law obligations bind us. A responsibility we fulfil through our treaty obligations, our actions and our practice, as well as through our public statements. And a responsibility I believe extends to cyberspace.

The very pervasiveness of cyber makes silence from states on the boundaries of acceptable behaviour in cyberspace unsustainable. If we stay silent, if we accept that the challenges posed by cyber technology are too great for the existing framework of international law to bear, that cyberspace will always be a grey area, a place of blurred boundaries, then we should expect cyberspace to continue to become a more dangerous place.

Those around the world whose behaviours international law seeks to constrain of course resent it, and they will seize on any excuse to say international

law is outdated and irrelevant and can therefore be ignored. We must not give them that opportunity by conceding that applying international law principles to cyberspace is just too difficult.

And we need not, and should not, make that concession.

Cyber space is not – and must never be – a lawless world. It is the UK's view that when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain. The UK has always been clear that we consider cyber space to be an integral part of the rules based international order that we are proud to promote. The question is not whether or not international law applies, but rather how it applies and whether our current understanding is sufficient.

What this means is that hostile actors cannot take action by cyber means without consequence, both in peacetime and in times of conflict. States that are targeted by hostile cyber operations have the right to respond to those operations in accordance with the options lawfully available to them and that in this as in all things, all states are equal before the law.

These are principles best developed with others.

UK has made great efforts across the last decade to develop shared understanding and agreement on how international law applies in cyberspace. We have engaged across UK government departments and agencies and worked closely with industry; we have consulted with academics, international organisations and the wider international law community. And we have engaged both bilaterally, regionally and multilaterally with our international counterparts in other states and those in international organisations – some of whom I am very pleased to see here today.

To build international consensus on the role of international law in this area, the UK, together with other states, has engaged in negotiations under a mandate from the UN Secretary General to progress multilateral agreement on the parameters of responsible state behaviour in cyberspace.

In 2013, the UN Group of Governmental Experts on the use of cyber technologies, affirmed the application of existing international law to states' cyber activities. On 26 June 2015, the UN Expert Group, including not just the UK and the US but also Russia and China recognised that the UN Charter applies in its entirety to cyberspace. The Group affirmed the relevance of a state's inherent right to act in self-defence in response to a cyber operation meeting the threshold of an armed attack. In addition, the 2015 Report confirmed that the fundamental protections of international humanitarian law: necessity, proportionality, humanity and distinction, apply in cyberspace.

Whilst these may seem to be cautious advances, it is no small achievement given negotiations involved states with vastly different resources, cyber capabilities, and approaches to international law. And in the current political climate, the fact that consensus was achieved at all among the nations I have mentioned is not to be underestimated.

So wherever possible we can and should work with others, but every state should be clear about the legal principles and thresholds it believes apply in cyberspace and I want to be as clear as I can be about the UK's position.

Perhaps the most useful starting point is the UN Charter and three specific rules are particularly relevant.

First, there is the rule prohibiting interventions in the domestic affairs of states both under Article 2(7) of the Charter and in customary international law. This prohibition means that any activity in cyber space which reaches the level of such an intervention is unlawful. Any activity of this nature by a state could only become permissible in response to some prior illegality by another state.

The next relevant provision of the UN Charter is in Article 2(4) which prohibits the threat or use of force against the territorial independence or political integrity of any state. Any activity above this threshold would only be lawful under the usual exceptions – when taken in response to an armed attack in self-defence or as a Chapter VII action authorised by the Security Council. In addition, the UK remains of the view that it is permitted under international law, in exceptional circumstances, to use force on the grounds of humanitarian intervention to avert an overwhelming humanitarian catastrophe.

Thirdly, the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter.

If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means.

And in addition to the provisions of the UN Charter, the application of international humanitarian law to cyber operations in armed conflicts provides both protection and clarity. When states are engaged in an armed conflict, this means that cyber operations can be used to hinder the ability of hostile groups such as Daesh to coordinate attacks, and in order to protect coalition forces on the battlefield. But like other responsible states, this also means that even on the new battlefields of cyber space, the UK considers that there is an existing body of principles and rules that seek to minimise the humanitarian consequences of conflict.

Of course there are also particular challenges posed by the international law

that regulates cyber activities in peacetime. I have already touched on the prohibition against interventions in the internal affairs of states.

In certain circumstances, cyber operations which do not meet the threshold of the use of force but are undertaken by one state against the territory of another state without that state's consent will be considered a breach of international law.

The international law prohibition on intervention in the internal affairs of other states is of particular importance in modern times when technology has an increasing role to play in every facet of our lives, including political campaigns and the conduct of elections. As set out by the International Court of Justice in its judgment in the Nicaragua case, the purpose of this principle is to ensure that all states remain free from external, coercive intervention in the matters of government which are at the heart of a state's sovereignty, such as the freedom to choose its own political, social, economic and cultural system.

The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space. But the practical application of the principle in this context would be the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system. Such acts must surely be a breach of the prohibition on intervention in the domestic affairs of states.

Furthermore, a breach of this principle of non-intervention provides victim states with the ability to take action in response that would otherwise be considered unlawful, but which is permissible if it is aimed at returning relations between the hostile state and the victim state to one of lawfulness, and bringing an end to the prior unlawful act. Such action is permissible under the international law doctrine of countermeasures. Put simply, if a hostile state breaches international law as a result of its coercive actions against the target state's sovereign freedoms, then the victim state can take action to compel that hostile state to stop.

Consistent with the de-escalatory nature of international law, there are clear restrictions on the actions that a victim state can take under the doctrine of countermeasures. A countermeasure can only be taken in response to a prior internationally wrongful act committed by a state, and must only be directed towards that state. This means that the victim state must be confident in its attribution of that act to a hostile state before it takes action in response. In cyberspace of course, attribution presents particular challenges, to which I will come in a few moments. Countermeasures cannot involve the use of force, and they must be both necessary and proportionate to the purpose of inducing the hostile state to comply with its obligations under international law.

These restrictions under the doctrine of countermeasures are generally accepted across the international law community. The one area where the UK departs from the excellent work of the International Law Commission on this

issue is where the UK is responding to covert cyber intrusion with countermeasures.

In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it. The covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.

In addition, it is also worth stating that, as a matter of law, there is no requirement in the doctrine of countermeasures for a response to be symmetrical to the underlying unlawful act. What matters is necessity and proportionality, which means that the UK could respond to a cyber intrusion through non-cyber means, and vice versa.

Through the principle of non-intervention, it is clear that the international community has set a boundary at which interference in another state's sovereign freedoms is considered internationally wrongful and as such, in breach of international law, giving rise to the right to take action which may otherwise be unlawful in response. As I have already mentioned, the precise parameters of this principle remain the subject of ongoing debate in the international law community, but a further contested area amongst those engaged in the application of international law to cyber space is the regulation of activities that fall below the threshold of a prohibited intervention, but nonetheless may be perceived as affecting the territorial sovereignty of another state without that state's prior consent.

Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent.

Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.

Online as well as everywhere else, the principle of sovereignty should not be used by states to undermine fundamental rights and freedoms and the right balance must be struck between national security and the protection of privacy and human rights.

I have talked about the behaviour to be expected of states in cyberspace and their entitlement to defend themselves, but having a legal framework within which to act is not the same as having the practical capacity to act, and the UK needs that too.

One of the biggest challenges for a state that finds itself a victim of a hostile cyber operation is determination of who was behind it. Without clearly identifying who is responsible for hostile cyber activity, it is

impossible to take responsible action in response.

There are obviously practical difficulties involved in making any attributions of responsibilities when the action concerned is capable of crossing traditional territorial boundaries and sophisticated techniques are used to hide the identity and source of the operation. Those difficulties are compounded by the ready accessibility of cyber technologies and the resultant blurring of lines between the actions of governments and those of individuals.

The international law rules on the attribution of conduct to a state are clear, set out in the International Law Commissions Articles on State Responsibility, and require a state to bear responsibility in international law for its internationally wrongful acts, and also for the acts of individuals acting under its instruction, direction or control.

These principles must be adapted and applied to a densely technical world of electronic signatures, hard to trace networks and the dark web. They must be applied to situations in which the actions of states are masked, often deliberately, by the involvement of non-state actors. And international law is clear – states cannot escape accountability under the law simply by the involvement of such proxy actors acting under their direction and control.

But the challenge, as ever, is not simply about the law. As with other forms of hostile activity, there are technical, political and diplomatic considerations in publicly attributing hostile cyber activity to a state, in addition to whether the legal test is met.

There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based, or to publicly attribute hostile cyber activity that it has suffered in all circumstances.

However, the UK can and does attribute malicious cyber activity where we believe it is in our best interests to do so, and in furtherance of our commitment to clarity and stability in cyberspace. Sometimes we do this publicly, and sometimes we do so only to the country concerned. We consider each case on its merits.

For example, the WannaCry ransomware attack affected 150 countries, including 48 National Health Service Trusts in the United Kingdom. It was one of the most significant attacks to hit the UK in terms of scale and disruption. In December 2017, together with partners from the US, Australia, Canada, New Zealand, Denmark and Japan, we attributed the attack to North Korean actors. Additionally, our attribution, together with eleven other countries, of the destructive NotPetya cyber-attack against Ukraine to the Russian government, specifically the Russian Military in February this year illustrated that we can do this successfully. If more states become involved in the work of attribution then we can be more certain of the assessment. We will continue to work closely with allies to deter, mitigate and attribute malicious cyber activity. It is important that our adversaries know their actions will be held up for scrutiny as an additional incentive to become more responsible

members of the international community.

Addressing our capacity more broadly, in November 2016, the Government launched its new National Cyber Security Strategy, which included the establishment of the National Cyber Security Centre with a mandate to pursue the action required to better protect the UK's interests in cyberspace.

As part of its strategy, the Government is investing 1.9 billion in cyber security.

And the UK's active cyber defence programme has now been underway for over a year. In this time it has prevented on average 4.5 million malicious emails per month and has carried out more than 1 million security scans and 7 million security tests on public sector websites.

In tandem, our National Offensive Cyber Programme is building a dedicated capability allowing the UK to act in cyberspace. We believe each state has the right to develop a sovereign offensive cyber capability. It does not destabilise nor weaponise cyber space to do so, as there is an obligation on each state to ensure use and development are carried out in accordance with international law. We have therefore been and will continue to be transparent about the existence of this programme.

As I have outlined, the UK is a leading voice on cyber at an international level: in the United Nations and in regional organisations including the Organisation for Security Co-operation in Europe.

In 2010 the UK Foreign Office initiated the London Process, an annual global conference on cyber space which has now become an established annual event. Subsequent conferences have taken place in Hungary, South Korea, the Netherlands and India and welcomed attendees from over 120 countries and from governments, academia and the private sector.

Cyber security is something which this Government has consistently taken very seriously. It remains a very significant threat to the UK's economic and national security – we all need to play our part and take responsibility as individuals, organisations and businesses. Much of the work of the NCSC and other parts of Government in cyber defence is in this area – helping all of us to help ourselves and to keep the UK as the safest place to be online.

But for all the work I have described, both domestic and international, it remains the case that defining the appropriate principles of international law to apply to cyberspace is difficult. Around the world there are many who would not bother trying – some because they have scant regard for international law more generally and some because they see little advantage in being explicit about rules of acceptable behaviour.

We do. The clearer we are about the boundaries of acceptable behaviour, the lower the risk of miscalculation and the clearer the consequences can be for transgressing them. I have tried to offer some of that clarity this morning, to say in terms that, for example, the targeting of essential medical facilities, the downing of civilian aircraft, the sabotage of nuclear power

stations, are no less unlawful and no less deserving of a robust and legitimate response when they are undertaken by cyber means than when they are done by any other means.

The United Kingdom has always taken its international law responsibilities seriously, despite the restrictions on our freedom of action those responsibilities entail. We do so because we believe that a rules-based international order makes the world a safer place and that no nation can make a strong case for such an order if it is unprepared to accept the rules itself. But it must also follow that a rules-based international order can only prevail when the rules can be clearly understood and that where they are unclear we seek to bring clarity. It must be for those of us who believe in the benefits of international law to ensure it remains effective, that it continues to constrain and deter, online as well as offline, the worst failings of human nature.

Cyberspace is getting larger, not smaller. Its influence on international relations is growing not shrinking. So it is ever more important, and part of the UK's role in global leadership, to do what we can to ensure the law applies in cyberspace too.