Foreign, Commonwealth
& Development Office

# UK Statements at the Seventh substantive session of the OEWG on Security of and in the Use of ICTs.

## STATEMENT BY THE UNITED KINGDOM ON EXISTING AND POTENTIAL THREATS

Chair, you asked states to consider the potential role of the OEWG in considering the threats presented by proliferation and the ready availability of sophisticated commercial and open-source ICT capabilities to non-State and private actors.

As we stated in December, the United Kingdom is concerned that the growing commercial market for cyber intrusion capabilities has the potential to increase instability in cyberspace.

This market includes:

- So-called “Hacking-as-a-service” companies that provide advanced, ‘plug-and-play’ cyber intrusion tools, including spyware, to access victim devices globally;

- So-called “Hackers for hire”, who carry out bespoke cyber intrusion for paying clients;

- Commodity cyber tools – often designed to improve cyber security through penetration testing, but with the potential to be misused, and finally;

- The vulnerability and exploit marketplaces.

These market components - in their totality - are having a transformational impact on the cyber threat landscape.

As the market grows, it is expanding the range of actors with access to advanced, commercially available cyber intrusion capabilities and is increasing the potential for irresponsible use.

The UK has observed, for example, the misuse of commodity penetration testing tools - tools designed originally to support cyber security - to instead support ransomware attacks and to threaten our critical national infrastructure.

Without international cooperation, we expect this phenomenon to increase the volume and the severity of cyber-attacks that we face. This will make it more difficult for our cyber defences to protect public institutions, organisations and individuals.

There is a need for States to agree on higher, consistent standards of oversight, accountability, and use, to discourage irresponsible activity across the market, whilst at the same time recognising the legitimate uses of these capabilities for national security and law enforcement.

This is why, last month, the United Kingdom and France partnered with 25 other States and 26 industry and civil society representatives to launch the Pall Mall Process. The Pall Mall Process is an international, multistakeholder initiative through which we will establish guiding principles and highlight policy options to address this complex issue.

The Pall Mall Process is inclusive, with representation from States, civil society and the private sector itself, and we welcome further state and non-state participants willing to commit to joint action, guided by the principles of Accountability, Precision, Oversight and Transparency, to mitigate the threat from irresponsible activity across the market.

We welcome the invitation in your guiding questions to discuss this issue here today. We recognise, equally, that this is only one aspect of the evolving cyber threat landscape.

Ransomware remains one of the greatest cyber threats to the United Kingdom’s Critical National Infrastructure and we should remain vigilant of its potential impact on international peace and security. Whilst criminality online is the most significant threat faced by the United Kingdom in terms of volume, the most advanced threats to UK Critical National Infrastructure still come from nation states. In December we made a statement on unacceptable attempts to use cyber operations to interfere in our democratic institutions and processes.

Beyond ransomware and the threat from malicious activity conducted by states, 2023 also saw state-aligned actors become a new and emerging cyber threat to critical infrastructure. The cyber activity of these groups often focuses on Distributed Denial of Service attacks, website defacements or the spread of misinformation, but some have stated a desire to achieve a more disruptive and destructive impact.

Thank you, Chair.

## STATEMENT BY THE UNITED KINGDOM ON RULES, NORMS AND PRINCIPLES

Chair,

Thank you for the draft discussion paper on a norms checklist.

While the norms are designed to be universal, their implementation is context dependent. We think the ‘voluntary, practical actions’ in your paper are at the right level of detail to allow states to decide the most appropriate ways to implement the norms.

Taken as a whole, the paper outlines a baseline of cybersecurity capacities. Establishing such a baseline is one of the recommendations of the Global Cyber Security Capacity Centre (GCSCC) based at the University of Oxford. Their recent research project, based on discussions with states and stakeholders, considered ‘Cybersecurity Capacities for the Application of UN Cyber Norms’.

They recommend - and my delegation agrees - that the future Programme of Action should support states to work towards a capacity baseline. This focus on baseline capacities echoes UNIDIR’s important work on Foundational Cyber Capacities, and has similarities to the evaluative approach taken by the UN Programme of Action [on] Small Arms and Light Weapons. Your draft paper is a promising step towards a universal baseline.

The University of Oxford’s findings also highlight the importance of raising awareness of the norms among policymakers responsible for cyber capabilities, and we encourage states to continue to do this within their national systems.

Our final observation on the draft guidance paper is that it includes some consensus guidance from the 2021 GGE Report, and some new content. As the United States has just said, we could further clarify the different levels of consensus contained in the draft document.

Chair,

Turning to your question on improving norms implementation, we will build on our remarks made yesterday on the growing commercial market for intrusive ICT capabilities.

The existing rules, norms and principles of responsible state behaviour, confidence-building measures and capacity building, provide a robust framework to guide the behaviour of States when interacting with this market.

Yesterday we outlined the main components of this market because the commercial dimension is significant. Market dynamics are super-charging the development and availability of advanced intrusion capabilities in a way that is new.

At the Sixth session of the OEWG the United Kingdom and France emphasised that there are legitimate uses for commercially available intrusive cyber tools. The private sector has, and will continue to have, a legitimate role in this market for cyber tools and services. States will continue to make use of these tools and services for national security and law enforcement. In this context, one of the questions for states, is what does responsible activity look like in practice?

This could include the following:

- First, states can set out their collective expectations with regard to the commercial market, so that it does not undermine stability in cyberspace and works to prevent commercially available cyber intrusion capabilities from being used irresponsibly.

- Second, governments can ensure that we are taking the appropriate regulatory steps within our domestic jurisdictions, through enforcing existing legal frameworks, evaluating or developing new domestic laws, or making use of policy levers, to identify and respond to irresponsible activity in the market.

- Third, it is incumbent upon states to conduct procurement responsibly, including by discouraging irresponsible behaviour when engaging private actors.

- Finally, when States choose to use cyber capabilities in support of national security and law enforcement, it is important that they do so in a way that is not only lawful but also responsible. States can share what 'responsible' state behaviour means in practice, for them. We believe this kind of transparency helps to avoid miscalculation and builds confidence.

    - Examples of this practice from the UK include our publication National Cyber Force: Responsible Cyber Power in Practice in 2023 and the exposition of our Equities Process in 2018, which outlines how decisions about the disclosure of vulnerabilities in technology are taken.

The Pall Mall Process seeks to provide a framework for inclusive dialogue between states and with stakeholders on this issue. The UN framework for responsible state behaviour is at the heart of the Process, and is referenced extensively in the Pall Mall Declaration published last month.

More work is needed to determine collectively what additional norms guidance might be needed in the context of advanced commercial cyber tools, but further recognition in the draft guidance that the norms guide not only states but also how states engage with the market for commercially available cyber capabilities, could be beneficial.

Our aim is that the outcomes of the Process will ultimately help to inform further good practice in the implementation of the norms

Thank you.

**STATEMENT BY THE UNITED KINGDOM ON INTERNATIONAL LAW**

Chair,

The United Kingdom welcomes this discussion on how international law applies in cyberspace. The UK underscores that it is through focussed and detailed discussions on this important issue that we are able to deepen our common understanding.

We are grateful for your guiding questions, and indeed your guidance throughout this process which has allowed areas of convergence in our common understanding to materialise.

The UK is also grateful to those delegations who have dedicated time outside of this room to further develop our detailed understanding of particular topics of international law.

We listened with interest to the statement of the distinguished delegate from Switzerland, given on behalf of a cross-regional group of 13 States, on the application of international humanitarian law.

The UK recalls that IHL applies to operations in cyberspace conducted in the furtherance of hostilities in armed conflict. 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.

As explained by Switzerland, the key principles of IHL – distinction, proportionality, humanity and military necessity – apply to attacks by cyber means in the same way as they do to an attack by any other means. IHL seeks to limit the effects of armed conflict. Its application to cyber operations in armed conflict does not encourage the militarisation of cyberspace.

We also echo the intervention by a cross-regional group of states, which identifies further areas of convergence in our common understanding of how international law applies. The UK highlights the content on state responsibility as a particularly important contribution.

Chair, we must build upon these efforts as we move forward in this process. International law discussions will be at their most effective when all states have a strong voice. We continue to encourage states to share their interpretations of how international law applies, and we commend the recent common position adopted by the African Union as a critically important contribution. We continue to underline the value of dedicated sessions in the OEWG and elsewhere for such focused discussions. In line with your guiding questions, the UK considers that scenario based discussions will enable us to turn those statements of principles into a practical application of the law.

The usefulness of the workshops hosted by United Nations Institute for Disarmament Research demonstrate that scenario based discussions are one of the best mechanisms that we have to take forward our discussions.

In response to your guiding questions, the UK would suggest that a focus on the sectors that States are most concerned to protect could be a fruitful way to build upon our discussions. For example, scenarios built around the healthcare sector and the provision of essential medical services, or critical energy infrastructure, or the conduct of free and fair elections.

Expert training and education has a critical role to play in furthering these discussions, and allowing broad participation in such scenario based discussions. A number of independent, non-governmental organisations are active in this area. The United Kingdom continues to support such training initiatives, often in partnership with regional organisations, and we welcome the continued work of UNIDIR in this area.

Chair, as we look to the future, the Programme of Action presents an exciting opportunity. Expert briefings and training from academics, civil society, or international organisations will enhance our collective international law capacity. This will provide the opportunity for a richer and more detailed exchange of views on the core doctrinal legal principles, as well as the application of those principles in practice through scenario based discussions. The UK looks forward to progressing our discussions.

Thank you, Chair.

## STATEMENT BY THE UNITED KINGDOM ON CAPACITY BUILDING

Thank you chair,

I'd like to begin by thanking the delegation of the Philippines for their presentation, which we will study further.

Chair, tomorrow marks International Women's Day celebrating the social, economic, cultural, and political achievements of women. My delegation would like to address your guiding question on gender perspectives, and reflect on the relevance of gender and inclusion issues in the context of (i) cyber threats and (ii) capacity building, both in the United Kingdom and internationally.

My delegation is troubled by the use of cyber capabilities by state actors to exploit social divisions based on gender, ethnic and religious identities. We are equally concerned about increases in repressive cyber activity targeting politically active women and human rights-defenders.

Chair, this trend is part of a wider, persistent effort to undermine democratic systems and open societies.

Non-Governmental Organisations are often targeted as part of this trend. In a 2023 survey of Non-Governmental Organisations by the CyberPeace Institute, over 40% had been a victim of cyber incidents, and a 2023 report by Microsoft found that Think Tanks and NGOs were the third-most targeted sector by state-sponsored threats. The International Centre for Journalists estimates that 40% of women journalists have been exploited by cyber activity while carrying out their work, with 20% reporting physical violence as a result.

With these trends in mind, we support Fiji's suggestion for further discussion of the cyber threats affecting women and vulnerable groups.

Domestically, we recognise that the equal participation of women in the cyber security sector is directly related to our ability to recognise and tackle the cyber threats faced by women. Our CyberFirst initiative aims to develop a skilled and diverse pipeline of talent. Since 2017, 56,000 girls between the ages of 12-13, have participated in the CyberFirst Girls Competition.

To protect open societies and democratic systems, we are working with international partners to deliver effective cyber security capacity building for civil society and other high-risk communities.

Reliable data shining a light on the scale of malicious cyber activity targeting vulnerable communities and civil society organisations remains a challenge. Cyber Threat Intelligence companies do not typically focus on threats to civil society, resulting in lower prioritisation of the cyber threat they face. Research conducted by several organisations, including CyberPeace Institute and the Centre for Long-Term Cybersecurity at the University of California, Berkeley is helping to provide a more complete picture. These organisations have applied to be accredited, but were blocked by Russia. This represents a needless hinderance to information sharing on this topic at the OEWG.

Chair, despite this challenging context, this OEWG remains a positive reminder of what is possible with the strong participation of women. The United Kingdom is a proud donor of the UN Women in Cyber Fellowship, and we commend the work of women, in all their diversity, who are shaping the governance of cyberspace.

Thank you.

## STATEMENT BY THE UNITED KINGDOM ON REGULAR INSTITUTIONAL DIALOGUE

Chair,

Thank you for your paper on draft elements for the permanent mechanism and thanks also to the delegation of France for their presentation on the possible structure of a Programme of Action.

Your paper, and France’s presentation, referred to thematic meetings to Implement the Framework. We see this as a significant opportunity to enhance dialogue on ICT security at the UN; to deepen our common understanding; and to build confidence.

As we have already heard, themes might include existing and potential threats such as ransomware, or specific sectors of critical national infrastructure such as the financial, energy or health sectors.

Thematic discussions should employ scenarios as a discussion tool to identify and foster convergence between states.

The agreed UN Framework of norms, international law, CBMs and capacity building could be used to consider each theme in a cross-cutting way. This would allow us to apply the agreed framework in a way that would relate closely to the priorities of UN members. It would be essential to have sufficient time in plenary to consider the whole framework against agreed themes.

The flexibility of a Programme of Action allows thematic, expert briefings, which would add further depth to discussions by states. We have a vibrant ecosystem of side events under this current OEWG but more of this discussion should be brought inside the future mechanism.

Experts could include, for example, cyber incident responders, international lawyers or even victims of cyber incidents. A mechanism that gives more time for delegations to interact with such stakeholders would add immeasurably to our discussions. In this way, dialogue under the future mechanism could become not only a confidence building measure but also an opportunity to build capacity.

International law will be a particularly important topic under the future mechanism. UNIDIR's workshop has been cited extensively but we should have these discussions inside the future mechanism. Future discussions on international law should seek to summarise and consolidate, in a detailed form, areas of convergence and agreement among States on how the UN Charter and the acquis of international law applies in cyberspace.

International law capacity building, conducted according to the agreed Capacity Building Principles, should be deployed to support states to participate in such discussions. The outputs of international law discussions under the future mechanism should use hypothetical examples to illustrate the application of international law. This will clarify the uncertainties that have been raised in this OEWG.

Chair, this week you noted that "we need to not only maintain the role of stakeholders but make it better." It is essential to involve stakeholders if we are to fulfil the 'functions' outlined in your paper, specifically the implementation of the framework and capacity building. We would like to see stronger and more concrete recognition of this in your paper and agree with Switzerland's recommendation in this regard. We reiterate that a strong voice for stakeholders is essential to discussions on cyber security issues. A Programme of Action provides the flexibility to deliver this, and we should take advantage of it.

Building on the aim of the future mechanism articulated in the previous APR, we believe that the scope of the future mechanism must clearly relate to the 'use of ICTs by states and the existing and potential threats to international security arising from this'. We would like to see this reflected more clearly in your paper.

On the question of meeting frequency under the future mechanism, we recognise the need to strike a balance between providing opportunity for progress whilst not overburdening states. The model of periodic Review Conferences and Biennial Meetings of states offered by other POAs could be a good example to follow.

Within the cycle of Review Conferences, we should spend a majority of our time on thematic discussions. We support the suggestion made by France relating to

Voluntary Reporting, to give an opportunity for states to show how they are meeting our collective commitments.

Finally, we strongly support the integration of hybrid meetings into the future mechanism, to facilitate the participation of all delegations.

Thank you.