



Position of the United Kingdom of Great Britain and Northern Ireland for the purpose of the conference held by Forum for 21st Century on 29 November 2011 reflected in the second draft of the negotiation paper, regarding the global cyber security issues.

The UK would like to thank the Forum for 21st Century for the prompt execution of the second draft.

After an in-depth analysis of the draft proposed by the Forum for 21st Century, the UK has come to following conclusions and suggestions.

- 🇬🇧 The UK welcomes Forum's initiative to attempt to create legal basis for usage and control of the Internet and local intranets. The UK recognises the complexity of this huge and difficult task at hand, as well as urgency to achieve this goal as the time is past due considering the current state of matters.
- 🇬🇧 Given the completely porous nature of boundaries and frontiers in the face of advances in information technology, the UK is also well aware that coordinated international cooperation based on consensus and global harmonisation of national cyber laws is required to cover the problem effectively and in its entirety. Over the past few years, many states, intergovernmental organizations, and think tanks have offered proposals for new norms and principles to govern activity in cyberspace. The UK fears, that the world is nearing a bifurcation between east and west, as there is little overlap between the norms from the USA, UK and International Telecommunication Union (ITU) and the worldview and norms agreed to by the nations of the Shanghai Cooperation Organization (SCO). For this reason the UK sees the upcoming conference as an unique opportunity to engage in discussion on cyber law related topics with nations of both ITU and SCO and firmly believes that this discussion will be a step forward towards building a better common understanding with regards to cyberspace among these nations.








The Model Conference Global Security Issues

Faculty of International Relations, University of Economics in Bratislava



Modelová konferencia Bezpečnostná sekcia

Fakulta medzinárodných vzťahov, Ekonomická univerzita v Bratislave

-  The UK can not stress enough that no negotiations would be possible or durable without the full participation of all three actors in cyber space (governments, private sector and civil society), each as a legitimate and absolutely essential stakeholders. The UK is more than convinced that it would be a serious mistake to believe that government alone can negotiate the elements of a comprehensive legislation.
-  The UK supports the proposal of creating a definition of participants on the Internet, their rights and commitments.
-  The UK suspects that the attempt to define sanctions in accordance with the type of criminal or illegal activity in cyber space could prove to be problematic. *At the present moment little consensus exists among countries regarding exactly which crimes need to be legislated against.* Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement attempts to combat cyber-crime are complicated. The UK sees it as sensible that instead of a premature attempts to determine sanctions for illegal or harmful activity in cyber space, the international community should rather channel the focus on finding a common agreement on what these crimes are in the first place. Only after establishing internationally accepted cyber crime „nuts and bolts“ is it possible to open a discussion on such topics as is a catalogue of cyber crime sanctions.
-  In this respect, the UK shares the view with the specialised Cyber crime working group at Second Worldwide Cyber Security Summit in June 2011 in London on their conclusions for internationally required steps to fight cyber crime:
 - to harmonise national frameworks is essential to better combat cyber crime
 - to establish a minimal set of standards to apply internationally recognised approaches to cyber crime
 - to include existing procedural instruments already applied by many states
 - and to develop existing regulation on jurisdiction and standards for international cooperation.
-  With regards to the proposed definition of cyber space, the UK believes that this need has been successfully addressed to in joint US-Russian effort to define cyber security terminology. The



outcome paper of this effort - *Critical Terminology Foundations* - provides nonbinding definition of twenty terms that define cyber and information security. The paper was presented and broadly accepted by international community on the Second Worldwide Cyber Security Summit in June 2011 in London and the EWI Worldwide Security Conference in October 2011 in Brussels.

🇬🇧 The UK has carefully considered a proposal to broaden the Universal Declaration of Human Rights as well as proposal to outline a new document with the view to integrate into international law the cyber space related human rights and freedoms. The UK regards such measures in proposed scope as unnecessary and duplicate step with regards to an already existing international legal framework, as almost all principles suggested by the Forum are already rooted as a set of accepted legal standards, in particular by Universal Declaration of Human Rights and International Convention on Civil and Political Rights (especially Article 19 in both documents). Practically all nations have joined these pacts and they are now considered international customary law. These provisions set the fundamental principles and create the basic international law framework which, without any doubt, also extends to cyber space.

These two basic international covenants also define state's obligations to protect human rights (even in cyber space), but these obligations need to be applied more creatively and more comprehensively to the cyber space.

From the proposed principles, the UK shares the view with the Forum on the item: "*No one shall be arbitrary deprived of having access to cyberspace*" and will actively promote this principle in any further discussion on cyber space. The UK views cyber space as part of common heritage of mankind. Access to its benefits is a legitimate right for all peoples.

Other proposed items in fullness of their wording are from UK's point of view already embedded in two above mentioned international agreements.

With regards to human rights in cyber space, the UK finds it crucial to address especially these 3 areas:

- 1) Restrictions on freedom of opinion and expression



- 2) The scale of interference with privacy on Internet
- 3) The scale of state's censorship
- 1) It is UK's firm belief that restrictions on free speech in cyber space just as well as anywhere else should comply with following principles:
 - they must be provided by law
 - they must pursue an aim recognised as legitimate
 - they must be necessary or appropriate for the accomplishment of that aim.
- 2) Privacy as a fundamental human right is threatened by commercial exploitation of personal data without consent by business as well as by governments that pursue surveillance or allow intrusive law enforcements practices.

To date, government policies have created an uneven patchwork of rules designed to protect privacy in cyber space. But the borderless flow of personal data over international networks poses yet another problem, one that of international discrepancies. The differences in legal standards and practices for protecting privacy around the world undermine domestic levels of protection. Even if one state has robust privacy laws, it cannot currently guarantee equivalent levels of protection once the data flow beyond its borders.

Absence of privacy legislation and the global nature of personal data flow call for an urgent need to develop minimum standards or rules at international level governing the collection, storage, handling and use of personal data in international networks.

To outline or harmonise any piece of legislation at an international level is never an easy task. The UK therefore suggests to take into consideration the document *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Information* adopted by OECD when setting out core international privacy protection principles for cyber space:

- When data is collected, the purpose for the collection must be disclosed.
- The data collected must be relevant to the purpose for which it is collected.
- The data must reflect standards of quality and accuracy.



- Security safeguards must be established to prevent unauthorised access to the data.
- The data must only be used for the purpose for which it was collected, unless the consent of the individual has been obtained.
- The collector of the data must establish open policies regarding the nature of the data and the manner of its storage.
- The individual must have knowledge of and access to the data.
- The collector of the data must be accountable for its collection and use of the data
- To destroy the data after the purpose is achieved.

UK sees the significant advantage of these guidelines in that they already represent international consensus (even outside OECD countries) on general guidance concerning the collection and management of personal information.

As to the proposed hard sanctions for malevolent misuse of personal data for politic and economic reasons, the UK is convinced of necessity of their establishment and will take an active role in their creation as soon as international legislation on privacy protection is agreed upon. It also needs to be stressed that their outlining must be governed by rules of adequacy and proportionality.

- 3) A worsening record of Internet censorship by governments via filter technologies and without legal constraints becomes a growing human rights problem. At least 25 governments today are prone to these practices. The most states concentrate their intervention on banning political content, but many go further. Although the intensity and thoroughness of control varies, the rule, however, is that government censorship is exercised without limits and over a broad segment of human knowledge, without any explanation of the underlying role (these practices were coined a term „cyber repression“ by the EU). Citizens are not only curtailed in their rights under international law, they are also cut off from important benefits of information age.

The UK sees a possible source of threat that stems from such a practice - massive cyber repression can alter the collective state of mind of a nation, as they receive a skewed view of world reality. The lack of common understanding not only impedes the process of international cooperation but also, and more importantly, can evolve into a serious source of conflict – the




very thing nations around the world aspire to diminish. The current state of matters can not be ignored.

Despite legal intricacy and political sensitivity the UK feels bound to suggest to open an opinion-sharing discussion on defining the limits of internationally acceptable Internet filtering and possible cooperation in this field and thus paving the way for more global awareness of the problem.

Furthermore, the UK suggest to submit Internet political censorship under mandate of Internet Governance Forum.

To counteract cyber repression as a continued violation of international law, the UK also suggests to insert the topic of cyberspace / Internet freedom and censorship in U.N. Human Rights Council so that they would be assessed within a periodic country review in U.N. Human Rights Committee.

The final shape of international cooperation is yet to strike a balance between individual rights and collective responsibility or between individual rights to information and privacy in cyber space.

 The UK acknowledges that an issue of combating cyber attacks urgently calls for an immediate action as these pose an ominous threat. Combined with the chaos surrounding cyber attacks and uncertainty of the legal framework that govern the actions taken during such events could have devastating impact on national as well as global safety and stability.

As stated in the first draft, the UK supports the discussion on establishing international thresholds for circumstances under which a cyber attack would be classed as an act of aggression. When discussing how much evidence of a cyber attack is needed to secure international assistance and protocols for collecting relating evidence, the UK suggests to address following topics:

- what is the excessive force in cyber space
- how to determine that attackers are military combatants



- what constitutes an act of cyber warfare
- what international cooperation is required
- proportionality of a defensive response
- how to ensure that countries do not respond too hastily to cyber attacks before the aggressor is properly identified.

The UK feels obliged to stress that far more financial resources and intellectual capacity are being spent figuring how to conduct cyber warfare than are being spent figuring how to prevent it. In an interconnected world where cyber space knows no borders countries need to begin the dialogue on cyber stability by addressing international cooperation, confidence building and dispute resolution.

The UK suggests that this should include, among other aspects, a discussion on establishing an *early warning system for cyber attacks*. International mechanism needs to be developed and the cooperation between states as well as public and private sector needs to be deepened in a way that gives confidence, allows for flexible response and, most importantly, provides the point of contact in all countries needed for a credible response. National point of contacts would be interlinked in a global network.

The UK furthermore suggest to hold an open discussion on findings and recommendations of first joint Russian-U.S. report on cyber conflict: *Working toward Rules for Governing Cyber conflict: Rendering the Geneva and Hague Conventions in Cyberspace*.

- 🇸🇰 The UK supports the creation of Joint Criminal Database. The UK suggests a cooperation with an already established and well running platform in Europe – ENISA, as European cyber security centre and pool for exchange of information, best practices and knowledge in the field of Information Security. It is the UK's firm belief that such cooperation would considerably contribute to better effectivity and operative capability of the Joint Criminal Database.
- 🇸🇰 Suggestions to establish Cyberpol and introduce voluntary ID numbers for individuals were submitted to UK's relevant governmental bodies and at the present moment are being subject of trans-governmental analysis and discussion. The official position on these issues is yet to be reached.



The Model Conference

Global Security Issues

Faculty of International Relations, University of Economics in Bratislava



Modelová konferencia

Bezpečnostná sekcia

Fakulta medzinárodných vzťahov, Ekonomická univerzita v Bratislave

The UK confirms that as one of Europe's leading cyber security advocates is determined to be at the forefront of efforts to shape a shared vision of cyberspace's future.



FORUM FOR
21ST CENTURY

