Response to General Assembly resolution 70/237
“Developments in the field of information and telecommunications in the context of international security”

United Kingdom of Great Britain and Northern Ireland, May 2016

Executive summary

The United Kingdom welcomes the opportunity to respond to General Assembly resolution 70/237 entitled “Developments in the field of information and telecommunications in the context of international security”, which builds on its response to resolution 69/28 in 2015. The United Kingdom uses its preferred terminology of ‘cyber security’ 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 that cyberspace is a fundamental element of critical national and international infrastructure and an essential foundation for economic and social activity online. The United Kingdom makes reference to the 2015 National Security Risk Assessment that confirmed cyber continues to be a Tier One threat to National Security. The United Kingdom’s allocated funding of £860m during the life of the previous National Cyber Security Strategy (2011-2016) will be supported by an additional allocation of £1.9bn over the next five years. A new National Cyber Security Strategy will be published in 2016, including the establishment of a new National Cyber Security Centre.

The United Kingdom recognises that international collaboration is central to successful cyber security. We continue to promote a free, open, peaceful and secure cyberspace so its economic and social benefits are protected and available for all. The United Kingdom takes a lead on cross border cyber security challenges through initiatives such as the WePROTECT Global Alliance to End Online Child Sexual Exploitation. We are also committed to sharing best practice internationally and to ensuring that the global community has access to assistance in developing their cyber security capabilities.

The United Kingdom continues to participate actively and constructively in the international debate on cyber security. We have provided experts for all four United Nations Groups of Governmental Experts (UNGGEs) and consider that the consensus report of the last group made valuable progress in re-affirming that international law is applicable in
cyberspace and that States’ adherence to international law, in particular their UN Charter obligations, is an essential framework for their actions in their use of ICTs.

The United Kingdom also welcomes continued discussion of potential future confidence-building measures in cyberspace at the Organisation for Security and Cooperation in Europe (OSCE) and similar work in other regional organisations.

The United Kingdom is pleased to be actively engaged on these important issues and looks forward to further participation in strengthening capability and international cooperation on cyber security.
Submission

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to respond to General Assembly resolution 70/237 entitled “Developments in the field of information and telecommunications in the context of international security.” This submission builds on the United Kingdom’s response to General Assembly resolution 69/28 in 2015.

General appreciation of the issues of information security

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

The actual and potential threats posed by activities in cyberspace continue to be of great concern to the United Kingdom. Like many countries, the United Kingdom’s reliance on cyberspace as a fundamental element of critical national infrastructure means that significant failure due to an incident or attack could cause severe disruption, economic damage or loss of life.

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 and combating cyber threats. Given that the majority of cyberspace’s infrastructure is owned and operated by the private sector, continued engagement with them is crucial.

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

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

National approaches

The United Kingdom published a National Cyber Security Strategy in November 2011 which set out a vision for the next five years to derive economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values, enhance prosperity, national security and a strong society. The strategy was supported by the National Cyber Security Programme (NCSP), which with dedicated funding of £860m over the course of the programme, continued to support a wide range of activities to develop and strengthen cyber security. The following outlines some of these activities that supported the 2011-2016 NCSP.

The United Kingdom has continued to invest in capabilities and technical infrastructure to increase its ability to understand and defend against increasingly sophisticated cyber threats, and to integrate
cyber into defence planning. The government has also strengthened the cyber security of the United Kingdom’s critical national infrastructure, and has invested in cross-government research into cyber standards and best practice. We have also enhanced national capabilities to protect and defend ourselves against cyber attack.

CERT-UK, the United Kingdom’s Computer Emergency Response Team, was launched at the end of March 2014. It has responsibility for national-level cyber security incidents and aims to work closely with government departments and industry partners to enhance cyber resilience, including by collaborating with national CERTs worldwide to improve understandings of the cyber threat. The CyberSecurity Information Sharing Partnership (CiSP), based within CERT-UK, provides a safe space for businesses and government to exchange information on cyber threats and develop responses in real time. CiSP now has over 5,800 members from over 2,200 organisations. Working with Police and Regional Organised Crime Units, CERT-UK has also begun a nationwide initiative to introduce regional nodes on CiSP that promote the sharing of cyber security information regionally to help local businesses to protect themselves from cyber attacks.

CERT-UK has also launched an exercising programme for critical national infrastructure organisations and government departments. The aim of these is to walk organisations through the actions they would need to think about in the event of a major cyber incident and test their responses in real time.

We are committed to tackling cyber crime and making the UK one of the most secure places in the world to do business online. 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 (ROCu), the UK continues to develop technological and investigative capabilities that underpin British law enforcement’s ability to tackle the cyber criminal threat. Through its specialist skills, and work with local, national, and international partners, UK efforts focus on understanding the cyber criminal threat, disrupting cyber crime activity, protecting the British public and industry, and preventing new actors engaging in cyber criminality.

The United Kingdom continues to invest in innovative initiatives to raise awareness and develop cyber skills at all levels. Much of the work is focused on inspiring young people to consider science, technology, engineering and maths (STEM) careers and on ensuring the correct educational provision at all levels from aged 14 to postgraduate. This will guarantee that all people leaving education have a basic understanding of cyber security before entering the workforce, and motivate those with the aptitude to pursue a career in cyber security.

The United Kingdom also supported efforts by:
- Funding a Massive Open Online Course in cyber security run by the Open University. As well as raising awareness amongst a mass audience the course aims to encourage those with an interest to take the subject further. Over 60,000 students had taken the course by October 2015;
- Increasing the number of British universities recognised as academic centres of excellence in cyber expertise. In addition, three ‘virtual’ research institutes have been established to focus on the science of cyber security, automated programme analysis and verification, and trustworthy industrial control systems and facilitate collaboration between leading researchers;
- Encouraging more apprenticeships and other formation routes through activities including developing new cyber programmes that match private sector needs and raise awareness of future cyber security careers.

The United Kingdom also works with businesses to help understand the risks that they face. Refreshed at the start of 2015, the ‘Ten Steps to Cyber Security’ were first launched in 2012 and aim to offer a framework for businesses to protect themselves against the most common cyber threats. To date, the various products offered by the Ten Steps programme have been uniquely downloaded by
over 50,000 UK businesses. The guidance now includes an accompanying paper “Cyber Attacks: Reducing the Impact”, which sets out what a common attack looks like and how it’s executed, in addition to an online security training course for small businesses.

The use of the Ten Steps guidance has been backed by a Cyber Security Governance Health Check for the 350 largest companies by market capitalisation listed on the London Stock Exchange. The third health check took place in 2015.

Because all sizes of business are affected by the cyber security threat, tailored guidance for smaller companies has been published, a free online learning package is available and a cyber action plan for small businesses worked up by industry. In 2014, a government-backed and industry-supported organisational scheme for cyber security, known as Cyber Essentials, was developed to give industry a clear baseline to aim for in addressing cyber security risks to their company. Since its launch, 2,413 Cyber Essentials and Cyber Essentials Plus certificates have been issued.

Improving cyber security is a long-term project. Forward-looking plans currently include:

- Investment of an additional £1.9bn to our cyber security efforts over the next five years including an ambitious skills programme and growing the cyber sector a programme of active cyber defence;
- The establishment of a new National Cyber Security Centre (NCSC) in late 2015, which will simplify the current cyber security landscape and establish a “one stop shop” for cyber security;
- 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 knowledge 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 internet is making the world a better place, but recent events remind us that good online security is crucial in the modern digital economy. The NIS Directive (Network and Information Security), informally agreed in Brussels in 2015 will make businesses in the UK and Europe safer and more secure. The United Kingdom has helped ensure the deal strikes a good balance: enabling cooperation between countries across Europe, whilst being flexible, proportionate and minimising the impact on business.
No national government can tackle the cyber threat alone, and international collaboration is central to our strategy. The United Kingdom reiterates that it unequivocally supports the multistakeholder 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 for its emphasis on shared responsibility.

The United Kingdom’s aim internationally is to improve the free, open, peaceful and secure cyberspace so that the economic and social benefits of cyberspace are protected and available for all. The United Kingdom continues to help stimulate international debate about the future of cyberspace through the series of conferences which began in London in November 2011, and welcomed the successful conference in The Hague in April 2015. In particular, The Hague’s Global Conference on Cyberspace developed firm capacity building commitments from many participating countries and companies.

The United Kingdom has provided an expert for each of the four United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security (UNGGE). We will again send an expert to the next UNGGE beginning in August 2016. These groups offer a valuable opportunity for further developing common understandings of norms of state behaviour in cyberspace, and how international law applies.

The United Kingdom actively participated in negotiations at the OSCE, leading to the adoption of an additional set of regional Confidence Building Measures to reduce the risk of cyber conflict through improved understanding, communication and cooperation, and will continue to work constructively on the implementation of these and development of further measures.

A UK expert seconded to the NATO Co-operative Cyber Defence Centre of Excellence in Estonia has led projects during 2015 to support the Centre’s strategic priorities. GCHQ have also shared with NATO details of their work to certify Masters Degrees in cyber security. This has sparked interest from both NATO and individual Allies keen to replicate the programme in their respective countries.

The United Kingdom has 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 larger tranche of Commonwealth countries.

The United Kingdom signed the Convention on Cybercrime (the Budapest Convention) in 2001 and ratified it in 2011. The Convention aims to facilitate international cooperation on cybercrime, provide for national criminal procedural powers necessary for the investigation and prosecution of offences, and promote greater law enforcement cooperation. Fifty five countries have signed up to the Convention to date with 49 having ratified. The United Kingdom continues to encourage other states to adopt suitable legislation and reiterates that it sees the Convention as the best model in the bid to tackle international cybercrime.

The NCA works with partners in key jurisdictions to build worldwide capability and capacity to tackle cybercrime operationally. The NCA houses the United Kingdom’s national bureaus for Interpol and Europol, and the NCCU has officers seconded to both organisations to improve the international fight against cybercrime.

The United Kingdom is committed to tackling the sexual exploitation of children online. Since the first WePROTECT Summit was hosted in London in 2014, 63 countries and international organisations, as well as leading technology companies and NGOs have signed up to this initiative. In November 2015 a merger between WePROTECT and The Global Alliance Against Child Sexual Abuse Online was announced, with a view to creating a single global initiative with the influence,
expertise and resources to transform how online child sexual exploitation is dealt with worldwide. The secretariat of this new organisation will be hosted within the United Kingdom Home Office.

The United Kingdom takes a strong lead in developing and sharing best practice, experience and information with regard to cyber security. It is committed to ensuring that the global community has access to assistance in developing their cyber security capabilities. The Foreign and Commonwealth Office’s International Cyber Security Capacity Building Fund has a proven track record of building cyber resilience around the world. With our 2015/16 programme we have funded a total of 30 projects to help deliver scalable and sustainable solutions, especially to developing countries. We continue to build on previous successes and productive relationships with governments, academia, industry and civil society around the world.

These projects have covered a wide geographical sweep and activities have included helping to develop national cyber security strategies, cybercrime capabilities, legislation and CERTs. For instance, the United Kingdom has worked with the Organisation of American States to develop national cyber strategies in the Americas which will help those countries protect themselves and mitigate upstream risks to the United Kingdom. In the past year it has also worked with the Global Prosecutors E-Crime network to improve prosecutors’ ability to tackle cyber crime worldwide and we continue to work with the UN Office on Drugs and Crime in building cyber security capacity in East Africa to prevent and respond to cybercrime.

Furthermore, the Global Cyber Security Capacity Building Centre, hosted by the University of Oxford, aims to improve the impact, scale and pace of international capacity building efforts, in part through aggregating, assessing and open sourcing information. It has developed a capability maturity model to help countries understand their own strengths and vulnerabilities and is developing a model to help countries and companies better understand the complex harms caused by cyber attacks.

**Relevant international concepts aimed at strengthening the security of global information and telecommunications systems**

The United Kingdom supports the consensus agreement of the previous UNGGEs that existing international law applies in cyberspace. The next UNGGE presents a valuable opportunity to consider further how it applies and what norms of behaviour, agreed internationally, can help to promote cyber security and cooperation between states and prevent conflict. We see the UNGGE discussion as the best means of taking forward these understandings and do not believe that attempts to conclude comprehensive multilateral treaties or similar instruments would make a positive contribution to enhanced international cyber security at present.

The United Kingdom is 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 courses 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. Four workshops have been delivered to date, in Colombia 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 particular in the UNGGE 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 multistakeholder 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.