SCHOOL FOR
INTERNATIONAL STUDIES

Outer Space and Cyberspace: A Tale of Two Security Realms

Paul Meyer

Simons Papers in Security and Development

No. 51/2016 | April 2016

The **Simons Papers in Security and Development** are edited and published at the School for International Studies, Simon Fraser University. The papers serve to disseminate research work in progress by the School's faculty and associated and visiting scholars. Our aim is to encourage the exchange of ideas and academic debate. Inclusion of a paper in the series should not limit subsequent publication in any other venue. All papers can be downloaded free of charge from our website, www.sfu.ca/internationalstudies.

The series is supported by the Simons Foundation.

Series editor: Jeffrey T. Checkel
Managing editor: Martha Snodgrass

Meyer, Paul, *Outer Space and Cyber Space: A Tale of Two Security Realms*, Simons Papers in Security and Development, No. 51/2016, School for International Studies, Simon Fraser University, Vancouver, April 2016.

ISSN 1922-5725

Copyright remains with the author. Reproduction for other purposes than personal research, whether in hard copy or electronically, requires the consent of the author(s). If cited or quoted, reference should be made to the full name of the author(s), the title, the working paper number and year, and the publisher.

Copyright for this issue: Paul Meyer, pmeyer(at)sfu.ca.

School for International Studies
Simon Fraser University
Suite 7200 - 515 West Hastings Street
Vancouver, BC Canada V6B 5K3

SCHOOL FOR INTERNATIONAL STUDIES

SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

Outer Space and Cyber Space: A Tale of Two Security Realms

Simons Papers in Security and Development
No. 51/2016 | April 2016

Abstract:
The concept of "global commons" has been applied under international law to certain special environments for which states have agreed to prohibit national appropriation and to treat these spaces as "the province of all mankind" (Outer Space Treaty 1967). After tracing the origins of the concept with reference to the law of the sea, the paper examines two relatively new environments, outer space and cyberspace, for which the status of "global commons" can facilitate the emergence of a cooperative security regime. The various diplomatic efforts to develop international security arrangements for these vital, if fragile, environments are reviewed and prospects for their successful adoption assessed.

About the author:
Paul Meyer is currently an Adjunct Professor of International Studies and Fellow in International Security at Simon Fraser University and a Senior Fellow at The Simons Foundation, Vancouver, Canada. From 1975 to 2010 Paul Meyer was a career diplomat in Canada's Foreign Service with a professional focus on international security policy. He served as Canada's Ambassador to the UN and the Conference on Disarmament in Geneva in 2003–2007.

About the publisher:
The School for International Studies (SIS) fosters innovative interdisciplinary research and teaching programs concerned with a range of global issues, but with a particular emphasis on international development, and on global governance and security. The School aims to link theory, practice and engagement with other societies and cultures, while offering students a challenging and multi-faceted learning experience. SIS is located within the Faculty of Arts and Social Sciences at Simon Fraser University. Our website is www.sfu.ca/internationalstudies.

Outer Space and Cyberspace: A Tale of Two Security Realms

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 – territory, people, resources, infrastructure etc. – 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" that have been the subject of special regimes devised by sovereign states.[1] These regimes recognized 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".

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 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 several centuries and has received its most comprehensive codification in the UN Law of the Sea Convention of 1982. There are two other environments however 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 usage 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 "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 measures of confidence building 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.

The Similarities

The first similarity of 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, 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) 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, underscores "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 U.S. national security establishment. In a policy document outlining defense 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 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 currently are being utilized to provide a wide array of services and benefits, overwhelmingly civilian in nature. Approximately 1200 satellites are currently operating in outer space on behalf of 60 states or commercial consortia.[9] Space-based services are being utilized 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 now reside.

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 "weaponized" or transformed into active battle zones. In this context, "weaponization" 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 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 for verifying compliance with possible cooperative arrangements.

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]

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 time frame 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. In contrast cyberspace 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 privatization 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 to which the two realms have been treated to date under international law. Outer space has benefited from an early 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 (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…"[12]) it nonetheless provides an authoritative reference point. No similar treaty has yet been devised to define cyberspace and efforts to formalize cooperation via international legal instruments (e.g. the 2001 Budapest Convention on Cyber Crime) have not met as yet with wide spread support amongst states.[13]

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 to ensure that these unique spaces are indeed preserved for peaceful utilisation by humanity in the future. To achieve this goal will require the forging of new agreements and the development of innovative measures of practical cooperation.

In the last few years, we are beginning to witness the commencement of official efforts at the preventive diplomacy that this author would advocate for safeguarding both outer space and cyber space. 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 the long-standing benign environments and that stirred governments into preparing some measures in an effort to forestall devastating consequences down the road.

For outer space, the disturbing events prompting governmental 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 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 situated in low earth orbits.[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. Governmental agencies tend not to be forthcoming with their cyber attack statistics, but it is widely acknowledged that state institutions are far from being immune from 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.

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 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 that 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 of the Code, 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 organized a session at UN HQ in New York that it hoped would constitute a multilateral negotiation of its draft Code to 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 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: i) test or use a weapon against a satellite so as to damage or destroy it; ii) deploy any weapons in outer space and iii) 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 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.

One particular recommendation from the GGE that is due to be realized 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 characterized 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 GGE. The sponsors decided nevertheless to proceed to a vote on the resolution, which was adopted with a 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.

Diplomatic Proposals for International Cyber Security

Diplomatic proposals for international security in cyber space are more recent and less numerous than for outer space, but are also starting to surface. The United States, 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 same year, Russia and China (in conjunction with Tajikistan and Uzbekistan) circulated 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 cyber space from becoming a new battlefield, prevent an arms race in information and cyber space 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 via 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, 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

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 upon the earlier report another UN Group of Governmental Experts, which, like its outer space counterpart, 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 (20 members versus the usual 15) GGE produced a consensus report in the summer of 2015 that will be considered at the General Assembly this October. 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 international 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.

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 cyber space are too important a set of objectives to leave only in the hands of the military. In both the case of outer space and cyber space, 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 cyber space and 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 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 cyber space, 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 Organisation for Security and Cooperation in Europe (OSCE) has been active on the international security dimension of cyber space 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 organization’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.

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 cyber space 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.

Notes

[1] For the evolution of this concept in international relations, I have relied especially on John Vogler, "Global Commons Revisited", *Global Policy* Volume 3, Issue 1, February 2012, pp. 61-71.

[2] John Gerrard Ruggie, "Multilateralism: the anatomy of an institution", *International Organization*, Vol 46, Issue 3, Summer 1992, p. 575.

[3] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space", opened for signature 27 January 1967, available at http://disarmament.un.org.

[4] "Declaration of Principles", World Summit on the Information Society, WSIS-03/GENEVA/DOC/4-E 12 December 2003, paragraph 1, available at www.itu.int.

[5] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", UN General Assembly, A/70/174, 22 July 2015, p.12.

[6] "Sustaining US Global Leadership: Priorities for 21st Century Defense", Office of the Secretary of Defense, Washington, January 5, 2012 p. 3.

[7] Barrett, Mark; Bedford, Dick; Skinner, Elizabeth; Vergles, Eva, *Assured Access to the Global Commons*, Supreme Allied Command Transformation, NATO, Norfolk, USA. April 2011, p xii.

[8] Ian K. Adam, "The Character of Conflict", in Scott Jasper (ed), *Conflict and Cooperation in the Global Commons*, Georgetown University Press, Washington, 2012, p. 45.

[9] *Space Security Index* 2014, p. 23 (www.spacesecurityindex.org).

[10] WSIS "Declaration of Principles", paragraphs 35 and 56.

[11] *National Security Strategy*, the White House, Washington, May 2010, p. 8.

[12] UN General Assembly resolution "Prevention of an Arms Race in Outer Space" A/RES/69/31 adopted on 2 December 2014.

[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 CETS No 185 http://conventions.coe.int.

[14] "*Space Security Index* 2014", p. 10, available at www.spacesecurityindex.org.

[15] See Conference on Disarmament document CD/1679, 28 June 2002, for the original China-Russia working paper. and CD/1839 29 February 2008 and CD/1985 12 June 2014 for the draft PPWT, www.unog.ch/disarmament.

[16] The most recent version is entitled " Draft International Code of Conduct for Outer Space Activities", European Union 31 March 2014, available at www.eeas.europa.eu.

[17] "69th Session of the UN General Assembly First Committee – EU Statement on Outer Space" EU Delegation, 27 October 2014, New York.

[18] "BRICS Joint Statement Regarding the Principles of Elaboration of International Instruments on Outer Space Activities" July 27, 2015, New York.

[19] "On the Merits of Certain Draft Transparency and Confidence-Building Measures and Treaty Proposals for Space Security", working paper submitted by Canada to the Conference on Disarmament, CD/1865, 5 June 2009.

[20] *Securing the Skies,* Union of Concerned Scientists, 2010, p. 18 (http://www.ucsusa.org/search/site/the%20skies#.Vv1HF0Y43Gs).

[21] UN General Assembly resolution "Transparency and confidence-building measures in outer space activities" A/RES/65/68, adopted 8 December 2011.

[22] "Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities" UN General Assembly, A/68/189, 29 July 2013 p. 12.

[23] Ibid. 13.

[24] "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World" the White House, May 2011, p. 8.

[25] Wang Qun, "Work to Build a Peaceful, Secure and Equitable Information and Cyber Space", statement made at the First Committee of the 66th session of the UN General Assembly, 19 October 2011

[26] "International Code of Conduct for Information Security" UN General Assembly, A/66/359, 14 September, 2011

[27] "International Code of Conduct for Information Security" UN General Assembly, A/69/723, 13 January 2015 p. 5.

[28] Ibid p. 5.

[29] "Report of 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 p. 8.

[30] "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, p. 7.

[31] 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.

[32] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", UN General Assembly, A/70/174, 22 July 2015, p. 8.

[33] " International Cybersecurity Norms", Microsoft Corporation White Paper 2015 , www.microsoft.com/security/gssd, p. 14.

[34] "Civil Society statement to First Committee on cyber, disarmament and human security" October 28, 2014, www.reachingcriticalwill.org

[35] "Decision No. 1039, "Development of Confidence-Building Measures to Reduce the Risks of Conflict stemming from the Use of Information and Communication Technologies", Organization for Security and Cooperation in Europe, Permanent Council, PC.DEC/1039, 26 April 2012.

[36] 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", Organization for Security and Cooperation in Europe, Permanent Council PC.DEC/1106 3 December 2013.