Delegation from **People's Republic of China**

Represented by **University of Calgary**

Position Paper for the General Assembly

The General Assembly Plenary is concerned with the following issues: The Role of Telecommunications in the Context of International Security; and Preventing Non-State Actors from Accessing Weapons of Mass Destruction. The Delegation of the People's Republic of China is dutifully enthusiastic to discuss the role of E-governance in cyber security regarding ICT internationally within the General Assembly Plenary.

I. The Role of Telecommunications in the Context of International Security

The People's Republic of China (PRC) pursues the following three goals in constructing internet security legislation: I) State security, II) Public interest, III) Protection of children[1]. At the root of the majority of our enforcing mechanisms regarding cyber security an intersection of these three focal points can be observed.

The PRC has always noted with pride its proactive and advanced approach to cyber governance. We find ourselves at the forefront of establishing sustainable means of assessing and addressing contemporary technologies in a manner which takes into account both the positive and negative aspects of such. In 1994, during the initiation of internet technology in the PRC, the State Council introduced the Ordinance for Security Protection of Computer Information Systems. The workings of such a forward-thinking piece of legislation established that the PRC recognized the potential of technologies which can both help and harm the state. The Ordinance contained a clause which noted that internet security belongs under the jurisdiction of the Ministry of Public Security[2]. This concreted an equation which remains paramount in any PRC legislation regarding the matter; that internet security is public security and shall always be regarded as such in the interests of the people. The document goes onto define harmful information and activity which remains to be interpreted as anything which speaks against, or threatens to destabilize the unity and security of the people of the PRC, their country, or their government; anything which promotes violence or unjust behaviour; anything which explicitly illustrates or depicts actions deemed unlawful[2].

In 1998 the State Council introduced a large scale operation to address domestic and international cyber security concerns, the Golden Shield Project (GSP). The GSP gave the Ministry of Public Security the ability to monitor traffic into or out of the country; this includes the monitoring and preventing of intelligence leaks regarding the State Council, the National People's Congress, or any measures of the Central Military Commission. Not only are these measures in the best interests of the state, but are preventatively assessing security issues which could harm the populace[3]. The advanced system of the GSP which monitors international traffic involves the standard packet filtering analysis methods combined with specific international gateways making the GSP one of the most sophisticated and comprehensive monitoring systems in the world[4].

When observing the efforts of the international community the PRC alongside the Russian Federation have had a starkly different approach than the United States of America. Despite the heightened collaborative efforts between President Xi Jinping and President Obama post 2009, and the significant shifts of American policy regarding the focal points of what cyber security meant for the US Department of State, the divide in the international discourse still exists[5]. The goals which can be found driving our

policies since the introduction of the internet to the PRC can also be seen as the factors which divide our cyber governance policies from the Western World, and ultimately manage to protect the PRC's citizenry from the dangers of illicit cyber behaviour and misinformation which plagues those nations who have been unable to create and establish a safe online environment for their people. In 2011, the Draft Code of Conduct for Information Security circulated in the 66th session of the UN General Assembly, a consensus regarding the norms of cyberspace sought to be achieved. Any such consensus, however, was not established and the 'East' and 'West' remain divided regarding cyber governance. The PRC continues to be a staunch advocate for E-Government and cyber security of the highest, most sophisticated level. These differentiating factors have resulted in the PRC's strong advocacy and promotion for integrated cyber governance platforms at the international level. Proactive measures against cyber crime, cyber terrorism, and the future realities of cyber warfare which are measures in the interests of the state and the public.

II, Preventing Non-State Actors from Accessing Weapons of Mass Destruction

The PRC is no stranger to the imminent threat of terrorist organizations; the most recent Ürümqi attacks, and the global dimensions of the Uighur militants have influenced policy measures against subversive groups[6]. Parallel to this recognition of the dangers of terrorist groups, the State Council has made a concerted effort to analyze and emphasize the threat of weapons of mass destruction (WMDs), warfare with such capacities, and the volatility of a situation in which non-state actors have access to and sophisticated WMD technology. China is the first and only nuclear weapon state to be recognized by the Nuclear non-proliferation treaty, which was ratified in 1992. The PRC is also a signatory for the International Convention on the Suppression of Acts of Nuclear Terrorism. China also has a strict no-first strike rule adhering to a deterrence-only policy regarding nuclear power, also maintaining a relatively small arsenal[7]. The PRC was keen to sign on to the Chemical Weapons Convention in 1993, and destroying our miniscule stockpile of chemical weapons before ratifying the document in 1997. Despite the minor controversy surrounding the PRC's signature of the Biological and Toxin Weapons Convention, in 2002 the situation was remedied with the export protocol on dual use biotechnology[7]. The PRC believes that the first step in monitoring and countering the proliferation of WMDs to non-state actors is in first detecting the presence or construction of such technologies. International collaborative measures with organizations such Mesa Labs (BIOS International), Morphix Technolgoies (K&M Environmental), North Safety Products, OHD LLC, Sensit Technologies (J&N) provide expert means of identifying the primary stages of WMD production. Enabling local authorities, such as police forces, to harness the technologies of these companies to identify early stages of manufacturing within communities is a thorough preventative measure.

Universal standards for storing the existing stockpiles of WMDs within states is essential in maintaining control over these facilities. International efforts to prevent the uranium-enrichment and plutonium-reprocessing markets from being accessed by new states not already engaged. And isotope production should be government sanctioned, non-military grade, and persistently monitored. These measures should be pursued by the NPT, specifically ratified members of the NPT. The key players in maintaining the balance of international WMDs have been the United States of America and the Russian Federation, but as the international community shifts in influence and volatility the PRC is seeing an emergence in its influence and ability to maintain balance within the Eastern states, specifically having a stronghold in the Southeast Asian region[8].

Works Cited

1. Bristow, Michael. "China Defends Internet Censorship." *BBC News*. BBC, 8 June 2010. Web. 10 Dec. 2014. <http://news.bbc.co.uk/2/hi/8727647.stm>.
2. "Technical Appendix - Empirical Analysis of Internet Filtering in China." *Technical Appendix - Empirical Analysis of Internet Filtering in China*. Web. 13 Dec. 2014. <http://cyber.law.harvard.edu/filtering/china/appendix-tech.html>.
3. "How the Great Firewall of China Is Blocking Tor." *How the Great Firewall of China Is Blocking Tor*. Web. 13 Dec. 2014. <http://www.cs.kau.se/philwint/static/gfc/>.
4. Fallows, James. ""The Connection Has Been Reset"." *The Atlantic*. Atlantic Media Company, 1 Mar. 2008. Web. 12 Dec. 2014. <http://www.theatlantic.com/magazine/archive/2008/03/-the-connection-has-been-reset/306650/?single_page=true>.
5. "Cyber Space Governance: Moscow and Beijing's Efforts at the UN." *Cyfy*. Web. 16 Dec. 2014. <http://cyfy.org/cyber-space-governance-moscow-and-beijings-efforts-at-the-un/>.
6. "China Terrorism." *The Guardian*. Web. 14 Dec. 2014. <http://www.theguardian.com/commentisfree/2014/may/06/terrorism-china-uighur-militants-afghanistan-pakistan>.
7. "Compliance with WMD Treaties." *Compliance with WMD Treaties*. Web. 12 Dec. 2014. <http://slhscif.tripod.com/benchmark3/documents/Nina_Baker.htm>.
8. "Profile for China | NTI." *NTI: Nuclear Threat Initiative*. Web. 13 Dec. 2014. <http://www.nti.org/country-profiles/china/treaties/>.