CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org
F: +44 (0)20 7957 5710 www.chathamhouse.org
Charity Registration Number: 208223

International Security Discussion Paper

Countering Threats in Space and Cyberspace: A Proposed Combined Approach

Lorenzo Valeri

LUISS Guido Carli

January 2013

This paper presented at the workshop *Making the Connection: The Future of Cyber and Space*, Chatham House, 24 January 2013.

INTRODUCTION

Throughout history the pursuit of secure access and control of global commons has been one of the pivotal aims for military superiority as well as national and international stability. Unfettered access has allowed states and organizations to operate in a globalized economic environment that has cultivated strategic partnerships and alliances. Hence the fact that adversaries have aimed to (or disrupted) access to one common as to achieve strategic and political goals.[1] Still, unlike the past, today's global commons (sea, air, space and cyberspace) are not in 'silos'. They experience strong inter- and intra-dependency. Therefore, temporary disruptions of one global common can undermine the efficiency of the others. This condition of dependency becomes particularly clear in the case of cyberspace and space.[2]

Cyberspace and outer space are core elements of today's global information space – more commonly known as the 'cloud' or the 'big data' age.[3] More importantly, their preponderance has spillover effects on the effectiveness and efficiency of the more 'traditional' commons: land, sea and air. Information technologies and space communication systems allow, *inter alia*, for more efficient land, sea and air activities via GPS and other geographic location systems. They represent the information infrastructures of global supply chain structures where internet-based open networks allow sharing localization data. In a defense context, the combination of space and cyberspace functionalities allows for seamless tactical and strategic communication, intelligence and space situational awareness.[4] Therefore, it is feasible to argue for a combined space and cyberspace common where the constant stream of technological and commercial developments allows for a seamless integration of Internet-based capabilities into space systems.[5]

---

1 Although with a US hegemonic focus this point is focused on Barry Posen (2003), 'Command of the Commons', *International Security*, 28:1, 5-46 with a specific focus on pp.10-5; For a debate about the evolution of warfare, see Colin Fleming (2009), 'New and Old Wars? Debating Clausewitzian Future', *Journal of Strategic Studies*, 32:2 pp.213-1.

2 Abraham M. Denmark (2010), 'Managing the Global Commons', *The Washington Quarterly,* 33:3, pp.165-82.

3 The expression 'big data' refers to the capacity of organizations to extrapolate information and knowledge from the large array of data to which they may have access from inside their organization or through outside players. For a perspective see James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh and Angela Hung Byers (2011), *Big Data: The next frontier for innovation, competition, and productivity.* McKinsey Global Institute. http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation (visited 18 December 2012).

4 For an overview see Thomas Single (2009), *JAPCC NATO Space Operations Assessment* in particular pp.21-30.

5 See Mark Berrett, Dick Bedford, Elisabeth Skinner, Eva Vergles (2011), *Assured Access to the Global Commons*, Supreme Allied Command Transformation, NATO, April, pp.20-32.

Dependency between space and cyberspace commons would not be of any concern except that there is a growing number of vulnerabilities whose exploitation can undermine their strategic functions. First, both commons experience evolving technological development due to the constant exploitation of new software/hardware solutions and infrastructures. Although this allows for positive network externalities, it creates the basis for 'cybervulnerabilities' such as, hardware, software or other design failures.[6] At the same time, both commons are exposed to physical vulnerabilities such as telecommunication cable disruptions.[7] In the case of space, physical vulnerabilities may also include solar weather conditions and natural meteorites. There are also man-made vulnerabilities such as operational mistakes, dispersion of satellite debris and cascading general design failures.[8]

EMERGING THREATS

The complex and vulnerable setting of space and cyberspace commons is confronted by a threatening environment that is difficult to map.[9] In the context of cyberspace, malicious individuals and organized criminals easily exploit access to new technologies by carrying out cybercrimes.[10] At the same time, over the years there has been a growing confluence between cybercriminal activities and alleged state-sponsored malicious activities. In fact, as NATO recently argued, several rogue states are capitalizing on information technologies for carrying out cybercrimes, and perhaps outsourcing them to unattributable third parties, including criminal organizations.[11]

---

6 For a perspective on positive network externalities and cybersecurity see Carl Shapiro and Hal Varian (2002), *Information Rules*, Harvard Business School Press, in particular pp.173-227.
7 An example is the January 2008 submarine cable disruptions affecting internet communication between India and several parts of Europe.
8 For an overview on space threats see *United Kingdom's Development, Concepts and Doctrine Centre, Space: Dependency, Vulnerabilities and Threats*, Report on behalf of the Multinational Experiment 7 (MNE7) Community, 2012.
9 For a more comprehensive perspective see Gary Hart (2011), 'After bin Laden: Security Strategy and the Global Commons', *Survival: Global Politics and Strategy*, 53:4, pp.19-25.
10 For an overview, see Louis Marinos and Andreas Sfakianakis (2013), *ENISA Threat Landscape*, January, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape (visited 10 January 2013). Ses also Thomas Rid and Peter McBurney (2012), 'Cyberweapons', *The RUSI Journal,* 157:1, pp.6-13; for an interesting perspective to the comprehensiveness nature of the term cybersecurity see Nazli Choucri, Gihan Daw Elbait, Stuart Madnik (2012), 'What is Cybersecurity: Explorations in Automated Knowledge Generation', MIT-Political Science Department, Working Paper 30.
11 This is strongly emphasized in NATO Strategic Concept 2012, which states 'Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.'

These malicious activities are often classified as cyber-attacks[12] or, perhaps more realistically, cyber-actions through which state and non-state organizations conduct information operations such as subversion, espionage and sabotage.[13] Due to the complexity of information infrastructures and the continuous introduction of new technologies, these operations can lead to the discovery of new entry points into enemy networks, damage specific IT systems through the use of malware, and steal classified or 'grey data' for private or state intelligence activities.

Different from cyberspace, space threats can be more identifiable but still potentially extremely damaging. This is primarily due to the higher technological point of entry required to perform malicious activities, as in the case of anti-satellite systems. Several states have demonstrated the technological, financial and political willingness to acquire control of satellites for maneuvering and approaching targets such as advanced ground-based laser systems, and interfering with satellite sensors or ground-based missiles used for destruction by direct impact or 'kinetic kill'.[14] However this restricted threat environment may only be a temporary condition. Over the next decade, an array of anti-satellite warfare capabilities, including space-based weapons, will likely emerge and become more easily available to a larger array of potentially malicious non-state actors.[15] This does not imply that current threats cannot lead to substantive risks. Malicious actors can undertake less sophisticated activities, such as jamming and spoofing, which are targeted against satellites themselves. More importantly, these activities are well within the current technological capability of the same actors who are also capable of carrying out cybercrimes or cyber-attacks, hence confirming the close inter-dependency between space and cyberspace.

---

12 The term cyberattack has also been debated in the international law literature. Recent examples are: See Scott J. Shackelford (2009), 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', *Berkeley Journal of International Law*, 29, pp.192–250, Matthew Waxman (2011), 'Cyberattacks and the Use of Force: Back to the Future of Article 2(4)', *Yale Journal of Internal Law*, 36, pp.421-58. A more comprehensive overview is provided by Michael N. Schmidt (ed.) (2013), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press).

13 There is growing academic literature that calls for a better assessment of the potential of a cyberwar and applies a Clausewitzian framework of analysis. See Adam Liff (2012), 'Cyberwar: A New Absolute Weapon?: The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies*, 35:1, pp.1-28 and Thomas Rid (2012), 'Cyber war will not take place', *Journal of Strategic Studies*, 35:1, pp.5-32. For a more operational criticism of cyberwarfare, see Martin Libicki (2012), 'Cyberspace Is Not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society*, 8, 2, pp.325-40.

14 For a layman description of potential space-targeted threats, see David Wright, Laura Grego, and Lisbeth Gronlund (2005), *The Physics of Space Security: A Reference Manual*, American Academy of Science, Section 11 and Section 12, pp.117-57.

15 William Lynn (2011), 'A Military Strategy for the New Space Environment', *The Washington Quarterly*, 34:3, pp.7-16. A historical perspective is provided in Laura Grego (2012), 'A History of Anti-Satellite Programs', Union of Concerned Scientists, January, in particular pp.13-4.

As technology continues to evolve and becomes even more accessible to a larger array of rogue states and non-state actors, the overall vulnerability and threat setting becomes even more complex. Therefore, it is evident that the most pressing policy question, which could also be a military and strategic perspective, refers to the need to maintain safe access to these two commons by protecting their capabilities to deliver positive network externalities and, at the same time, avoiding their securitization through restrictive measures.[16] Realizing this balance is a persistent challenge in international politics that calls for the capability to 'navigate the critical disconnects between the 'demand' for managing a global agenda and the supply of authoritative mechanisms'.[17]

COHERENT COOPERATION

Achieving this balance is more complex for two interrelated reasons. First, the private sector has a preponderant role in the overall service development, delivery and management of the two commons. In the case of space, states may find themselves in the future competing with the capacity needs of the private sector and therefore, confronting prospective scarcity and price hikes. In the case of cyberspace, access to technical or communication capacity is not an issue by itself. However, the core elements of its physical and IT infrastructures are in the hands of the private sector whose operating logic often differs from that of governments. The second reason refers to the fact that both commons, at different levels, have inadequate governance, insufficient norms and regulations, verification measures and limited mechanisms for enforcement. Since the 1960s an international space regulatory structure has evolved preventing its weaponization, and has promoted its use for peaceful purposes (for example through the work of the UN Committee on Peaceful Uses of Outer Space[18] and the UN Office of Outer Space Activities[19]). However, several elements of the extant regulatory infrastructure are now dated or lack institutionalization. In the case of cyberspace, the situation has increasingly become more chaotic with different

16 The notion of securitization builds upon Barry Buzan, Ole Waever and Jaap de Wilde (1998), *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Publishers). For a criticism of the application of securitization to space policy see Alison J. Williams (2010), 'Beyond the Sovereign Realm: The Geopolitics and Power Relations in and Outer Space', *Geopolitics*, 15:4, pp.785-93, Columba Peoples (2008), 'Assuming the Inevitable: Overcoming the Inevitability of Outspace Weaponisation and Conflict', *Contemporary Security Policy*, 29:3, pp.502-20 and (2011), 'The Securitisation of Outerspace: Challenges for Arms Control', *Contemporary Security Policy*, 32:1, pp.76-98.
17 Nazli Choucri (2012), *Cyberpolitics in International Relations*, (Boston: MIT Press) pp.10-2.
18 http://www.oosa.unvienna.org/oosa/COPUOS/copuos.html
19 http://www.oosa.unvienna.org/oosa/en/OOSA/index.html

regulatory and enforcement regimes competing or contrasting among themselves.[20]

These two factors should not prevent us from reflecting on a possible conceptual frameworks that respond to the coherence of addressing space and cyberspace's joint capabilities, especially if applied to a defense setting such as NATO.[21] Such a framework could provide the basis for advanced innovative system concepts assessing the strategic and military utility for combining new and emerging cyberspace and space approaches. This response could well start by providing the basis for managing previously indicated threats and vulnerabilities while preserving the asymmetric advantages provided by space and cyberspace.[22] This is particularly applicable in the case of outer space capabilities where NATO seems to have a tactical approach focused more on functional areas such as communications, intelligence and situational awareness. There is the need to go beyond this functionalist focus by moving towards the identification of existing and emerging challenges, threats and opportunities.[23] A similar functionalist approach seems to have been applied to the need to protect cyberspace by providing NATO with necessary instruments to defend against and deter cyberattacks.

The starting point of this response should be the need to safeguard the open nature of space and cyberspace commons as to protect their positive network externalities and, thus, support information awareness and superiority. There is the need to start to develop some form of intellectual and doctrinal leadership that may guide combined responses to space and cyberspace threats within a large military and strategic setting. Particular attention should be directed to elaborate concepts, strategies and operational frameworks aimed at preventing, deterring and countering 'hybrid' malicious activities against elements of the infrastructures supporting the two commons.

It is also necessary to develop a strong partnership with all stakeholders focused around principles of mutual benefit and mutual respect, as well as the

---

20 These complexities may also impact on possible deterrence mechanisms. For a perspective see Tim Stevens (2012), 'A Cyberwar of Ideas: Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33:1, pp.148-70.

21 This approach has also been recently suggested in Larry Martinez (2012), *Is There Space for the UN: Trends in Outer Space and Cyberspace Regime Evolution*, European Space Policy Institute (ESPI) Perspective n.56, January.

22 This approach also extends upon specific work exploring interaction between international relations and cybersecurity. See Cindy Williams (2011), Ap*plications of ECIR Modeling Work to Cyber Policy Problems*, ECIR Working Paper, March. http://ecir.mit.edu/images/stories/Williams%20cyber%20policy%20applications%20032311%202.pdf (visited on 21 December 2012).

23 One example of this functional approach is NATO RTO Space Science and Technology Advisory Group Recommendation for Space Research Topics, RTO Technical Memorandum TM-SPS-02, February 2007.

overall strategic goal to push for its operational capabilities and information awareness. The first priority would be to improve the sharing of critical information about current and future threats and vulnerabilities jointly affecting both commons. In cyberspace information sharing is already a strategic principle that has been implemented at the national, European and international levels through different mechanisms. In the context of space, information sharing operates primarily at the operational and technical level and involves intelligence activities and assessment of the security impact of emerging technologies as to ensure proper military planning. These interactions need to go beyond the mere exchange of threats and vulnerability data. They should develop into public-private partnerships bringing concerned actors around the table to examine the intricacies of a combined approach for the preservation of access to both commons, and for identifying prudent and cost-effective solutions to address the intricacies revealed by this joint perspective.[24] This will also facilitate the ability to rapidly assess emerging space and cyberspace technologies and their potential use by malicious actors and develop technological and operational solutions.

A joint approach would also take into strong consideration the human dimension of a combined space and cyberspace common. It is important to foster the development of strong human resources and capabilities through appropriate training and education capable of examining and assessing current and future threats targeted jointly against space and cyberspace. Currently, these two dimensions are addressed via two separate settings with limited interactions from an operational, doctrinal and strategic perspective. However, it would be of value to explore innovative ways to examine the interdependency of the two commons by conducting appropriate studies and analysis, as well as new war games and exercise planning experiences using scenarios that generate realistic outputs. These activities would also lead to advances in the operational and tactical use of privately owned infrastructural elements of space and cyberspace, as well as in assessments of risks, associated threats and vulnerabilities.

Finally, such a proposed response would also focus on the fostering an even stronger promotion of an active partnership with other organizations particularly with the European Union. The EU, in fact, considers both outer space and cyberspace as core multipliers for the overarching policy

24 The need for public/private partnerships for the protection of IT infrastructures has been a constant policy advice with different degrees and methodologies for its implementation. A recent contribution to the debate is Manuel Suter (2012), *PPPs in Security Policy: Opportunities and Limitations*, CSS Analysis in Security Policy, n.111, April.

objectives.[25] More importantly, they fall into the categories of critical infrastructures which, if disrupted or destroyed, would have a serious impact on the health, safety, security and socio-economic wellbeing of citizens or the overall functioning of national government institutions. Hence, the development of a large array of policy activities and initiatives for preserving the overall security of space elements and IT infrastructures and services. Such experiences and knowledge can be shaped into a legal and policy framework and shared through the most appropriate information sharing mechanisms and structures.

As argued at the beginning of this paper, space and cyberspace are the two commons upon which today's information society depend. They are also confronted with a continuously evolving set of vulnerabilities and threats that may undermine their access and capacity to deliver upon the expected functionalities. More importantly, space and cyberspace are increasingly interdependent. Hence the need, especially in a military context, to define policy responses against threats and vulnerabilities using a more coherent approach bringing together the knowledge and the experiences of all involved stakeholders into a comprehensive framework.

ABOUT THE AUTHOR

Dr Lorenzo Valeri has worked in the field of information security and IT technologies for many years, and since 2010 has been the Scientific Manager of the School of Government of Libera Università Internazionale degli Studi Sociali (LUISS). His research experience involves primarily the socio-economic and public policy implication of the growing pervasiveness of ICT, and international cooperation and development in university management and research.

25 For an overview of EU Space Policy, see Jana Robinson (2012), *Enabling Europe's Key Foreign Policy Objectives Via Space*, European Space Policy Institute, Report 30, February. For an overview of EU cybersecurity policy, see Directorate General for External Policies of the Union, European Parliament, (2012) *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, April.