Response to General Assembly resolution 69/28
“Developments in the field of information and telecommunications in the context of international security”

United Kingdom of Great Britain and Northern Ireland, May 2015

Submission

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to respond to General Assembly resolution 69/28 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 68/243 in 2014.

General appreciation of the issues of information security

The United Kingdom reiterates that it will use its preferred terminology of ‘cybersecurity’ and related concepts in the present submission. ‘Cybersecurity’ 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 and the International Covenant on Civil and Political Rights.

The actual and potential threats posed by activities in cyberspace continue to be of great concern to the United Kingdom. These activities may be carried out by state or non-state actors, including criminals and terrorists. Like many countries, the United Kingdom’s reliance on cyberspace as a fundamental element of critical national infrastructure and underpinning of daily life means that significant failure due to an incident or attack could cause severe disruption, economic damage or loss of life.
Cybersecurity 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, it is essential that the public and private sectors work closely where appropriate.

It is also important to ensure that efforts to increase cybersecurity 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 cybersecurity strategy in November 2011 which set out a vision 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 is supported by the National Cybersecurity Programme (NCSP), which with dedicated funding of £860 million over five years continues to support a wide range of activities to develop and strengthen cybersecurity. The following outlines some of these activities.

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 cybersecurity of the United Kingdom’s critical national infrastructure, and has invested in cross-government research into cyber standards and best practice.

CERT-UK, the United Kingdom’s Computer Emergency Response Team, was launched at the end of March 2014. It has responsibility for national-level cybersecurity incidents and works closely with government departments and industry partners to enhance cyber resilience, including by collaborating with national CERTs worldwide to improve understanding 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 1000 members. Working with police Regional Organised Crime Units, CERT-UK has also begun a nationwide initiative to introduce Regional Cyber Information Sharing Partnerships. These aim to promote the sharing of cybersecurity information regionally to help local businesses to protect themselves from cyber crime.

The United Kingdom continues to invest in innovative initiatives to raise awareness and develop cyber skills at all levels. A government-funded Massive Open Online Course in cybersecurity run by the Open University opened for registration in 2014. As well as raising awareness amongst a mass audience the course aims to encourage those with an interest to take the subject further. 55,000 people have enrolled as of May 2015 and we are looking to expand the scheme internationally.
As of March 2015, a total of 13 British universities are now recognised as academic centres of excellence in cybersecurity research. In addition, three ‘virtual’ research institutes have been established to focus on the science of cybersecurity, automated programme analysis and verification, and trustworthy industrial control systems and facilitate collaboration between leading researchers.

To ensure a wide pool of talent, the United Kingdom is also working to encourage apprenticeships and other formation routes through activities including developing new cyber programmes that match private sector needs and raise awareness of future cybersecurity careers. In March 2015, the United Kingdom launched a new Cyber First scheme, an elite development programme for the next generation of UK cybersecurity talent. Each student in the initial pilot will receive £4000 per year to study relevant undergraduate science, technology, engineering and mathematics courses. During summer vacations or years out they will work either within government or in leading UK cybersecurity companies. Cyber First is the latest in a series of initiatives supporting the UK’s interventions at every level of of the education system from aged 11 to postgraduate, building up a skilled workforce and supporting the development of cyber specialists and a more cyber capable workforce. This includes new apprenticeships, introducing cybersecurity into the National Citizen Service, and ensuring that cybersecurity is included in relevant courses leading to computing and digital qualifications for 16-19 year olds.

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 Cybersecurity’ were first launched in 2012 and aim to offer a framework for businesses to protect themselves against the most common cyber threats. 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. The use of the Ten Steps guidance has been backed by a Cybersecurity Governance Health Check for the 350 largest companies by market capitalisation listed on the London Stock Exchange. The second health check took place in 2014; carried out by the department for Business, Innovation and Skills in partnership with the audit community, it assessed how the boards of top UK companies are managing cyber risks and enables them to benchmark themselves against their peers and competitors.

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. Cyber Essentials comprises the core actions necessary to mitigate the majority of cyber threats by unsophisticated threat actors using attack tools widely available on the internet. A Cyber Essentials badge is awarded to organisations successfully independently assessed and certified through the scheme’s assurance framework, and to ensure the scheme is cost-effective and suitable for smaller businesses there are two levels of assurance available, Cyber Essentials and Cyber Essentials Plus.

Improving cybersecurity is a long-term project and over the coming months we will be looking to refresh our strategy as part of the wider review of the UK’s National Security Strategy and Strategic Defence and Security Review. However, our focus on building resilience, growing skills and business, reducing cyber crime and tackling the threats we face will remain central to our approach.
International approaches

No national government can tackle the cyber threat alone, and international collaboration is and will remain central to our strategy.

The United Kingdom’s aim internationally is to improve the openness, vibrancy, security and stability of cyberspace so that the economic and social benefits of cyberspace are protected and available for all while upholding national and international security and values. We pursue this aim through extensive bilateral and multilateral engagement, participating in a range of regional and international organisations and fora (both government-focused and involving industry, academia and civil society), and through specific programmes of work.

For example, 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 United Kingdom welcomed the launch of the Global Forum for Cyber Expertise which represented an important step forward in developing a more coordinated approach to capacity building internationally.

The 50th meeting of the Internet Corporation for Assigned Names and Numbers’ (ICANN) was held in London in June 2014 and was well-attended, with a record number of some 3000 participants. The United Kingdom’s investment in this process is helping promote a model for governing the internet which remains open, accountable, transparent and secure.

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), which presents a valuable opportunity for further developing common understandings of norms of state behaviour in cyberspace, and how international law applies.

The United Kingdom participated in negotiations at the Organisation for Security and Cooperation in Europe, leading to the adoption of the first 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.

In September 2014 the NATO Summit in Wales agreed the Enhanced NATO Policy on Cyber Defence. Concrete steps have been taken to protect NATO’s own networks and make progress across the Alliance on a number of key policy priorities including prevention, detection, resilience, recovery and defence. The United Kingdom’s initiative for a NATO Industry Cyber Partnership was agreed at the Summit and was highlighted in the Summit Declaration. In June 2014 the United Kingdom became a full member of the NATO Cooperative Cyber Defence Centre of Excellence.

The United Kingdom also funded the Commonwealth Telecommunications Organisation to develop and implement a national cyber governance model for the Commonwealth countries. Ratified this year, this is now in the process of being implemented by several Commonwealth members.
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. The United Kingdom encourages other states to adopt suitable legislation and reiterates that it sees the Convention on Cybercrime as the best model in the bid to tackle international cybercrime.

The #WeProtect Summit to tackle online child sexual exploitation was hosted by the Prime Minister in London in December 2014. A Global Fund to support programmes to protect children has been launched to take forward the objectives from the Summit, which include global action to identify and protect victims, to remove child sexual abuse material from the internet, to strengthen co-operation across the world to track down perpetrators, and to build global capacity to tackle sexual exploitation of children online.

CERT-UK played a significant role in protecting the Commonwealth Games and the NATO Summit in Wales. CERT-UK will be leading joint exercising with its American counterpart later this year. It also works with other CERTs internationally to ensure the response to transnational incidents is prompt and coordinated and that the United Kingdom can benefit from international sharing of information on cybersecurity threats.

The United Kingdom takes a strong lead in developing and sharing best practice, experience and information with regard to cybersecurity. It is committed to ensuring that the global community has access to assistance in developing their cybersecurity capabilities. The Foreign and Commonwealth Office’s International Cybersecurity Capacity Building Fund has funded thirty projects in 2014/15 to help deliver scalable and sustainable solutions, especially to developing countries.

These projects have covered a wide geographical sweep and activities have included helping to develop national cybersecurity 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 Caribbean which will help those countries protect themselves. It has also worked with the Council of Europe to help establish a National Cyber Crime Centre in Romania, which acts as a co-ordinating body for all Council of Europe capacity building activity relating to cyber crime and has also led cyber crime investigations. The Centre has enabled the Council of Europe to manage the growing number of assistance requests and is now able to support countries worldwide in their efforts to tackle cyber crime, recently including Sri Lanka and South Africa.

The United Kingdom is keen to see increased engagement in the international debate on cybersecurity. Alongside other governments, we are pleased to be supporting the work of ICT4Peace, which provides training modules and courses to public officials, technical staff, academics and non-governmental organisations to enable them to promote and negotiate international norms of responsible state behaviour, confidence building measures and international cooperation. We continue to work with ICT4Peace to widen state participation on cybersecurity 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. Two workshops were delivered in Colombia in 2014 and Kenya in 2015.

At the heart of these efforts, the Global Cybersecurity 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 (CMM) in order to identify national and regional needs for capacity building, which is being rolled out internationally by working with several international organisations including the World Bank, the Organisation for American States and the Commonwealth Telecommunications Organisation. The Centre’s other product, its online Portal, has been designed to facilitate greater information exchange among cybersecurity researchers and consumers of research. The Portal is also the central information-sharing platform for the Global Forum on Cyber Expertise.

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

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 cybersecurity should recognise the importance of this model, in particular for its emphasis on shared responsibility.

The United Kingdom supports the consensus agreement in the previous UNGGE that existing international law applies in cyberspace. The current UNGGE presents a valuable opportunity to consider further how it applies and what norms of behaviour, agreed internationally, can help to promote cybersecurity 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 cybersecurity at present.

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 cybersecurity 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 cybersecurity 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;
- Enhanced engagement and dialogue with industry and the private sector more broadly to ensure that work in this area is complementary to their critical role and ownership in the cyber domain, and strengthens the security and resilience of cyberspace.