Contribution by United Kingdom to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security, February 2020

The UK considers that the proper implementation of the comprehensive framework outlined in the existing acqui, in its entirety by all States, provides a practical starting point for our efforts to increase stability in cyberspace. Universalization and operationalization of the cumulative assessments and recommendations contained in the three consensus reports of previous Groups of Governmental Experts (GGE) would be a practical step forward. The value placed on this body of work and the guidance it already provides to States grappling with the newfound opportunities and challenges presented by the ongoing development of Information and Communication Technologies (ICTs) is notable.

**THREATS: A strategic and technology neutral picture of the emerging threat provides the context in which all subsequent report recommendations are set.**

ICTs continue to provide immense opportunities for social and economic development underpinning all areas of our daily lives. As General Assembly engagement on this issue increases, we have both an opportunity and a responsibility to support all States in our shared pursuit of the Sustainable Development Goals by emphasising that ICTs are not in and of themselves a ‘threat’. Rather it is when States (or other actors) choose to use them ‘for purposes inconsistent with international peace and security’ that the threat or risk arises.

We must focus on those threats that relate to the mandate of the Open-Ended Working Group (OEWG) and our international peace and security remit, as well as avoiding duplication caused by addressing threats dealt with elsewhere in the UN system. We fully support the newly adopted Freedom Online Coalition Joint Statement on Human Rights Impact of Cybersecurity Laws, Practices and Policies, and its recommendations.

**INTERNATIONAL LAW: International law is a critical tool for ensuring stability and security in cyberspace. The UK considers that the existing framework of international law, voluntary and non-binding norms, confidence building measures and capacity building provides the basis of what we need.**

Our mandate, set out in A/73/27 is to continue to ‘study, with a view to promoting common understandings….how international law applies to the use of ICTs by States’. We cannot reach a common understanding on how international law applies to ICTs, without first sharing and better understanding our respective positions. Key in this regard is increased transparency and sharing by States of their positions and approaches. This should be our focus.

The UK publically acknowledges that all existing international law, including respect for human rights and fundamental freedoms and the application of international humanitarian law to cyber operations in armed conflict, forms part of our mutual commitment to behave responsibly in cyberspace. We do not consider it is for States to pick and choose which international law instruments are applicable – we have agreed international law applies in its entirety in the same way it applies to state activities offline.

In this regard, we welcome the call by the International Committee of the Red Cross for all States to reaffirm that international humanitarian law applies to the conduct of cyber operations during armed conflicts. When States engage in cyber operations, they are governed by international law just like activities in any other domain. The application of international humanitarian law to cyber operations in armed conflicts provides both protection and clarity. It does not encourage such conflict and ensures that the existing body of principles and rules that seek to minimise the humanitarian consequences of conflict apply. We also continue to be guided by the principle that the human rights that apply offline also apply online, as set out in Human Rights Council Resolution 20/8.
However, we believe we all need to go further as individual States and set out our own understandings of how international law applies in cyberspace. We recognise developing such positions may not be straightforward and may take time. Indeed debates and differences on how international law applies are not confined to cyber and our mandate is not to further international law. Pursuing alternative routes such as the development of new treaties is only likely to entrench existing divides in this area and will progress us no further on the question of how International Law applies.

We also recognise the need for capacity building in relation to international law, including through possible exercises relating to our understanding of the application of international law. Capacity building in this area could make a tangible difference to the ability of States to develop their own positions and defend their national interests in the OEWG, as well as to ensure we do not inadvertently further the digital divide in this way.

RULES, NORMS AND PRINCIPLES: We need stronger awareness and understanding by all countries of the framework in general, and this includes the voluntary and non-binding norms of responsible State behaviour. The UK’s immediate priority is universalising and implementing the norms we have already agreed and we are not convinced new ones are needed at this stage. We should use regional organisations and improved coordinated capacity building to support this aim.

We welcome widespread confirmation of the recommendations of the 2010, 2013 and 2015 GGE reports – and specifically that existing international law is applicable to State activity in cyberspace. These consensus reports, on which we build, have taken us partway through the lifecycle of norm elaboration - from discussing the concept in 2010, to testing them out in 2013, before committing fully to a significant expansion in agreed voluntary and non-binding norms in 2015. The logical next step in this cycle is a focus on effective embedding of the norms.

Norms need to be implemented to be effective. We think that requires three things. Firstly, increased awareness. Not just in Governments around the world but also in civil society to ensure these norms take full root in our societies. An important element of this work is developing a shared understanding of the value of the norms – where they came from, why they matter and importantly how they can make a difference to a State’s cybersecurity.

Secondly, increased resource. Some States are fully aware of the norms and would like to implement but cannot do so. There is a clear link between norms and capacity building in this regard. The UK continues to support a range of States in building their national cyber capacity. How norms relate to each States’ national situation will depend on a variety of factors that are specific to that State and should be seen in the context of a national cyber security strategy. Implementation of the norms can and should form an element of any national cyber security strategy. In 2019 only 40% of States had such a strategy.

Thirdly, availability of best practice guidance on implementation. The UK recognises the value of norm implementation itself and has shared two submissions describing how the UK Government has implemented the agreed norms and how the efforts of stakeholders in the UK are crucial to supporting norm implementation in the UK and beyond. Both submissions make a start on building best practice in this area. Again, regional organisations have a role to play here – promoting the operationalisation of norms and learning from best practice.

With regard to those seeking new norms we welcome elaboration of how their proposals relate to both the existing agreed voluntary and non-binding norms, and to our international peace and security remit. We remain concerned that the elaboration of new norms could undermine the existing norms by weakening the overarching protection they provide, or their technology neutral and ‘future-proofed’ nature. For example, the critical infrastructure norm was purposefully drafted to leave the question of what does and does not constitute critical infrastructure in the hands of policy makers. We would be concerned to see discussion
return to listing types of critical infrastructure. We also remain concerned about the concept of internet having a public core, while fully supporting idea that general availability of internet must be protected.

**On Attribution.** Previous GGE reports have mentioned attribution only briefly, noting uncertainty (2010), the difficulty (2013), and challenges (2015) associated with it. We consider that the existing framework discussed in this forum already underpins a State’s ability to carry out attribution, based on:

- international law – that a State is required to bear responsibility for its internationally wrongful acts;
- the voluntary and non-binding norms – framing our understanding of responsible State behaviour;
- cooperation and trust in partners - strengthened through CBMs; and
- technical, legal and policy capability – strengthened through capacity building.

But this is an area that is new to many and we consider there is more the GGE and OEWG can do to support States on this topic, including through technical capacity building. The UK can and does attribute malicious cyber acts to States where we believe it is in our best interests to do so, and in furtherance of our commitment to clarity and stability in cyberspace. We continue to consider that the decision to attribute malicious cyber activity to a State, and crucially to make that attribution public, is ultimately a political decision for States based on technical evidence, legal advice and wider diplomatic and political considerations.

**On the issue of State’s use of ICTs in an offensive capacity.** In the development and use of ICTs by States - military or otherwise – States must comply with international law and should be guided by the GGE reports. We all agree that it is in the interest of all States to promote the use of ICTs for peaceful purposes. Our predecessors also took care in 2015 to note the inherent right of States to take measures consistent with international law. In this context, furthering the conversation about how States understand their obligations under international law apply when acting in cyberspace is a practical step to increasing stability and mitigating associated risk.

The UK is one of a number of countries who have publicly confirmed that we are developing such capabilities. We recognise that ICT capabilities can be developed and used, in a manner consistent with international law. We will use these capabilities in line with our rights and obligations under international law and taking the framework of responsible State Behaviour championed by the OEWG and GGE into account.

Indeed, in some cases the use of ICT capabilities may be preferable to use of kinetic weapons and can be de-escalatory. An example is the cyber operations undertaken by the UK’s GCHQ to systematically and persistently degrade Daesh’s propaganda and hindering their ability to coordinate attacks.

So we reconfirm that ICTs are not in and of themselves a ‘threat’. Rather it is when States (or other actors) choose or are perceived to use them ‘for purposes inconsistent with international peace and security’ that the threat or risk arises. We do not condemn the development of such capabilities per se or suggest that it inherently encourages aggression or escalation. But we also do not consider that such capabilities should be used in a manner that is incompatible with the maintenance of international peace & security.

We know that many other States have – or are developing – operational cyber capabilities. Not all States have formally acknowledged these operational, or military, cyber capabilities, even when the fact of their existence is common knowledge. Some countries continue to use these capabilities in a manner that is not in line with their international obligations or is inconsistent with the framework of responsible State behaviour which the OEWG and GGE
champions. We consider it is important that States find ways to draw attention to acts contrary to these rules, norms and principles of responsible State behaviour in order to increase accountability, transparency and help build patterns of responsible behaviour.

Equally, we believe that it is in the interests of international stability for States to demonstrate transparency about cyber capabilities. We encourage other States to join those acknowledging their development of such capabilities as an indicator of good faith and to promote the transparency that breeds much needed predictability and common understanding.

CONFIDENCE BUILDING MEASURES: We consider confidence-building measures (CBMs) as the glue that holds our framework together. Without trust, the other elements of the framework are undeliverable. We are less concerned overall with encouraging new CBMs, than with ensuring we have globally operationalised those that we have already agreed.

We consider that regional organisations are important vehicles in the universalisation of and operationalization of the previous GGEs recommendations, alongside the private sector, academia and civil society organisations. It is important to support such organisations to help advance our own implementation. We consider that the Secretariats of these organisations are well placed to detail both the obstacles and challenges faced in supporting Member State implementation of CBMs, and how implementation might be progressed more quickly and effectively. Notwithstanding the specifics of regional context, we also encourage interregional outreach where such organisations learn from each other.

However, other States may not be part of a relevant regional organisation, or may not be actively engaged in the implementation of CBMs. Limitations on the ability of any State to implement any part of the Framework is a cause for concern and all States should consider how they can improve bilateral CBM partnerships with such States in particular.

CBM operationalisation - including through regional organisations - remains limited, leaving a major gap in the potential efficacy of the wider framework. CBMs, by their very nature, can only be successful where individual States choose to use them. Despite this, it may be possible to promote global operationalisation of key CBMs in which all States see value.

The UK considers that there is potential to strengthen the implementation of a Point of Contact (PoC) network, and build capacity to exercise that capability in national and regional contexts to ensure credible national responses. The challenges of joining up effectively across a State’s own government should not be overlooked in this regard. We may wish to draw on regional organisations’ Secretariats to capture existing lessons learned in implementing such PoC networks to ensure a practical approach to the challenge.

We also note that the establishment (and sustainment) of national CERTs as recommended in 2015 remains beyond the reach of some States. The UK considers the establishment of such an organisation a crucial building block in the practical implementation of CBMs. As such, we continue to work with States to fill this gap where they wish to do so.

CAPACITY BUILDING: The UK supports calls for guiding principles around capacity building. Such principles can increase trust between participants and enhance efficiency and effectiveness.

The most effective capacity building will always be targeted, based on national priorities, and informed by local stakeholder input. In this context, we support the important role of the Global Forum for Cyber Expertise (GFCE), including as a matchmaker. The GFCE have agreed the Delhi Communique principles, to which the UK already adheres, and these may be a useful guide.
In a time of increasing demand for capacity building, we must consider how we focus our efforts within the OEWG on supporting the framework of responsible State behaviour. Funding and resource availability is what makes the difference to a State’s ability to implement our framework. We call on the OEWG to use the opportunity provided by our report to encourage improved donor mobility, encouraging all relevant stakeholders to allocate funding and expertise for capacity building – whilst applying the capacity building principles and coordinating initiatives.

**REGULAR INSTITUTIONAL DIALOGUE:** The UK considers that the six GGE’s and first OEWG have constituted regular institutional dialogue and we fully support them. This dialogue continues to grow and adapt – whether through regional outreach, broader State membership, or stakeholder engagement.

The open and inclusive nature of the OEWG has been widely welcomed and we are fortunate to also be able to benefit from the expert based format of the GGE that continues to add value through deep dive discussions of challenging topics. We commend the efforts of the Chairs of the GGE and OEWG to work collaboratively in this regard and remain confident that they can produce complementary and mutually reinforcing outcomes.

We have not yet fully understood what shape the call for new ‘regular institutional dialogue’ could take. It is important to begin with the key question of what we want to achieve. Any future dialogue must also fit clearly within the remit of First Committee and avoid duplication. It would require broad participation, including from regional organisations and from stakeholders, building on the positive elements of the current GGE and OEWG formats. Whilst regular dialogue is crucial to building trust, it is also important that all States feel able to contribute to the discussion and that States with less capacity do not feel excluded due to inability to resource ongoing meetings.

Given the challenges we face in mobilising donors to support States in their efforts to build cyber capacity, we consider it would be inappropriate to divert large amounts of resource to new administrative functions at this time and would expect any future discussions be funded from within existing funding streams.