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 Summary

Making the Connection: Building Stability in Cyber and Space

7 May 2013

In partnership with Finmeccanica UK and Istituto Affari Internazionali

The views expressed in this document are the sole responsibility of the author(s) and do not necessarily reflect the view of Chatham House, its staff, associates or Council. Chatham House is independent and owes no allegiance to any government or to any political body. It does not take institutional positions on policy issues. This document is issued on the understanding that if any extract is used, the author(s)/ speaker(s) and Chatham House should be credited, preferably with the date of the publication or details of the event. Where this document refers to or reports statements made by speakers at an event every effort has been made to provide a fair representation of their views and opinions, but the ultimate responsibility for accuracy lies with this document's author(s). The published text of speeches and presentations may differ from delivery.

INTRODUCTION

This is a summary of a workshop held at Chatham House on 7 May 2013. The second event of the Cyber and Space Series, the workshop brought together experts from the public and private sectors to examine the nexus between cyber security and outer space security. The workshop built upon the achievements of the first workshop (‘Making the Connection: The Future of Cyber and Space’) in identifying technological trends and developments, international policy development, and common vulnerabilities, dependencies, and differences.

The purpose of this workshop was to discuss how to build stability in the domains of space and cyberspace, and how to facilitate increased understanding and knowledge transfer between experts from the cyber and space security communities. Over the course of the workshop participants assessed the potential for and implications of conflict in cyber and space, and considered the rules, norms and values that govern current operations in these areas, and how they can be developed. Finally, discussion explored how to balance stability with security without limiting the commercial benefits and opportunities in both domains.

KEYNOTE ADDRESS

The keynote address opening the workshop provided an expert and substantive overview of the differences and commonalities of the domains of space and cyberspace and the existing regulations and proposed norms. The speaker noted that the core problems in both domains are unchanging; it is the politics that surround these domains that are evolving.

The speaker highlighted a number of differences between the two domains: the definition of the space domain is easily identifiable; cyberspace is not. Additional differences are the length of time each dimension has been utilized by states and identified in international agreements, the number of actors and problems of attribution, and the cost of entry.

A number of common issues within the space and cyberspace domains were identified including: cutting-edge technologies used in both sectors; the importance the domains have upon contemporary lives and economies; and the resultant vulnerability of public and private sectors upon the exploitation of space or cyberspace-based services. Another common issue is the growing awareness and high-level international discussion regarding the potential of armed conflict in both the space and cyber domains – termed the fourth and fifth dimensions of warfare. Uncertainty regarding what a conflict in these domains would look like, especially with regards to proportionate response or asymmetric dependencies, has led to the development of different models and codes of conduct to address the issues. Yet, interestingly, it is a similar group of states that holds controversial views within both domains. The final commonality is the challenge of identifying what constitutes a weapon in each domain, exacerbated by the use of dual-use technology, and the lack of verification mechanisms that pose a major challenge to traditional arms control.

The speaker suggested that transparency and confidence-building measures are particularly important, and that it should be considered to what extent existing law is applicable to these domains. Current international trends regarding space include a thematic discussion on the 'Prevention of an Arms Race in Outer Space' at the Conference on Disarmament, the draft treaty submitted by Russia and China in 2008, and the European Union's strong interest of a draft International Code of Conduct for Outer Space Activities. Within the cyber dimension, recent proposals are the draft resolution 'International Code of Conduct for Information Security' introduced by China, Russia, Tajikistan and Uzbekistan to the UN General Assembly in 2011, which contrasts greatly to the concept of cyber security in the recently published, 'Cyber Security Strategy' by the European Union.

The speaker argued that in the foreseeable future a serious conflict will not be confined to space or cyberspace but will necessarily have a kinetic aspect. However, actions and misperceptions in the cyber and space domain have the capability to effect international relations and stability and it is therefore important that they are understood and addressed in international security.

CONFLICT IN CYBER AND SPACE

The first session considered the threat and actualization of conflict in cyber and space. The session focused on the effect of states' interaction upon domain stability (including US-Chinese relations), existing and future processes to improve international dialogue, and current trends in action in cyberspace. The discussion was predicated upon the acknowledgment that the cyber and space domains are not isolated from the other domains, and that any conflict in these domains will take place within a wider political context.

The first speaker considered the current debate as to whether the United States should treat China as a competitor or partner in the space domain. There are two schools of thought regarding this issue, exacerbated by the dual-use technology utilised in both cyber and space domains. The isolationist approach advocates for the United States to not cooperate with China because of concerns of space technology transfer and as a matter of political principle. However, it was argued that space is inherently international due to the nature of the threats (e.g. space debris, situational awareness and planetary defence) and thus these challenges require international cooperation.

China's increasing responsibility as a stakeholder in space is a net benefit, the speaker argued. The risk of China acting to the detriment of other space stakeholders (e.g. China's ASAT test in January 2007 in comparison to the United States' low-altitude missile test in February 2008) would be reduced, and overall space stability increased because of the interconnected nature of space and space-based issues. To have China as a recognized and responsible member of the international space community will require a number of steps to be taken to improve US-Chinese relations. Increased dialogue is a key issue, and progress could be made here between space agencies. For example, NASA is currently legislatively prohibited from working with China in any way. Benefit could also come from greater data exchange and a space programme upon which the United States and China can collaborate (suggested topics were space science and human space flight). In broader terms, greater transparency and confidence-building measures, a formal code of conduct, and legal framework could improve US-Chinese relations and international space security.

One speaker elaborated upon Multi-National Experiment 7 (MNE7) – an 18-to-20-state series of collaborative workshops with participation coming primarily from national defence organizations, whose aim was to address international security issues. One purpose of MNE7 was to develop concepts to maintain freedom of access and action in the 'global commons', and to consider the interrelationships between space and cyberspace. Within the space domain, discussion in MNE7 raised awareness regarding space dependencies and vulnerabilities, and actions related to influence and mitigation. In the cyber domain, the group discussed vulnerabilities and risks, information-sharing, legal frameworks, technologies and situational awareness. Due to the increasing dependency upon and the permeation of cyber and space in international functions, greater understanding requires greater international and cross-sector communication – such as through the information-sharing framework of MNE7.

Discussions highlighted the increasing contrast between state-based and private sector driven communication and dialogue on cyber and space issues. State-based approaches were viewed as encumbered by national bureaucratic policies and isolationist views, though there has been an increasing multilateral shift in China’s perspective in space and cyber to a more pragmatic approach. Although there is evidence of US-Chinese cooperation at a tactical level in cyberspace (such as the information sharing between US and Chinese Computer Emergency Readiness Teams – CERT), and potential involvement at the international level, the majority of communications have been instigated through private sector actions. A view was expressed that the momentum developed in MNE7 could be retained in its existing framework to further contribute towards increasing state-based multilateral communication.

When focusing upon the conflict in cyber and space, one speaker introduced the threat of GPS jamming. Funded by the UK government’s Technology Strategy Board and involving a number of public- and private-sector organizations, the aim of the SENTINEL and GUARDIAN Projects was to establish the extent to which GPS interference and jamming is a serious threat. Jammers are easily accessible online and can be used by civil actors, criminals, terrorists and states – for example the use of jamming by North Korea that affected aircraft navigation systems at Incheon International Airport in Seoul disrupted a joint US-South Korean military exercise and impacted the mobile phone network in Seoul. It was noted that the ease of accessibility and use of jammers is a serious concern for operators of critical national infrastructure such as airports, harbours and utilities, as well as financial institutions and other GPS-dependent services.

Consensus in the discussion was that current actions in cyber and space are identified more as industrial espionage rather than direct military threats. It was suggested that traditional arms control mechanisms will not work within these domains – the prevailing impression was that an actor’s aims can be achieved without entering into a military action due to the autonomy supplied by cyberspace. Thus focus should be upon mitigating rather than constraining these threats and increasing transparency not security. An additional hindrance towards military action in these domains is the interconnection between services and assets in space and cyberspace, which increases the risk of unintended consequences. However, it was mentioned that the targeted actor's response would likely determine whether the conflict escalates into kinetic military action.

Finally, a participant raised the concern that emerging countries are likely to be more dependent upon the cyber and space domains than existing developed countries. These states would not have the same extent of cyber and space threat mitigation and resiliency inherent in the existing legacy infrastructure possessed by developed countries. It was agreed that this is a concern which needs further consideration.

RULES AND NORMS IN CYBER AND SPACE

The second session addressed the themes of norms and rules in space and cyberspace. The debate focused upon whether the existing international norms and legal frameworks can be adapted or whether new rules and norms need to be created for the cyber and space domains. It was understood that how these two diverging geopolitical views are resolved will impact the future progress and process in cyber and space domains. The discussion primarily focused upon the United Kingdom, Japan and Russia's policies and approaches towards the cyber and space domains.

United Kingdom

From the perspective of the UK representative, there is a missing piece at the multilateral level regarding existing space legal regimes. Similar to the US stance, as laid out in the US National Security Space Strategy 2011, the United Kingdom's's view of space is that it is increasingly crowded, congested, contested and competitive. The number of space objects and actors are increasing rapidly; the risks they pose are also growing at an exponential rate – as demonstrated by the Iridium-Cosmos collision in 2009 and multiple 'evacuations' of the International Space Station in 2012. Emerging and established space powers are becoming increasingly economically and militarily dependent upon space-based capabilities and services, yet paradoxically, due to dual-use technology used within the space domain, there has been no legally binding measure opened for signature since 1979.

Norms-based 'soft-law' such as the Space Debris Mitigation Guidelines 2007 has in part complemented and built upon existing legal frameworks by raising the political cost of irresponsible behaviour. However, the speaker argued that there is a need for an overarching normative framework to complement the Outer Space Treaty – suggesting the International Code of Conduct for Outer Space Activities to fulfil this role. Through the realization of the non-discriminatory nature of risks such as space debris, and recognition of the common means and normative measures which can be utilized, the speaker noted that it is in the United Kingdom's best interest to support the International Code of Conduct and engage in multilateral efforts to ensure that space is not seen as a domain for potential conflict and tension.

Japan

The speaker highlighted a number of key policies such as free access to outer space, and within cyberspace the assurance of openness, interoperability and application of international law (including human rights and humanitarian law). It was noted that practical rules to cope with imminent challenges in the two domains should be adopted at the earliest possible opportunity, however it was mentioned that although rule-making in the UN is widely viewed as legitimate, it is very difficult to achieve. Therefore an alternative approach, such as developing norms outside the UN and subsequently expanding the number of supporting countries, would be pragmatic. The speaker mentioned that global strategies among like-minded states are necessary, and that it is important to develop capacity-building measures for emerging countries to include them as fellow stakeholders.

Discussants remarked that the existing norms and rules in space and cyberspace have worrying gaps that do not adequately address space collision, debris and asset disposal, or the regulation of cyber attacks and espionage. Additionally, there is a lack of formal mechanisms to enable transparency and build confidence in the cyber and space domains. Thus, the speaker noted that to achieve these aims, further development of the existing rules and norms for space and cyberspace is necessary to address all current concerns.

One participant remarked that two distinct approaches towards the cyber and space domains have become evident in international discussions, based on one group comprised of Russia, China, Tajikistan and Uzbekistan and another group including the United States, Japan, the EU and Australia. The different approaches towards improving existing norms and rules applicable to current operations in cyber and space were categorized into three major challenges by the speaker. These challenges are (1) the differing opinions regarding the use of the domains, (2) the form and process of rule-making and (3) the entry of new actors into strategic aspects of the two domains.

There are some current attempts to establish norms and mechanisms such as the International Code of Conduct on Outer Space Activities (supported by Japan), discussions in the UN First Committee's Group of Governmental Experts as well as other regional forums, and through bilateral mechanisms. However, it was noted that there are 'gaps' within current and proposed norms. For example norms on cyberspace do not consider 'unrecoverability' [sic] of damages to space assets, and the International Code of Conduct fails to address cyber attacks on space assets or ground facilities relating to space assets that do not cause kinetic damage. It has only been in 2013 that Japan has constitutionally permitted the government to utilize space for security purposes. The Japanese Ministry of Defense intend to launch its own satellites, thus there is particular impetuous to consider counter-measures against cyber attacks on space-based assets.

Russia

The discussion turned to the Russian approach to establishing international norms and rules in cyberspace. In addition to the fundamental challenges of attribution and identifying whether it is the responsibility of the state or citizen for actions that constitute cyber conflict, the speaker identified two key challenges from the Russian perspective.

The first challenge is regarding the two diverging understandings of cyberspace. One group identifies cyberspace as a global domain within the interdependent information technology network and infrastructure. However, Russia's understanding of the information space contains the additional dimension of the information itself and its effect and influence on individual and social consciousness. The speaker noted that this fundamental difference in perspective inhibits the formation of an internationally agreed classification framework of cyber threats, provokes serious disagreement on the international level, and creates challenges in cooperation regarding international norms.

The second difference of opinion is whether to adapt existing rules or create new rules for cyberspace. The main states that advocate new regulatory mechanisms are Russia, Tajikistan, Uzbekistan and China. The speaker argued that existing law is too specific to apply to the cyber dimension. He noted that while there are some recent proposals for new norms and legal frameworks, they are either politically unfeasible, or the value of the rules and agreements are undermined by the lack of comprehensive verification and compliance mechanisms. Discussants pointed out that this particular opinion is also applicable to the Russian view of international norms and regulations regarding outer space.

WAYS FORWARD: BALANCING STABILITY WITH OPPORTUNITY IN CYBER AND SPACE

The final session explored the challenge of balancing enhanced stability and security in space and cyberspace without unduly impacting potential commercial opportunities. The discussion covered public- and private-sector opinions, and explored what the next steps could be to establishing a sustainable approach in these domains.

One speaker discussed industry awareness of public and private sector dependence upon space and digital services. The evolution of technological development and user requirements has resulted in multiple generations of satellites, many of which are still in use. In conjunction with these developments, security of these services has also increased through processes such as hardening the communication network by sectioned encryption as well as developing operational procedures. Resilience has been developed through overlapping compatibility as well as operational backup.

It was noted that the success of a commercial company depends upon its reputation for delivering top quality of services to end-users. Many companies operate a rolling development in order to stay on the cutting edge of technology and security – accompanying these developments are also vulnerabilities. Security is therefore very important; however there is often divergence of opinions within companies themselves of how to implement the security measures without negatively impacting commercial opportunities.

The final speaker advocated the integration of satellites into existing terrestrial systems to improve national security and resilience. This could enhance communications systems, situational awareness, and satellite position and timing utilized for critical system infrastructure operations. The speaker recommended that these systems would need to be constantly used (ideally commercially) in order have the maximum value, and government procurement systems should be attuned to this long-term benefit.

Classifying existing cyber and space security threats within a broad spectrum of Commercial, National, and Global, the speaker suggested that the best way to enhance security and stability without limiting commercial benefits and opportunities would be to avoid the traditional approaches, which have had limited effect. The suggestion was to adopt a collaborative multinational approach with emphasis on pace and agility.

It was noted that there is a fine balance between opportunity and stability regarding standards and governments. Policy enforcement is required at both a national and global levels to address commercial infrastructure – however regulation is only beneficial when it creates a framework in which innovation can take place, not when it stifles growth.

A specific concern in the discussion was regarding the relation between states and commercial service providers. Much of the space industry is intrinsically tied to governments, and vice versa with 80 per cent of US military traffic utilizing commercial satellites. However there is also concern from a commercial perspective of appearing to be open to specific state interests (such as halting the provision of their service in a specific area) to the detriment of the company's commercial aspects in other countries. This concern was effectively demonstrated in the US Air Force Space Command Schriever V Wargame, 2009 – the first inclusion of the commercial space sector within the Schriever Wargame series, which focused upon the use of space and cyber in a future conflict – where industry contested shutting down a global service.

Further information

The International Security Research Department thanks Emma Skye MacLeod (MScEcon Strategic Studies, Aberystwyth University) for compiling this summary.

If you have any questions about this event, please contact Dave Clemente at dclemente@chathamhouse.org

More information about the work of the International Security Research Department can be found at www.chathamhouse.org/research/security