International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 8

Outer Space and Cyberspace: A Tale of Two Security Realms

Paul Meyer

International security policy has most often been a function of competition between sovereign states over divergent national interests. This competition is rooted in the requirement of the state to defend its national assets, including territory, people, resources and infrastructure, from encroachment by other states or external forces. This requirement leads in turn to the creation of armed forces and the other components of national security establishments in order to protect these sovereign assets. But what is the appropriate security posture to assume with respect to spaces beyond the claims of sovereign states and national appropriation? These spaces are comprised of the so-called 'global commons' which have been the subject of special regimes devised by sovereign states.[1] These regimes have recognised the importance of access to and use of the spaces concerned by states for a variety of security and economic ends, while sometimes granting them a distinctive status as a 'common heritage of mankind'.

1. Global Commons

The earliest example of such a space and a special regime applied to it was the maritime domain. The initial navigational accomplishments of Portugal and

1 For the evolution of this concept in international relations, I have relied especially on John Vogler, 'Global Commons Revisited,' *Global Policy* 3 (2012): 61-71.

Spain in the fifteenth and sixteenth centuries (unlike their terrestrial conquests) could not be translated into enduring control over the world's oceans. Other powers also wanted to exploit the new maritime routes and the only alternative to permanent conflict was to arrive at some generally acceptable governance of the seas. Building on the writings of the international legal pioneer Hugo Grotius, states gradually embraced his concept of an international maritime order which consisted of two parts: a territorial sea under exclusive sovereign control (which custom eventually set at three miles because that was the range of land-based cannons at the time) and the 'high seas' that were opened for common use and owned by none.[2] This construct has been largely upheld by states over the intervening centuries, and received its most comprehensive codification in the UN Law of the Sea Convention of 1982. There are two other environments to which access has only been possible much more recently and for which common understandings and international agreements are just beginning to emerge. These environments are becoming increasingly important for a range of security, commercial and scientific pursuits although their character under international law and the practice of states is only now being shaped. What international security order, if any, will be established for these two environments remains to be seen, but the expansion of access and use of both should act as a spur to states to agree on a common approach sooner rather than later.

The two environments in question are outer space and cyberspace (or, as some prefer it, 'information space'). In considering these realms from an international security perspective, one is struck by several key similarities, but also some significant differences between them. In policy terms, this article will argue that there is room in both 'spaces' for an exercise of preventive diplomacy and the development of Confidence-Building Measures (CBMs) and cooperative security. We will first review the parallels between the environments and then proceed to an examination of the differences including how well the 'global commons' designation applies to them. On the basis of this comparative analysis we can discuss the case for sustaining the present, essentially benign operating environment of the two spaces through a conscious policy of international security cooperation. This cooperation frequently develops through a continuum that begins with the expression of principles or norms for state conduct, proceeds through the elaboration of political arrangements or measures and culminates in binding international agreements. The chief diplomatic proposals that have been put forward to secure such cooperation in the space and cyber realms will be examined and the article will conclude with an assessment of the prospects for cooperation in these two special security realms.

2 John Ruggie, 'Multilateralism: The Anatomy of an Institution,' *International Organization* 46 (1992): 575.

2. The Similarities

The first similarity between outer space and cyberspace, beyond their relative vastness, is their 'global commons' character. In both cases the international community has acknowledged that these environments in some way belong to humanity and are beyond national appropriation. In the case of outer space, this 'global commons' status is explicitly set out in the foundational Outer Space Treaty of 1967. Article I of that treaty stipulates that the use of outer space 'shall be carried out for the benefit and in the interests of all countries … and shall be the province of all mankind'. Article II reinforces this concept of global ownership by specifying that outer space, including the moon and other celestial bodies, is 'not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means'.[3] With respect to cyberspace, this 'global commons' status is not as explicitly or legally set out as is the case with outer space, but a similar vision animates the pronouncements of states. The most authoritative of these statements to date were those agreed to by consensus at the UN-mandated World Summit on the Information Society (WSIS), which was held in two stages in Geneva and Tunis in 2003 and 2005 respectively. The Declaration of Principles adopted by WSIS described 'a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge … '.[4] More recently, through the results of a series of UN Group of Governmental Experts (GGE) meetings on 'Developments in the Field of Information and Telecommunications in the Context of International Security' the notion of cyberspace as a special realm to be used for the good of humanity and in a peaceful manner has also been advanced. The latest GGE report, for example, '[u]nderscor[es] the aspirations of the international community to the peaceful use of information and communication technologies (ICTs) for the common good of mankind'.[5]

Other analysts have suggested that the question of access is the defining characteristic of a commons. Within an international security perspective, national security actors have stressed the importance of maintaining free access to the global commons. Illustrative of this perspective and policy orientation are the pronouncements of the US national security establishment. In a policy document outlining defence priorities for the 21st century, the US Department of Defense declared: 'America, working in conjunction with allies and partners around the world, will seek to protect freedom of access throughout the global commons – those areas

3 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty)*, 10 October 1967, *United Nations*, http://www.nti.org/media/pdfs/aptospc.pdf?_=1316555222&_=1316555222.

4 First Phase of the World Summit on the Information Society, *Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/4-E (12 December 2003), para. 1, http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

5 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), para. 12, http://www.un.org/ga/search/view_doc.asp?symbol=A%2F70%2F174&Submit=Search&Lang=E.

beyond national jurisdiction that constitute the vital connective tissue of the international system'.[6] In a NATO document entitled *Assured Access to the Global Commons* the authors identify this commons as comprised of the four domains of maritime, air, space and cyber and assert that 'the security and prosperity of our nations, individually and for the Alliance as a whole, rely on assured access to and use of the maritime, air, space and cyberspace domains that are the commons'.[7] Another military writer has described cyberspace, the newest of the domains, as 'characterized by permeable physical, political and social boundaries and a cyber culture that vigorously resists state control … the cyber domain is available to all nations and regarded as part of the global commons'.[8]

The second similarity is that both outer space and cyberspace are currently being used to provide a wide array of services and benefits, overwhelmingly civilian in nature. Approximately 1,200 satellites are currently operating in outer space on behalf of 60 states or commercial consortia.[9] Space-based services are being used by consumers around the globe. The exploitation of cyberspace is even more extensive, with over three billion Internet users and an increasing penetration in the developing world, where the majority of users are now found.

The third common feature is that while military activity is present in both environments, and has been for several years, these environments have not yet been 'weaponised' or transformed into active battle zones. In this context, weaponisation means the general introduction into an environment of offensive arms capable of destroying or damaging objects within that same environment. Moreover beyond exercising restraint regarding the introduction of weapons, there is an evident direction on the part of states to maintain a peaceful character for these environments. Again the 1967 Outer Space Treaty is explicit in this regard with its preambular references to the 'use of outer space for peaceful purposes' and its prohibition on any deployment of weapons of mass destruction or military activity on the moon or other celestial bodies. The WSIS Declaration of Principles is more indirect in its espousal of a peaceful character for cyberspace, although this orientation can be inferred from its affirmation that 'the Information Society should respect peace …' and its call that '[a] global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders … '.[10]

A fourth commonality is that both spaces pose particular difficulties for the monitoring and verification of state behaviour. Although there is a large-scale effort to monitor outer space anchored in the US military-operated Space Surveillance Network, this is primarily directed at tracking space debris and avoiding collisions

6 Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, 2012), 3, http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf.

7 Mark Barrett, et al, *Assured Access to the Global Commons* (Norfolk: North Atlantic Treaty Organization, 2011), xii, http://www.alex11.org/wp-content/uploads/2013/01/aagc_finalreport_text.pdf.

8 Ian K. Adam, 'The Character of Conflict,' in *Conflict and Cooperation in the Global Commons:* A Comprehensive Approach for International Security, ed. Scott Jasper (Washington: Georgetown University Press, 2012), 45.

9 Cesar Jaramillo, ed., *Space Security Index 2014* (Canada 2014), 23, http://spacesecurityindex.org/wp-content/uploads/2014/11/Space-Security-Index-2014.pdf.

10 First Phase of the World Summit on the Information Society, *Declaration of Principles,* paras. 35, 56.

and is not geared towards verifying the state of space assets generally. Verification of any potential restrictions on military activity in space has been viewed as a difficult task, and one that, in the opinion of some, would render any eventual arms control measures in space unverifiable. An analogous situation pertains in cyberspace, in which the extent and nature of the technology employed poses major challenges for monitoring activity, making attribution and verifying compliance with possible cooperative arrangements challenging.

Finally, and probably linked to the last point, is that neither outer space nor cyberspace has been subjected to much in the way of international governance or regulation to preserve their peaceful character with the important early exception of the Outer Space Treaty. This limited governance presence is the current reality even as it is widely acknowledged that both environments would be highly vulnerable if destructive attacks were to occur in them. The Obama Administration's *National Security Strategy* stated for example: 'The space and cyberspace capabilities that power our daily lives and military operations are vulnerable to disruption and attack.'[11]

3. The Differences

In turning to the differences between the two spaces, the first and most obvious is that outer space is a natural environment whereas cyberspace is a human-made one. Outer space is a vast, timeless domain in which humankind is only gradually projecting itself. Cyberspace, while equally vast at one level, has been developed in the timeframe of a generation and its nature is purely within human control.

A second major difference between the two spaces might be described as the 'threshold of entry' to them. To enter and use outer space requires sophisticated and costly assets and capabilities, usually possessed by a small number of states and a few multinational companies. Cyberspace, by contrast, can be explored by anyone with a personal computer or mobile device. The basic equipment is relatively cheap and users are numbered in the billions.

A third difference between the realms is that outer space activity is still dominated by state actors although there is a recent trend towards privatisation of some services. Currently there are only ten spacefaring nations possessing an independent orbital launch capacity. In contrast, the infrastructure of cyberspace is largely owned and operated by the private sector and civil society.

Finally, there is a difference in the manner in which the two realms have been treated to date under international law. Outer space has benefited from an early

11 The White House. *National Security Strategy* (Washington, 2010), 8, https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

foundational treaty that defined its character. Although this treaty is now 48 years old and many states believe that the legal regime it created for outer space needs to be reinforced,[12] it nonetheless provides an authoritative reference point. No similar treaty has yet been devised to define cyberspace and efforts to formalise cooperation via international legal instruments such as the 2001 Budapest Convention on Cyber Crime have not as yet met with widespread support amongst states.[13]

4. External Drivers

Taking into account the results of this brief survey of the similarities and differences of the two environments of outer space and cyberspace, there are two preliminary conclusions to be drawn for the purposes of international security. The first is that the current benign environment for operating in outer space and cyberspace provides major benefits to the international community and should be preserved. The second is that this current benign condition should not be taken for granted and that states (and stakeholders) should engage diplomatically now in order to ensure that these unique spaces are indeed preserved for peaceful use by humanity in the future. Achieving this goal will require the forging of new agreements and the development of innovative measures of practical cooperation.

In the last few years, we have begun to witness the beginning of official efforts at the preventive diplomacy that this author would advocate for safeguarding both outer space and cyberspace. It would have been gratifying to have been able to attribute these initiatives to far-sighted and well-reasoned policies by key states. Regrettably, this recent activism was more likely prompted by external actions that threatened these long-standing benign environments which stirred governments into preparing some measures in an effort to forestall devastating consequences down the road.

For outer space, the disturbing events prompting government action were most probably the anti-satellite weapon (ASAT) tests carried out by China and the US in 2007 and 2008 respectively. The impact of these military actions, which raised the long dormant threat of ASAT employment, were exacerbated by the accidental collision of a defunct Russian satellite and an active American one in 2009 which further

12 See notably the resolution on the 'Prevention of an Arms Race in Outer Space' which is annually adopted by the UN General Assembly with near universal support and which in reference to the legal regime for outer space states that 'there is a need to consolidate and reinforce that regime and enhance its effectiveness …': United Nations, General Assembly resolution 69/31, *Prevention of an Arms Race in Outer Space*, A/RES/69/31 (11 December 2014), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/31.

13 The Convention developed by the Council of Europe has only been ratified or acceded to by 47 states of which only eight are non-member states of the Council of Europe, see *Convention on Cybercrime*, Budapest, 23 November 2001, *Council of Europe Treaty Series*, No. 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

contributed to the already disconcerting increase of space debris. Such debris, of course, poses a significant hazard for space operations and there are already warnings from informed observers that the build-up of such debris poses a constant and significant threat to all spacecraft, especially those in low earth orbit.[14]

For cyberspace, the external developments which seem to be spurring nascent diplomatic initiatives are the publicly revealed initiation of state-sponsored offensive cyber attacks in the form of the 'Stuxnet' and 'Flame' malware payloads, and the generally higher publicity being given to cyber attacks against a range of public and private institutions. Government agencies tend not to be forthcoming with their cyber attack statistics, but it is widely acknowledged that state institutions are far from being immune to penetrations of their computer networks and the exfiltration of sensitive data. Although the magnitude of attacks in cyberspace eclipse those in outer space, in both realms the diplomatic proposals now surfacing represent an effort by states to preclude destructive actions in these fragile environments and to promote a cooperative security approach with respect to them.

5. Diplomatic Proposals for Outer Space Security

The diplomatic proposals for outer space security that have been advanced consist of four main types. Russia and China have been developing for some time elements of a treaty that would prohibit the placement of weapons in outer space. The genesis of this effort can be traced back to 2002 when Russia and China first introduced a working paper at the Conference on Disarmament in Geneva presenting several elements for such a treaty. This initiative was probably in response to the decision by the United States the year before to abrogate the Anti-Ballistic Missile (ABM) Treaty and with it one of the few legally binding prohibitions on deployment of weapons in outer space (in this case, space-based ABM systems). China and Russia have developed these elements over the next years and in February 2008, a draft treaty 'on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects' (better known by its acronym PPWT), was formally presented at the Conference on Disarmament.[15] In essence this accord seeks to reinforce the Outer Space Treaty's prohibition on stationing WMD in outer space by extending this ban to all weapons in space. The draft met with criticism from several quarters. Some faulted its failure to address ground-based anti-satellite

14 Jaramillo, ed., *Space Security Index 2014*, 10.

15 See 'Possible Elements of the Future International Legal Instrument on the Prevention of Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects', CD/1679 (Conference on Disarmament, 28 June 2002), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G02/624/84/PDF/G0262484.pdf?OpenElement for the original China-Russia working paper and CD/1839 29 February 2008 and 'Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects', CD/1985 (Conference on Disarmament, 12 June 2014), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/050/66/PDF/G1405066.pdf?OpenElement for the draft PPWT.

weapons although given the inherent ASAT capability of ballistic missile interceptors, any effort to include ground-based systems would have run up against the US commitment to deploy ballistic missile defences. Other states complained about the lack of verification provisions for the treaty given the significant military prohibitions contained in it. The Chinese and Russian sponsors attempted to respond to these critiques and in June 2014 presented a revised version of the PPWT, which included a new article acknowledging the need for verification measures and suggesting that these could be elaborated in a subsequent protocol to the treaty. Whatever the merits of the draft text, further consideration of it has been stymied by the general blockage of the Conference on Disarmament and to date the treaty's sponsors have not decided to take their draft text to any other forum.

The second initiative was brought forward by the European Union, originally in December of 2008. It took the form of a 'Code of Conduct for Outer Space Activities' a politically-binding 'set of best practices' designed to support safe operations in space. While in many ways a re-packaging of existing commitments and principles regarding state activity in outer space, the Code does include provision for significant institutional support for the multilateral review of outer space activity via annual information exchanges, biennial meetings of subscribing states and a central 'point of contact' performing secretariat-like functions. The Code also foresees consultative mechanisms in the eventuality that activities are undertaken which could be contrary to the Code's commitments and which might pose a risk of damage to others. The EU has issued revised versions of its original proposal in 2010, 2012 and most recently in March 2014. Over this period the EU has conducted several bilateral and three multilateral consultations.[16] The EU's initial effort to confine consultations with others to bilateral tracks in a sort of 'hub and spoke' process was not well received, and important states such as China, India, South Africa and Brazil voiced concerns. The EU Code of Conduct initiative has also suffered from various disconnects and changes in responsible personnel and has experienced difficulty in maintaining diplomatic momentum for wider acceptance, despite an endorsement by the US in January 2012. EU representatives have indicated that they are ready to 'move the process from a consultation to a negotiating phase in an inclusive and transparent manner', but the exact way forward favoured by the EU is still unclear.[17] In July 2015 the EU, in cooperation with the UN Office of Disarmament Affairs, organised a session at UN HQ in New York that it hoped would constitute a multilateral negotiation of its draft Code and set the stage for its adoption. Several participating states, notably the BRICS grouping (Brazil, Russia, India, China and South Africa), opposed this approach insisting that the future elaboration of the Code be held 'in the format of inclusive and consensus-based multilateral

16 The most recent version is entitled European Union, *Draft International Code of Conduct for Outer Space Activities* (31 March 2014), http://www.eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_31-march-2014_en.pdf.

17 United Nations, *Speakers in First Committee Urge Balance of Conventional Forces in Hotbeds of Tension, Non-Militarization of Outer Space*, GA/DIS/3511, 27 October 2014, http://www.un.org/press/en/2014/gadis3511.doc.htm.

negotiations within the framework of the UN'.[18] It would seem in this light that any future negotiation of the EU's Code of Conduct would depend on seeking a resolution in the UN General Assembly to mandate such a multilateral process.

The third proposal was made by Canada in 2009 in the form of a working paper submitted to the Conference on Disarmament and reiterated in the context of the UN General Assembly.[19] This proposal consisted of a series of unilateral 'pledges' that would have states declare that they would not: test or use a weapon against a satellite so as to damage or destroy it; deploy any weapons in outer space; or use a satellite itself as a weapon. These commitments were seen as providing some of the security content missing in the EU Code while avoiding the problems associated with the PPWT's new treaty approach. Canada, however, has not actively promoted these ideas subsequently and other states have not come out in favour of them, although some concerned NGOs have suggested similar measures.[20]

The last initiative concerns the UN Group of Governmental Experts (GGE) that began its work in July 2012 pursuant to a Russian-led resolution that has been adopted for several years by the UN General Assembly.[21] The fifteen-member UN GGE was mandated to consider possible transparency and confidence-building measures for outer space, and produced a consensus report in the summer of 2013 that was presented to the General Assembly for consideration. The report described transparency and confidence-building measures as 'a means by which Governments can share information with the aim of creating mutual understanding and trust, reducing misperceptions and miscalculations and thereby helping both to prevent military confrontation and to foster regional and global stability'.[22] The report enumerated several potential transparency and confidence-building measures, including information exchange and notification, risk reduction measures, visits to space-related facilities, and consultative mechanisms. The report said that these transparency and confidence-building measures should be considered as non-legally binding voluntary measures and that they were 'neither a substitute nor a precondition for arms limitation and disarmament measures'.[23] Although the GGE was successful in producing a substantive report with specific recommendations for transparency and confidence-building measures, it could do no more than present this menu of potential action items to the international community and see if states were prepared to adopt the measures proposed.

18 United Nations, *BRICS Joint Statement Regarding the Principles of Elaboration of International Instruments on Outer Space Activities*, New York, 27 July 2015.

19 'On the Merits of Certain Draft Transparency and Confidence-Building Measures and Treaty Proposals for Space Security', CD/1865, (Conference on Disarmament, Canadian Government, 5 June 2009) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G09/615/92/PDF/G0961592.pdf?OpenElement.

20 Union of Concerned Scientists, *Securing the Skies: Ten Steps the United States Should Take to Improve the Security and Sustainability of Space* (November 2010), 18, http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/securing-the-skies-full-report-1.pdf.

21 United Nations, General Assembly resolution 65/68, *Transparency and Confidence-Building Measures in Outer Space Activities*, A/RES/65/68 (13 January 2011), http://www.unidir.org/files/medias/pdfs/general-assembly-resolution-eng-0-420.pdf.

22 United Nations, General Assembly, *Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities*, A/68/189 (29 July 2013), 12, http://www.unidir.org/files/medias/pdfs/outer-space-2013-doc-2-a-68-189-eng-0-580.pdf.

23 Ibid, 13.

One particular recommendation from the GGE that is due to be realised this fall is a joint session of the UN General Assembly's First and Fourth Committees, the committees that have dealt respectively with the security and peaceful uses of outer space themes. This special joint session, which is to address possible challenges to space security and sustainability, could provide a forum for focused consideration of the proposed transparency and confidence-building measures generated by the GGE. Regrettably the cooperative atmosphere that characterised the work of the GGE and contributed to its ability to fashion a consensus report has deteriorated in the post-2013 period, with the revival of East-West tensions over Ukraine that will render more difficult agreement on any new cooperative arrangements concerning outer space. Symptomatic of this current problematic diplomatic environment was the decision by Russia and several other states to push forward in 2014 with a new UN General Assembly resolution on 'no first placement of weapons in outer space' despite opposition from a significant minority of states. These states believed that declaratory commitments not to be the first to place weapons in outer space, as urged in the resolution, did not meet the criteria for true transparency and confidence-building measures as earlier agreed by the UN GGE. The sponsors decided nevertheless to proceed to a vote on the resolution, which was adopted with 126 states in favour, 4 opposed (Georgia, Ukraine, Israel and the US), and 46 abstaining. The divisive nature of this result was in contrast with the consensual status of most space-related resolutions in the General Assembly and reflects the gap that is opening up amongst space powers that may impede the adoption of any new cooperative agreements or arrangements in the near term.

6. Diplomatic Proposals for International Cyber Security

Diplomatic proposals for international security in cyberspace are more recent and less numerous than for outer space, but are also starting to surface. The US, while not bringing forward any specific proposal of its own, officially called for the forging of a consensus on 'norms for responsible state behaviour' in its path-breaking *International Strategy for Cyberspace* released by the White House in May 2011.[24] Having issued this important call for an urgent dialogue amongst states to develop these norms, the Obama Administration has found it difficult to translate this policy aim into any multilateral diplomatic process to yield the desired result. In the event, other states were the first off the mark in proposing some specific content to meet the goal of 'norms for responsible state behaviour'. In September of that year, Russia and China (in conjunction with Tajikistan and Uzbekistan) circulated

24 The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), 8, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

at the UN General Assembly a proposal for an 'International Code of Conduct for Information Security'. In presenting the proposal, Ambassador Wang Qun of China, declared that 'countries should work to keep information and cyberspace from becoming a new battlefield, prevent an arms race in information and cyberspace and settle disputes on this front peacefully through dialogue'.[25]

Originally, the key commitment of this voluntary code would be for states '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'.[26] After having carried out consultations with other states on the margins of the UN General Assembly, China and Russia decided to issue a revised version of their Code of Conduct in January 2015. Significantly, the arms control orientation of the initial draft has been dropped in favour of a much more general formulation by which subscribing states would commit 'not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security'.[27] Presumably the consultations with others had persuaded the sponsors that the original arms control orientation was not feasible at this stage given the practical problems associated with it such as the lack of any agreed definition of an 'information weapon'. The revised Sino-Russian Code still retains a 'security' focus, however, especially in the elements aimed at countering content from information and communications technologies that is perceived to incite 'terrorism, separatism or extremism … [or threaten states'] … political, economic and social security'.[28] These provisions are aligned with Sino-Russian views on the necessity to police content and on the sovereign rights of states to exercise control over their information infrastructure. The very term 'information security' preferred by China and Russia to the term 'cyber security' favoured by the West is illustrative of the former's concern with content as opposed to the latter's focus on system integrity.

Diplomatically, the Sino-Russian partnership on new approaches to outer space security has carried over into cyberspace with a similar leadership being shown by Beijing and Moscow on arrangements to promote 'information security'. Their activism on the space and cyber security files also reflects a pragmatic capacity to refine their proposals in light of the prevailing diplomatic context. For example, the Russian-Chinese decision to present their set of cyber security norms as a voluntary, politically binding Code of Conduct instead of as an international legal instrument

25 Wang Qun, 'Work to Build a Peaceful, Secure and Equitable Information and Cyber Space' (Statement made at the First Committee during the 66th session of the General Assembly, New York, 20 October 2011), http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

26 United Nations, General Assembly, *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), https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

27 United Nations, General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/69/723 (13 January 2015), 5, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

28 Ibid.

suggests that they had absorbed the lessons from their earlier joint initiative of the PPWT. With respect to the new cyber initiative the co-sponsors were opting now for a simpler format and one which would be easier and quicker for states to adopt. Russia and China as chief sponsors of this proposal have also proceeded with some care and have taken the time to conduct consultations with other states regarding their draft Code of Conduct, thus enabling them to present their revised version as reflecting input received from others. Arguably this has increased the eventual acceptability of their proposal for a Code of Conduct on Information Security and positions China and Russia to press for the adoption by the UN General Assembly of their text when they judge the time is propitious to do so.

One reason why Russia and China have decided not to move forward more rapidly with their draft Code of Conduct may be linked to the other major diplomatic initiative related to international cyber security that is currently on-going within the UN context. This is the work of the UN Group of Governmental Experts (GGE) on 'Developments in the Field of Information and Telecommunications in the Context of International Security' referred to earlier. These UN GGEs originated with a Russian-led UNGA resolution and first yielded a consensus report in 2010. The 2010 report observed that states were developing Information and Communications Technologies (ICTs) 'as instruments of warfare and intelligence' and called for 'confidence-building, stability and risk reduction measures to address the implications of state use of ICTs'.[29] Following close on the earlier report, another UN Group of Governmental Experts also got underway in the summer of 2012 and succeeded in producing a report in June 2013. The 2013 GGE report went further than its predecessor to warn that 'the absence of common understandings on acceptable State behaviour with regard to the use of ICTs increases the risk to international peace and security'.[30] The report recommended that states consider taking action on norms and principles of responsible behaviour, on confidence-building measures, and on capacity-building measures. Again while the GGE produced a set of practical if modest measures for states to consider, actual implementation is essentially left to the initiative of those states. Having already been instrumental in the establishment of the 2010 and 2013 GGEs, Russia decided to maintain the diplomatic momentum it had generated on the issue of international cyber security by initiating yet another GGE. This expanded GGE (20 members rather than the usual 15) produced a consensus report in the summer of 2015. In addition to its existing mandate on norms of responsible state behaviour and confidence-building measures, the GGE was mandated to consider 'the issues of the use of ICTs in conflicts and how inter-

29 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010), 8, http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

30 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 June 2013), 7, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

national law applies to the use of ICTs by States'.[31] The GGE report succeeded in further developing norms and rules for state cyber conduct, suggesting for example that states refrain from ICT activity 'that intentionally damages critical infrastructure'.[32] The report recommends that a further GGE be created in 2016, although mere continuation of GGE studies may begin to suffer from diminishing returns. It is evident in the cyber security field that as countries move beyond statements of lofty general principles and begin to address specific measures, divisions of views become more pronounced and concrete outcomes more elusive. Ultimately, states will need to move beyond the restricted participation of the GGEs and embrace some form of broader, multilateral negotiating forum if the ideas being generated by the GGEs are to be transformed into agreed commitments.

7. Prospects for Cooperation

Despite the challenges that international cooperation on outer space and especially in the new domain of cyber security faces, there is also a growing parallel concern that the preservation of the peaceful environments of outer space and cyberspace are too important a set of objectives to leave only in the hands of the military. In both the case of outer space and cyberspace, and especially with the latter, there is a large and potentially influential civilian lobby comprised of business and civil society actors that is increasingly aware of the threats to cyberspace and is engaged in prodding governments into some preventive action. The private sector's refrain is that the time has come to establish a public-private partnership to address global cyber security threats and to develop policy responses, including the formulation of cyber security norms. As one large multinational firm has stated:

> 'The development of cybersecurity norms cannot be a niche foreign policy issue reserved for diplomats. Cybersecurity norms are an imperative for all users, governments, the private sector, non-governmental organizations, and individuals, in an Internet-dependent world – each contributes to the peace, security and sustained innovation of a globally interconnected society.'[33]

This civil society concern over the harmful consequences of a lawless cyberspace is starting to be manifested in diplomatic forums. At the UN General Assembly's fall

31 United Nations, General Assembly resolution 68/243, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/68/243 (9 January 2014), http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2014-2015-a-res-68-243-eng-0-589.pdf.

32 United Nations, General Assembly, *Group of Governmental Experts*, A/70/174, 8.

33 Microsoft Corporation, *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*, White Paper (23 January 2015), 14, http://www.microsoft.com/en-us/download/details.aspx?id=45031.

session in 2014, nine NGOs delivered a joint statement seeking action by states to adopt 'an effective international legal framework that will prevent cyber attacks and protect the networked infrastructure upon which societies rely for their wellbeing'.[34]

Barring another dramatic external event that draws attention to the vulnerability of these operating environments to disruption through irresponsible state behaviour, it may in fact be this private sector and civil society lobbying which will spur governments to take more decisive action. Although the work on outer space security pre-dates that on cyber security, it may well be in the latter realm that the first international security arrangements are devised. State authorities may feel a priority need to put down some initial markers of restraint regarding their conduct in cyberspace and to reassure the civilian sector that the government will not endanger this critical infrastructure through irresponsible action. The articulation of norms for responsible state behaviour, especially in the form of voluntary, political undertakings are likely to be the preferred route for states given their inherent flexibility and timeliness and the avoidance of the need to develop verification provisions that would have to underpin new international legal instruments.

Given the intrinsically global character of both outer space and cyberspace, it is understandable why much of the diplomatic consideration of the problem of security in these realms has occurred within the universal, multilateral context of the UN. Important complementary work has also been underway at the regional level, especially concerning cyber security. In Europe the Organization for Security and Co-operation in Europe (OSCE) has been active on the international security dimension of cyberspace and in April 2012 set itself the goal of developing a first set of CBMs 'to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs'.[35] The OSCE initiative yielded an initial set of CBMs that were approved at the organisation's December 2013 Ministerial meeting. Although the eleven measures adopted are primarily voluntary exchanges of information on various aspects of ICTs, there is provision for on-going institutional support by means of a dedicated working group that is to meet at least three times a year to discuss the information exchange and explore further CBM development.[36] The deterioration of East-West relations attendant upon the Ukraine crisis has likely put a damper on some of the cooperation envisaged by the CBMs, but the OSCE action stands out as the first multilateral agreement on cyber security CBMs and will probably serve as a model for others.

34 Women's International League for Peace and Freedom, *Civil Society Statement to First Committee on Cyber, Disarmament, and Human Security* (28 October 2014), http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com14/statements/28Oct_cyber.pdf.

35 Organization for Security and Co-operation in Europe, Permanent Council decision No. 1039, *Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1039 (26 April 2012), http://www.osce.org/pc/90169?download=true.

36 Organization for Security and Co-operation in Europe, Permanent Council decision No. 1106, *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1106 (Organization for Security and Co-operation in Europe, Permanent Council, 975th Plenary Meeting, 3 December 2013), http://www.osce.org/pc/109168?download=true.

Whether it occurs at the universal or regional level, the initiation of bilateral and multilateral consultations on how to ensure the continued peaceful exploitation of both outer space and cyberspace would usefully contribute to increased awareness, confidence-building and eventually the development of cooperative security arrangements. Given the potential mass disruption stemming from offensive cyber operations or space negation actions there should be an inherent interest on the part of states to engage in preventive diplomacy in these two realms. The intrinsically universal character of these two 'global commons' militates in favour of as inclusive a regime as possible and this in turn puts a premium on developing measures that can be agreed under UN auspices. It will be crucial for all concerned stakeholders to be pro-active in this regard and to begin to move now to preclude the most damaging manifestations of conflict in these vulnerable environments and thereby help sustain safe and secure access to them for all people at all times.