Response to General Assembly resolution 68/243 “Developments in the field of information and telecommunications in the context of international security”

United Kingdom of Great Britain and Northern Ireland,
May 2014

Submission

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to respond to General Assembly resolution 68/243 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 67/27 in 2013.

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. 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. 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.

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, continued engagement with them is crucial.

It is also important to ensure that efforts to increase cybersecurity are not misused to impose restrictions on freedom of expression beyond those permitted in 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 has four core objectives and progress so far has been strong. It has been underpinned by an allocation of £650 million to be used in a four-year programme to transform the United Kingdom's response to cyber threats. That funding was increased in 2013 by an additional £210 million for 2015/16. The following outlines some key activities conducted by the United Kingdom to strengthen cybersecurity in the context of defence, crime, major incidents and skills.

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.

The National Crime Agency (NCA) was established in October 2013 by the Crime and Courts Act. The NCA brought together the Serious Organised Crime Agency's Cyber Unit and the Metropolitan Police's Central e-Crimes Unit into the National Cybercrime Unit (NCCU), which brings together and strengthens cyber capabilities across the United Kingdom's law enforcement community. It leads the United Kingdom's response to cybercrime and chairs a multi-agency Strategic Governance Group which brings together key stakeholders to have the greatest impact against cyber threats.

The United Kingdom's Computer Emergency Response Team (CERT-UK) was launched at the end of March 2014. It has responsibility for national-level cybersecurity 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.

CERT-UK includes the United Kingdom's Cybersecurity Information Sharing Partnership (CISP) which was launched in March 2013 as a collaborative initiative between government and industry to share threat and vulnerability information. CERT-UK will run cyber exercises with key sectors both nationally and internationally.

The United Kingdom continues to invest in awareness-raising at all levels and the development of cyber skills. In conjunction with private sector partners and professional bodies, the United Kingdom launched the Get Safe Online campaign in 2005. The campaign aims to raise awareness of cybersecurity and give practical day-to-day advice to consumers and small businesses. A further campaign, Cyber Streetwise, was launched in January 2014 to encourage good cybersecurity behaviour. Cyber Streetwise has strong support from industry and its second phase is planned for launch in the autumn.

The United Kingdom also works with businesses to help understand the risks that they face. The 'Ten Steps to Cybersecurity' were launched in 2012 and aim to offer a framework for businesses to protect themselves against the most common cyber threats. In April 2014, the Government launched the Cyber Essentials, a scheme which identifies the essential technical controls that organisations must have in place in order to mitigate threats. An accompanying assurance framework will allow organisations to be independently assessed.

A total of 11 British universities are now recognised as academic centres of excellence in cybersecurity research. Three 'virtual' academic institutes have been established to focus on the science of cybersecurity, automated program analysis and verification, and trustworthy industrial control systems. To ensure a wide pool of talent, the United Kingdom is also working to encourage apprenticeships in cyber and other formation routes by activities including developing new cyber programmes that match private sector needs and raise awareness of future cybersecurity careers.

Improving cybersecurity is a long-term project. Forward-looking plans currently 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, including by setting up nine regional organised crime units and broadening cyber training in local police forces;
- Ensuring critical UK systems and networks are robust and resilient by working with lead government departments and regulators to find and tackle vulnerabilities and establishing a Security Operations Centre for public sector networks;
- Improving cyber awareness and risk management among UK business, as well as highlighting the economic opportunity that cybersecurity provides through exports;
- Ensuring members of the public know what they can do to protect themselves and are demanding good cybersecurity in the products and services that they consume;
- Bolstering cybersecurity research and education, so we have the skilled people and know-how needed to keep pace with this issue into the medium-term. This will include increasing cyber internships and the launch of a Massive Open Online Course in cybersecurity by the Open University;
- 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'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. 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, followed by Budapest in 2012 and Seoul in 2013. The next conference will take place in the Netherlands in 2015. Each of the conferences has included valuable debate on cybersecurity alongside other issues.

The United Kingdom has provided an expert for each of the three United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security (UNGGE) and will also do so for the 2014/15 Group, 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. On behalf of the European Union, the United Kingdom has exchanged views on the development of CBMs with the ASEAN Regional Forum and looks forward to further dialogue with the ARF and other regional organisations in this field.

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 National Crime Agency works with partners in key jurisdictions to build worldwide capability and capacity to tackle cybercrime operationally. The National Crime Agency houses the United Kingdom's national bureaus for Interpol and Europol, and the National Cyber Crime Unit will soon have officers seconded to both organisations to improve the international fight against cybercrime.

CERT-UK aims to work with other states in relation to national cyber incidents at bilateral and multilateral levels (depending on the nature and scale of the incident) and will seek opportunities to share information in relation to cyber threats and vulnerability to increase the overall situational awareness. It is in the process of establishing international contacts with other countries' own CERTs.

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 backed over twenty projects in 2013/14 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.

Furthermore, 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 been developing a capability maturity model against which nations can benchmark themselves and will soon launch an online portal collating information on available assistance.

The United Kingdom also aims to help ensure that future cadres of global leaders will have a good understanding of cybersecurity issues. We have created a new engagement process in which Chevening, Commonwealth and Marshall Scholars from Africa, Asia and America will be selected to attend the annual academic centres of excellence conference.

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

The United Kingdom supports the consensus agreement in the last UNGGE that existing international law applies in cyberspace. The forthcoming UNGGE presents a valuable opportunity to consider further how it applies and what norms of behaviour, agreed internationally, can help to promote cybersecurity 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, codes of conduct or similar instruments would make a positive contribution to enhanced international cybersecurity at present.

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.

The United Kingdom is also pleased to see the development of initiatives such as the recent NETmundial meeting hosted by Brazil, which helped to strengthen global consensus on the multistakeholder model of internet governance and establish common ground. The United Kingdom 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.

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 a normative framework 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;
- Recognising that a multistakeholder approach to cyberspace will best serve the aim 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.