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 Workshop Summary

Making the Connection: The Future of Cyber and Space

24 January 2013

Chatham House in partnership with Finmeccanica UK
and Istituto Affari Internazionali

INTRODUCTION

This is a summary of a workshop held at Chatham House on 24 January 2013. The workshop brought together experts from both the cyber and space security communities in an effort to explore connections between the two areas. The purpose was to identify commonalities as well as differences to increase mutual understanding and facilitate a knowledge transfer between the two fields. Lessons learned also served as a platform to create a coherent, joint approach towards space and cyber security. To that end, the discussion explored trends and developments in both areas and identified possible connections through vulnerabilities and dependencies. Lastly, the workshop examined different policy approaches in order to identify the potential for international regulatory mechanisms and processes.

Keynote Address

The keynote address opening the workshop laid out the rationale and necessity for a combined, joint approach to cyber and space security from strategic as well as policy perspectives. These perspectives were based on an analysis of the specific nature of space and cyberspace as well as the threats and vulnerabilities common to both.

Traditionally, access to land, air, sea, space – and now cyberspace – has been pivotal for military superiority as well as national and international stability. The past few years have seen a growing role for space and cyberspace as both domains have become more central to the infrastructure of today's modern societies. Growing dependencies on these two domains, however, result in increased risks, systematic as well as operational. As systems become more integrated, the number of vulnerabilities grows. The keynote speaker pointed out that the constantly evolving threat environment in cyberspace is of particular concern due to the increased access of individuals and groups to disruptive technology.

Possible threats include major cyber attacks, although it remains unclear whether such attacks could be characterized as an armed attack under international law. A more likely possibility appears to be activities such as espionage, sabotage and subversion executed through cyber means. In the context of space security, relevant threats have been subject to academic debate for some years. Possible threats include anti-satellite weapons (ASAT), interference with satellite manoeuvring, jamming as well as spoofing.

Given the evolving threat environment, the keynote speaker subsequently addressed the question of how the international community should respond to these challenges facing both spaces. Any response should take into account the significance of preserving open access to the commons. Both cyberspace and space become more valuable if more people join or use it. Therefore, a policy response should strive to find a balance between the demand for global access and the need for authoritative mechanisms.

A good starting point is information sharing, a mechanism that has received particular attention in the cyberspace context. Information sharing on threats and vulnerabilities should ultimately develop into public-private partnerships preserving access to the commons and managing any risks arising out of it. Any policy approach should strongly consider the human factor as all technical elements and systems are managed by humans. Lastly, existing institutional partnerships should be expanded starting with a collaborative effort between the European Union and the North Atlantic Treaty Organization. Overall, the keynote speaker argued that, although combining both space and cyber security represents relatively uncharted territory, a joint conceptual approach in response to the challenges described would prove valuable.

Trends and Developments in Cyber and Space

The first session opened with an overview and discussion of major trends and developments in cyberspace and space. While the discussion focused on technology and its evolution, the complex task of international norm setting in these two areas was likewise addressed by the participants.

One of the speakers noted that the increasing interdependence and interconnectedness between space and cyberspace comprises an important development affecting both fields. On the one hand, space components, (including satellites and base stations) have become an integral part of cyberspace. An unprecedented quantity of data is being generated and transmitted by satellites on a daily basis with an accompanying rise in space-enabled services. This trend has been recognized by countries, and the number of states with satellite design and launch capabilities has increased steadily. As a result, competition for orbit slots and access to a finite range of transmission frequencies has increased.

It was argued that these circumstances will either drive the need for further international collaboration in the space field or fuel an environment of mistrust. On a political level, a speaker pointed out that existing regulatory frameworks appear insufficient as new entrants to the space arena challenge norms initially established by the initial space-capable countries. The current space security regime can therefore be characterized by a lack of consensus. Furthermore, military doctrine has placed an increasing emphasis on space in terms of national security policy. On a technical level, new solutions have evolved to manage greater frequency usage and to allow satellites to operate in closer proximity.

Both speakers and discussants acknowledged the increased interdependence between both spaces. It was explained that these inter- and cross-dependencies also create new vulnerabilities, particularly as the majority of space assets have become dependent upon cyber networks. While older satellites are more prone to interference such as jamming, newer satellites are equipped with on-board computers allowing for remote reconfigurations or upgrades. This renders them vulnerable to cyber attacks. Other likely targets for cyber attacks are also ground stations as well as the communication links to and from satellites. With over 2,000 active satellites in space, a review of space assets and their vulnerability to cyber attack should therefore be undertaken. While military assets are relatively well protected, civil assets appear to be more vulnerable. However, the military is increasingly dependent upon commercial space applications. This connection offers opportunities to use cyber warfare as a means to impact critical national infrastructure in space with low traceability.

A portion of the discussion focused on trends and developments predominantly affecting outer space. One of the speakers used the three ‘Cs’ – congested, contested, and competition – to characterize trends in outer space. As space has become an engine for economic growth worldwide, space has become congested: the number of available frequency bands is limited. Space has also become more contested illustrated by China’s test of a ASAT. Lastly, space has become characterized by competition for access slots. The policy response has revolved around three ‘S’s: safety, security and sustainability. These have been pursued through various governance forums such as the UN Committee on Peaceful Uses of Outer Space, the Conference on Disarmament and the International Telecommunication Union (ITU). Regulatory frameworks include the Outer Space Treaty and agreements on rescue, liability as well as registration.

Governance questions were identified as an important, yet challenging aspect of developments in outer space. One speaker pointed to the work of a UN Group of Governmental Experts that is currently looking at possible transparency and confidence building measures (including treaties, codes of conduct, inspections, and workshops). However, in light of the diversity of the group, which includes, among others, Russia, China and Brazil, a tiered approach to space security seems most feasible. In order to build consensus in the international community irresponsible behaviour in outer space should first be identified. Norms of behaviour proscribing such actions could then be internationalized through alliances and international partnerships.

It was emphasized that governance initiatives are complicated by the fact that space capabilities are being spread among an increasing group of states with different beliefs and values. This diversity naturally complicates consensus building. In addition, new entrants to this group of states perceive regulatory requirement as barriers for their development rather than as regulatory necessities. One participant proposed that a possible solution to overcome these political obstacles could be to seek consensus in scientific bodies first before taking the discussion to international political bodies.

With regard to short-term solutions addressing the increasingly congested, contested and competed environment of outer space, one of the speakers introduced possible tracking and categorizing methods. Accordingly, objects in outer space can be tracked and categorized according to risk factors. Yet problems arise with regard to objects which are between the size of 1cm and 10cm as they cannot be traced from ground-based radar/sensors. Therefore, mitigation techniques need to be supplemented by other measures including technological solutions. These should form part of an overarching effort to achieve safety, security and sustainability in outer space. The challenges of congestion, contest, and competition need to be met in order to guarantee a stable space environment.

Discussion turned towards a second trend affecting both cyber security and space security, namely the increased use of space systems for global connectivity. Telecommunication networks in space, particularly satcom services, remain to be the most profitable services. Unlike 20 years ago, 80 per cent of military satellite communication travels through commercially operated systems. Ever-increasing data volumes and rates drive the global demand for broadband and increased use of higher frequencies. For instance, frequency bands, such as the Ka-Band are suitable for both civilian and military communications.

This trend, however, results in larger and more open satcom architecture built to accommodate different types of platforms. As such, these parts of the telecommunication network become more probable targets. In addition, several factors have driven the development of largely automatized, distributed and collaborative space structures. These trends have put space systems at the heart of the information chain whether in terms of data collection and transmission, or in terms of information dissemination. The results of this trend, particularly the importance of potential vulnerabilities in terms of critical national infrastructure protection, were discussed among participants.

Lastly, one speaker pointed out that vulnerabilities can be related to hazards as well as hostile acts. Assessing the nature of an incident, however, represents a difficult task as it requires a thorough understanding of the incident and the intent behind it. Even understanding the incident in physical terms is a complex undertaking. As an example, jamming of satellite communications has sharply increased over the last few years. However, in order to geolocate the perpetrator at least two satellites are needed. Discussants agreed that overall vulnerabilities of satellites to cyber attacks are not well understood. One participant pointed out that the alleged cyber attack on the ROSAT satellite, for example, has not been widely discussed. As a result, challenges associated with the understanding and attribution of incidents involving space systems should not be underestimated.

Vulnerabilities and Dependencies

The second session addressed aspects arising out of the dependencies and vulnerabilities present in space and cyberspace. Cyberspace has become a key enabler for states, driving socio-economic activities for most of the world. Similarly, space systems have become increasingly important for growing communication demands as well as newer applications such as disaster monitoring and management.

One presentation contrasted the different levels of awareness regarding threats and vulnerabilities in cyberspace and space. Although countries have become dependent on services that originate from cyberspace as well as space, cyber vulnerabilities have received widespread public attention in the last few years. The same cannot be said about the space arena despite its 50-year history. The space arena has operated for decades free from attacks or disturbances despite existing vulnerabilities. This was partly the product of international cooperation forging norms of behaviour such as the 1967 Outer

Space Treaty. One hundred states are party to the treaty, which creates key parameters for the use of this global commons.

In addition, bilateral agreements were concluded between the United States and the Soviet Union as well as a tacit moratorium on the use of ASATs. These efforts have stabilized relations in outer space and minimized any residual fears of outer space weapons. With the increased use of space, the threat caused by debris has emerged as a concern in the international community. However, any cooperative remediation efforts dealing with debris have been disrupted by China's ASAT test in January 2007. Coupled with the destruction of a re-entering US satellite, these developments have led to renewed concerns over the militarization of outer space.

In contrast, vulnerabilities in cyberspace have received far more attention as user numbers have grown at a phenomenal pace. The internet is characterized by its openness and ease of access. As such, security concerns have not been an integral part in its development. Vulnerabilities can be identified, for example in the uplinks and downlinks of space objects. With an increasing number of states developing offensive cyber attack capabilities, the speaker argued that the militarization of cyberspace runs the risk of becoming a self-fulfilling prophecy. Although the threat of militarization can be characterized as more of a distant threat, the absence of international governance frameworks might facilitate developments in this direction. However, one of the participants pointed out that international frameworks are already in place. Arguably, the more important question revolves around their application in specific contexts.

In response to these concerns relating both to outer space and cyberspace, one speaker argued that preventive diplomacy could serve as a vehicle to forestall potential future conflict. Cooperation and restraint in cyberspace and outer space will be critical because conflict in these arenas would deny all users the benefits of these spaces. A possible way forward would be to build on the special status of the global commons. This status is enshrined in the Outer Space Treaty. Translating this concept into cyberspace might prove challenging as it is ultimately a human creation with identifiable physical infrastructure. But the general features of both spaces seem somewhat comparable. Therefore, one of the speakers asserted that cooperative efforts might be facilitated by labelling cyberspace a global commons. During the discussion of this argument, participants raised another aspect related to the potential for cooperative efforts, namely the increased number of stakeholders in both cyberspace and outer space. This circumstance might

help foster cooperative behaviour as more states stand to lose than gain from unstable relations in the two spaces.

The session also focused on specific vulnerabilities and threats to space assets, and one of the speakers introduced the specific threat of GPS jamming, which is the topic of a UK-funded research and development project called SENTINEL. The purpose of the project is to quantify the threat arising out of potential interference and jamming of GPS signals. More specifically, it concerns interference with the signal downlink from satellites as well as deliberate jamming of this signal. These effects can be caused by various phenomena such as space weather or poor workmanship. However, interference and jamming can also be used by individuals, for example to evade GPS-tracked car insurance. It can also be deliberately used by states as illustrated by the jamming activities of North Korea against South Korea.

One discussant pointed out that in addition to existing traditional physical threats to ground stations, new vulnerabilities and threats to space assets are created by the increased link between space and cyberspace. The sheer scale of data gathered, processed and transmitted by satellites on a daily basis offers great vulnerabilities to be exploited by a cyber attack. Furthermore, the increased number of states active in outer space coupled with the reduction of costs has led to an unprecedented scale of activity in this domain. As dependencies on space-based assets and services grow, so does the disruptive potential of threats. In response to the dangers posed by debris and unintentional collisions, the European Space Agency has initiated the 'Space Situational Awareness' programme designed to identify and track objects and natural phenomena that could harm satellites. The programme covers active and inactive satellites, space debris, as well as space weather and near-earth objects.

In comparing vulnerabilities in cyberspace and outer space, discussed turned to the different levels of risk management in both spaces. Whereas considerations with regard to risk management have been an integral part of space policy for some time, the same cannot be said with regard to policy in cyberspace. As a consequence, comprehensive risk assessments and management strategies need to be devised to cope with threats in cyberspace before a major incident occurs. This effort is complicated by the lack of awareness and information on incidents. Targeted industries such as finance are reluctant to publicize numbers on incidents, which hampers an accurate threat assessment necessary for ascertaining and managing risks.

POLICY DEVELOPMENTS

The last session of the workshop discussed different national and regional policy approaches. Underpinning the discussion was the recognition that although cyberspace and space present new challenges, these policy areas do not operate in a policy vacuum. Existing laws and governance frameworks should be taken into account when designing new strategies and policies in this field.

The European Union

With regard to the European Union's policy in the area of cyberspace it was noted that overall it relies on the resilience of its member states. The EU's approach to cyberspace is fragmented within its pillar structure. Cyber crime issues, for example, are under the purview of the Directorates-General for Home Affairs (DG Home) and for Justice (DG Justice). Other departments involved include the Directorate General for Communications Networks, Content and Technology (DG Connect), the European Defence Agency and the European Union External Action Service. Past policy initiatives include efforts to harmonize the prosecution of cyber criminals (under the direction of DG Home and DG Justice).

More importantly, the European Commission is currently proposing a new Cyber Security Strategy to be adopted alongside a new EU directive. The strategy is supposed to bring the different policy areas of the EU together in one policy document. It outlines, *inter alia*, the position of the European Union supporting the current multi-stakeholder model for internet governance, as well as the application of existing legal frameworks to cyberspace. This position is to be stressed internationally where a stark contrast has evolved between liberal democracies and authoritarian regimes. In terms of domestic efforts the strategy calls for research and development investments, increased efforts to fight cyber crime and build up resilience, as well as the creation of synergies between different institutions.

The United Kingdom

From the perspective of the UK representative, there are a number of emerging threats arising out of the increasingly close connection between cyberspace and outer space. It was argued that a broad notion of cyberspace vulnerabilities also includes vulnerabilities of space assets as these form part of the global telecommunications network underpinning cyberspace.

However, in terms of policy, commonalities as well as differences exist in the approaches towards both spaces. For example, access is a key difference. Cyberspace has a very low access threshold while space retains relatively high entry barriers. Another difference is attribution, which seems to be somewhat less challenging in space than in cyberspace. Yet this may change in the future in light of novel and emerging space capabilities. More importantly, norms and confidence building measures in both fields represent very challenging policy aspects. As the speaker pointed out, views in the international community as to the significance and meaning of cyberspace diverge widely. The term information security would be defined in quite different ways by the United States, the United Kingdom, Russia, China or Saudi Arabia for instance.

Similarly, it was noted that views diverge with regard to the necessity of new legislation for outer space supplementing the current framework of the Outer Space Treaty. The United Kingdom would favour movement towards norm setting in these areas. Yet arriving at a consensus internationally will be a long process. In terms of domestic initiatives, new impetus at ministerial level has been given to space policy aspects that had been formulated in the National Space Security Policy. However, this process which, among other things, seeks to link up the space community with relevant government actors and industry is still in its early stages. Irrespectively, space will become increasingly critical for defence. A challenging aspect for government policy lies in the fact that both space and cyberspace, as topics, cut across various governmental ministries. They are also being perceived as very technical subjects.

The United States

The discussion turned to the policy approach of the United States regarding cyberspace and space. This approach has been characterized by an early acknowledgment of the substantial overlap between the policy areas. However, in recent years there has been a process of disaggregation in the current administration in an effort to conceptually separate the two domains. Nonetheless, the two issues are coordinated on a daily basis within the executive branch of the US government. Outer space policy issues are fairly well understood as they have traditionally been viewed through the national security lens.

Though debates in this area have traditionally been focused solely on US policy, interest in engaging more fully with the international community is

slowly growing. However, the United States does not call for a change of international mechanisms regulating outer space. The current regulatory frameworks are seen as sufficient although the United States is committed to the idea of a code of conduct as proposed by the European Union. The overarching goal underpinning this policy is to maintain navigation in space and to protect US space assets effectively. In contrast, cyberspace is not exclusively addressed through the national security perspective but represents a rather broad issue encompassing different considerations such as commerce, privacy, or law enforcement.

With regard to international regulations, the speaker addressed the increasingly dissatisfied stance of the United States with regard to regulatory efforts made through the ITU. The United States sees no need for a new treaty but prefers regional or bilateral solutions. The policy goal is to ensure internet freedom while guaranteeing certain standards of data protection.

India

Lastly, India's policy approach was presented, noting out that India considers security aspects related to both spaces as future threats. Particularly India's understanding of cyberspace is in the early stages. The speaker asserted that the area of space security offers a limited number of regulatory mechanisms and global governance regimes to consider. In contrast, cyberspace is characterized by a lack of clarity in terms of its institutional and legal architecture. Consequently, there is a need to define the boundaries of permissible behaviour in cyberspace.

Throughout the workshop, two views emerged in the debate. On the one hand, Western countries, in particular the United States, have placed great emphasis on the free flow of information in cyberspace. On the other hand, China, Russia and a number of developing countries, view the use of social media and other information-sharing platforms as a threat to their national security because of its potential to incite social tensions or unrest. In addition, broader issues in the cyber security field include fraud, privacy intrusions, espionage and sabotage. Given these diverse topics and view points, the speaker argued that it becomes imperative to find the right balance between internet freedom and cyber warfare. Finding this balance is a challenging but essential step towards a safe and secure cyberspace.

India's position within this discourse is influenced by the fast spread of military space capabilities in Asia fuelling rivalry and mistrust in the region. A second factor is the proliferation of small satellites accompanied by an increased

number of active state and non-state actors in this field. Cyber-enabled space threats are also a major concern. Although India's official position has been based on the non-weaponization of space, the Chinese ASAT test of 2007 has somewhat triggered a debate on this stance.

The speaker noted that India's position with regard to cyberspace has been driven by two aspects: national security and the concern for social cohesion. In terms of national security, ensuring deterrence is seen as a key aspect for both space and cyber security. To that end, clear boundaries of acceptable behaviour need to be elucidated. However, establishing those boundaries is going to be far more challenging in the cyber domain due to difficulties with attribution. Therefore, international efforts at building consensus in this area should begin with the least common denominator – norms of responsible behaviour or transparency and confidence building measures. The challenges associated with building international governance mechanisms were acknowledged, and one discussant argued that in order to succeed, any broad framework will have to address the shifting balance of power and take the concerns of Asian countries into account.

Further information

The International Security Research Department thanks Elaine Korzak (PhD candidate, King's College London) for compiling this workshop summary.

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