

UK response to Chair's initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

The following comments are provided in response to the Chair's request as per his letter of 16 March 2020. The UK welcomes the opportunity to provide these comments and extends its sincere thanks to the Chair and his team for their significant and continued efforts. Comments are provided by section, and not line-by-line, as requested. We look forward to the opportunity to provide that more detailed comment in due course.

General Comments

We recall the Chair's guidance that we should aspire in our report to focus on areas of convergence between States, whilst reflecting the diverse range of national positions. We continue to support this aim. The pre-draft could clarify its focus on areas of convergence, whilst making clear where the text aims to reflect rounded discussion. It is important to reflect accurately the different arguments raised, and the support for them, to avoid creating false impressions of consensus.

In the current context, we particularly recognise the potential for risks to international peace and security arising from malicious activity that seeks to exploit periods of reduced national and international resilience. We welcome the helpful framing of the challenges faced in protecting critical national infrastructure (B19) in this regard, which may include the challenge of protecting medical facilities. We emphasise the international focus required to deliver capacity building in support of this (F49) in periods where national resources available for cybersecurity may be restricted.

Discussion in the Open-Ended Working Group (OEWG) highlighted the need to accurately capture and reflect the relationship between binding international law and voluntary, non-binding norms. We welcome the framing of this in Chapeau D which we consider could be strengthened through the addition of the words '*...in the use of ICTs. They do not stand alone*'. We would welcome greater clarity in a range of references to this interplay (A12 '*regulate and guide*', C26 '*normative framework*', D38 '*upgrading norms*', C29 '*binding commitments*'; D34 '*consistent with international law*'; H67 '*reinforce and complement*'). We stress that the norms guide state behaviour, together with international law that regulates it. Both are part of the framework setting out what constitutes responsible State behaviour in the use of Information and Communication Technologies (ICTs).

We welcome the substantive references within the pre-draft to the inclusive mandate of the OEWG and its implementation through engagement with stakeholders (A7, D40, E47, F54 and G64, G65). We consider we could extend existing references to stakeholder engagement into A10 '*in various UN bodies and agencies and beyond*'.

We suggest that wording addressing the impetus for States to continue work together should be consistent and may be most helpfully based around the need to promote common understandings (B20 '*urgent need for ... cooperative measures*'; B21 '*actively strengthen its collective resolve*'; Chapeau G '*to continue to work together*'; G57 '*intensify international cooperation*'; H66 '*urgent need to collectively address*').

A. Introduction

We welcome the manner in which the context of our discussions is set out, clearly noting the relevance of developments in the field of ICTs to all three pillars of United Nations (UN) activity (A1) and particularly noting the importance of the opportunities inherent therein (A2). The description of the sections of the pre-draft as '*complementary and interdependent*' (A12) is helpful and reflective of our discussions. We are also pleased to see substantive references to the participation and leadership of women in decision-making processes (A9).

We suggest caution in the reference to '*civilian and military applications*' (A3) which appears set to define a separation in technologies from the outset of the pre-draft. Whilst our mandate expresses concern about the development of capabilities for military purposes, it is also careful to describe them as 'dual-use technologies'. This distinction makes clear that it is the way in which the technology is used that can be problematic, and not that the technology itself is inherently civilian or military.

We note that the reference to the OEWG being '*uniquely positioned*' (A6) is a theme which recurs throughout the pre-draft. The UK fully supports both the inclusive nature of the OEWG and the fundamental importance of these discussions. However, we also recognise the existence of other important discussions forums, including the Group of Governmental Experts (GGE), which bring their own important contributions to the global debate. As such, we are reluctant to rank one above another but seek to engage in each on their own merits.

We suggest strengthening references to the complementarity of the OEWG and GGE processes (A4/A5) and encourage all references to the elements of our framework (A5) to include the fact that they are '*underpinned by capacity building*'.

B. Potential Threats

We welcome the approach to concerns regarding specific technological trends and the requirement for a technologically neutral approach (B18). We endorse the approach taken in Chapeau B to frame the discussion but consider it could be clarified. It could start with the main factors that have led to a change in levels of risk – increased sophistication and ubiquitous technology, before moving onto the nature of threat that is enabled by these changes – increased frequency of attacks, increased vulnerability etc. We do not recognise the increased precision of attacks as a threat. Indeed, we consider this may be positive in terms of reduction of any potential for so-called 'collateral damage'.

The current draft does not accurately reflect the discussion related to the development or use of offensive ICT capabilities (B15). Whilst we recognise that some States held concerns about the '*militarisation of cyberspace*', others – including the UK – also clearly recognised that ICT capabilities can be developed and used, in a manner consistent with international law and called on States to be transparent about the existence of their own capabilities. Indeed, as the UK noted in its intervention in February, the use of ICTs in military contexts may be preferable to use of kinetic weapons and can be de-escalatory.

Overall, we suggest the pre-draft would benefit from additional text early in this section identifying the threat from States that undertake activity that is not in line with their obligations under international law or the expectations of the international community outlined by the norms of responsible State behaviour. Such behaviours undermine trust and stability in the system and increase the risk of misperception. We also note that discussion regarding the consequences and the impact of cyber operations such as the loss of life, and negative impact on economies, development, and human rights could be emphasised here.

C. International Law

We welcome the strong context setting provided by Chapeau C that international law applies in cyberspace, and that it is now necessary to exchange views on how it applies. The reaffirmation of the applicability of international law (C22) is significant. We strongly support reflection of the views that existing international law, complemented by the agreed voluntary, non-binding norms provides the framework that we need (C26). We also welcome the reference to capacity building to allow States to participate on an equal footing (C33).

Paragraphs C27-C29 do not fully reflect our discussions as currently drafted. The pre-draft should present arguments given for the development of new law through a treaty alongside the counter arguments also given by States, including the UK. These counter arguments and others raised by States must be reflected. Further, where principles from the UN Charter are listed (C23) all those mentioned during the discussion should be included. The pre-draft should use the exact language of the Charter, without expansion, for any references and clarify that the purpose of focusing on a specific area is to deepen discussion, not to pick selectively from the Charter (C32).

We note international humanitarian law (IHL) also applies to relevant military activities (which might include cyber operations) during a non-international armed conflict (C25, sentence 1). We strongly support the sentiment presented (C25, sentence 2) but suggest clarification to distinguish between questions of IHL and the use of force: '*neither encourages militarisation nor legitimises resort to conflict in any domain*'. For accuracy the wording '*including... civilian objects*' should be deleted (C27), and it should be clarified '*the issue of the applicability of [IHL]... be handled with prudence*' was not a majority view.

Regarding the reference to the proposal of a possible '*politically-binding commitment*' (C29), the UK is clear that resolutions of the UN General Assembly are themselves politically binding. We would therefore welcome clarification of the aim of such an additional commitment. Any references to the proposal for '*a common approach to attribution*' (C32) must equally reflect the views of those who proposed an alternative of sharing best practice and capacity building whilst maintaining a sovereign approach.

D. Rules, Norms and Principles for Responsible State Behaviour

We welcome the approach to Chapeau D that sets the voluntary, non-binding norms of responsible State behaviour in context alongside other elements of the framework.

The pre-draft could more strongly reflect consensus around the need to support improved implementation of the norms (D37). This should include the fact that norms can only be effective when implemented and that we have yet to complete the lifecycle of norm elaboration. Discussion of norms as a concept in 2010 led to the GGE testing them out in 2013, and then to committing fully to a significant expansion in agreed voluntary and non-binding norms in 2015. To complete the cycle, it is imperative that the OEWG takes the logical next step to focus on effective implementation of the norms.

We must consider any proposals for new norms (D39) in relation to both existing agreed norms and the remit of the OEWG. Many of the current proposals represent alternative wording to existing norms. Here, our clear focus must be on protecting the valuable consensus that exists in the General Assembly's endorsement of the 2015 GGE report.

Other proposals relate to existing norms but go deeper into a specific aspect of them. As we maintain our focus on providing support to States in their implementation efforts, it is possible that these could form the basis of explanatory text supporting possible approaches to implementation. An example of this could be the UK's proposal in previous submissions that under norm b) from the 2015 report, it may be helpful to describe the elements of

decision making involved in publicly or privately attributing malicious activity. These being that a decision to attribute will be based on an objective technical assessment and international law considerations. States will also want to take a national decision, based on diplomatic considerations, about whether to make known the results of any attribution they have conducted – publicly or privately.

Further proposals touching on principles of existing international law, such as that of the principle of non-intervention,^f may be better reflected in Section C. A final group of proposals, whilst worthy of concerted international attention, address topics that the UK considers to be beyond the mandate of the OEWG for instance: data protection, internet governance, national regulation, and free trade. We continue to actively support international discussion of these topics in appropriate fora.

E. Confidence Building Measures

We welcome the focus placed on operationalisation of confidence building measures (CBMs) (E41). It could be prefaced by a reference to the fact that States reaffirmed the value of CBMs. Listing all those CBMs mentioned in discussion may be challenging (E42). It could be better to note that there was detailed discussion of many existing, agreed CBMs, as well as some new proposals. The pre-draft could then move onto specific CBMs such as the Points of Contact (E44). On this issue, we note that Points of Contact are not just a prerequisite to CBMs, but also a CBM in their own right.

We consider that the importance of national and regional structures being in place (E46) cannot be underestimated. Such structures enable States to provide credible and well-exercised responses to incidents and require effort and resource to maintain. National Computer Emergency Response Teams (CERTs) are particularly important in this regard and should be highlighted. Equally important, but different, is the work regional organisations do to develop and implement CBMs. We consider this element, including the need for inclusion and possible universalisation could merit its own paragraph.

F. Capacity Building

The crucial nature of capacity building in supporting both the international cyberspace stability framework and the Sustainable Development Goals is well captured (Chapeau, F48). We fully support the references to two-way processes (F53) and the United Nations Women, Peace and Security agenda (F56). We consider any mention of the concept of the 'development of a global capacity-building agenda' (F55) would benefit from some clarification.

We suggest that additional text could be included in this section to note the richness of the discussion on this topic, as well as strengthening the reference to the need for cyber diplomats to participate in OEWG discussions (F50). We consider that this section of the pre-draft must recognise that coordination is key (F55), but should also highlight the need for all States and stakeholders to contribute to the mobilisation of funding and resource for capacity building wherever possible, as this underpins our ability to implement the framework and achieve the recommendations made in this pre-draft.

G. Regular Institutional Dialogue

We welcome the description of the history of the processes (G58) and the capturing of the proposal for Regular Institutional Dialogue based on the existing process (G62). Efforts to capture the proposals for Regular Institutional Dialogue based on new arrangements (G59, G60, G61) must reflect the call from several Member States that it was important to start from the purpose of any possible dialogue and how it would further international peace and

security. It would be beneficial to note that there was no consensus on such a purpose. A separate paragraph regarding possible characteristics of a dialogue would be welcome (G59 and G63).

H. Conclusions and Recommendations

We welcome the structure of this section and wealth of possible recommendations for consideration. We suggest streamlining these recommendations – for instance, multiple repositories may be unmanageable or ineffective. Where consensus exists, we may then consider whether the specifics of implementation of each recommendation can be agreed, including on a cost-neutral basis.

The UK will be pleased to consider supporting, subject to further discussion and specifics, many of these recommendations. However, we are currently unable to support referral to the International Law Commission (H68A). We think it would be premature to engage the ILC at this time, and consider it advisable to wait until there is a broader and deeper understanding amongst States as to how international law applies.

The UK may be able to support inclusion of certain recommendations subject to modifications and discussion of specifics of implementation. This includes:

- *'a repository of national practices regarding international rules, norms and principles...'* (H68B). Recommendations H68A and H68B should not overlap. If both are to be pursued H68B should focus on State implementation of norms whilst H68A addresses international law.
- *'establish a global mechanism for enhancing coherence in capacity-building efforts...'* (H68D) Our primary concern is to see as much resource as possible directed to capacity building in a coordinated manner. The establishment of additional mechanisms could increase the existing coordination challenge, whilst diverting much needed funding to its set up costs. We propose the following alternative wording: *The Secretary General be requested to call on Member States and stakeholders, including traditional development organizations and industry partners, to make available funding and resource in support of international capacity building on cybersecurity. All those in a position to contribute such expertise or resources to existing global mechanisms for enhancing coherence in capacity-building efforts in the use of ICTs, including at the regional and sub-regional levels, should do so.* (H68D)
- *'to identify and protect national and transnational critical infrastructure...'* (H68D) We propose the inclusion *'to cooperate, including with stakeholders'* on the basis of the extensive involvement of a broad range of stakeholders in the provision, operation and maintenance of critical national infrastructure.

The UK proposes inclusion of the following recommendations:

- As part of H68C: *Member States which have, or are developing, ICT capabilities which may be used in military contexts, be encouraged to acknowledge the existence of these capabilities at the organisational level and provide general information on the legal and oversight regimes under which they operate.*
- *'ICT-related capacity-building efforts in the field of international security should be guided by the following principles: Inclusive partnerships and shared responsibility; Ownership; Sustainability; Trust, transparency and accountability.* (H68D) These principles reflect the Busan Principles adapted to the ICT context.
- That the report of the Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019) be annexed to the OEWG report.