Global Commission
on Internet Governance

ourinternet.org

Rapporteur Summary of the Meeting of the Global Commission on Internet Governance

Wilton Park, United Kingdom

February 14, 2015

The Global Commission on Internet Governance (GCIG) convened at Chatham House, in London, United Kingdom, on Friday February 13th 2015 and at Wilton Park, United Kingdom, on Saturday, February 14th 2015. Carl Bildt, former Swedish Prime Minister and former Minister of Foreign Affairs, chaired the meeting. The meeting was hosted by Chatham House, the Royal Institute of International Affairs. The GCIG, Chatham House and the Centre for International Governance Innovation (CIGI) are grateful to the British Foreign and Commonwealth Office for their generous support of this meeting.

The GCIG discussed a number of topics, including the most immediate threats to the open Internet, the developing of norms in the use of digital intelligence, issues surrounding the emerging dark web, how best to enable open access to the Internet for all, and the future work agenda of the Commission. The following is a rapporteur summary of the day's events. The meeting was held under the Chatham House rule.

Day 1, Session 1: Communication Strategy

During the first day, several members of the Commission met informally at Chatham House to discuss the Commission's communication strategy. Over the past six months, there have been several events that threaten the freedom, openness and security of the Internet. These events – or 'flashpoints' – can jeopardize the Commission's vision for the Internet and accelerate the potential of fragmentation. There is a moment of opportunity for the Commission to craft clear messaging about what is at stake, develop new and big ideas to safeguard the future of the Internet, and issue appropriate statements on major debates in a timely manner. On the following day, the Commission's communication strategy was discussed again in more detail at Wilton Park.

Day 2, Session 1: Briefing on WSIS Process

During the first session, the Commission discussed the upcoming World Summit on the Information Society (WSIS) +10, which will be held in December 2015 at the UN General Assembly (UNGA). WSIS+10 will provide a review of the changes in the 'information society' and related issues in the decade since the Tunis Agenda of 2005. The Commission discussed difficulties within UN proceedings on this issue. It noted that the topic of Internet governance will feature heavily and may prove to be a particularly contentious issue. Potential issues of disagreement will likely be more concerned with process than substance.

The Commission discussed the current status of the Internet Governance Forum (IGF), founded in the immediate aftermath of the 2005 Tunis Agenda. The IGF is now seen as an accepted part of UN discussions about Internet governance. However, there is still a suggestion that the IGF is not sufficiently multistakeholder and may, at present, be seen by many as little more than a 'talk-shop'. The majority of the Forum is comprised of Internet insiders, thus the Commission suggested that, in the future, the IGF could aim to include a more diverse group of representatives from government, business and civil society. If the IGF incorporated such actors, its impact and reach could be significantly increased.

Multilateral processes play a role in Internet governance. Upcoming summits will be primarily geo-political in focus, thus the Commission must decide whether to engage in these processes. Issuing clear and precise statements could transcend debates between specific nations. The Commission debated how best to construct and subsequently disseminate such statements. If the Commission issued a communiqué in advance of the upcoming summit, it could encourage a more multi-stakeholder approach, whilst also placing an emphasis on the vast changes that have occurred within the domain of Internet governance in the past decade. Any contribution from the Commission will sit alongside a number of other documents, such as the UNESCO Internet study, thus any such statements must contain novel creative thinking about the future, rather than placing too much focus on events in the past. The Commission commented on the static nature of the UN approach and how it is often difficult to apply to dynamic issues such as Internet governance.

Following the 2005 Tunis Agenda, UN attention to issues around the Internet significantly decreased. Many moved on to other equally pressing issues such as climate change and development. It was agreed that a direct message from the Commission on the central role that the Internet will play in the future could help to remedy this situation and bring the attention back to key issues of ICT governance. Focus should be placed on key topics that will inevitably be central to future governance; the role of ICT in development, issues surrounding big data and security, and the potential risks and benefits of the emerging Internet of Things. The Commission must ensure that it maintains a forward thinking approach in order to have a positive impact on the various upcoming UN discussions.

Session 2: Specific and Immediate Threats to the Free and Open Internet

The Commission continued to focus on the key issue of disseminating the work of the GCIG in the following session. The diversity of Commission members can be harnessed to ensure output has a truly global impact. The Commission also discussed how to reach policymakers who are responsible for shaping the future of Internet governance. Media will play a central role in the dissemination of the Commission's message, thus outputs must be bold, direct, and, most importantly, consistent. The Commission noted the urgency in deciding upon a coherent message, with the next meeting in The Hague only two months away. The vast networks of each of the Commission members should be employed to properly disseminate the GCIG's messages, but, in order for this to have genuine effect, the key aims of the GCIG as a whole must be agreed and clearly laid out, an issue that was returned to at greater length later in the day's discussions.

The Commission then discussed the recent hacks of Sony Pictures and the potential involvement of North Korean actors. The company suffered embarrassing leaks as well as attacks that destroyed approximately 80% of its IT

infrastructure. The Commission discussed the US response to this episode, with particular focus on the description of Sony as 'critical infrastructure'. This was a controversial reading of the situation, as no companies involved within the entertainment industry feature on the agreed list of the 17 critical infrastructures that require protection from attack. Expanding the list of critical infrastructure risks diluting the value of such a list. And sets a potentially dangerous precedent for the future, as attacks of this type become more common. It also raises important questions, such as the role of governments in responding to attacks against corporations The Commission argued that a distinction should be made between *critical* infrastructure and industries that are *critically* important to the economy.

In the days following the attack, the Internet connection for the entirety of North Korea was shut off and no nation or group has yet claimed responsibility. The Commission agreed that this could be a dangerous trend for the future and debated whether this should ever be a legitimate response to future cyberattacks.

Questions were raised about where the responsibility lies for the protection of private companies in the online space. Comparisons were made between the response to the Sony episode and the violent attack on Charlie Hebdo earlier this year. Charlie Hebdo received the full protection and support of the French government, and, in the weeks that followed the attack, online surveillance across France and Europe was increased.

The Commission discussed calls by others to allow the implementation of back doors into encrypted communication technologies following the Charlie Hebdo attacks. The GCIG noted that the response of liberal democratic governments seems to suggest an approach of believing in an open and free Internet *until* an act is committed that jeopardizes national security.

The Commission then debated moves by the major Internet players, such as Apple, Google and Yahoo, to increase encryption in their users' communications. In the fallout from Snowden's NSA revelations, a number of these companies came out and declared they were opposed to building back doors in their technology. The Commission debated the issue of user data, with an emphasis on the companies that possess such data acting responsibly and within the boundaries of the law. The Commission noted how the standard business model for the majority of Internet companies is for consumers to pay with their data rather than their money. Thus, these companies wield huge power through this large scale information gathering. It is becoming increasingly difficult for governments to maintain oversight and control, and this may only become more pronounced in upcoming years.

Contributing further to the issue of big data is the emerging Internet of Things, an area where there is much still to be understood. The Internet of Things is not an 'Internet' in any traditional sense because the various devices are based around proprietary protocols that do not necessarily interoperate. It is, therefore, more similar to a closed phone line, yet without any commonly agreed standards. The Commission can play an active role in the construction of these standards and help to ensure consistent data integrity going forward.

The security of the huge data sets collected by the millions of devices now online also needs to be urgently addressed. The Commission noted that centralized silos of data are emerging. A scenario could occur where few private companies own this data, and are unaccountable to any external body other than their shareholders. The

Commission agreed that it could act as an educator on this issue by providing governments with recommendations on how best to regulate in both the present and future.

With regards to any public awareness of the above issues, the Commission acknowledged recent attempts by the World Wide Web founder Tim Berners-Lee to crowdsource an updated Magna Carta for the digital age. Over the next 6 months, he is asking the global public to contribute to a set of rules and regulations for the future of safety and security online, and the GCIG could play a role in this process.

Session 3: Developing norms in Privacy and Digital Intelligence

Throughout the third session of the day, the Commission discussed a number of key issues related to intelligence work and the security services online. It was agreed that intelligence work is a legitimate function of all governments, with the primary aim being to reduce ignorance and thus improve decision making, often in times of crisis. Whilst the aims of intelligence work remain unchanged, the Internet has brought with it a number of new and difficult challenges, in terms of legality, ethics and accountability.

The GCIG noted that law enforcement agencies are currently far behind the criminals with respect to the online sphere. Law enforcement requires help from the intelligence service in order to stop online criminal activity, yet, at present, there is little agreement as to how far they can go in order to do so. Since the NSA leaks, a number of governments have been heavily criticized for not being open about their use of the Internet in intelligence work. Thus, the Commission agreed that a new compact has to be drawn up between the intelligence arm of governments and the publics they are served with protecting, with a set of ethics and norms agreed upon by all, private companies included.

Further attention was paid to the issue of responsible data use by private companies. Increasing amounts of data are being held in the hands of a few companies and there is very little transparency about how these companies use the data and what ethical standards they are guided by. Most users also have little idea about what happens to their data once it is generated and collected by online companies.

The Commission recommended that government regulation could potentially be used to encourage companies to be open and transparent about the ethics they employ with respects to use of data. It was argued that the Commission could make this one of their key messages for public consumption, and help to ensure that international agreements are made regarding what global companies are allowed to do with the data they gather.

The issue of the legal accountability of these companies was discussed further. At present, most Internet giants are based in Silicon Valley and thus are accountable primarily to courts in California, even though the majority operates at an international level. Traditional legal mechanisms are thus challenged in the digital age. There is a distinct lack of a platform for appeals in cases relating to online issues. The recent EU ruling on the ‘right to be forgotten’ has since been employed in over 200,000 cases, yet there has been little-to-no public assessment on the details of these cases. The Commission agreed that the opacity surrounding these issues needs to be dealt with in the coming years. It was suggested that ethical and legal concerns should play a role at the design stage of the

services provided by these companies. Recent examples have demonstrated that such concerns are often added in at a later date and in an ad-hoc fashion.

The Commission discussed the potential of a universally accepted community-driven set of rules for the responsible use of data by both the private companies and government agencies. Specific and agreed upon principles could form the foundation for a common practices surrounding the collection and use of data online. The GCIG could play an active role in helping develop these principles, especially since it appears that there aren't many other bodies currently looking into this matter. It was suggested that the Commission could begin to draft a list of norms that all must adhere to when gathering data for intelligence online. The primary principle that should be stressed is that of complete transparency.

This central issue of transparency was discussed further. The GCIG noted that very little is known about the algorithms that decide the content that users receive. A majority of Internet users now get their news through search engines and social platforms that may not provide neutral unfiltered results. The Commission agreed that there should be attempts made to assess how these ordering decisions are made. The companies in question should provide insights into how they filter information for their users, particularly as their hold on public opinion and debate will only become more and more significant in the upcoming decade. In order to keep these companies in check, the Commission recognized the importance of educating and informing both the public and the judiciary on the technicalities of potential cases. Judges must be provided with the necessary expert assistance when dealing with cases that involve the Internet, and should be trained themselves.

Law enforcement agencies in the developing world, where the next 1 billion users will come from, are in especial need of training on how to police the online space due to the rapid emergence of the Internet in these countries. Efforts should be made by bodies such as Europol, INTERPOL and the International Court of Justice to bring countries that have only recently achieved widespread Internet diffusion into the discussion about best practices and cooperation regarding law enforcement, as the issue will only become more globalized in the future.

Session 4: Addressing Cyber-Crime and the Dark Web

The Commission discussed the emergence of technologies such as Tor, which allow users to anonymously browse certain hidden sections of the Internet. Some of these hidden sections are commonly referred to as the dark web. Traditional web browsers do not allow access to the dark web. Users must download technologies such as Tor[1] that route traffic through a global network of many thousands of individual relays, thus obscuring the original user's location and identity. Tor itself was originally developed as part of a US Navy project in order to allow for more secure communications amongst the US intelligence community, but has been available for public use for the past decade.

TOR, and the various alternatives, can be seen as dual-use technologies. The Commission discussed that there are many noble and necessary uses for Tor that require the network's anonymity. For example, political dissidents, freelance journalists, and research scientists may use TOR in order to keep their work safe and secret. At the same

[1] There are now alternatives to TOR, but TOR remains by far the most popular

time, there are significant criminal elements using the anonymous networks to plan their activities, buy and sell drugs and weapons, and operate an exchange of child abuse images. The Commission agreed that the dark web may not have caused an increase in criminal activity; rather it has provided a new medium for particular crimes that benefit from the total anonymity that the software offers.

Suggestions were made about the potential of unmasking those who use TOR for nefarious activity, through methods such as watering hole attacks. If the key nodes in these criminal networks can be identified, then law enforcement can begin to counter the illegality taking place. Whilst certain criminal activities, such as the illegal arms trade and the drugs trade, have largely remained offline some intelligence figures have suggested those who wish to exchange images of child abuse have widely embraced the dark web. An issue such as this requires cross-border international cooperation in order to be properly dealt with.

While this issue may be less one of Internet governance and more a law enforcement matter, the GCIG noted that it could still bring attention to the importance of international cooperation necessary to counter the illegal activities taking place on the dark web. The Commission noted that thus far there has been little evidence of such cooperation and thus law enforcement are currently struggling to keep up with the criminality, further emphasizing the urgency of dealing with this problem promptly and directly.

Session 5 (1): Enabling Internet Access For All

The Commission touched on two major topics surrounding the wider issue of ensuring the Internet is open and accessible to all. Firstly, current trends on internet access in West Africa were discussed. At present there is rapid growth in Internet use across many African nations, with e-banking often being at the forefront of this digital development. The example of Ghana was looked at where there have been early efforts to move towards a cashless society, where the majority of payments will be done through either mobile banking or online. Yet the Commission recognized that crime will be a major issue as many of these countries begin to move online, particularly with regards to fraud. Akin to the aforementioned situation with the dark web, it is essential that law enforcement bodies such as INTERPOL offer their expertise and experience to governments across Africa and help them to deal with the criminal activity that widespread Internet use brings, ensuring that the public feels safe in adopting the new technology rapidly being made available to them.

The issue of availability of access was discussed further. At present there are huge variations in the cost of Internet access across Africa. The GCIG recognized that if we are to see the Internet as a truly global technology, then we must ensure that there is some consistency in the costs involved in its use.

Further measures to ensure that the Internet can be considered globally accessible are also required. Investment in African Internet companies should be a priority, so that they can encourage the development of services by local people for local people and in the various local dialects and languages in which they communicate. Current projects being launched by the primarily American private Internet companies could reduce the profitability of local telecommunication companies and impede adequate investment in local infrastructure. Thus, the Commission further stressed the importance of encouraging increased and responsible investment in the Internet industry across Africa.

The Commission moved to discuss the issue of ensuring that the Internet remains accessible to those with disabilities. At present there are various national guidelines concerning website design, particularly in terms of the user interface, with regards to ease of access for all potential users. Yet the GCIG noted that unfortunately these regulations are not enforced at an international level. Whilst nations such as Germany and Sweden were commended for their consistency in maintaining high levels of accessibility, other nations were lamented for their failure to enforce such rules.

The Commission agreed that this was one issue where they could potentially make a significant impact. There is very little contention to be had in this matter, it isn't particularly complicated to educate governments and private companies about the rules they are meant to follow and the international networks of the Commission members could be ideal for spreading the message about a matter of which many are unaware.

Session 5 (2): Net Neutrality

The Commission outlined the key principles that need to be enshrined in any future policy documents on the topic of net neutrality. Ensuring that the Internet remains a site of open innovation, that the freedom and access of all users are safeguarded, and that the quality of the connection should never be throttled or manipulated by the ISP. Yet the GCIG also recognized the difficulty in agreeing upon a definitive description of net neutrality as a whole.

Emphasizing the need to further study the implications of net neutrality decisions on innovation, competitiveness and social welfare, the Commission decided to place the topic high on the agenda for the upcoming meeting in The Hague. With the Netherlands being one of the foremost countries in the fight for maintaining net neutrality, it could be a perfect opportunity for the Commission to return to the issue in more detail and construct a statement that could help to shed light on the issue.

Session 6: Future Work of the GCIG

The final session of the day's proceedings focused on the future work of the Commission. The Hague meeting of the GCIG falls right before the Global Conference on Cyberspace, which will bring together governments and the private sector to discuss cybersecurity issues. The GCIG was keen to ensure that such an opportunity for exposure, both to the public and to ministers in government, was taken full advantage of. It was recommended that any outreach to media would have to take place well in advance of the meeting in order to ensure that it has time to disseminate and start a discussion about the major issues.

The relationship between the GCIG and the media was discussed further. It was suggested that there needs to be an increase in the amount of media exposure for the work of the Commission. Press briefings need to be more regular, and relationships with the press in general need to be strengthened. Whilst discussing this topic of media relations, the Commission accepted that there was still debate over the specific audience that they most wanted to reach; be it the public figures, government, representatives from private industry or a combination of all three. It was suggested that the launch of a new paper on norms in digital intelligence might be an opportunity for media engagement.

The Commission also discussed the issue of representation. With no involvement at all from either Russia or China, and not yet enough representation from Africa and South America, there is a risk that the phrase championed by the Commission, ‘our Internet’, may in fact limit the global appeal of the GCIG.

The original aim of the Commission was to represent the liberal democratic view of the future of Internet governance. Yet comments were made that this approach may in fact alienate many of the key players in the upcoming debates at the UN and elsewhere, both in government and industry. It was agreed that the Commission’s primary focus should be that of providing educated policy direction. It should aim to promote a common understanding of the key issues at hand and make sure to emphasize what is unique about the challenges facing the Internet in the next decade.

With regards to the Commission’s work itself, the idea of working groups was proposed. A follow up Commission-wide email could lay out the already agreed upon statements and then call for further suggestions and potential for breaking up into smaller groups that can focus on specific issues depending on each Commission members own background and expertise. This approach could ensure that the GCIG is able to fulfil its role as educator, whilst also ensuring that the final output of the Commission remains focused and provides genuinely new insights for emerging problems. The Commission noted that failure to disseminate its message could lead to its irrelevance. Public and private engagement is key.

The Commission discussed a number of different formulations for the key principles that the GCIG will advance, as well as potential headline grabbing ‘bumper stickers.’

The Commission closed the day’s proceedings by discussing potential locations for the GCIG meeting following the upcoming event in The Hague. The earlier discussed South Africa meeting was now considered unlikely to happen and suggestions were made to host an event in Ghana towards the end of the summer, if budget allows.

Finally, there was an update on the progress of the research volume and the related papers.