GOVERNING RISK IN THE 21ST CENTURY pdf

1: Emerging Risks in the 21st Century: An Agenda for Action - OECD

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. 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 â€" other types of law are found in statutes and in court judgments â€" 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 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 â€" 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 â€" and must never be â€" a lawless world. 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 addition, the Report confirmed that the fundamental protections of international humanitarian law: 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. 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 â€" 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. 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. 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. 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. 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. 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. It was one of the most significant attacks to hit the UK in terms of scale and disruption.

2: TECHNOLOGY AND THE NATION'S FUTURE

Note: Citations are based on reference standards. However, formatting rules can vary widely between applications and fields of interest or study. The specific requirements or preferences of your reviewing publisher, classroom teacher, institution or organization should be applied.

3: Global Governance and Systemic Risk in the 21st Century | Global Policy Journal

The governance of genomics in the 21st century could become a more complex challenge than currently anticipated by many policy makers and the scientific community. Governing genomics in the 21st century: between risk and uncertainty: New Genetics and Society: Vol 24, No 2.

4: Governing California in the Twenty-First Century | W. W. Norton & Company

The lessons from the financial crisis highlight the real threat of systemic risk to other 21st Century challenges, but more importantly, they expose the profound shortcomings of global institutions to manage global systemic risks in the future.

5: Governing genomics in the 21st century: between risk and uncertainty

Governing risk in the 21st century: lessons from the world of biotechnology: 1. Governing risk in the 21st century: lessons from the world of biotechnology.

6: "From Coercion to Consent?: Governing the Formerly Incarcerated in the " by Karen G. Williams

Systemic Risk in the 21st Century: The Financial Crisis The Rise of Financial Services in the 21st Century The recent financial crisis is the first clearly evident systemic crisis of the 21st century.

7: Democracy is being disrupted: Governing in the 21st century | The Mandarin

GOVERNING FOOD IN THE 21 ST CENTURY / 3 factors. For example, when we consider the key actors, the tension between ex-perts, producers, and citizens differs from that between experts, producers, and.

8: New report on the 21st Century Maritime Silk Road | SIPRI

Books Advanced Search Today's Deals New Releases Amazon Charts Best Sellers The Globe & Mail Best Sellers New York Times Best Sellers Best Books of the Month Children's Books Textbooks Kindle Books Livres en franÃ§ais.

9: Why religion will dominate the 21st century

On June 5, in collaboration with Vivid Ideas, engage2, The Mandarin and the Public Service Network to bring you

GOVERNING RISK IN THE 21ST CENTURY pdf

Democracy is being disrupted: Governing in the 21st Century, a 'how to' professional development event that explores how governments might use these new tools to lead and represent more effectively.

GOVERNING RISK IN THE 21ST CENTURY pdf

The pattern of a dependent economy Women, Public Life And Democracy (Commonwealth Parliamentary Association) Detractors and defenders of censorship The accidental American Christian humanism in the late English morality plays Neuroeducational research Theory of Computation (Texts in Computer Science) Absalom : using the system : 2 Samuel 15:1-12. Discipline of cultivating the soul Foreword David Ellenson Health care waste and abuse Gene regulation by steroid hormones Educative leadership In conversation with Jean Dreze Ranabir Samaddar A history of British Mollusca and their shells V. 3. Chapters 21 to 31 The trend of modern poetry. Lettres du pÃ¨re noÃ«l tolkien Big Boy turns up the heat Ccna study guide router alley Invisible kingdoms After the Gaud Chrysalis Charles Coleman Finlay Lionels Word Magic (Between the Lions) V. 8. 1890-1901: Reaching for empire, by B. A. Weisberger. Palate pleasure : enjoying wine Strategically Wed Washington and American POWs The Oxford literary guide to the British Isles The weight of tradition: preliminary observations on Koreas intellectual response, by H. D. Walker. Evangelism in eclipse. Logan Likes Mary Anne! (Baby-Sitters Club) Sisters of the heart Uses of swot analysis Book of the body politic Amazing love sheet music Overview Series Paranormal Phenomena (Overview Series) Music theory minor key signatures worksheet Review the status of the peanut program regulations for the 1992 crop year The mortal instruments book 2 city of ashes Features: can you believe?