Foreign &
Commonwealth
Office

Response to General Assembly resolution 71/28 "Developments in the field of information and telecommunications in the context of international security"

United Kingdom of Great Britain and Northern Ireland, July 2017

Executive summary

The United Kingdom welcomes the opportunity to respond to General Assembly resolution 71/28 entitled "Developments in the field of information and telecommunications in the context of international security", which builds on its response to resolution 70/237 in 2016. The United Kingdom uses its preferred terminology of 'cybersecurity' and related concepts throughout its response, to avoid confusion given the different interpretations of the term 'information security' in this context.

The United Kingdom recognises cyberspace as a fundamental element of securing critical national and international infrastructure and an essential foundation for economic and social activity online. Actual and potential threats posed by activities in cyberspace continue to be of great concern. Our new National Cyber Security Strategy, published in October 2016, will shape our efforts over the next 5 years to defend our assets, deter our adversaries and develop our cyber security sector.

The United Kingdom continues to take a leading role in the international debate on cybersecurity. We provided experts at all five United Nations Groups of Governmental Experts (UN GGE). Despite the lack of consensus in the 2017 group, we are committed to promoting an international stability framework for cyberspace based on the application of existing international law, agreed voluntary norms of responsible state behaviour and confidence building measures (CBMs), supported by coordinated capacity building programmes. The United Kingdom also welcomes efforts in the Organisation for Security and Cooperation in Europe (OSCE) and in other regional fora to provide proposals for implementing CBMs and will look to continue to lead by example in adopting such measures.

This response outlines the United Kingdom's work on supporting and improving cyber security and sharing best practice domestically and worldwide, including with international

partners to tackle cybercrime, major incidents and building capacity. The United Kingdom looks forward to seeing further progress and is pleased to be actively engaged on these issues. We will continue to participate fully in strengthening capability and international cooperation on cybersecurity.

Submission

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to respond to General Assembly resolution 71/28 entitled "Developments in the field of information and telecommunications in the context of international security". This submission builds on the United Kingdom's previous responses including the General Assembly resolution 70/237 in 2016.

"General appreciation of the issues of information security"

The United Kingdom continues to reiterate it will use its preferred terminology of 'cyber security' and related concepts throughout this submission. 'Cyber security' denotes efforts aimed at the preservation of confidentiality, availability and integrity of information in cyberspace, including the internet and other networks and forms of digital communication. The term 'information security' may cause potential confusion as it is used by some countries and organisations as part of doctrine regarding information itself as a threat against which additional protection is needed. The United Kingdom does not recognise the validity of 'information security' when used in this context since it could be employed in attempts to legitimise controls on freedom of expression beyond the Universal Declaration on Human Rights (UDHR) and the International Covenant on Civil and Political Right (ICCPR).

The actual and potential threats posed by malicious activities in cyberspace continue to raise concerns in the United Kingdom. Like many countries, our reliance on cyberspace as a fundamental element of critical infrastructure means that significant failure due to an incident or attack could cause severe disruption, economic damage or loss of life. We identified an increase in three trends that will require further consideration by the global community: states use of proxy actors for malicious cyber activity; the growing use by states of cyber capabilities with other techniques to achieve so-called hybrid attacks; and, the cumulative, destabilising effect of persistent, lower impact, state-sponsored cyber-attacks on a victim state or states.

Cyber security provides an essential foundation for activity online, enabling significant opportunities for economic and social development and growth. All parts of society have a role and duty in countering cyber threats. Given the majority of cyberspace's infrastructure is owned and operated by the private sector, continued engagement with them and other stakeholders is crucial.

It is also important to ensure cyber security efforts are not used to impose restrictions on freedom of expression beyond those in accordance with the UDHR and ICCPR. The United Kingdom supports the Human Rights Council's resolution 20/8, issued in 2012, which states the rights people enjoy offline, must also be protected online. The role of civil society organisations to ensure accountability and continued protection for human rights online is therefore particularly important.

"Efforts taken at the national level to strengthen information security and promote international cooperation in this field."

National approaches

The United Kingdom first published a National Cyber Strategy in 2011. In October 2016, a second edition issued, supported by funding of £1.9bn, outlining UK goals for the continued shaping and investment in cyber security over another five-year term.

The current strategy defines our vision and ambition to be secure and resilient to cyber threats as well as prosperous and confident in a digital world. We will continue to pursue

economic and social value from cyberspace where our actions, guided by our core values, will enhance prosperity, national security and a strong society. The strategy contains three main pillars, which the whole of our society has a role in helping to deliver:

- **Defend** our people, businesses and assets across the public and private sectors;
- **Deter** and disrupt our adversaries: states, criminals and hacktivists;
- **Develop** our critical capabilities and grow our cyber security sector.

Building on progress made under our 2011 strategy, the United Kingdom will pursue a more active and interventionist approach to improve overall levels of cyber security. The National Cyber Security Centre (NCSC) opened officially in February 2017. It is our definitive operational authority on cyber security and will lead this approach. The NCSC will act as the single authoritative voice on cyber security, helping to make the UK a safe place to live and do business online. The NCSC brings together key organisations that previously worked separately on cyber security and incorporates law enforcement elements to enhance its operational work. This is crucial to delivering improved cyber security to the UK.

The United Kingdom's efforts to tackle cybercrime are led by the National Cyber Crime Unit (NCCU) in the National Crime Agency (NCA), as well as its extended capability from its Regional Organised Crime Units (ROCUs). The UK continues to develop technological and investigative capabilities to support British law enforcement's ability to tackle the cyber-criminal threat. Through these specialist skills, and work with local, national and international partners, UK efforts focus on understanding the cyber-criminal threat, disrupting cybercrime activity, protecting the British public and industry, and preventing new actors engaging in cyber criminality. The NCS use experience and expertise from domestic initiatives to deliver capacity-building projects to increase the strength and speed of the global response to cybercrime.

Our new strategy underlines the UK's commitment to develop the cyber security sector and a skills base by continuing the integration of cyber security into the education sector, establishing two innovation centres and launching a £10 million Cyber Innovation Fund. We have three new interventions designed to increase the supply of cyber skills into the UK economy: an ambitious schools programme, apprenticeships in three critical sectors, and a retraining scheme to enable those who show a high potential for cyber security to transition into the profession. The NCSC's CyberFirst Programme 2017, launched on 2 February, offers over 1,250 free student places and up to 250 student bursaries worth £4,000 per annum on offer to develop a cyber-savvy cohort of students to help protect the UK's digital society. It is designed as a focal point that government and industry cyber skills initiatives can coalesce around; for example, in February 2017 over 8,000 schoolgirls aged 13 – 15, representing 2,100 school teams, completed the CyberFirst Girls 7-day competition, with over 200,000 answers submitted.

The United Kingdom advocates a multi-stakeholder approach and a primary NCSC objective is to bring the public and industry together with our intelligence sector to bolster resilience, but equally to integrate the private sector as a key actor in protecting and managing cyber security. We aim to work with business to help understand the risks that they face – the 2015 'Ten Steps to Cyber Security', accompanied by 'Cyber Attacks: Reducing the Impact' offer guidance and a framework for businesses to protect themselves against the most common threats. In addition, the NCSC's Industry 100 Programme, announced in February 2017, offers 100 people in industry the chance to join NCSC, to test and challenge government's thinking before returning to the private sector to drive change in industry.

The NCSC provides a unified source of advice, guidance and support on cyber security. The NCSC website (www.ncsc.gov.uk) is available to all organisations with an interest in cyber

security and provides tailored advice. For example, the Cyber-Security Information Sharing Partnership (CiSP) allows industry and government to exchange cyber threat information in real time and in a secure environment, increasing situational awareness and reducing the impact on UK business. More than 2,000 organisations are now part of CiSP. Those firms with a substantial stake in managing Critical National Infrastructure may also receive bespoke advice from NCSC cyber security advisors, including from the NCSC incident management, following a cyber incident and can benefit from tailored support.

To mark its launch in February 2017, the NCSC made freely available a tool to eliminate spoof emails that had been used to stop 300 million fake emails. Businesses in the most exposed sectors will also benefit from training facilities, exercises, testing labs, security standards and consultancy services provided or reinforced by the Government. Similarly, the NCSC's WebCheck service is available to scan websites for vulnerabilities and identifies strengths, weaknesses and out-of-date certificates all in an automatically generated report.

The United Kingdom recognises that improving cyber security is a long-term project – that is why we have pushed forward with a second five-year strategy and made further investment to support these goals. Forward-looking plans include:

- Further deepening our national capability to detect and address high-end threats;
- Ensuring law enforcement has the skills and capabilities needed to tackle cybercrime and maintain the confidence needed to do business on the internet;
- Improving cyber awareness and risk management among UK business, as well as highlighting the economic opportunity that cyber security provides through exports;
- Ensuring members of the public know what they can do to protect themselves and are demanding good cyber security in the products and services that they consume;
- Bolstering cyber security research and education, so we have the skilled people and know-how needed to keep pace with this issue into the medium-term;
- Exploiting the opportunities cyber offers to grow our domestic cyber security sector and improve cyber security exports; and
- Working with international partners to bear down on havens for cybercrime and build capacity, and to help shape international dialogue to promote an open, secure and vibrant cyberspace.

International approaches

The United Kingdom recognises our economic prosperity and social well-being increasingly depend on the openness and security of networks that expand beyond our own borders. We all stand to benefit from a free, open, peaceful and secure cyberspace and we have a shared responsibility and mutual interest in improving our collective cyber security.

No national government can tackle the cyber threat alone, and international collaboration is central to our strategy. We reiterate our unequivocal support for the multi-stakeholder model, whereby governments do not exercise exclusive control over a domain and infrastructure that is largely owned and operated by the private sector. The international debate on cyber security should recognise the importance of this model, in particular its emphasis on shared responsibility.

While the nature of our future relationship with the EU is still to be determined, our relations with European partners on cyber security in support of our common security and prosperity remains as important as ever. For example, the EU Foreign Affairs Council agreed in June

2017 to develop a framework for a joint EU diplomatic response to malicious cyber activities, the cyber diplomacy toolbox. Taken together with the EU Cyber Security Strategy, this demonstrates the importance the EU places on cyber security of the EU and its neighbourhood and the UK will continue to look for opportunities to build on this important work.

The NCSC will play a key role in the UK's work to promote international collaboration: engagement with a wide range of international partners will include building technical capabilities and capacity, incident handling, and information sharing and situational awareness.

Over the next five years, the UK will therefore pursue international action to:

- collaborate operationally in tackling threats to common interests;
- develop a common understanding of responsible state behaviour in cyberspace;
- develop the cyber security capabilities of our international partners; and,
- safeguard the benefits of a free, open, peaceful and secure cyberspace.

This work will build on and reinforce the United Kingdom's role in helping to stimulate international debate, showcased prominently through the launch of the London Process of Global Conferences on Cyberspace in 2011, which succeeded in putting this issue on the international agenda. Further work is required to help build global consensus around the rules of the road for state behaviour in cyberspace, and the next Conference in this series hosted by India in 2017 will provide an important platform to continue this debate.

The United Kingdom has been an active member of the United Nations Group of Government Experts (UNGGE) on developments in the field of information and telecommunications in the context of international security. Despite the lack of consensus in the 2017 group, we are committed to promoting an international stability framework for cyberspace based on the application of existing international law, agreed voluntary norms of responsible state behaviour and confidence building measures (CBMs), supported by coordinated capacity building programmes. This work will augment our efforts in the OSCE to encourage implementation of CBMs – the United Kingdom leads by example in adopting measures and we are pressing for movement from paper commitments to practical implementation.

We continue to work closely with the NATO Co-operative Cyber Defence Centre of Excellence in Estonia. The recognition by NATO of cyberspace as a domain of operations has sparked meaningful conversations on building resilience across the membership. In February 2017, the UK signed the NATO Cyber Defence Memorandum of Understanding so that we can share our expertise with our international allies, and learn from their experiences.

The UK also funded the Commonwealth Telecommunications Organisation (CTO) to develop and implement a national cyber governance model for Commonwealth countries. This had directly supported the Commonwealth in developing National Cyber Security Strategies with Botswana, Cameroon and Uganda. The CTO are now expanding that assistance to a second large tranche of Commonwealth countries.

The United Kingdom ratified the Convention on Cybercrime (the Budapest Convention) in 2011 and reiterates it is the best model in the bid to tackle international cybercrime. It aims to facilitate international cooperation on cybercrime, provide for national criminal procedural

powers necessary for the investigation and prosecution of offenders and promote greater law enforcement cooperation. We encourage all states to adopt suitable legislation. In addition, the NCA works with international partners to build worldwide capability and capacity, housing national bureaux for Interpol and Europol and seconding officers to both organisations. We are also committed to tackling child sexual exploitation online and the UK will be the home for the new secretariat of the joint WePROTECT/The Global Alliance Against Child Sexual Abuse Online organisation

The United Kingdom takes a strong lead in developing and sharing best practice, experience and information with regard to cyber security. This plays an important part of both the formal and ad-hoc dialogues the UK holds with bilateral partners on cyber security, which continued to grow in number and substance over the past year. Recognising the importance of multi-stakeholder approaches, we have also played an active role in the IGF's Best Practice Forum on cybersecurity and in relevant discussions at ICANN.

The United Kingdom Cyber Security Capacity Building Programme, delivered by the Foreign and Commonwealth Office, has a history of building cyber resilience around the world and will provide additional support over the next five years. Over the past four years, the UK has invested over £9.38m in efforts to increase cyber resilience around the world, helping more than 50 countries to improve their cyber security, reducing their own vulnerability to cyber harm and by extension the UK's. This support included national cyber security capacity assessments, public awareness raising, and advice on regulation, better industry standards, cybercrime exercises, law enforcement training and strengthening Computer Security Incident Response Teams. The programme has used and promoted UK private sector expertise, which underpins our multi-stakeholder approach.

With UK programme assistance, 49 countries have now conducted national cyber security capability self-assessments, using a model designed by government funded Oxford Global Cyber Security Capacity Centre. Several of these countries have gone on to develop national cyber security strategies, using the findings of the self-assessments. The success of the UK self-assessment approach has led other donors to adopt it. In 2016-17, the World Bank decided to expand their use of Oxford's self-assessment model with lending partners and the Oceania Centre in Melbourne agreed to support self-assessments in Asia Pacific.

We welcome the decision by several countries, including Germany, Singapore and Australia, to start new capacity building programmes.

"Relevant international concepts aimed at strengthening the security of global information and telecommunications system."

The United Kingdom supports consensus agreements of the previous UN GGEs that existing international law applies in cyberspace. We see the discussion of and development of normative behaviour and the operationalisation of CBMs as the key approach to shaping responsible state behaviour in cyberspace – we believe any attempts to conclude comprehensive treaties or similar instruments would not positively enhance cyber security at present. It will be important to build on the cumulative recommendations contained in UN GGE 2013 and 2015 reports to help take the debate forwards.

We reaffirm our commitment to a free, open, peaceful and secure cyberspace. The foundation for responsible state behaviour in cyberspace is our mutual commitment to existing international law, including the respect for human rights and fundamental freedoms, and the application of international humanitarian law to cyber operations in armed conflict. We reaffirm that the UN Charter applies in its entirety to state actions in cyberspace, including the prohibition of the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in self-defence in response to an armed attack (Article 51). The law of state responsibility applies to cyber operations in peacetime,

including the availability of the doctrine of countermeasures in response to internationally wrongful acts.

We are also keen to see increased engagement in the international debate on cyber security. Alongside other governments, we support the work of ICT4Peace, which provides training modules and course to public officials, technical staff academics and NGOs to enable them to promote and negotiate international norms of responsible state behaviour, confidence building measures and international cooperation. We work with ICT4Peace to widen state participation on cyber security issues, so that countries which are not regular contributors can establish themselves on a global stage; this will broaden the debate and give countries the tools, skills and knowledge to engage at an international level. In support of this initiative, four workshops have been delivered in Columbia in 2014, Kenya and Singapore in 2015 and Ethiopia in 2016.

"Possible measures that could be taken by the international community to strengthen information security at the global level."

In the view of the United Kingdom, the measures that could make the most significant contribution to strengthening cyber security at the global level include:

- Continuing discussions among States in regional and multilateral fora to develop common understandings of acceptable state behaviour in the interests of international cyber security based on existing international law;

- The future development of bilateral and regional confidence building measures for cyberspace aimed at increasing the transparency and predictability of state behaviour;

- The establishment of computer emergency response teams (CERTs) by States as a focus for incident-handling and information-sharing, and the development of regional and wider cooperation between CERTs;

- Encouraging greater law enforcement cooperation on cybercrime, and the adoption of suitable legislation such as the Convention on Cybercrime;

- Recognising that a multi-stakeholder approach to internet governance will best serve the aims of increasing security and stability as well as promoting economic and social progress;

- Enhanced engagement and dialogue with industry and the private sector more broadly to take account of their critical role and ownership in the cyber domain.