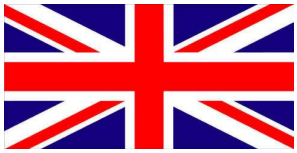

United Kingdom Mission
to the United Nations

One Dag Hammarskjold Plaza
(885 Second Avenue)
New York, NY 10017

Tel: +1 (212) 745 9200

Email: uk@un.int
http://twitter.com/UKUN_NewYork

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

UNITED NATIONS GROUP OF GOVERNMENTAL EXPERTS ON ADVANCING RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL SECURITY

APPLICATION OF INTERNATIONAL LAW TO STATES' CONDUCT IN CYBERSPACE

UNITED KINGDOM STATEMENT

This statement is submitted as part of the Group of Governmental Experts process ("GGE"), by the participating governmental expert from the United Kingdom in accordance with the mandate of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, established pursuant to General Assembly resolution 73/266A.

INTRODUCTION

1. International law is fundamental to maintaining security and stability in cyberspace and international law applies to States' conduct in cyberspace on the same basis as it applies to their other conduct. The application of international law to States' conduct in cyberspace is clearly recognised by the international community. In the recent 2021 OEWG report, States reaffirmed their understanding (as already set out in the 2013 and 2015 GGE reports) that 'international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment'.

2. The United Kingdom therefore welcomes the current initiative encouraging States to submit statements to be annexed to the report of the Governmental Group of Experts setting out their national positions on how international law applies in cyberspace. This will assist States in promoting a better understanding of international law and its development and facilitate greater transparency about, and mutual understanding of, what constitute acceptable behaviours in cyberspace. The greater the clarity on the boundaries of lawful behaviour, the lower the risk of miscalculation and the clearer the consequences can be for transgressing them. This statement is intended as a contribution to this initiative and briefly sets out, on a non-exhaustive basis, the United Kingdom's position on a number of specific issues relating to how international law applies to States' conduct in cyberspace.

3. The United Kingdom is committed to a free, open, peaceful and secure cyberspace. The use of cyberspace is in the interest of States and the international community as a whole and States have the right to exercise their cyber capabilities, subject to any restrictions imposed by international law. While there is no internationally agreed definition of "cyberspace" it is used in this statement to refer to the sphere of actions and conduct carried out using the interdependent network of information technology infrastructures that includes the internet, internet-related telecommunications networks, computer systems and internet connected devices.[1] The prefix "cyber" is used in this statement to characterise actions which are carried out using such information technology infrastructures.

[1] This definition is broadly based on the definition of cyberspace in HMG's National Cyber Security Strategy 2016-2021 which can be found here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf which defines cyberspace as 'the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.'

UN CHARTER

4. The Charter of the United Nations applies to States' conduct in cyberspace, as it does to their other conduct.

5. Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the purposes of the United Nations. Depending on the facts and circumstances in each case, conduct by States carried out in cyberspace is capable of constituting a threat or use of force if the actual or threatened conduct has or would have the same or similar effects of conduct using kinetic means. The circumstances in which the threat or use of force is not unlawful under international law are the same irrespective of whether the conduct is by kinetic or cyber means.

6. An operation carried out by cyber means may constitute an armed attack giving rise to the inherent right of individual or collective self-defence, as recognised in Article 51 of the UN Charter where the scale and effects of the operation are equivalent to those of an armed attack using kinetic means. Factors in considering the scale and effects of an attack may include the (actual or anticipated) physical destruction of property, injury and death. The exercise of the inherent right of self-defence against an imminent or on-going armed attack whether by kinetic or cyber means, may itself be by cyber or kinetic means and must always fulfil the requirements of necessity and proportionality. Whether or not to have recourse to the exercise of the inherent right of self-defence will always be carefully considered having regard to all the circumstances.

7. Article 2(3) and the provisions of Chapter VI of the Charter on the peaceful settlement of disputes can equally apply in relation to States' activities in cyberspace. Thus, in accordance with Article 33(1), States that are party to any cyber-related international dispute the continuation of which is likely to endanger the maintenance of international peace and security, shall endeavour to settle such dispute by peaceful means as described in Article 33 of the Charter: negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.

NON-INTERVENTION & SOVEREIGNTY

8. Below the threshold of the threat or use of force, the customary international law rule prohibiting interventions in the domestic affairs of States applies to States' operations in cyberspace as it does to their other activities. As set out by the International Court of Justice in its judgment in the Nicaragua case, the purpose of the rule on non-intervention is to ensure that all States remain free from external coercive intervention in matters

affecting a State's powers, which are at the heart of a State's sovereignty such as the freedom to choose its own political, social, economic and cultural system.[2]

9. As the UK has noted previously, while the precise boundaries of this rule continue to be the subject of on-going debate, it provides a clearly established basis in international law for assessing the legality of State conduct. Thus the use of hostile cyber operations to manipulate the electoral system in another State to alter the results of an election, to undermine the stability of another State's financial system or to target the essential medical services of another State could all, depending on the circumstances, be in violation of the international law prohibition on intervention.

10. The International Court of Justice has established that a prohibited intervention is one bearing on matters which each State is permitted, by the principle of State sovereignty, to decide freely. Sovereignty, as a general principle, is a fundamental concept in international law. The United Kingdom recalls that any prohibition on the activities of States whether in relation to cyberspace or other matters, must be clearly established either in customary international law or in a treaty binding upon the States concerned. The United Kingdom does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention referred to above. At the same time, the United Kingdom notes that differing viewpoints on such issues should not prevent States from assessing whether particular situations amount to internationally wrongful acts and arriving at common conclusions on such matters.

STATE RESPONSIBILITY & ATTRIBUTION

11. A State is responsible under international law for cyber activities that are attributable to it in accordance with the rules on State responsibility. The responsibility of a State for activities that occur on its territory including in relation to activities in cyberspace is therefore determined in accordance with the rules of international law on State responsibility. As well as bearing responsibility for acts of its organs and agents, a State is also responsible in accordance with international law where, for example, a person or a group of persons acts on its instructions or under its direction or control.

12. UNGGE Norm 13(c) provides that States should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technology.

[2] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America),* Merits, Judgment, ICJ Reports 1986 at para 205: 'In this respect [the Court] notes that, in view of the generally accepted formulations, the principle forbids all States or groups of States to intervene 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 element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.'

This norm provides guidance on what may be expected to constitute appropriate State behaviour. The UK recognises the importance of States taking appropriate, reasonably available, and practicable steps within their capacities to address activities that are acknowledged to be harmful in order to enhance the stability of cyberspace in the interest of all States. But the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace.

13. The term 'attribution' is used in relation to cyberspace in both a legal and non-legal sense. It is used in a legal sense to refer to identifying those who are responsible for an internationally wrongful act. It is also used in a non-legal sense to describe the identification of actors (including non-state actors) who have carried out cyber conduct which may be regarded as hostile or malicious but does not necessarily involve an internationally wrongful act.

14. For the UK, there are technical and diplomatic considerations in determining whether to attribute publicly such activities in cyberspace. The decision whether to make a public attribution statement is a matter of policy. Each case is considered on its merits. The UK will publicly attribute conduct in furtherance of its commitment to clarity and stability in cyberspace or where it is otherwise in its interests to do so.

15. Whatever the nature of the attribution, there is no general legal obligation requiring a State to publicly disclose any underlying information on which its decision to attribute conduct is based.

COUNTERMEASURES

16. Resort may be had to countermeasures in response to an internationally wrongful act, in accordance with international law, in relation to States' activities in cyberspace as in relation to their other activities. This includes both resorting to countermeasures against a State whose cyber activities constitute internationally wrongful acts and carrying out countermeasures by means of cyber operations. Countermeasures need not be symmetrical: where the internationally wrongful act is itself not a cyber activity, the response may nonetheless involve cyber-based countermeasures (and vice versa).

17. An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations. Any measures adopted must be commensurate with the injury suffered. They must be carried out in accordance with the conditions and restrictions established in international law and must in particular not contravene the prohibition on the threat or use of force, must be necessary and proportionate to the purpose of inducing the responsible State to comply with its obligations and must not contravene any other peremptory norm of international law.

18. The application of international law to the use of countermeasures in cyberspace must take account of the nature of cyber activities, which might commence and then cease almost instantaneously or within a short timeframe. In those circumstances, a wider pattern of cyber activities might collectively constitute an internationally wrongful act justifying a response.

19. The UK does not consider that States taking countermeasures are legally obliged to give prior notice (including by calling on the State responsible for the internationally wrongful act to comply with international law) in all circumstances. Prior notice may not be a legal obligation when responding to covert cyber intrusion with countermeasures or when resort is had to countermeasures which themselves depend on covert cyber capabilities. In such cases, prior notice could expose highly sensitive capabilities and prejudice the very effectiveness of the countermeasures in question. However any decision to resort to countermeasures without prior notice must be necessary and proportionate to the purpose of inducing compliance in the circumstances.

INTERNATIONAL HUMAN RIGHTS LAW

20. Human rights obligations apply to States' activities in cyberspace as they do to in relation to their other activities. The UK continues to support the view set out in Human Rights Council Resolution 20/8 that 'the same rights that people have offline must also be protected online…'. States have an obligation to act in accordance with applicable international human rights law, including customary international law, and international conventions to which they are a party, such as the International Covenant on Civil and Political Rights, other UN treaties, and regional instruments such as the European Convention on Human Rights.

21. States' respect for their human rights obligations in relation to their activities in cyberspace is essential to ensuring an open, secure, stable, accessible and peaceful environment and certain rights may have particular relevance to States' activities in cyberspace including the right not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, the right to freedom of thought, conscience and religion and the right to freedom of expression.

INTERNATIONAL HUMANITARIAN LAW (IHL)

22. IHL applies to operations in cyberspace conducted in the furtherance of hostilities in armed conflict just as it does to other military operations.

23. IHL seeks to limit the effects of armed conflict - it protects persons who are not, or who are no longer, participating in hostilities, and limits the methods and means of warfare

employed by the belligerents. As noted above, recourse to the use of force in cyberspace is governed by international law other than IHL, in particular the UN Charter. IHL seeks to limit the effects of armed conflict and it is not therefore correct that its applicability to cyber operations in armed conflict would encourage the militarisation of cyberspace.

24. A cyber operation is capable of being an 'attack' under IHL where it has the same or similar effects to kinetic action that would constitute an attack. Where an operation in cyberspace amounts to an 'attack', the principles of distinction, proportionality, humanity and military necessity apply in the same way as they do to an attack by any other means. Those responsible for planning, deciding upon, or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is reasonably available to them at the relevant time. All relevant rules of IHL must be observed when planning and conducting operations whether by cyber or other means – the complexity of cyber operations is no excuse for a lower standard of protection to be afforded to civilians and civilian objects.

25. Civilians are protected from attack unless and for such time as they take a direct part in hostilities. To the extent that civilians carry out cyber operations in an armed conflict that amount to attacks, they would lose their protected status under IHL and, by taking a direct part in hostilities, become legitimate military targets.

LOOKING FORWARD

26. As noted above, the United Kingdom welcomes this initiative as part of ongoing cooperation between States to develop their understanding of the application of international law to cyberspace and the reinforcement of their capacities to achieve this. The UK will continue actively to engage with other States to ensure that how international law applies to cyberspace and the parameters of responsible State behaviour in cyberspace are clear. In so doing, it will be important to move 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.