Record number of city status winners announced to celebrate Platinum Jubilee

- Stanley named a city as the Falkland Islands becomes the first ever Overseas Territory to win competition for city status
- A record eight winners selected for city status as part of June’s Platinum Jubilee celebrations
- First crown dependency to win civic honours as Douglas becomes the first and only city on the Isle of Man

A record number of locations have won prestigious city status through a competition, as part of Her Majesty The Queen’s Platinum Jubilee celebrations.

The competition to receive civic honours was last run ten years ago to mark the Queen’s Diamond Jubilee, and this year for the first time ever the competition for city status was open to applications from the Crown Dependencies and Overseas Territories, with the Falklands’ Stanley and Douglas of the Isle of Man among the winners.

Eight places won the royal honour this year ahead of the Jubilee weekend, the highest number of awards in a single competition:

- Bangor, Northern Ireland
- Colchester, England
- Doncaster, England
- Douglas, Isle of Man
- Dunfermline, Scotland
- Milton Keynes, England
- Stanley, Falkland Islands
- Wrexham, Wales

The Platinum Jubilee Civic Honours Competition required applicants to demonstrate how their unique communities and distinct local identity meant they deserved to be awarded city status. They were also required to highlight their royal associations and cultural heritage.

For the first time, the competition was open to applicants from Overseas Territories and Crown Dependencies, with the Falklands’ Stanley and Douglas of the Isle of Man among the winners.

Chancellor of the Duchy of Lancaster Steve Barclay said:

> I am delighted that a record number of locations have been awarded the prestigious city status as part of Her Majesty The Queen’s Platinum Jubilee Celebrations.

> What was clear to me during the process of assessing each application was the pride that people felt for their communities, local cultural heritage and the Royal Family.
>
> As we celebrate Her Majesty The Queen’s colossal contribution to society, I am thrilled that we are able to recognise some of the many places that make Britain great.
>
> It is also incredibly reflective of Her Majesty’s global outlook and years of international service that applicants from the Overseas Territories and Crown Dependencies have been selected as winners for the first time.
>
> I look forward to the world coming together to show our pride and gratitude to Queen Elizabeth II on the Jubilee weekend.

The competition for city status has taken place in each of the last three jubilee years, with previous winners including Chelmsford, Lisburn and Newport.

Winning city status can provide a boost to local communities and open up new opportunities for people who live there, as is the case with previous winners Perth and Preston where residents have described how their success contributed to increased national and global standing, putting them on the international map as a place to do business.

Research shows that Perth, which was granted city status in 2012 as part of the Queen’s Diamond Jubilee, has reaped the full benefits, with the local economy expanding by 12% in the decade it was granted city status.

Culture Secretary Nadine Dorries said:

> City Status is a huge accolade and I congratulate our eight brilliant winners. This competition showcases the best of Britain and the Overseas Territories and will act as a lasting legacy of Her Majesty The Queen’s Platinum Jubilee.

The winner of the competition for Lord Mayoralty status was also announced today, with Southampton winning the coveted award. The city’s newfound status entitles the Mayor to be known as the Lord Mayor and has been granted to three cities as part of previous Jubilee Civic Honours competitions: Chester (1992), Exeter (2002) and Armagh (2012).

Applications were opened last year and almost 40 locations from across the UK and beyond put forward their bid to become a city. The applications, which were asked to follow a clear structure were subsequently evaluated by a panel of experts and Cabinet Office ministers, before a recommendation was put to Her Majesty The Queen.

‘Letters Patent’ will now be prepared which will confer each of the awards formally and will be presented to winners later in the year.

UK medical aid donations to Ukraine to reach 11 million items

- Latest aid deliveries will double number of medical items donated by the UK.
- Supplies including antibiotics, painkillers, dressings, and specialist medicines will help those injured by Russian attacks.
- Specialist brain and spinal injury equipment will treat severely injured, with further deliveries of ambulances in the coming weeks.

Medical aid donations from the UK to Ukraine will reach more than 11 million items in the coming days, helping save tens of thousands of lives.

A fourth tranche of aid left from across the UK during the last week, carrying:

- 4.2 million doses of medicines – including painkillers and antibiotics that are critical for treating infections caused by battlefield trauma and limited hygiene facilities
- 1.5 million items of other supplies – including PPE and respirators

The 5.78 million items in the latest deliveries more than double the 5.29 million items donated in the first three tranches, taking the total to 11.07 million.

Nearly 16 million people are reported to be in need of humanitarian assistance within Ukraine, with access to care badly needed for those in cities worst hit by Russian attacks like Mariupol and Irpin.

The latest supplies are being sent in direct response to a request from the Government of Ukraine. They will provide treatment for people injured in the brutal and intentional Russian attacks on civilians across Ukraine, as well as help the government prepare for potential future threats.

The UK Government will continue to work closely with Ukrainian Government officials to tailor our support and target supplies to reach those most in need. This will include further donations of both new and NHS ambulances in the coming weeks to bolster frontline life-saving efforts in Ukraine.

Foreign Secretary Liz Truss said:

> The UK stands shoulder to shoulder with our Ukrainian friends. As the medical emergency inflicted by Russia escalates, we have

> responded with life-saving medical supplies where they are needed most.
>
> As one of the largest humanitarian donors, Britain will continue to help care for those bravely resisting Putin’s vile aggression until Ukraine succeeds.

Health and Social Care Secretary, Sajid Javid, said:

> Russia’s unprovoked and illegal attacks on Ukraine have created a medical emergency, with Putin targeting healthcare facilities like maternity units, hospitals, and ambulances.
>
> The UK’s support for our friends in Ukraine is unwavering, giving medicines and equipment they desperately need, which has saved tens of thousands of lives.
>
> Thank you to the NHS in England, Wales, Northern Ireland, and Scotland for stepping up and donating vital medical supplies.

From the outset of the crisis the UK has helped Ukraine deal with its intensifying medical emergency. Earlier tranches of aid included items such as medical equipment, drugs for surgery, wound care packs and bandages.

The UK is also donating specialist equipment to treat spinal cord and brain injuries and help provide rehabilitation. This is donated from the UK Emergency Medical Team, which is on standby to deliver medical aid in global emergencies. It will help boost the capacity of a national rehabilitation centre in Ukraine, freeing up bed space in hospitals to accommodate other critical cases.

The additional shipments of medical aid have been drawn from donations from across the UK, including NHS England, Wales, Scotland and Northern Ireland, with NHS Wales contributing more than 1 million items to the latest tranche of aid.

Health and Social Services Minister, Eluned Morgan for the Welsh Government said:

> Wales stands in solidarity with the Ukrainian people and we will continue to offer any practical support and humanitarian assistance that we can.
>
> In addition to the funding we have given to the Disaster Emergency Committee and medical supplies we previously sent to Ukraine, this latest tranche of medical supplies includes a further 49 pallets from Wales of respirators, gloves and dressings to directly help the medical response and life-saving efforts in Ukraine.

ENDS

Notes to editors

- This latest donation comes as part of a wider package of humanitarian assistance to Ukraine, including £220 million to provide medical supplies and basic necessities on the ground, and a rapid donation of food supplies to save lives and protect vulnerable people. This includes support through the UN, the Red Cross and NGOs, including Disasters Emergency Committee and UK-Med.
- Some of the significant items sent to Ukraine so far include:
  - over 3,000 adult resuscitators
  - around 255,000 wound care packs
  - over 550,000 sterile needles
  - over 50,000 packs of bandages
  - around 1,800 pieces of equipment for ventilators
  - over 75,000 cannulas
  - around 6.8 million doses of medicine – including antibiotics and painkillers
  - around 1.1 million packs of gloves
  - 28,000 FFP3 masks
  - 13 newly procured and donated NHS ambulances to replace those damaged in the conflict

---

£300 million to cut youth crime and make streets safer

- new 'Turnaround' scheme to catch troubled young people teetering on edge of criminality
- up to 20,000 more children and young people to be helped over next 3 years

Thousands of troubled children and teenagers teetering on the edge of crime will be put back on the right track thanks to the largest youth justice funding boost in a generation – cutting crime and making streets safer.

Around 80 percent of prolific adult offenders begin committing crimes as children, and the estimated cost of late intervention to the economy is nearly £17 billion per year.

That's why the government is making the biggest investment in a generation – worth £300 million over the next 3 years – to support every single council across England and Wales in catching and preventing youth offending earlier than ever, helping to stop these children and teenagers from moving on to further, more serious offending.

And for the first time ever, local authorities will be given specific cash to intervene early with teenagers displaying signs such as poor school attendance, troubles at home, and a history of substance abuse which are known to be factors which often drive young people into crime – so they can steer them away from law-breaking before an offence is even committed.

Through ‘Turnaround’, a new early intervention scheme backed by £60 million, local Youth Offending Teams will be given extra funding to connect children and teenagers to targeted, wraparound support to stop them going down a path of criminality.

This could include mentoring, extra school tuition, sports clubs, help to address any issues at school or at home, with their mental health or with substance misuse, tackling the root causes of their behaviour and helping them to get their lives back on track.

Funding will also be used to bolster the day-to-day running of youth justice schemes and initiatives across the country, as well as support the work of the 20,000 additional police officers the government is committed to recruiting.

As part of today’s news, the Deputy Prime Minister, Dominic Raab, visited a community boxing scheme in Blackpool that is giving local children and teenagers an alternative to anti-social behaviour, giving them skills such as discipline and teamwork, and steering them away from potential offending and back into education and training.

Deputy Prime Minister, Lord Chancellor, and Secretary of State for Justice Dominic Raab said: > > Diverting more young people from gangs, drugs and violence will make our streets safer.

> So, we’re investing £300 million in preventative initiatives, to deter criminal behaviour.
>
> Our plan will ensure thousands more young people can turn their lives around – which will transform their lives and make our communities safer.

Minister for Youth Justice Victoria Atkins said:

> Youth offending is a destructive force that blights communities and rips families apart.
>
> This vital new funding will help us stop youth crime in its tracks by ensuring these children stay in education and rebuild ties with their families, helping us build safer, more prosperous communities.

Youth Justice Board Chair Keith Fraser said:

> This is a smart and insightful investment by the government. If our youth justice teams are well-resourced to help children and families, we all benefit – from healthier, happier, safer children and from safer communities with fewer victims.
>
> This investment highlights the importance of their work and is a huge opportunity for youth justice teams across England and Wales. I hope they feel rightly proud of the contribution they make to the safety of communities and the lives of children.

Ministers estimate that the Turnaround programme will reach up to 20,000 more children over three years who would not otherwise have received support to turn away from offending.

While many local authorities already run successful early intervention programmes, by providing funding over a three-year period, councils will have greater certainty and be able to plan longer-term – ultimately steering more children and teenagers than ever away from crime.

Ministers will also set out plans in due course to improve how funding is targeted to local authorities, to ensure funding reaches areas who need it most and to ensure local authorities' interventions are effective.

International Law in Future Frontiers

It is fantastic to be standing here today in Chatham House to speak to you all about cyber and international law.

In 1982, on a visit to Japan, Margaret Thatcher presented a ZX Spectrum to the Japanese Prime Minister. "This is a Small. Home. Computer," she told the bemused premier, before purposefully pressing a button on the keyboard which changed the screen to reveal a game of chess. Although by the end of the decade the British entrepreneur Sir Clive Sinclair had sold two and half million units of his ZX in the UK, for most people the personal computer was always just a bit of fun. Why would you painstakingly key in your contacts when you already had an address book?

40 years on, it's hard to understate our reliance on computers. Just imagine how Margaret Thatcher would have reacted in 1982 if you had told her that the small electronic box in front of her would require defence from a dedicated state agency with a budget running into billions of pounds! As a sound fiscal conservative, she may have been tempted to knock it off the table, rather than showcase the British creation across the world.

Once-novel uses of cyber technology, like making a medical appointment or shopping online, have now become routine and sometimes unavoidable. And since an event occurring in cyberspace can have real world consequences, it’s clear that it requires increasing levels of international co-operation, as can be seen in the India-UK cyber statement agreed during the Prime Minister’s recent visit there. Such agreements help States to trade goods, services and ideas. Cyber activity is also now part of how some disputes or tension between countries play out.

Our reliance on cyber has, of course, created huge challenges. Events over the past 10 years, in particular, have demonstrated the vulnerability of critical sectors to disruptive State cyber activity. Perhaps most notoriously, the 2017 NotPetya cyber-attack, which masqueraded as ransomware but served principally to disrupt, affecting in particular Ukraine’s financial, energy and government institutions. But its indiscriminate design also caused wider disruption across the globe, costing firms in sectors of industry as varied as shipping, food production, pharmaceutical research and advertising, hundreds of millions in recovery costs. More recently, Microsoft reported that shortly before Russian’s illegal invasion of Ukraine, the Russian Main Intelligence Directorate (the GRU) targeted destructive malware against hundreds of systems across Ukraine affecting the IT, energy and financial sectors.

The ongoing conflict in Ukraine has demonstrated, on the part of Russia, a callous disregard for established international rules. However, the unprecedented and united international response in support of Ukraine has also reinforced the value of having a framework that makes clear when State action is unlawful.

Cyber is part of the conflict. As Sir Jeremy Fleming recently noted, we have seen cyber in this conflict, and lots of it. The UK, US, EU and other allies announced last week that Russia has been behind a series of cyber-attacks since the start of its illegal invasion. The most recent attack on communications company Viasat in Ukraine had a wider impact across the continent, disrupting wind farms and internet users in central Europe. Putin is also waging a dangerous disinformation war, hiding the truth from the Russian people.

Shaping the international order

Commentators often talk in hushed tones of cyber weapons, with little understanding of what they are, or of the rules which govern how they are used. This misunderstanding means we can see every cyber incident as an act of warfare which threatens to bring down the modern world around us and it’s not uncommon for even seasoned observers to think in this way, as they speak of cyber as a new battlespace where no rules apply. But cyberspace is not a lawless ‘grey zone’. International law governs and plays a fundamental role in regulating cyberspace.

Which is why today I would like to set out how the UK considers international law applies in cyberspace during peacetime, against the backdrop of the Prime Minister’s Integrated Review and the Government’s National Cyber Strategy. With particular focus on the rule on non-intervention, its application to key sectors, and avenues for response.

I’m focusing on the law applicable in peacetime because the UK has already set out that cyber operations are capable of breaching the prohibition on the threat or use of force, and that the law applicable in armed conflict applies just the same to the use of cyber means as other means of waging war. And I want to be clear that in the same way that a country can lawfully respond when attacked militarily, there is also a basis to respond, and options available, in the face of hostile cyber operations in peacetime.

The UK was one of the very first States to articulate publicly its views on the application of international law in cyberspace. I will build on what one of my predecessors, Jeremy Wright QC, said when he was Attorney General in May 2018, here in Chatham House. At that time, it was considered necessary to set out the fundamentals of the UK view – that the rules-based international order extends to cyberspace, and that there are boundaries of acceptable State behaviour in cyberspace as there are anywhere else.

More recently, in June 2021, the UK published a statement as part of the United Nations ‘Group of Governmental Experts’ process, setting out the ways in which international law applies in cyberspace. And the UK continues to attach importance to States clearly setting out their views like this. Significantly, that UK statement concluded by noting the importance of moving “beyond discussion of general concepts and principles, and to be clear about what constitutes unlawful conduct in those sectors which are most vulnerable to destructive cyber conduct”.

One of the Integrated Review’s stated goals is for the United Kingdom to “shape the international order as it develops in future frontiers”. Cyberspace stands out among these future frontiers. The National Cyber Strategy priorities include promoting a “free, open, peaceful and secure cyberspace”. International leadership and partnerships will be essential aspects of shaping and strengthening the international cyber governance framework to deliver these objectives. Partnerships like the ‘Quintet’ of Attorneys General, with my counterparts from Australia, Canada, New Zealand and the United States.

The United Kingdom’s aim is to ensure that future frontiers evolve in a way that reflects our democratic values and interests and those of our allies. We want to build on increasing activism by likeminded States when it comes to international cyber governance.

This includes making sure that the legal framework is properly applied, to protect the exercise of powers derived from the principle of State sovereignty – to which this Government attaches great importance – from external coercion by other States.

The law needs to be clear and well understood if it is to be part of a framework for governing international relations and to rein in irresponsible cyber behaviour. Setting out more detail on what constitutes unlawful activity by States will bring greater clarity about when certain types of robust measures are justified in response.

The rule on non-intervention

Turning to the law – one of the rules of customary international law which is of particular importance in this area is the rule on non-intervention.

Customary international law is the general practice of States accepted as law. As such, it is not static. It develops over time according to what States do and what they say. It can adapt to accommodate change in the world, including technological advances. Customary international law is a framework that can adapt to new frontiers and which governs States’ behaviour.

A well-known formulation of the rule on non-intervention comes from the International Court of Justice in its Military and Paramilitary Activities judgment. According to the Court in that case, all States or groups of States are forbidden from intervening –

> …directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social, and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.

The UK’s position is that the rule on non-intervention provides a clearly established basis in international law for assessing the legality of State conduct in cyberspace during peacetime.

It serves as a benchmark by which to assess lawfulness, to hold those responsible to account, and to calibrate responses.

This rule is particularly important in cyberspace for two main reasons.

First, the rule on non-intervention lies at the heart of international law, serving to protect matters that are core to State sovereignty. As long ago as 1966, the UK made clear its position that:

> …the principle of non-intervention, as it applied in relations between States, [is] not explicitly set forth in the United Nations Charter but flow[s] directly and by necessary implication from the prohibition of the threat or use of force and from the principle of the sovereign equality of States…

Four years later, in 1970, the UK set out its view that “non-intervention reflected the principle of the sovereign equality of states.” And that these principles were equally valid and interrelated. More colloquially, we might say that sovereignty and non-intervention are two sides of the same coin.

States have expressed different views on the precise significance of sovereignty in cyberspace. The UK reiterated its own position on this point as recently as June 2021. Namely, that any prohibition on the activities of States, whether in relation to cyberspace or other matters, must be clearly established in international law. The general concept of sovereignty by itself does not provide a sufficient or clear basis for extrapolating a specific rule of sovereignty or additional prohibition for cyber conduct going beyond that of non-intervention.

What matters in practice is whether there has been a violation of international law. Differences in legal reasoning must not obscure the common ground which I believe exists when it comes to certain types of unacceptable and unlawful cyber behaviours. I think that common ground also extends to an appreciation that we must carefully preserve the space for perfectly legitimate everyday cyber activity which traverses multiple international boundaries millions of times a second.

Second, the rule on non-intervention is also of increasing relevance due to the prevalence of hostile activity by States that falls below the threshold of the use of force or is on the margins of it. In such circumstances, the rule on non-intervention becomes particularly significant as another benchmark by which States can define behaviour as unlawful.

Threshold for a prohibited intervention

Having identified the importance of the rule on non-intervention, I will now turn to the threshold for its application. The fact that behaviour attributed to another State is unwelcome, irresponsible, or indeed hostile, does not mean that it is also unlawful. A core element of the non-intervention rule is that the offending behaviour must be coercive.

Coercion was rightly described in the Military and Paramilitary Activities case as “the very essence” of a prohibited intervention. It is this coercive element that most obviously distinguishes an intervention prohibited under international law from, for example, more routine and legitimate information-gathering and influencing activities that States carry out as part of international relations.

But what exactly is coercion?

Some have characterised coercion as forcing a State to act differently from how it otherwise would – that is, compelling it into a specific act or omission. Imagine, for example, a cyber operation to delay another State’s election, or to prevent it from distributing tax revenues to fund essential services. To my mind, these are certainly forms of coercion.

But I want to be clear today that coercion can be broader than this. In essence, an intervention in the affairs of another State will be unlawful if it is forcible, dictatorial, or otherwise coercive, depriving a State of its freedom of control over matters which it is permitted to decide freely by the principle of State sovereignty. While the precise boundaries of coercion are yet to crystallise in international law, we should be ready to consider whether disruptive cyber behaviours are coercive even where it might not be possible to point to a specific course of conduct which a State has been forced into or prevented from taking.

Of course, in considering whether the threshold for a prohibited intervention is met, all relevant circumstances, including the overall scale and effect of a cyber operation, need to be considered. But I believe that we can and should be clearer about the types of disruptive State activity which are likely to be unlawful in cyberspace.

Illustrative examples

It is therefore important to bring the non-intervention rule to life in the cyber context, through examples of what kinds of cyber behaviours could be unlawful in peacetime. To move the focus to the types of coercive and disruptive behaviours that responsible States should be clear are unlawful when it comes to the conduct of international affairs in peacetime.

And being clear on what is unlawful means we can then be clearer on the range of potential options that can lawfully be taken in response. That is, the kinds of activities which would require legal justification, for example, as a proportionate response to prior illegality by another State. This is crucial in enabling States to act within the law whilst taking robust and decisive action.

With that in mind, today I will set out new detail to illustrate how this rule applies. A non-exhaustive list, to move this discussion forward. I will cover four of the most significant sectors that are vulnerable to disruptive cyber conduct: energy security; essential medical care; economic stability; and democratic processes.

Ensuring the provision of essential medical services and secure and reliable energy supply to a population are sovereign functions of a State. They are matters in respect of which international law affords free choice to States. The Integrated Review highlights the interconnected nature of the global health system, and the importance of building resilience to address global health risks. Covid is a clear example. Likewise, energy security is recognised as including protection of critical national infrastructure from cyber security risks.

Covert cyber operations by a foreign State which coercively restrict or prevent the provision of essential medical services or essential energy supplies would breach the rule on non-intervention.

Of course, every case needs to be assessed on its facts, but prohibited cyber activity in the energy and medical sectors could include:

- disruption of systems controlling emergency medical transport (e.g., telephone dispatchers);
- causing hospital computer systems to cease functioning;
- disruption of supply chains for essential medicines and vaccines;
- preventing the supply of power to housing, healthcare, education, civil

administration and banking facilities and infrastructure;
- causing the energy supply chain to stop functioning at national level through damage or prevention of access to pipelines, interchanges, and depots; or *preventing the operation of power generation infrastructure.

Turning to economic stability, covert cyber operations by a foreign State that coercively interfere with a State's freedom to manage its domestic economy, or to ensure provision of domestic financial services crucial to the State's financial system, would breach the rule on non-intervention.

Such cyber operations could include disruption to the networks controlling a State's fundamental ability to conduct monetary policy or to raise and distribute revenue, for instance through taxation. Or disruption to systems which support lending, saving and insurance across the economy.

Lastly, democratic processes. Free and open elections, using processes in which a population has confidence, are an essential part of the political system in democratic States. All States have the freedom to make their views known about processes in other countries – delivering hard, sometimes unwelcome messages, and drawing attention to concerns. This is part and parcel of international relations. However, covert cyber operations by a foreign State which coercively interfere with free and fair electoral processes would constitute a prohibited intervention.

Again, every activity needs to be assessed on its facts, but such activities could include:

- operations that disrupt the systems which control electoral counts to change the outcome of an election; or
- operations to disrupt another State's ability to hold an election at all, for example by causing systems to malfunction with the effect of preventing voter registration.

I hope that these illustrative examples will assist in the future when considering what is unlawful in cyberspace.

I should also add that the nature of cyberspace means that it may not be evident, at least at first, whether a State is responsible for a particular action. This is also a space in which criminal gangs operate for financial profit. To be clear, State direction or control of non-State actors who undertake cyber operations of the kind I have described today would also represent unlawful conduct by that State, in line with international law on State responsibility. Cyber is no different from other spheres of activity in this sense. Provided that it is exercising the requisite degree of direction or control, a State is no less responsible for internationally unlawful cyber operations conducted by a ransomware gang than it would be for the unlawful actions of an armed group, or a corporation.

Response options

If a State carries out irresponsible, hostile, or unlawful cyber activity, what then are the options available to the victim State?

There are a wide range of effective response options available to impose a cost on States carrying out irresponsible or hostile cyber activity, regardless of whether the cyber activity constitutes an internationally unlawful act. These kinds of measures, referred to as acts of retorsion in international law, could include economic sanctions, restrictions on freedom of movement, exclusion from international groupings and wider diplomatic measures. So, there are always options available to stand up to unacceptable behaviour. And you do not have to look far to see how the impact of taking these kinds of measures is amplified when acting alongside other like-minded States.

Let me be clear. This means that when states like Russia or China carry out irresponsible or hostile cyber activity, the UK and our allies are always able to take action, whether or not the activity was itself unlawful. Today that might be in response to hostile cyber activity occurring in Ukraine, tomorrow it could be a response to hostile activity in Taiwan.

Where a State falls victim to unlawful cyber activity carried out against it by another State, it may also be appropriate to pursue remedies through the courts. Current events in Ukraine have demonstrated the continued relevance of forums like the International Court of Justice (ICJ) in the context of a wider response. The UK has accepted the compulsory jurisdiction of the ICJ, and we encourage others to do likewise.

Beyond this, under the international law doctrine of countermeasures, a State may respond to a prior unlawful act, in ways which would under normal circumstances be unlawful, in order to stop the offending behaviour and ensure reparation. The UK has previously made clear that countermeasures are available in response to unlawful cyber operations by another State. It is also clear that countermeasures need not be of the same character as the threat and could involve non-cyber means, where it is the right option in order to bring unlawful behaviour in cyberspace to an end.

However, some countries simply do not have the capability to respond effectively by themselves in the face of hostile and unlawful cyber intrusions. It is open to States to consider how the international law framework accommodates, or could accommodate, calls by an injured State for assistance in responding collectively.

Free, open, peaceful and secure cyberspace

I’ve focused today on the application of international law to cyberspace, but I also want to touch on the broader context. Applying the international law framework to this new frontier is just one part of a wide-ranging international effort, by the UK and other like-minded States, to promote a free, open, peaceful and secure cyberspace.

There are a range of additional measures currently being taken domestically and internationally to counter harmful behaviour in cyberspace. Improving cyber resilience is central to reducing cyber-attacks and their real-world impact. Over the last decade the UK has delivered a wide range of interventions aimed at strengthening the UK’s cyber resilience, including through the creation of the National Cyber Security Centre (NCSC). Resilience is a core element of the UK's National Cyber Strategy. My colleague the Chancellor of the Duchy of Lancaster spoke last week at the annual CYBER UK conference about the importance of resilience – how this is something we all need to take responsibility for, across the public and private sectors, to ensure that the benefits of technology are felt by the whole of society.

States have always had a duty to protect their external border from foreign attack but cyber has, in a sense, increased the size of that border, by an unimaginable factor. Viewed this way, the UK's external border is no longer just around the corners of Great Britain and around Northern Ireland. It is located in every household and business in the country. But just because the scale of the challenge has increased, it does not change our fundamental duty to protect citizens, families and businesses from the array of threats present in cyberspace.

The UK has also developed a cutting-edge capability to carry out cyber operations to keep ourselves and our friends and allies protected from those who seek to harm us – the National Cyber Force. The National Cyber Force draws together personnel from intelligence and defence in this area under one unified command for the first time. It can conduct offensive cyber operations – flexible, scalable measures to meet a full range of operational requirements. And, importantly, the National Cyber Force operates under an established legal framework. Unlike some of our adversaries, it respects international law. It is important that democratic States can lawfully draw on the capabilities of offensive cyber, and its operation not be confined to those States which are content to act irresponsibly or to cause harm. This goes to the heart of how the UK operates as a responsible cyber power.

The role of law enforcement is also important. The police and National Crime Agency are focused on addressing the cybercrime threat here in the UK. Our domestic legislation such as the Computer Misuse Act enables the prosecution of criminals attacking our computer systems, and I have no doubt we will ensure that the law here in the UK will continue to evolve as the threat does. Law enforcement authorities are also working together across the globe, including on the basis of international agreements such as the Budapest Convention. This encourages a common approach to cybercrime, adopting appropriate domestic criminal law frameworks and fostering international cooperation. And closer cooperation in the criminal justice space means that ransomware gangs cannot act with impunity.

Coordination between States, in a more general sense, is also crucial in responding to hostile State activity in cyberspace and imposing a cost on those who seek to abuse the freedom and opportunity that technological progress has provided them. States are developing more sophisticated and coordinated diplomatic and economic responses. This can be seen in the response to the recent operation targeting Microsoft Exchange servers, where 39 partners including NATO, the EU and Japan coordinated in attributing hostile cyber activity to China. It can also be seen in the response to the Russian SolarWinds hack which saw coordinated US, UK and allied sanctions and other measures.

Working with States to reach shared agreement on prohibited behaviours for key sectors, like those I have set out today, will help us move beyond theoretical discussions around sovereignty and non-intervention. To help define what responsible cyber power means in practice.

When taken in collaboration with other efforts – improving resilience, promoting cyber security, international cooperation, and having the operational capability to respond effectively to those seeking to harm us – international law can help us all to realise this vision of a free, open, peaceful and secure cyberspace.

Closing

In closing, I will make a few final remarks.

International law matters in cyberspace because if we don’t shape the rules here, if we don’t have a clear framework to counter hostile activity in cyberspace, and if we don’t get cyber security right, the effects will be likely to be felt more often and in hugely disruptive ways by ordinary people.

For example, a single cyber breach in 2020 cost a local council here in the UK an estimated £10 million in recovery costs and significantly disrupted services provided to the local population for months by shutting down IT systems and stopping the council from carrying out property purchases within the borough.

Championing a cyber governance framework that is founded in international law means we can also provide a secure foundation for international partnerships on technology. To unlock the potential of fields such as Artificial Intelligence and quantum computing.

The UK and its allies are at the forefront of this work. Earlier this year, the Foreign Secretary concluded a Cyber and Critical Technology Partnership with her Australian counterpart to strengthen global technology supply chains and promote the UK’s positive technology vision.

Providing further detail on how international law applies in cyberspace, as I have sought to do today, will help us to more effectively ‘call out’ the most egregious hostile State behaviour as unlawful. The UK will continue to call out behaviour – both irresponsible and unlawful.

Our approach will also encourage more agile and decisive international action in response to specific threats, using our full freedom of manoeuvre within the law. It will help all States understand the parameters and thresholds of lawful or unlawful action. It will serve to avoid inadvertent or damaging escalations. And our approach will enable us to do these things in close partnership with the many other States who share our ambition to shape and strengthen the international order in future frontiers.

Thank you.

Home Secretary and Rwandan Minister Biruta visit Geneva

Home Secretary Priti Patel and Rwandan Minister for Foreign Affairs and International Co-operation, Dr. Vincent Biruta, today (Thursday, 19 May) carried out a series of joint engagements in Geneva.

Five weeks after the signing of the Migration and Economic Development Partnership (MEDP) in Kigali and following their meeting in London yesterday, the ministers travelled to Geneva to brief key figures working in the field of international migration.

The Home Secretary and Minister Biruta met with UN Permanent Representatives from Australia, Canada, New Zealand and the United States. Both ministers set out how the partnership of equals agreed between their two countries was facing up to a shared, global challenge and seeking to save lives. They emphasised their belief that further collective engagement was necessary to tackle the global migration crisis.

During the afternoon the Home Secretary and Dr. Biruta then had further engagements, including with Filippo Grandi, the United Nations High Commissioner for Refugees, and Nada Al-Nashif, the United Nations Deputy High Commissioner for Human Rights.

At both meetings, the Home Secretary and Dr Biruta sought to highlight the UK and Rwanda’s leadership on the international stage in addressing the issue of illegal migration while reinforcing their commitment to working in collaboration with UN agencies in this sphere.

They noted that the UK government’s assessment found Rwanda to be a fundamentally safe and secure country with a proud track record of supporting asylum seekers, including working with the UN Refugee Agency which itself has said the country has a safe and protective environment for refugees.

Furthermore, they emphasised that under our partnership Rwanda will process claims in accordance with the UN Refugee Convention and national and international human rights laws.

They recommitted to maintaining a positive ongoing dialogue with international partners and underlined how the ground-breaking partnership between the two countries will directly address the challenge of illegal migration while saving lives.

Rwandan Minister for Foreign Affairs and International Co-operation, Dr. Vincent Biruta, said:

> Rwanda and the UNHCR have historically partnered to provide safe haven to those in need. Rwanda, with the agency’s support, evacuated African migrants from Libya to safety in Kigali.
>
> This is just one example of Rwanda’s long history of offering those in need safety, dignity, and protection. While the UNHCR are entitled to their views on this partnership, they have no reason to doubt our motivations or our ability to offer sanctuary and opportunity to those seeking it – as we already are doing so for 130,000 refugees.
>
> We welcome the opportunity to discuss this partnership with colleagues in the UNHCR to address their concerns and advance their understanding of what we’re proposing.

Home Secretary Priti Patel said:

> All nations and international agencies must work together to address the issue of illegal migration collectively and urgently save lives.
>
> Rwanda and the UK stand together in promoting a new, fairer, more effective global asylum system. Our Migration and Economic Development Partnership will deter criminality, exploitation and abuse, while supporting the humane and respectful treatment of refugees.
>
> It was incredibly useful to discuss the partnership in detail with UN partners in Geneva today and assuage any concerns. We pay tribute to the UNHCR for their tireless efforts to support some of the most vulnerable people around the world.