“Can Cyber Conflict be Defused? Diplomatic Options for International Cyber Security”

Paper presented to the Academic Council of the UN System, Annual meeting, Istanbul June 21, 2014

Paul Meyer, School for International Studies, Simon Fraser University, Vancouver, Canada, pmeyer@sfu.ca

Please do not circulate or cite without permission of author

Conflict has always been a feature of the international system and states have devised means of dealing with it along the diplomacy-defence spectrum. Today however the international community is confronted with a special challenge regarding conflict in a domain of an entirely new sort, one that has only existed for 15 years or so and is a human and not a natural creation, such as the land, sea and air. This domain is the Internet, or more broadly cyberspace and constitutes an environment that possesses features significantly different from other realms of internationally regulated activity. It would be hard to exaggerate the importance of this environment for the functioning of global society and the high level of dependency that has developed on a cyberspace free from threat of deliberate damage or disruption from state actors.

It would also be difficult to overstate the rapidity of developments in this new realm. International cyber security diplomacy is an area of activity that barely existed a decade ago. The human made environment of cyberspace itself is but a generation old. The very term “cyberspace” was coined by a Vancouver sci-fi writer, William Gibson, and popularized in his novel “Neuromancer” thirty years ago. Gibson defined the term as “a consensual hallucination experienced daily by billions…”. This prescient metaphor has become a household word as the use of the Internet exceeds the two billion mark.

Exponential Growth of the Internet:

In addition to its rapid growth, the pattern of Internet usage has also changed considerably. Until recently the majority of Internet users were located in Europe and North America. Today the majority of Internet users live in the global south. Developing countries have increased their share from 44% in 2006 to 62% in 2011[1]. Asia itself has half of the world’s Internet users. The rate of increase in connectivity is incredible. Nigeria had approximately 200,000 Internet users in 2002. In 2013 it had 49 million. Indonesia alone is said to add 800,000 new users each month.

The growth of the internet and the even more pervasive use of “smart phones” with some 4 billion users worldwide has transformed telecommunications and brought a myriad of benefits for the social, cultural, political and economic life of people everywhere. Of course there are, as with any technology, dark forces that will exploit the capabilities of that technology for malicious ends. Cybercrime is a real and costly threat and it is not surprising that the initial steps to promote inter-state cooperation in cyberspace have been directed at joint efforts to combat cybercrime. Indeed the first and to this day the only international legal agreement dealing with cyber security is the 2001 Budapest

Convention on Cybercrime that was initiated by the Council of Europe. This treaty entered into force in 2004 and now has 42 states parties that have ratified and another 11 states that have signed. The treaty has however been slow to attract support from states outside the members of the Council of Europe: from the Asia Pacific region only Australia and Japan have ratified the treaty and in Africa, South Africa remains the only state to have ratified. This is not only an issue with developing countries; although Canada was an early signatory back in 2001 it still has not ratified the convention. These difficulties with developing acceptable arrangements to foster state cooperation in cyberspace, even when it is non-state actors that are the sole objects of this cooperation, should alert us to the problems that await if we look to constrain the conduct of states themselves.

The issue of State behaviour:

It is relations among states that concern us if we wish to pursue international cyber security through the avenue of diplomacy. A 2012 survey by the UN institute for disarmament research (UNIDIR) revealed that 114 states have some form of national cyber security program and of these 47 assign some role to the armed forces in carrying out the national program. Yet according to the UNIDIR research only six states have published military cyber security strategies with varying degrees of specificity.[2] There is clearly a question of transparency here that merits attention. There is also the fact that we seem to be well on the way to the "militarization" of cyberspace without having given the matter much thought or deciding that permitting state-sponsored cyber attacks in this new, human-made environment is an appropriate activity. This concern is not an abstract one as recent developments show. The U.S. military for example created its Cyber Command in 2009 and its initial budget allocation was $114million in FY2010. Just four years later its allocation in the FY2014 budget is $447million a fourfold increase. A similar increase of personnel is also underway with Cyber Command seeking to augment its force by over 4,000 new staffers.[3] Perhaps most troubling is the express emphasis on offensive over defensive operations in the strategy being proclaimed.

Courtesy of Mr. Snowden we now have a detailed grasp of the U.S. policy for offensive cyber operations set out in Presidential Policy Directive (PPD) 20 of October 2012.[4] It suggests that offensive operations would not be limited to efforts to counter imminent threats or cyber attacks but could also be carried out to advance unspecified national interests. If these provisions for damaging cyber operations abroad are disconcerting for those wishing to preserve cyberspace for peaceful purposes, the upper rungs of the cyber ladder of escalation are alarming. Cyber effects operations that will result in what the PPD euphemistically terms "significant consequences" allow for actions causing "loss of life" and "significant damage to property", although this level of operation would apparently require presidential approval. Although the PPD states that any external cyber operations would be conducted by the U.S. in a manner "consistent with its obligations under international law" the implications of such offensive cyber operations for international security are not really addressed. The policy does acknowledge that among the "risk" factors that should be taken into account in approving foreign cyber operations are whether "unwelcome norms of international behavior" would be introduced and whether “the security and stability of the Internet” would be impacted. Regrettably the policy doesn’t indicate a diplomatic dimension beyond a reference to a prior call by the Obama Administration for the development of “an international consensus around norms of [responsible state] behavior in cyberspace”. The revelation of this employment policy for offensive cyber operations alongside the rapid increase in military cyber capabilities is likely to overshadow the limited earlier appeal to forge a global consensus. As has often been the case in the past, other states are likely to take their lead from US policy and action in determining what posture they should adopt in this new realm of international security. One might hope that this unintended “transparency” measure by the U.S. would lead states (and civil society) to question whether they really want cyberspace to be a domain of international conflict or cooperation in future and what might be done to preclude or at least mitigate the weaponization of this special environment.

Tense U.S.-Chinese cyber security relations:

Even the most casual observer of the Western media will have been struck in recent months by the growing attention being paid to cyber attacks and the losses of information being suffered by both public and private entities. In particular, accusations have been levied against China for alleged state-sponsored cyber espionage directed at U.S. governmental and business interests. After years of discreet avoidance of naming China as the culprit in these cyber attacks, the U.S. Government has decided in recent months to identify Beijing as the principal perpetrator of these attacks and to call upon it to desist.

The U.S. Department of Defense has been especially vocal in accusing China of being behind these cyber intrusions and linking them to the compromise of several American weapon systems. U.S. Secretary of Defense, Chuck Hagel, has referred to cyber threats as “terribly dangerous” and has called for talks with China and others to “establish international norms of responsible behavior in cyberspace”.[5] The issue of cyber espionage has figured prominently in US-China bilateral relations and has found its way onto the agenda of the highest levels of discussion, such as the summit between Presidents Obama and Xi in June of last year. It would appear though that the political attention to the problem has not yielded sufficient results. In May, the US Department of Justice took the unprecedented step of indicting five serving officers of the People’s Liberation Army for engaging in cyber espionage against American corporations. There are also reports that US authorities are considering denying visas to Chinese nationals who had intended to attend popular hacker conferences held in the US in August. Chinese officials have angrily denied these charges and have even suggested that the U.S. “fabricated” the evidence against the PLA officers. [6] These publicized actions represent a significant escalation over the previous reliance on behind the scene diplomatic protests or expressions of concern during high-level discussions.

It is noteworthy that even as the U.S. military moves to significantly enhance its cyber security capacities, including its capabilities for offensive cyber operations, the Defense Secretary is advocating an alternative approach to address potential cyber conflict. This approach is premised on diplomatic rather than military initiatives and would seek to agree on “rules of the road” to govern state behavior in cyber space. Whether global and regional cyber security will be characterized by adversarial or cooperative approaches may depend on the success or failure in the near term of efforts to develop these norms of responsible state behavior.

The Quest for Norms of Responsible State Behaviour:

The idea of agreeing upon such norms is not a novel concept in the international system. States have long worked out common standards to cover their interaction, including how to manage their conflicts. In the subset of international security relations there have been agreements developed over time to manage or moderate those conflicts. These agreements have applied to the traditional domains of land, sea and air and have evolved to accommodate changes in technology and the introduction of new armaments. Cyberspace constitutes a unique domain that raises special concerns and considerations for states and their national security establishments.

States and their governments generally have been slow to articulate policies on international cyber security. Most have confined themselves to promulgating national cyber security strategies with only passing references to the desirability of cooperation at the international level. This emphasis on the national perspective is understandable given the priority attached to securing computer systems domestically and the tendency to view the problem of cyber security through the lens of law enforcement and regulatory agencies. The Internet is, however, a quintessentially global phenomenon and its continued secure operation would inevitably require some degree of global cooperation.

The United States was the first country to recognize officially the inter-relationship between national and global cyber security and to set out its vision as to how the international community should proceed. In May 2011, the Obama administration issued its *International Strategy for cyber space*. This path breaking policy statement acknowledged the immense dependency of society on the operation of networked technologies and the increasing threats to the safe and secure use of these technologies. The policy noted that “Cyber security threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace”. To counter this tendency for some states to “exert traditional power in cyber space” the policy called for the development of a new international consensus on “norms for responsible state behavior” in cyber space. The statement promised early and energetic action in this regard: “We will engage the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace…”. [7] The policy directions set out in the *International Strategy* are progressive and infused with a cooperative security spirit. Having expressed the goal and stressed the urgency of the requirement, the Obama administration however has found it difficult to translate its policy vision into a diplomatic process with which to achieve it. Although it has been more than three years since the promulgation of its *International Strategy* the U.S. has yet to endorse any multilateral process to develop norms for state behaviour and has struggled to establish even bilateral dialogues on the issue with key states. The remarks of Defense Secretary Hagel cited earlier however, suggest that the pursuit of agreed norms on responsible state behaviour in cyberspace remains the chief aim of its cyber security diplomacy.

The Sino-Russian Code of Conduct Initiative:

The US endorsement of the idea of a set of global norms to govern inter-state behavior in cyber space constituted an important diplomatic step that set the stage for other international actors to offer up a draft of such norms. In the event, it was China and Russia that proved first off the mark in presenting a proposal for a package of global norms to govern state behavior. This initiative was presented in an official document circulated at the UN General Assembly session in September 2011. The proposal was entitled an *International code of conduct for information security* and was submitted by the delegations of China, the Russian Federation, Tajikistan and Uzbekistan.[8] In the covering note explaining the proposal, the delegations stated that the rapid development of "information and telecommunication technologies could potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security". It went on to say that the proposed international code of conduct had been elaborated in the form of a potential General Assembly resolution and called for deliberations within the UN framework on this text "with the aim of achieving the earliest possible consensus on international norms and rules guiding the behavior of states in the information space".

By means of this initiative, China and Russia (as the chief authors of the proposal – Tajikistan and Uzbekistan being added in to provide some desirable developing country cover) had adroitly taken advantage of the opening provided by the Obama administration's *International Strategy.* The two states had promptly filled the diplomatic void with a proposed set of norms for responsible state behavior in cyber space (or "information space" as the Chinese and Russians prefer to term it). The co-sponsors of this initiative were also clever in the form they chose for their set of norms. It was presented as a politically-binding code of conduct rather than as a legally-binding agreement. This approach appeared to be geared to the increased aversion U.S. administrations have shown towards entering into international agreements which require Senate ratification as opposed to politically-binding arrangements to which the Executive Branch alone is able to commit. Beyond the particular problematic case of the U.S., the relative ease of state engagement and general rapidity to conclude (as compared to frequently protracted treaty negotiations) have tended to favor these forms of political arrangements over legal instruments in international security affairs (for example the draft international code of conduct on outer space activities currently being promoted by the European Union).

The Devil is in the Details:

If the form of the proposed code was skillfully designed to appeal, the content of the code was more controversial and introduced several ambiguous formulas; which would pose problems in any eventual multilateral consideration. The core of the code was contained in a set of eleven actions that states were invited to voluntarily subscribe to. While many of these were rather innocuous with references to bolstering regional and international cooperation and assisting developing countries to close the digital divide, a few of the actions were problematic. Two of these actions were especially significant; both for their potential impact on state behavior, but also in highlighting the challenge inherent in trying to have the international community arrive at a common understanding of certain key terms.

The first such action was "Not to use information and communication technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies".

The second major action was "To reaffirm all the rights and responsibilities of states to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage".

It does not take a veteran diplomat to point out that several of the terms used in these provisions are ambiguous and could be open to wide and differing interpretation. This is a condition which one normally wishes to avoid in framing any sort of international agreement that is to govern state behavior.
Take for example the phrase "hostile activity"; hostility may be in the eye of the beholder and might be deemed to cover the hosting on one's territory of a server supporting a web-site of an opposition group. Or consider the prohibition on"proliferation of information weapons or related technologies". Beyond the fact that information weapons as a category is yet to be defined, what would constitute proliferation of these items is also obscure. Would offering on-line subscriptions to a publication critical of Russian or Chinese state actions be judged as a proliferation of information weapons? As a cyber attack mounted from someone's laptop could be viewed as constituting an information weapon, would the ban on proliferation of related technologies extend to the marketing of these basic computer items? Establishing mutually acceptable definitions of the very equipment or capabilities the code would aim to preclude would represent a major hurdle for any future negotiators.

Similarly, the affirmation of the right of states to protect their "information space" could prove highly problematic in practice. What one state might view as a "disturbance" or even "sabotage" of their information space, could be considered by another state as simply a case of exercising the right to freedom of expression. Although the code has a provision "to fully respect rights and freedom in information space" it also has a reference to international cooperation "in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment". It is clear that such a broadly drawn injunction could be cited to justify restrictions on information that other states might consider perfectly normal manifestations of the freedom of expression and opinion. The broad scope given to this curbing of information dissemination is all the more problematic in the absence of any mechanism for adjudicating differing interpretations states might hold as to what represents acceptable information or not. These examples of inherently problematic features of the text are not to suggest that the problems of a code of conduct for cyberspace are insurmountable or that they render the pursuit of some common ground rules as futile. They do however indicate the difficulty in arriving at provisions that would have comparable implications for conduct amongst states that hold different ideological worldviews.

Moscow and Beijing seem to be aware that their proposed code of conduct might provoke skepticism (and diplomatic opposition) in some quarters and are proceeding cautiously with their initiative. The two states have not followed through with the next logical step for their draft code, which in the context of multilateral diplomacy, would be to incorporate their code of conduct into an actual resolution for consideration at the UN General Assembly. They have not been idle however, having conducted consultations on their draft code on the margins of the UN General Assembly. Chinese representatives have suggested that the initial proposal is being revised in the light of comments received, but no new version has yet to be presented before the international community. In addition to action at the universal level of the UN, the code has also been promoted by China and Russia in regional security organizations such as the ASEAN Regional Forum (ARF) seminars devoted to confidence-building measures in cyberspace.

China provides conceptual underpinnings:

China in particular has been active in elaborating a conceptual framework in which to situate eventual multilateral consideration of the code. Chinese representatives have expressed five principles that should govern state conduct in cyberspace. First is the principle of peace and the use of "active preventive diplomacy" in order "to keep information and cyberspace from becoming a new battlefield". Specifically, states should not "research, develop or use cyber weapons". Second is the principle of sovereignty: "Cyber sovereignty is the natural extension of state sovereignty into cyberspace and should be respected and upheld". Third is the principle of balance "between freedom and security in information flow". The free flow of information "shall not be used as the excuse for illegal and irresponsible information rampant on the Internet". Fourth is the principle of equitable development with emphasis on the obligation of developed countries to help developing countries to "narrow the digital divide". Fifth is the principle of cooperation as "Given the cross-border, fluid nature of the internet, countries must strengthen cooperation in order to tackle cyber security threats effectively". [9] These five principles are designed to appeal to concerns of many states in the international community while creating an intellectual foundation for the type of measures set out in the code of conduct.

Beijing is conscious that the reaffirmation of sovereignty, the emphasis on capacity-building in the developing world and the prohibition on cyber weapons are all likely to resonate well with a majority of UN member states and may serve to mitigate concerns over other aspects of the principles such as the potential for information control embedded in the "balance" principle.

The UN Group of Governmental Experts:

The measured pace China and Russia are following in building support for the code proposal may also be tied to a related but distinct UN process currently underway. This is the UN Group of Governmental Experts (GGE) on "Developments in the Field of Information and Telecommunications in the context of International Security", which was established by a Russian-led resolution in 2011 that enjoyed wide support. The GGE (comprised of representatives of the P5 and ten other states) met in three one-week sessions in 2012 and 2013 and was successful in producing an agreed report to the General Assembly for its fall 2013 session. The GGE had a mandate to "study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behavior of States". [10] This orientation was also clearly in line with the objectives being affirmed in the Sino-Russian draft code.

The GGE report acknowledged the growth in threats to cyber security and the use of information and communication technologies (ICT) for crime and "the conduct of disruptive activities".[11] The report further recognized that "States also have an interest in preventing conflict arising from the use of ICTs" and concluded that "international cooperation is essential to reduce risk and enhance security". The form this international cooperation should take is reflected in the report's sections on norms, confidence building measures and capacity building. Under the section on norms the report affirmed that "The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability". This assertion of the relevance of international law to the new domain of cyberspace was a key objective of the U.S. and other Western states. At the same time, the affirmation of the applicability of existing international law is immediately conditioned by references to the need for further study on how such norms shall apply to State behaviour and the potential for further norms to be developed. Similarly, later reference to international law is caveated by recognition of state sovereignty in the conduct by states of ICT-related activities and in their jurisdiction over ICT infrastructure on their territory.

The role of confidence building measures, as voluntary steps to promote trust among states was another focus of the report. The GGE recommended, "States should consider the development of practical confidence building measures to help increase transparency, predictability and cooperation". The report set out an illustrative list of possible measures, including exchange of information on national strategies and policies; the creation of bilateral, regional and multilateral consultative frameworks for confidence building; greater information sharing on ICT security incidents and enhanced mechanisms for law enforcement cooperation. Although this section presented a useful menu of confidence building measures, their actual adoption is left up to states for future action. Finally, and in light of the great disparities in cyber capacity, the report included a call for states "to provide technical and other assistance to build capacities in ICT security". The report concluded on a modestly upbeat note, declaring that "Progress in international security in the use of ICTs by States will be iterative, with each step building on the last". A more somber outlook might stress that the iterative process may not simply be in the direction of enhanced security and that state actions can detract from as well as contribute to the level of international security in cyberspace. Indeed the revelations of sophisticated state-conducted actions of cyber espionage and sabotage that emerged around the time the GGE report was being finalized served to underscore the risks to global cyber security if "norms of responsible state behavior" are not developed and implemented.

In order to maintain diplomatic momentum on the issue of cyber security and the role of states, Russia and other sponsors of the GGE process decided to immediately build on the 2013 report by having the General Assembly agree to a further round of GGE study. In its new mode an expanded GGE (with 20 versus 15 members) would be established in 2014 with a reporting deadline of 2015. In addition to the existing mandate with its focus on norms of responsible state behavior and confidence building measures, the GGE is to study "the issues of the use of information and communication technologies in conflicts and how international law applies to the use of information and communication technologies by States,"[12]. These additional aspects will likely prove more difficult for the new GGE to agree on, but point to the type of more specific problems the international community will need to address if it is to ever realize the call for the development of general norms. Despite its initial success, it remains to be seen if the GGE process can contribute significantly to the enterprise of global norm creation especially as states begin to articulate differing visions of what constitutes responsible state behavior in cyberspace. Although Russia and China were unable to have the 2013 GGE report go beyond a neutral "taking note" of their proposal for a code of conduct, these states will no doubt present the GGE result as validating their code of conduct initiative. It is possible that Beijing and Moscow may even believe that the stage is set to bring their proposal forward and seek its adoption by the General Assembly this fall.

A Western Response is called for:

Whatever the diplomatic strategy ultimately to be pursued by Beijing and Moscow, it is evident that Western states so far are reacting warily to the proposed code. In the near term therefore any push for early adoption of the draft code of conduct is likely to result in a new East-West divide over the best way to proceed in devising some rules of the road for state behavior in cyberspace. At the same time, the West (in particular its leading nation the U.S.) having called for the development of a global consensus around a set of norms for defining responsible state behavior can hardly object when states respond by suggesting a set of norms of their own. Indeed one can discern behind the cool reception being shown the Russian-Chinese proposal in some Western capitals, an irritation that Beijing and Moscow have effectively stolen a march on leading Western powers in being the first to present the international community with a draft set of global norms.

In this light, it would be prudent for Western states to come up with their own version of what these global norms for state behavior should consist of and not simply critique what has been brought forth by China and Russia. A Western counter-proposal would also assist those states not enamoured with the Sino-Russian text to think through some of the problems inherent in any effort to delineate responsible state behavior in cyberspace. The distinction between offensive and defensive cyber operations in cyber security strategies will be critical as militaries begin to establish cyber units and develop their capacities. In turn, governments will need to decide on policy limits to inform eventual rules of engagement. The Snowden-sourced revelation of Presidential Policy Directive 20 outlining U.S. policy will spotlight this key issue for other cyber powers although as an unintended "transparency" measure it could also contribute to strategic confidence building.

Similarly, the difference between computer network attack and computer network exploitation (a crucial demarcation for the military and intelligence establishments respectively) will require serious debate as states may seek to maintain cyber espionage while cooperating to curtail cyber warfare. These are illustrative of the type of thorny policy issues over which even like-minded Western states may differ. It will be important for detailed consultations on these questions to get underway amongst allies and partners so that a more coherent cyber security foreign policy can emerge over time.

Conclusion:

The quest for a global consensus on norms of responsible state behavior in cyberspace needs to be purposefully taken up. The international community can ill afford to leave the security of cyberspace to the self-proclaimed 'cyber warriors'. The initial manifestations of official recognition that such norms are desirable (e.g. the U.S. *International Strategy*, the Sino-Russian code of conduct, and the UN GGE) require sustained follow-up. Concerned capitals will have to invest considerable political and diplomatic energy in any effort to forge a consensus around such norms. An intensification of bilateral cyber security consultations on the part of leading cyber powers, such as those underway between the U.S. and Russia and the more recently agreed upon working group between China and the U.S. will be a vital complement to multilateral efforts to develop agreed norms for state behavior in cyberspace. At the same time, the universal character of cyberspace and the extensive socio-economic engagement in it, points to a need for norms that will be global rather than particular in nature. This in turn suggests a dedicated multilateral process under UN auspices. It is time for states to move from airing broad principles to initiating a more focused diplomatic process to negotiate the content of the new norms. Preserving cyberspace for peaceful purposes on behalf of humanity requires pro-active work to forge some common arrangements to govern state actions. Although states will have to step up to the plate to address this challenge, the private sector and civil society, as the chief stakeholders of cyber space, cannot afford to be idle on this issue and will need to press their governments to take early and appropriate action if the benign character of cyberspace is to be preserved.

[1] Ronald J. Deibert *Black Code :Inside the Battle for Cyberspace* (Toronto, McClelland & Stewart 2013) pg 88

[2] *The Cyber Index: International Security Trends and Realities* (Geneva, UN Institute for Disarmament Research, 2013). Accessible at www.unidir.org pp1-2

[3] Brian Fung "Cyber Command's exploding budget" *The Washington Post,* January 15, 2014

[4] "Presidential Policy Decision 20 – U.S. Cyber Operations Policy" text of document available at www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-fulltext

[5] For recent reporting on U.S. Government reactions to Chinese cyber intrusions see Ellen Nakashima "Confidential Report lists U.S. weapon system designs compromised by Chinese cyberspies" *The Washington Post*, May 27, 2013; David Alexander "Cyber threats pose 'stealthy, insidious' danger: defense chief" *Reuters* May 31, 2013; Jane Perlez "Hagel, in Remarks directed at China, speaks of Cyberattack Threat" *New York Times* June 1, 2013

[6] Megha Rajagopalan, "China suggests U.S. may have fabricated evidence of cyber attacks" *Reuters,* May 29, 2014 (www.reuters.com/article/2014/05/29 us-china-usa-diplomacy)

[7] *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, the White House, Washington, May 2011, pg 4 and 11

[8] *International Code of Conduct for information security*, Annex to letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, 14 September 2011

[9] The citations in this paragraph are drawn from two authoritative statements by Chinese Foreign Ministry officials: a speech by UN Ambassador Wang Qun at the First Committee of the 66th Session of the UN General Assembly, New York, 19 October 2011 (www.china-un.org) and the statement by Dr. Huang Huikang, Director-General of the Department of Treaty and Law, Ministry of Foreign Affairs, delivered to the Budapest Conference on Cyberspace, Budapest, 4 October 2012 (www.cyberbudapest2012.hu/plenary-sessions-speakers)

[10] *Developments in the field of information and telecommunications in the context of international security* UN General Assembly resolution, A/RES/67/27, 11 December 2012

[11] See report "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" UN General Assembly, A/68/98, 24 June 2013. All subsequent citations of the report are from this document.

[12] UN General Assembly resolution "Developments in the field of information and telecommunications in the context of international security" A/RES/68/243, 9 January 2014