Foreign & Commonwealth Office

Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.

United Kingdom of Great Britain and Northern Ireland, September 2019

Executive summary

In this non-paper, the United Kingdom aims to share our approach to the 11 norms of responsible state behaviour that were part of the 2015 Group of Government Experts (GGE) report, and endorsed by the General Assembly.

These agreed, voluntary and non-binding norms build on GGE reports in 2010 and 2013 and form a key part of establishing how international law applies in cyberspace, and the United Kingdom is setting out our approach to help encourage transparency, sharing of best practice, and increase mutual understanding.

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.

This paper details some of the practical steps we have taken to implement the voluntary, non-binding norms recommended in previous GGE reports and endorsed by the UN General Assembly in 2010, 2013 and 2015. Whilst we continue to support and reinforce the application of international law in cyberspace, the activity set out in this paper is UK best practice and is not evidence of state practice with regard to the emergence of customary international law. We have included both steps we have taken domestically, and information as to how we have coordinated, cooperated and built capacity internationally.

UK approach

The United Kingdom is clear that international law applies in cyberspace, as it does in all other domains of operation, including the UN Charter in its entirety. In his speech in May 2018, the then UK Attorney General set out the UK's view on the applicability of international law in cyberspace. 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.

The UK is also clear why the use of 'cyber security' rather than 'information security' is an important distinction. '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.

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 Universal Declaration of Human Rights and ICCPR; the rights people enjoy offline must also be protected online.

The UK's approach to cyber deterrence has four principles. First, we will always seek to discover which state or non-state actor was behind any malign cyber activity. Secondly, we will respond. That could include public attribution, in concert with partners, exposing not only who carried out the action but, so far as possible, how it was done, thereby helping the cyber security industry to develop protective measures. Thirdly, we will aim to prosecute those who conduct cybercrime, demonstrating they are not above the law. And finally, with partners, we will consider further steps, consistent with international law, to make sure we don't just manage current cyber attacks but deter future ones as well.

UK policy and practical steps to ensure norms of responsible state behaviour are implemented

Norm 1 (UNGGE 2015 report, paragraph 13a) – Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are agreed to be harmful or that may pose threats to international peace and security.

The United Kingdom is committed to promoting an international stability framework for cyberspace based on the application of existing international law, agreed voluntary, non-binding norms of responsible state behaviour and confidence building measures (CBMs), supported by coordinated capacity building programmes.

We work with partners across the OSCE to encourage implementation of CBMs – leading by example in adopting measures, including championing OSCE CBM 5 on exchange of best practice, awareness raising and information sharing on capacity building. We are pressing for movement from paper commitments to practical implementation. Transparency in this regard also helps build trust and confidence between states in cyberspace, which is essential to maintain peace and security in cyberspace. We participate constructively in existing international and multi-stakeholder fora (including the EU, NATO, UN, G7, G20, OSCE, OAS, ASEAN, ITU, OECD, WSIS and others) for discussing both responsible state behaviour in cyberspace and internet governance.

The UK also engages in bilateral dialogues on cybersecurity with a wide range of other states, which contributes to our mutual understanding of respective approaches to cyber security, which helps increase stability and security in cyberspace.

We have also worked closely with our partners in the Commonwealth. At the Commonwealth Heads of Government Meeting in London in 2018, all Commonwealth states agreed to the Commonwealth Cyber Declaration[1]. It is the world's largest inter-governmental commitment to cyber security cooperation signed by Heads of Government. It is an important expression of our shared desire to maintain a free, open, inclusive and secure cyberspace. The Declaration contains a particular emphasis on promoting stability in cyberspace through international cooperation, including CBMs, common standards and approaches, the application of international law in cyberspace, and tackling cybercrime. The UK supports this Declaration with £15m in programme funding, to help low and middle income Commonwealth countries build capacity to help tackle cyber threats.

The UK continues to develop approaches and policies, alongside international partners, to increase stability and security in the use of ICTs, and prevent those practices that may threaten international peace and security. We work with partners,

[1] https://www.chogm2018.org.uk/sites/default/files/Commonwealth Cyber Declaration pdf.pdf

both bilaterally and multilaterally, to help maintain international peace and security in cyberspace. We also contribute to setting international standards for new technologies, which can help prevent ICT practices that are harmful.

On behalf of the UK, Jeremy Wright QC MP, the then Attorney General, set out the UK's position on the application of international law in cyberspace in a speech at Chatham House on 23 May 2018.

The UK 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.

We also look to develop industry standards on security of technology, which help build cyber resilience globally. We continue to be active in the international standards space, as in order for this issue to be resolved, we know that there will need to be alignment at an international level. For example, in February 2019 the first globally applicable technical standard for Internet of Things security was released, based on the Code of Practice for Consumer Internet of Things Security[2], which we published in October 2018. We are now working to transpose this into a European Standard (EN), and we encourage ETSI members to play an active role in shaping this before then.

<u>Norm 2 (UNGGE 2015 report, paragraph 13b)</u> – In case of ICT incidents, States should consider all relevant information, including, inter alia, the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences

The United Kingdom, through its National Cyber Security Centre (NCSC) has developed an integrated approach to national incident management in the public and private sectors. This has brought together several approaches that existed for different sectors and, in doing so, has simplified the process. The new incident management approach has been operating since mid-2016. Since it became fully

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

operational in 2016, the NCSC's cyber security front line has helped to support with 1,167 cyber incidents – including 557 in the last full 12 month period (October 2017-October 2018). The latest NCSC annual report reveals most attacks against the UK that are managed by the NCSC, are carried out by hostile states.

Since January 2018, the UK's cyber community has implemented a new incident categorisation framework. This new approach fully aligns the NCSC's work with law enforcement agencies to defend against the growing threat, with incident responders now classifying attacks into six specific categories (C1-6) rather than the previous three. The new system ranges from attacks targeting the Government and critical national infrastructure through to individual citizens.

The NCSC will produce an impartial assessment of the nature of the incident drawing upon and weighing up the evidence from a wide range of sources. Incident Assessment Reports usually answer the following questions: based on intent and past form, and who is most likely to be responsible, and is this incident part of a wider trend? The report will open with a set of key judgements, followed by a confidence statement, which is based on the certainty behind the source material used. Further commentary is provided to support and expand upon the key judgements.

Based on this assessment, the UK will consider how to respond. The UK will use a range of options across diplomatic (including but not limited to attribution), economic and law enforcement to respond. Any decision to respond will take into account the wider context at the time and be in accordance with international law.

On attribution specifically, the UK Government's starting point is that attribution is a political decision and can be a powerful deterrence tool when deployed effectively. The UK will decide whether attribution – public or private – is in the UK's national interest. We consider attribution a sovereign political decision on a case by case basis. Attributing is a first step and opens up further response options, in the UK national interest and under international law.

When considering attribution, the UK Government will consider, alongside a technical assessment from the National Cyber Security Centre:

a. **Geopolitical and bilateral factors:** our wider objectives towards the State in question, including national security objectives, regional stability, the sensitivities of our allies and the likelihood of counter-response.

b. **Impact on victim:** the impact of UK attribution (especially public) on the victim(s) of a cyber-incident will be reviewed.

c. **Impact on law enforcement activity:** the impact of UK attribution (especially public) on the law enforcement investigation of a cyber-incident; for instance the effect on our ability to arrest and prosecute.

d. **UK values and ability to operate:** attribution should not limit the UK's ability to carry out our own cyber operations in full adherence to domestic and

international law. Attribution should be in line with our stated positions in national and international fora, where we champion a free, open, peace and secure cyberspace, and adhere to norms of state behaviour. It should enhance the UK's reputation as a competent cyber actor and weigh up the risk of misattribution.

e. **Wider response options:** the effect of UK attribution on other deterrence activity, which the UK government has agreed or is implementing. The timing of attribution should be calibrated to enhance the impact of other responses.

There are challenges to attribution in cyberspace, but this does not mean it is impossible. Nor should it be viewed in isolation; it is one tool amongst many in a range of options (political, diplomatic, and economic) to respond to malicious cyber activity, with the aim of deterring this activity.

Norm 3 (UNGGE 2015 report, paragraph 13c) – States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

The United Kingdom has criminalised wrongful acts using ICTs through, for example, the Computer Misuse Act[3]. This makes it an offence to conduct unauthorised access to computer systems, and to use this access to facilitate other offences, such as modifying or damaging computer systems and networks.

Overall Strategy: The 2015 National Security Strategy (NSS)[4] confirmed that cyber remains a top threat to the UK's economic and national security. The threat posed by cyber attacks continues to grow in scale and complexity. The National Cyber Security Strategy (NCSS) recognised that to achieve the desired outcomes over the five years of the strategy required the UK Government to intervene more actively and to use increased investment. The NCSS is supported by £1.9billion of transformational investment up until 2021.

Active Cyber Defence: Through the National Cyber Security Centre, the UK has taken an interventionist approach aimed at making the UK an unattractive target to criminals or states. The UK's Active Cyber Defence Programme (ACD) is an automated set of interventions intended to tackle a range of commodity attacks. It aims to tackle, in a relatively automated way, a significant proportion of the cyber-attacks that hit the UK. In other words, ACD aims to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time. This has demonstrated that there are targeted interventions that governments can take – alongside the private sector – to improve the digital homeland.

UK ACD measures have:

---

3 https://www.legislation.gov.uk/ukpga/1990/18/contents

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf

- Taken down nearly 140,000 phishing sites in the last two years and protected 1.3 million government internet users;
- Helped the UK tax authority block half a million attempts to spoof it in the programme's first year. HMRC used to the 16th most spoofed brand in the world. Now, in 2019, it is the 146th.
- Reduced the UK's share of global phishing attacks from 5.3 per cent to 2.2 per cent. The UK used to account for 1 in 20 attacks, now that is around 1 in 50.

These measures are already having a tangible security benefit by reducing the return on investment and making the UK an unattractive target for cybercriminals. We now need to incentivise others to do similar things to scale up the benefits. The NCSC has also commenced pilot ACD initiatives in CNI sectors, and we will continue to design and pilot new tools to help protect customers and businesses from commodity cyberattacks.

<u>Norm 4 (UNGGE 2015 report, paragraph 13d)</u> – States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

The United Kingdom has a well-established law enforcement response, which works with other states to prosecute cybercrime. Within the National Crime Agency (NCA), the National Cyber Crime Unit (NCCU) is the UK lead for tackling this threat. The NCCU has the responsibility and capability to lead the operational response, coordinate activity across a range of partners and provide specialist cyber support and expertise across law enforcement. The NCA also has a network of international liaison officers and is responsible for a number of national functions, including responsibility for liaising with Europol and Interpol to cooperate with other States to tackle cybercrime

The National Cyber Security Centre also helps to share information and combat common cyber threats with international partners. The UK has a very good level of bilateral cooperation with many allies and partners. This cooperation includes sharing of best practices, including on policy and advice, sharing of assessments and understanding of threats.

The UK ratified the Cybercrime ('Budapest') Convention[5] in 2011, as the foremost international instrument on enhancing cooperation against cybercrime. Through this, the UK actively exchanges information to prosecute cybercrime, including through a 24/7 law enforcement network of contacts specified in the Convention. The UK is also an active participant, and has provided voluntary contributions to work to

[5] https://www.gov.uk/government/publications/convention-on-cybercrime--2

develop a Second Additional Protocol to the Convention to enhance the speed and efficiency of international evidence sharing.

The NCSC is committed to publishing its advice and guidance on its website[6]. In doing so, it takes its understanding of cyber security, distills it into practical guidance and makes this available to all, including international partners.

The UK is also an active donor to support countries develop their own cybercrime capabilities. This:

- Establishes strong international partnerships, e.g. our National Cyber Crime Unit (NCCU) has developed strong ties with its foreign counterparts, for example, in Eastern Europe, South East Asia and Africa, including through capacity building initiatives.
- Builds cybersecurity capacity of partners: As part of the National Cyber Security Strategy (2016-2021), the UK has committed to developing cybersecurity capacity of partners. The UK's international cyber security programme funds projects and activities globally, and has since 2012 funded activities aimed at building cyber security capacity in over 100 countries, including some cybercrime specific programmes.
- Works with international organisations, e.g. UK also works closely with Europol Cybercrime Centre (EC3), Interpol Cyber Fusion Centre, Global Forum on Cyber Expertise, National Cyber-Forensics and Training Alliance (within USA), as well as other forums.

On preventing terrorist use of the internet, the UK established the first Counter Terrorism Internet Referral Unit in 2010, following which, the UK has actively engaged with communication service providers (CSPs) to encourage a proactive industry-led response to detecting and removing terrorist content from their platforms. In 2017, following five terrorist attacks, the UK called for a greater, collaborative effort from CSPs, resulting in the establishment of the Global Internet Forum to Counter Terrorism in June 2017. Together with France and Italy, the UK also brought the issue to global attention at a UN event in September 2017, following calls for further action through the G7 and G20. The UK has encouraged CSPs to develop automated technology to tackle the threat and have worked with data science companies to develop bespoke technical tools, to aid the efforts of industry, particularly smaller platforms. The UK supports initiatives to regulate on the dissemination of terrorist content online and on 8 April, the UK published the Online Harms White Paper, which sets out our intention to legislate domestically on a comprehensive range of online harms.

Norm 5 (UNGGE 2015 report, paragraph 13e) – States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions

[6] https://www.ncsc.gov.uk/section/advice-guidance/all-articles?q=&defaultTypes=guidance,information,blog-post,collection&sort=date%2Bdesc&start=0&rows=20

A/HRC/RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age), to guarantee full respect for human rights, including the right to freedom of expression;

The United Kingdom is committed to a free, open and secure internet, where people can, without undue obstruction, communicate and access information online.

The UK is firmly committed to the right to privacy, freedom of expression in line with international human rights law. The UK co-sponsored the 2012, 2014 and 2016 UN Human Rights Council resolutions on the protection, promotion and enjoyment of human rights on the internet. In accordance with those resolutions, we continue to affirm that the same rights people have offline must be protected online. The UK has also supported Human Rights Council and General Assembly resolutions on the right to privacy in the digital age. At Human Rights Council 41, the UK co-sponsored a resolution on New and Emerging Digital Technologies and Cyber. The UK is also a party to various human rights treaties under the UN and Council of Europe and is a member of the Organization for Security and Cooperation in Europe whose remit includes human rights.

The UK has put in place a combination of policies and legislation to give effect to the human rights treaties that it has ratified. Those which are relevant in this case include:

- **The Human Rights Act 1998**[7] (HRA), sets out in domestic legislation certain rights contained in the European Convention on Human Rights, including freedom of expression and the right to privacy. This has been further articulated by the Freedom of Information Act 2000[8] and the Data Protection Act 2018[9].
    - Article 8 of the ECHR protects the right to respect for private and family life, home and correspondence (online and offline). This also includes the protection of personal data.
    - Article 8 also stipulates that there shall be no interference by a public authority with the exercise of this right except in accordance with the law and where it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
    - Article 9 of the ECHR protects freedom of thought, conscience and religion, Article 10 protects freedom of expression and Article 11 protects freedom of assembly and association. The Convention

[7] https://www.legislation.gov.uk/ukpga/1998/42/contents
[8] https://www.legislation.gov.uk/ukpga/2000/36/contents
[9] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

stipulates that there shall be no interference by a public authority with the exercise of these rights except where prescribed by law, where necessary in a democratic society and in the interests of one of the aims given in the Articles. Additional legislation (such as the Public Order Act 1986) further regulates the State's intervention in the exercise of these rights.

- **The Data Protection Act 2018** sets new standards for protecting general data, in accordance with the General Data Protection Regulation (GDPR), giving people more control over use of their data, and providing them with new rights to move or delete personal data. The Act provides a bespoke framework tailored to the needs of the UK's criminal justice agencies and the intelligence services, to protect the rights of victims, witnesses and suspects while ensuring we can tackle the changing nature of the global threats the UK faces. It also allows the unhindered flow of data internationally whilst providing safeguards to protect personal data.

- **The Investigatory Powers Act 2016**[10] provides a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies. A new independent Investigatory Powers Commissioner, Lord Justice Adrian Fulford, was appointed in February 2017 to authorise and oversee the use of Investigatory Powers. The Investigatory Powers Act 2016, and indeed all UK communication surveillance legislation, is entirely consistent with the UK's international human rights obligations. The cornerstone of the Investigatory Powers Act is that use of the powers must be considered necessary and proportionate.

- In April 2019, the UK Government published the **Online Harms White Paper**[11], setting out plans for world-leading legislation, in order to make the UK the safest place in the world to be online. This approach will make companies more responsible for tackling a comprehensive set of online harms and protecting users' safety, especially children and other vulnerable groups. The new regulatory framework will be overseen by an independent regulator, with a statutory obligation to protect users' rights online, particularly the rights to privacy and freedom of expression. The framework will also increase transparency and accountability of companies, including with regard to any restrictions on the right to freedom of expression. Moreover, the UK's approach to tackling online harms broadly will enable more people to exercise their right to freedom of expression, by ensuring anyone can participate in online discussions without risk of bullying or being attacked on the basis of their identity, e.g. their gender, race, disability, sexuality, religion or age.

[10] http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
[11] https://www.gov.uk/government/consultations/online-harms-white-paper

<u>Norm 6 (UNGGE 2015 report, paragraph 13f)</u> – A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

The United Kingdom recognises that states have a legitimate right to develop sovereign cyber capabilities, but in doing so each state has an obligation to ensure their use is governed in accordance with international law.

On behalf of the UK, the then Attorney General Jeremy Wright QC MP set out the UK's position on the application of international law in cyberspace, including cyber operations, in a speech at Chatham House on 23 May 2018[12].

<u>Norm 7 (UNGGE 2015 report, paragraph 13g)</u> – States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account, inter alia, General Assembly resolution 58/199 (2003) "Creation of a global culture of cybersecurity and the protection of critical information infrastructure", and other relevant resolutions;

Regulatory Framework: Almost all UK critical infrastructure owned and operated by the private sector is covered by cyber regulation, requiring companies to have appropriate cyber resilience in place for their essential services, and to report cyber incidents. In 2018, the UK regulations implementing the EU Security of Networks and Information Systems (NIS) Directive came into force, representing the first instance of cross-sector CNI cyber regulation in the United Kingdom. In support of the NIS regulations the UK has produced sector-independent CNI cyber security guidance and has developed a framework which supports the assessment of the cyber resilience of regulated organisations.

Also in 2018, the General Data Protection Regulation (GDPR) came into force alongside the new Data Protection Act 2018, placing a comprehensive set of new obligations on public and private sector organisations to protect all the personal data that they collect and process. The NCSC and the Information Commissioner's Office (ICO) have developed a set of GDPR security outcomes. This guidance provides an overview of what the GDPR says about security and describes a set of security-related outcomes that all organisations processing personal data should seek to achieve.

Mapping Critical Systems: The NCSC, lead government departments and industry have worked together to develop a process which identifies the systems that are critical to the UK CNI, including dependencies between the sectors. We have mapped the critical systems that are vital to the everyday operation of the CNI. By better understanding the interconnectedness of the various sectors, we can improve their resilience. This work will provide an overarching view of our CNI, enabling

[12] https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

industry and government to concentrate their cyber security efforts where they will have the most impact.

International Cooperation: The UK both contributed to the development of and participated in the European Union Agency for Network and Information Security Cyber Europe 2018 exercise for the aviation sector. The exercise drew participants from 30 countries and enabled each to test their national incident response procedures as well as their ability to coordinate with European partners in the event of a widespread cyber incident.

Developing our Workforce: The UK is committed to building a cyber skills pipeline from school age through to Masters Degrees, apprenticeships and beyond. A key pillar of our national strategy remains the development of a cyber security workforce (in the private as well as the public sector). Over 25,000 young people have engaged with the NCSC's CyberFirst initiatives since 2016, including free courses, competition bursaries and apprenticeships. This activity is supported by work across government including the publication of a draft national cyber security skills strategy[13], working with schools, universities and the existing workforce to develop, train and retrain skills in cybersecurity:

We supported the development of the recent OECD Recommendation on Digital Security of Critical Activities, which aims to modernise the protection of critical information infrastructure protection (CIIP) in the era of digital transformation by applying the OECD digital security risk management approach to the protection of critical economic and social activities.

In the summer of 2019, we will launch a comprehensive review of the UK's cyber regulatory and incentives landscape, including NIS. This builds on our last review in 2016, to understand what has worked well, and where further action is needed to drive the necessary improvements in cyber security behaviours and practices.

<u>Norm 8 (UNGGE 2015 report, paragraph 13h)</u> - States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty;

The National Cyber Security Centre's international partnerships help to share information and combat common cyber threats. The United Kingdom is proactive in establishing constructive bilateral cooperation with allies and partners as well as NATO. This cooperation includes sharing of best practices, including on policy and advice, sharing assessments and our understanding of threats. The UK recognises that the increasingly global nature of cyber incidents requires strong relationships

[13] https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary

with appropriate authorities across the world. The National Cyber Security Centre's Incident Management team operates 24/7, and is the national point of contact for any requests for assistance. At the OSCE, the UK has supported efforts on Confidence Building Measure 8 on the creation of a list of national policy and technical points of contact. And in NATO, the NCSC has encouraged members of the Alliance to embrace their role as lead responders to global attacks from state and non-state actors.

We also have set up a 24/7 point of contact within the National Crime Agency to exchange information with States to tackle all cybercrime related threats, in accordance with the Budapest Convention.

Norm 9 (UNGGE 2015 report, paragraph 13i) – States should take reasonable steps to ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

As risks, threats and technology change it is important that states are able to respond. That is why the United Kingdom has undertaken a thorough review of the 5G supply chain to ensure the secure and resilient rollout of 5G. The Telecoms Supply Chain Review introduced a tougher, strengthened new security regime for our telecoms infrastructure.

Secure by Design: We are addressing this through implementation of our national strategy, and investment in our national programme. The NCSC has produced public advice and guidance aimed at all sections of the UK economy and society; this has helped improve awareness across the UK.

The UK published a Code of Practice for Consumer IoT Security in October 2018. This outlines 13 high-level and outcome focused guidelines that manufacturers should embed into their products to make them 'secure by design' and to take the burden from consumers having to secure their own products. We have made this available for international partners. It has been translated into Japanese, Mandarin, German, Korean, French, Spanish and Portuguese.

In the UK, we are preparing to place the priority guidelines of the Code of Practice on a regulatory footing. Alongside this, one area we are actively exploring is how to build an effective labelling scheme that will inform consumers and retailers of manufacturers' cyber security standards, without overburdening consumers.

We are supporting manufacturers of all sizes to implement the Code, which is why we published a mapping document to support implementation. A number of core manufacturers (including Centrica Hive and HP Inc.) have already made a formal pledge, and support from DCMS and NCSC is available to manufacturers and retailers who wish to make a public commitment to proactively protect their consumers in advance of expectations being mandatory.

Advice and Guidance: Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats. From 1 October 2014, Government required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

The UK, primarily through the NCSC, provides advice on supply chain issues. This has included the accreditation of products, services and consultants under schemes run by the NCSC.

The NCSC has published guidance to provide organisations with an improved awareness of supply chain security, as well as helping to raise the baseline level of competence in this regard, through the continued adoption of good practise. This guidance proposes a series of 12 principles, designed to help organisations establish effective control and oversight of their supply chain.

Proliferation: To prevent the proliferation of malicious ICT tools and techniques, in 2013, the UK supported the inclusion of intrusion software in the control list of the Wassenaar Arrangement[14](WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

Norm 10 (UNGGE 2015 report, paragraph 13j) – States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

Equities Process: In November 2018 the United Kingdom published details of the Equities Process operated on behalf of the Government by GCHQ[15]. The Equities Process is the means through which decisions are taken on the handling of vulnerabilities found in technology to achieve the best overall outcome in the interests of the United Kingdom

Whilst carrying out operational activity, analysts working at GCHQ or elsewhere within Government may identify vulnerabilities in technology. These vulnerabilities may represent a risk to the security of systems in the UK and of our allies. These include Government departments, critical national infrastructure, companies and private citizens. In some cases, the same vulnerabilities might provide a means by which the UK intelligence community could obtain vital intelligence that could be used to protect the UK and its interests.

The Equities Process provides a mechanism through which decisions about disclosure are taken. Expert analysis, based on objective criteria, is undertaken to decide whether such vulnerabilities should be released to allow them to be mitigated or retained so that they can be used for intelligence purposes in the interests of the

[14] https://www.wassenaar.org/
[15] https://www.gchq.gov.uk/information/equities-process

UK. The starting position is always that disclosing a vulnerability will be in the national interest.

Advice and Guidance for Organisations: Over the past two years the NCSC has been working on the Vulnerability Co-ordination Pilot. The aim of the pilot is to identify the best way to take an organisation through the process of establishing their own vulnerability disclosure process. Over the next year or so, the NCSC will provide more information regarding the steps required to create an organisation-wide vulnerability disclosure process. This will include providing guidance for both the private and public sectors.

Vulnerability Reporting: The NCSC has recently launched its vulnerability reporting service[16], which acknowledges the crucial role security researchers play in helping to secure UK government web services. The quickest way to remediate a security vulnerability is to report it to the system owner. However as it can be hard to find the right contact, so researchers can now report the vulnerability to us (NCSC).

<u>Norm 11 (UNGGE 2015 report, paragraph 13k)</u> – States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity;

As a responsible state, the United Kingdom agrees a state should not conduct activity in relation to its own CERT or that of any other state which would be contrary to its legal obligations.

The UK has provided advice, training and exercises to enable the creation and maintenance of national Computer Security Incident Response Teams (CSIRT). In addition, the UK has supported international fora, funding e.g. the Forum of Incident Response & Security Teams (FIRST), to help them develop training material. For example, in the Americas, grants to the OAS helped them launch a virtual platform for the Americas CSIRT network (CSIRTAmericas.org) in September 2016. As of December 2017, the national CSIRTs of 16 countries were members of the platform network. The project also supported a training course in incident management for 61 government officials from 13 OAS member states; a set of cyber challenges for 265 participants from 18 OAS member states during the International CyberEx 2016; and another cyber exercise for 54 teams from 17 member states during the International CyberEx 2017.

Date: 05/09/2019

[16] https://www.ncsc.gov.uk/vulnerability-reporting