Research Paper

Caroline Baylon

International Security | December 2014

Challenges at the Intersection of Cyber Security and Space Security

Country and International Institution Perspectives

CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

Part I: Country Perspectives

Part II: Perspectives from International Institutions

Summary

This research paper is part of Chatham House's Project on Cyber Security and Space Security, a multi-year research project within the International Security Department examining the security challenges at the intersection of cyber security and space security. The paper aims to identify and raise awareness of the challenges common to both domains through a compilation of articles by cyber security experts and space security experts that assess each field and consider the linkages between the two.

Part I is made up of a series of country studies in which experts from eight countries (China, France, India, Italy, Japan, Russia, the United Kingdom and the United States), drawn from think tanks, academia and industry, set out their views on their country's cyber security and space security policies. Part II presents international institution perspectives, with contributors from three major bodies (the European Union, the Organisation for Economic Cooperation and Development and the UN) providing high-level assessments of challenges at the intersection of cyber security and space security.

Among the major security challenges described in the papers that are common to both the cyber and space domains – and all linked to a growing militarization in both sectors – are:

- **An 'escalatory cycle' of militarization in the cyber and space fields, prompted by the increasing militarization of a small number of states:** The militarization of both the cyber and space sectors appears in part attributable to a small number of states' increasingly militarized actions in these (and other) domains. Other states, responding to a 'perceived threat', are thus more likely to ramp up the military aspects of their own cyber and space programmes. This, in turn, prompts an even greater number of states to militarize.

- **Lack or inadequacy of national policy documents in the cyber and space realms:** The lack or inadequacy of national policy documents in the cyber and space spheres creates opacity concerning state objectives, which in turn fosters 'ambiguity of intent' surrounding state actions and renders states more likely to construe other states' actions as offensive. The absence of such documents also hinders dialogue, reducing prospects for international cooperation.

- **Lack or insufficiency of internationally agreed definitions of key terminology in the cyber and space domains:** Given that robust definitions are fundamental to the establishment of enduring treaties, the lack or insufficiency of internationally agreed definitions of key cyber security and space security terminology impedes the development of multilateral arms control agreements. It also hinders international cooperation.

- **A blurring line between 'non-military' and 'military' roles in the cyber and space sectors – including a rise in dual-use technologies:** The distinction between 'non-military' and 'military' roles is increasingly blurred in the cyber and space arenas, with many technologies being dual-use. This makes it more difficult to define key terminology (especially that involving warfare), contributing to the lack or inadequacy of internationally agreed definitions. Dual-use technologies also mean that banning certain technologies outright and implementing adequate measures to verify compliance are often unfeasible, leading to difficulties in reaching multilateral arms control agreements. Furthermore, dual-use technologies make it more difficult to ascertain whether a country is developing a military programme in addition to its civilian activities.

- **A blurring line between ‘offensive’ and ‘defensive’ actions in the cyber and space fields – or a shifting line to permit increasingly ‘offensive’ activities under the justification of ‘defensive’ activities:** The norms of acceptable behaviour in cyber and space are shifting towards the ‘offensive’ end of the spectrum, permitting increasingly offensive activities under the guise of ‘defensive’ ones.
- **Asymmetric threats in the cyber and space domains – i.e. ‘offence is easier and cheaper than defence’:** The cyber and space fields both face asymmetric threats. This contributes to the increasingly blurred line between ‘offensive’ and ‘defensive’ activities in cyber and space. Technologically, offence is easier and more cost-effective than defence. Geopolitically, the consequence is that highly advanced countries are particularly vulnerable to attack from less developed states (as well as from terrorist groups and other actors).

Devising a flowchart

In identifying and analysing some of the common challenges in the cyber and space domains, the submissions to this paper point to the existence of an escalatory cycle of militarization in both domains, apparently driven by a set of common factors. The paper examines the interactions of these factors, and presents a flowchart that depicts how they relate to one another and to the escalatory cycle.

Preface

Dr Patricia Lewis, Caroline Baylon

This research paper is part of Chatham House's Project on Cyber Security and Space Security, a multi-year research project within the International Security Department that is focused on examining the security challenges at the intersection of cyber security and space security. Launched in 2013, the research project has three principal objectives:

Objective 1: Identifying and analysing the challenges common to both the cyber security and space security domains. The cyberspace and outer space domains have a number of security challenges in common. For example, both are undergoing growing militarization; both are mired in some measure of deadlock regarding the potential for international treaties; and both are susceptible to asymmetric threats. The research project aims to identify and analyse these shared challenges, developing a greater understanding of their complex interrelationships. Its objectives also include suggesting and evaluating potential solutions that might be applicable to both domains.

Objective 2: Identifying and analysing cyber threats to satellites and other space assets. The cyber and space sectors are growing progressively interconnected and interdependent. The research project aims to identify and analyse the cyber threats to satellites and other space assets. Satellites, ground stations and other space assets rely increasingly on the internet and other cyber networks for their functions, which renders them vulnerable to cyber attack. For example, hackers could use internet-enabled remote configuration features to take control of a space system, resulting in anomalous behaviour or even catastrophic failure of a satellite. Conversely, the internet and other internet-enabled critical infrastructure rely increasingly on satellites and other space assets for information and other operations, making them more attractive targets for cyber attack. For example, hackers might intercept data or disrupt internet communications from telecommunications satellites, or else jam and spoof signals from GPS satellites, taking down mobile phone networks, the power grid or other critical infrastructure dependent on them.

Objective 3: Promoting communication between cyber and space experts. There is currently limited communication between experts in the cyber security and the space security communities, with many not being aware of the importance of sharing information and experience across domains. The research project aims to facilitate communication and knowledge transfer between cyber and space experts as well as their respective communities.

The project also involves a series of seminars and publications aimed at bringing together experts from both the cyber security and the space security communities to examine the connections between the two fields. A first seminar, titled 'Making the Connection: The Future of Cyber and Space', was held in January 2013 at Chatham House, and an accompanying workshop summary was published.[1] This was followed by a second seminar, 'Making the Connection: Building Stability in Cyber and Space', held at Chatham House in May 2013, following which a workshop

[1] *Making the Connection: The Future of Cyber and Space*, International Security Workshop Summary, 24 January 2013; http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/240113summary.pdf.

summary was also published.[2] A third seminar, 'Connecting Cyber Security and Space Security: International Perspectives', at which a preliminary copy of this paper was circulated for comment and discussion, took place in July 2014 at Chatham House. Some of the research project findings were also presented at the UN Institute for Disarmament Research (UNIDIR)'s Space Security 2014 conference, held in March 2014 in Geneva, Switzerland, and at the Association of Southeast Asian Nations (ASEAN) Regional Forum Workshop on Space Security, held in October 2014 in Tokyo, Japan.

Over the coming decades, the number and diversity of actors operating in cyberspace and in outer space will continue to expand. While beneficial in many ways, this also means that the security challenges that currently face us are going to grow. This is in large part attributable to declining barriers to entry in both sectors. In the cyber sphere, the cost of providing internet access is falling steadily, leading to explosive growth in connectivity for millions of people around the world. At the same time, cyber criminals have seized on this to develop and sell 'attack toolkits', making it ever cheaper for other cyber criminals with minimal cyber skills (including gangs working for rogue states) to launch automated cyber attacks[3] either for economic gain or to disable a country's infrastructure. In the space sector, the cost of building and launching a satellite is also declining, allowing an increasing number of countries, commercial entities and even private individuals to acquire access to space systems. This includes states with poor governance controls and those where non-state armed groups operate with relative impunity, which are increasingly attaining a presence in space. It is therefore critical to tackle these emerging challenges now.

This paper aims to identify and raise awareness of the challenges common to both the cyber security and space security domains by compiling 11 submissions from cyber security experts and space security experts that assess the challenges in each field and consider the linkages between the two, along with an Overview that analyses these shared features. Part I is made up of a series of country studies, in which experts from eight countries (China, France, India, Italy, Japan, Russia, the United Kingdom and the United States), drawn from think tanks, academia and industry, set out their views on their countries' cyber security and space security policies. Part II presents international institution perspectives, with contributors from three major bodies (the European Union, the Organisation for Economic Cooperation and Development and the UN) providing high-level assessments of challenges at the intersection of cyber security and space security.

The experts submitting country perspectives were given the following set of questions as guidelines:

- What are the strengths and weaknesses of your country's cyber security policies, relative to other primary competitors and collaborators?
- What are the strengths and weaknesses of your country's space policies, relative to other primary competitors and collaborators?
- What level of public and private sector capacity does your country have to handle the cyber security challenges of space-based platforms, ground stations and other space assets in terms of human resources, processes and technology?

[2] *Making the Connection: Building Stability in Cyber and Space*, International Security Summary, 7 May 2013; http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/070513summary.pdf.
[3] Including distributed denial of service (DDoS) attacks.

The contributions point to a range of potential policy implications. Given the importance of the issue, and how little attention has been hitherto paid to the critical intersection of the cyber security and space security domains, further research that brings together academics, industry representatives and senior policy-makers in both the cyber security and space security fields is now needed in order to formulate robust policy responses and assess the feasibility of their implementation. Recent press reports of cyber attacks on networks that handle space data,[4] and studies that have pointed to critical vulnerabilities at the intersection between the cyber security and space security domains[5] suggest that tackling these issues is pressing.

[4] Jason Samenow, 'Weather satellite data hack and outage: Why this matters for forecasting', *Washington Post*, 12 November 2014; http://www.washingtonpost.com/blogs/capital-weather-gang/wp/2014/11/12/weather-satellite-data-hack-and-outage-why-this-matters-for-forecasting/.

[5] US Department of Commerce Office of Inspector General Office of Audit and Evaluation, *Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission*, Final Report OIG-14-025-A, 15 July 2014; http://www.oig.doc.gov/OIGPublications/OIG-14-025-A.pdf.

Overview: Common Challenges in Cyber Security and Space Security – Contributing to an Escalatory Cycle of Militarization?

Caroline Baylon

The cyber and space domains have been growing in significance in recent decades, with space now regarded as the fourth domain of warfare and cyber as the fifth. Initially conceived for research collaboration between universities and government think tanks in the 1960s before undergoing explosive growth for mainstream commerce from the 1990s onwards, the internet has come to pervade nearly all aspects of modern society. This has made it an increasingly attractive target for cyber attack, with more than a dozen states thought to possess advanced cyberwarfare capabilities at present.

Similarly, at the inception of the space era in the 1950s, most states hoped that outer space would be used primarily for scientific exploration. However, the United States and the Soviet Union soon deployed spy satellites for gathering military intelligence, and developed anti-satellite weapons (ASATs) to destroy each other's satellites. At present, a growing number of states – including European Union (EU) countries, China and India – rely heavily on satellites for their military operations, including for espionage, communications and navigation, while commercial entities are increasingly entering the space arena as well, further augmenting the number of actors with which to contend.

This research paper sets out a number of security concerns facing the cyber security and space security sectors, drawing on a range of submissions providing country and international institution perspectives. Many of these joint challenges are linked to the growing militarization of both fields, including the role of economic factors in contributing to such an increase in military use. This overview highlights some of the security challenges common to both the cyber and space domains and draws attention to the parallels between them. How these challenges relate to and influence one another – in the wider context of increasing militarization – is set out in a flowchart (see p. 14). The analysis provides a preliminary foundation for future research that could focus on the policy implications of these findings.

Major security challenges common to both the cyber and space domains include:

An escalatory cycle of militarization in the cyber and space fields, prompted by the increasing militarization of a small number of states

The militarization of both the cyber and space sectors appears in part attributable to a small number of states' increasingly militarized actions in these (and other) domains. Other states, responding to a 'perceived threat', are thus more likely to ramp up the military aspects of their own cyber and space programmes. This, in turn, prompts an even greater number of states to militarize, which produces an 'escalatory cycle'.

Cyber domain. Cyberspace is on the brink of an arms race. A few states' pursuit of cyberwarfare capabilities – including capabilities intended to target the critical infrastructure of other states – has prompted other states to do the same, with at least a dozen countries now thought to possess cyberwarfare capabilities of an advanced form. A further 60–100 countries have acquired some level of cyberwarfare capabilities, and many are actively working to develop such capacity further.

Space domain. A number of the submissions to this paper have commented that the actions of selected states also appear to be driving the militarization of other states' space programmes. In Part I, the contribution on Japan asserts that the country's defence ministry is gradually recognizing the importance of having space assets in the context of the nuclear and missile threat from North Korea as well as recent disputes with China. Similarly, the contribution on India notes that while India has emphasized a peaceful space programme, the security imperatives pertaining to its neighbourhood may lead the country towards a more assertive military space policy.

Lack or inadequacy of national policy documents in the cyber and space realms

The lack or inadequacy of national policy documents in the cyber and space spheres creates opacity concerning state objectives, which in turn fosters 'ambiguity of intent' surrounding state actions and renders states more likely to construe other states' actions as offensive. This contributes to the perceived threat, and thus to the escalatory cycle. Moreover, the absence of such documents also hinders dialogue, reducing prospects for international cooperation. This leaves states unable to benefit from the transparency and confidence-building that international cooperation engenders – activities that would help reduce ambiguity of intent and the perceived threat, and thus forestall a further increase in the escalatory cycle.

Cyber domain. A number of submissions point to the incompleteness of national policy documents in the cyber sector as a key challenge that contributes to ambiguity surrounding state actions. The contribution on India cites the lack of a clear and comprehensive cyber security policy as a major weakness. It states that while India has issued a document on national cyber policy, it did not clearly articulate the policy's objectives. Similarly, the contribution on China emphasizes that country's need for a more developed cyber security[6] policy, commenting that although China has also issued a policy document, this is rather more an industry development policy that provides business guidance to the commercial sector than a comprehensive information security policy setting out government principles.

The submissions to this paper also identify the lack of development of national cyber policy documents as an impediment to international cooperation. The Chinese contribution, for example, comments that issuing a more comprehensive information security policy would allow it to engage more effectively in international cooperation. By better clarifying objectives, such documentation can provide other countries with greater insight into a country's intentions, thus enhancing international trust and improving prospects for collaboration.

Space domain. Some submissions similarly describe the dearth of national policy documents in the space field, and how this contributes to ambiguity as to states' intentions. The submission on India argues that an 'open' policy could possibly alleviate the fears of other states, build confidence in India's objectives and prevent ambiguities concerning its intentions. At present, India's space policy has to be pieced together from the statements of Indian officials in parliament and at multilateral forums such the Conference on Disarmament and other UN channels, which leaves the country's actions open to misunderstanding and misinterpretation.

[6] China favours the term 'information security' over 'cyber security', which is predominantly used by Western states. The implications of this are discussed in a subsequent section.

The submissions also show that the absence of national space policy documents additionally hinders international cooperation. The contribution on China contends that the country has no space policy at all, and that the development of an official space policy would bring it many advantages since a space policy would enable China more effectively to take part in international cooperation. Increasing China's transparency in this area would bolster the country's international reputation and increase other countries' willingness to collaborate with it.

Lack or insufficiency of internationally agreed definitions of key terminology in the cyber and space domains

Given that robust definitions are fundamental to the establishment of enduring treaties, the lack or insufficiency of internationally agreed definitions of key cyber security and space security terminology impedes the development of multilateral arms control agreements. This lack of agreements further contributes to the ambiguity of intent and perceived threat that feed the escalatory cycle. Moreover, it also hinders international cooperation. This means that countries cannot take advantage of the trust-building derived from such activities, which would also help reduce the factors described above that fuel the escalatory cycle.

Cyber domain. The submissions to the paper indicate that limited consensus surrounding accepted definitions of key terms in the cyber sector is a barrier to a potential treaty seeking to limit the development or use of cyber weapons. The contribution on Italy comments that although the definition of a 'cyber weapon' has been widely debated, it has generated little consensus. Furthermore, national differences in prevalent terminology compound the difficulty of arriving at such an agreement. While most states – led by the West – predominantly use the term 'cyber security' to refer to internet security issues, a few states – notably China and Russia – instead use the term 'information security'. ('Information security' encompasses a wider range of issues than 'cyber security', covering not only pure information technology concerns but also the internet's impact on people's beliefs and attitudes. This in itself reveals fundamental differences in perceptions of security concerns related to the internet: China and Russia view the unrestricted flow of information in cyberspace as a potential threat to the internal stability of their countries, while Western states tend to view internet freedom as a fundamental right.) As a consequence, when China and Russia introduced their proposed International Code of Conduct for Information Security (Code of Conduct) to the UN in 2011, ostensibly to reduce the risk of conflict in cyberspace, they used the term 'information weapon' rather than 'cyber weapon'. According to this terminology, even a social networking site like Twitter or Facebook could be considered an 'information weapon' if used to criticize a government. Given that Western countries would not countenance such restraints on free speech, the use of the term 'information weapon' has made potential agreement on the Code of Conduct near impossible from the start.

The submissions to the paper also indicate that the paucity of agreed definitions in the cyber sphere makes it more difficult for countries to communicate effectively, thus impeding international cooperation in cyberspace. Western states' preference for the term 'cyber security', as against that of China and Russia for 'information security', means that they may not fully grasp the nuances of each other's views when engaging in international dialogue. For example, the section on Russia comments that the term 'cyber security' does not exist in Russian legislation or in any official doctrines. This suggests that Russia's relative inexperience with the terminology may make it harder for the country to understand the subtleties of Western positions during negotiations. It also states that Russia's entire approach to internet security – especially its foreign policy dimension – is built on the concept of 'information security'. Thus, Western states' relatively infrequent use of this term – and Russia's heavy reliance on it – is a particular challenge in view of its centrality to understanding Russian perspectives. The Chinese submission puts a similar case, suggesting that China should clarify the connections between information security and cyber security in order to contribute to greater international understanding.

Space domain. In space, too, the lack of definitions is an impediment to arms control treaties. There is no internationally accepted definition of a 'space weapon', despite years of discussions within multilateral forums. This is a major obstacle to the negotiation of a treaty on the Prevention of an Arms Race in Outer Space (PAROS) under the auspices of the UN Conference on Disarmament: China and Russia introduced a draft Treaty on the Prevention of the Placement of Weapons in Outer Space (PPWT) in 2008, and a revised version in 2014; however, their proposed definition of a 'space weapon' has been heavily criticized since it does not cover ground-based ASATs, which are one of the greatest threats. Furthermore, states need not only to define these terms, but also to ensure that the definitions are stringent. Neglecting to define a term has been a problem in the past: in the 1967 Outer Space Treaty,[7] the lack of a definition of 'peaceful' use highlights the potential repercussions of weak or non-existent definitions. The resultant legal ambiguity created a loophole through which some states later justified increasingly militarized uses of space (further discussed below).

Finally, the lack of agreed definitions also inhibits international cooperation in space. For example, there is no internationally accepted definition of the term 'space debris'. This means that countries do not currently have the legal right to clean up space debris, impeding the potential for international cooperative efforts in this regard.

A blurring line between 'non-military' and 'military' roles in the cyber and space sectors – including a rise in dual-use technologies

The distinction between 'non-military' and 'military' roles is increasingly blurred in the cyber and space arenas, with many technologies being dual-use (i.e. used for both civilian and military purposes). This makes it more difficult to define key terminology (especially that involving warfare), contributing to the lack or inadequacy of internationally agreed definitions. The absence of definitions, in turn, impedes the development of multilateral arms control agreements and deters cooperation, furthering the ambiguity of intent and perceived threat that foster the escalatory cycle. Dual-use technologies also mean that banning certain technologies outright and implementing adequate measures to verify compliance are often unfeasible, leading to difficulties in reaching arms control agreements. Furthermore, dual-use technologies make it more difficult to ascertain whether a country is developing a military programme in addition to its civilian activities; this has a direct impact on ambiguity of intent surrounding countries' actions and thus further stimulates the escalatory cycle.

Cyber domain. The prevalence of dual-use technologies in the cyber sector makes it difficult to define a 'cyber weapon' and other key cyberwarfare-related terminology. In fact, the non-military and military applications of cyberspace are so intertwined that it is difficult to separate the two: one might consider all information technology to be dual-use – computer hardware and software, even the internet itself – given that both civilians and the military rely upon them for their daily activities. Thus, it has become difficult to determine where the boundary lies between peaceful civilian usage and a military-purpose weapon. For example, everyday commercial software or hardware can be instantaneously transformed into a missile in the realm of cyberwarfare: one state could acquire control of another's

[7] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies; http://disarmament.un.org/treaties/t/outer_space.

critical infrastructure by surreptitiously introducing malicious code into that state's vital computer systems, causing an explosion or other disaster bringing about loss of life.

The dual-use nature of cyberspace also means that seeking to limit or outlaw the technology used in cyber weapons, or implementing adequate measures to verify compliance with such a ban, are unlikely to be effective, impeding prospects for the development of international cyber arms control agreements. In Part II, the contribution on the EU explains that since both the cyber and space domains have dual-use capabilities, traditional arms control instruments which focus on prohibiting certain technologies are difficult, if not impossible, to employ – not least because of the problem of effective verification. Indeed, a traditional arms control agreement seeks to ban the technology needed to create a weapon. However, developing a cyber weapon requires only a computer (and of course technical skill). Thus, it is impossible to ban the requisite technology for cyber weapons, since computers are a pervasive and fundamental part of modern society.[8] Furthermore, traditional arms control agreements also rely on verification measures to monitor compliance. Since cyber weapons could conceivably be developed on a computer in any location, there is no way for inspection teams to verify that such weapons are not being produced. (In the case of nuclear weapons, for example, production facilities can be identified from the air and further monitored by inspection teams on the ground.)

Finally in this regard, the dual-use aspects of cyberspace also make it harder to determine whether states are pursuing cyberwarfare capabilities, or whether their use of cyberspace is primarily non-military. The covert nature of cyberwarfare, with states secretly penetrating and hiding malicious code in the networks of others, makes it particularly difficult to ascertain what countries are doing in this sphere, and contributes to ambiguity of intent surrounding state actions.

Space domain. Similarly, dual-use technologies in the space sector make it difficult to reach international consensus on the definition of a 'space weapon' and on other key terms that have military implications. A large number of technologies in space are dual-use, from satellites to rockets to GPS (Global Positioning System). The difficulty of defining a 'space weapon' is compounded by the potential for almost any space object to be used as a weapon in space. For example, a civilian satellite (e.g. for weather monitoring) could effectively be turned into a weapon by causing it to collide with and destroy another satellite.

The dual-use characteristics of space technologies likewise mean that traditional tactics such as banning certain technologies outright or verifying compliance are difficult to implement, hindering prospects for space arms control agreements. In particular, an implication of dual-use technology is that it is not possible to construct definitions that are robust enough to serve as a basis for potential international arms control agreements – i.e. that close any potential loopholes – without at the same time including non-military technology and thus inadvertently restricting the civilian applications of the technology. For example, GPS technology encompasses a highly precise military version for targeting missiles as well as a less accurate civilian version that has become widespread for providing positioning information in vehicle navigation systems and timing functions in critical infrastructure. An attempt to ban the GPS technology used in missile targeting would therefore also restrict civilian use. Moreover, verification of compliance is a challenge for any potential arms control agreement, given that the civilian applications of space technology make it easier to conceal military programmes.

[8] Neither is it possible to ban the acquisition of the technical skill required for cyber weapons, since developing a basic cyber weapon involves identifying a vulnerability and then designing and launching an exploit to take advantage of that vulnerability, which any moderate-level computer programmer would have the knowledge to do. Of course, a higher level of expertise is required to develop more complex cyber weapons, but this is still something that computer experts could teach themselves.

Finally, dual-use technologies in space also make it more difficult to determine whether their use is for purely civilian purposes, or whether a military programme is being developed as well. An example would be the private sector using rocket technology to launch satellites and other spacecraft for commercial and scientific purposes while the military employs this same technology as a missile or ASAT. A state's successful launch of an advanced civilian rocket may therefore cause other states to infer that it possesses similarly advanced missile or ASAT capabilities. This in turn contributes to ambiguity of intent, and might prompt other states to develop further their own missile or ASAT capabilities.

A blurring line between 'offensive' and 'defensive' actions in the cyber and space fields – or a shifting line to permit increasingly 'offensive' activities justified as 'defensive' activities

The norms of acceptable behaviour in cyber and space are shifting towards the offensive end of the spectrum, permitting increasingly 'offensive' activities under the guise of 'defensive' ones. This too contributes to ambiguity of intent surrounding state behaviour, and thus to the escalatory cycle.

Cyber domain. The submissions to this paper indicate that offensive actions in cyberspace are on the rise. A unique characteristic of cyberspace is that once an actor has penetrated a network for espionage purposes, that actor only needs to carry out a few more steps in order to launch a cyber attack. This blurred distinction between cyber espionage and cyberwarfare makes it easier to justify offensive capabilities under the guise of defensive ones. The submission on the United States comments that US policy is to employ 'active cyber defense' capabilities to defend military networks and systems, and to conduct 'full-spectrum military cyberspace operations' when directed to assist in that defence. The term 'active cyber defense' is commonly understood to include offensive actions in cyberspace, taken with defensive purposes in mind.

Space domain. In the space domain, too, states are shifting the moral line to justify the development of more forceful military capabilities as a defensive need. Part of this shift occurred early on. While most of the signatories to the 1967 Outer Space Treaty initially viewed their commitment to 'peaceful' use of outer space to mean *non-military* use, the US interpretation of 'peaceful' use as meaning *non-aggressive* use soon became the accepted standard among states. Although it appears difficult to justify *military* use as a form of 'peaceful' use, the US – buoyed by the perceived threat of the Soviet Union – had a compelling moral argument for the military use of space for defensive purposes. Even Japan, whose pacifist constitution long caused it to cling to the *non-military* use interpretation of the term, has changed its stance in recent years. As stated in the submission on Japan, the 2008 Basic Space Law defined one objective of Japan's space activities as being to contribute to the country's national security. It also reinterpreted 'peaceful' use to mean non-aggressive use – i.e. more closely in line with international norms – and thus opening the way for the possible use of space for defensive purposes. The contribution on the UN comments that the most significant obstacle to addressing future space policy development effectively is the dichotomy between 'peaceful' uses of outer space and non-peaceful uses.

Asymmetric threats in the cyber and space domains – i.e. 'offence is easier and cheaper than defence'

The cyber and space fields are both faced with asymmetric threats. This contributes to the increasingly blurred line between 'offensive' and 'defensive' activities in cyber and space. The EU submission describes how cyber and space have 'asymmetric vulnerabilities', from both technological and geopolitical standpoints. Technologically, offence is easier and more cost-effective than defence.

Geopolitically, the consequence is that highly advanced countries are particularly vulnerable to attack from less developed states (as well as from terrorist groups and other actors). Since states are faced with growing threats, and with the cost of defence increasingly elevated, many have chosen to ramp up their offensive activities instead in an effort at deterrence. Once again, this contributes to the ambiguity of intent and perceived threat that prompts other states to militarize in the escalatory cycle.

Cyber domain. In cyberspace, from a technological perspective, it is easier and cheaper to attack a country's networks than it is to defend against such an attack. In order to launch a cyber attack, a malicious actor needs to exploit just one vulnerability in a network. To mount an effective defence against cyber attacks, however, a country would need to identify and 'patch' all potential vulnerabilities, which is much more costly – and likely to be impossible.

This has implications at the geopolitical level, with countries that are highly reliant on the internet – such as the United States, the United Kingdom and other advanced economies – being highly vulnerable to cyber attacks. Since launching an effective cyber attack can be done with only a basic internet connection, countries with lower levels of internet dependency can thus inflict proportionally greater damage at lower cost to countries that are highly internet-reliant. (By contrast, if a highly internet-reliant country wanted to launch a retaliatory cyber attack against a country with a lower level of internet dependency, it would not be able to cause as much damage since there is less to attack.)[9]

Space domain. The situation with regard to space is similar. The US contribution best expresses this by commenting that 'offence is easier and cheaper than defence', citing the challenges involved in missile defence as an example. At the technological level, it is much easier and cheaper to attack a satellite than it is to block an attack. In order to destroy a satellite, an attacker would only need to launch an ASAT, which is relatively easy to obtain and can be adapted from existing technology. (Many types of rocket design can be modified in order to create an ASAT.) However, to defend a satellite against such an attack would require a highly sophisticated and costly missile defence system.

At the geopolitical level, this means that the leading space powers are highly vulnerable to asymmetric attacks. The US submission comments that the country's heavy reliance on satellite technology makes it particularly susceptible in this regard. It notes that while space assets are a valuable enabler of the information age, and a powerful force enhancement tool, US dependence on these assets has also created a potential 'Achilles heel' in terms of vulnerability to asymmetric attacks. While only space powers possess satellites and other space assets that can be attacked, a country does not need to be a space power in order to take down another country's satellite. This can be accomplished with an ASAT or – in what is becoming an increasingly plausible scenario – by waging a cyber attack (e.g. causing a satellite to spin out of orbit and self-destruct). If attacked by a non-space power, a space power would be unable to respond in kind, since its adversary would not have space assets to counterattack.

Conclusions

In identifying and analysing some of the common challenges in the cyber and space domains, the submissions to this paper point to the existence of an escalatory cycle of militarization in both domains, apparently driven by a set of common factors. The paper examines the interactions of these factors, and offers a visual representation of their interrelation in the form of a flowchart.

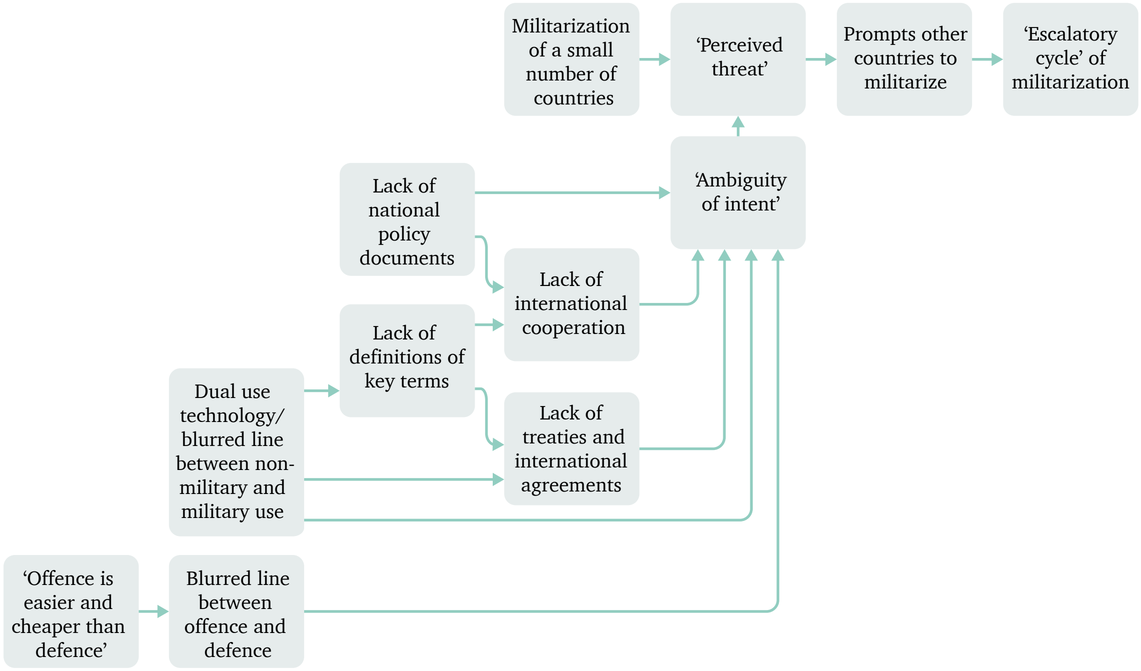
[9] At present, only states are believed to have the capability to launch sophisticated cyber attacks, but in the coming years non-state actors (e.g. terrorist groups) are likely to acquire these capabilities as well. In such cases, the asymmetric threat to internet-reliant countries will be even greater, since they will have to contend not only with states but also with non-state foes – which themselves have fewer targets to counterattack.

Given that each factor, in contributing to the cycle, has a magnifying impact on militarization, tackling any of these factors at any point in the chain could help break or dampen the escalatory effect. The flowchart can therefore serve as a foundation for future research aimed at identifying joint solutions to these common challenges. For example, as outlined above, the lack or inadequacy of national policy documents impacts ambiguity of intent surrounding state actions, thus contributing to the perceived threat that fuels the escalatory cycle. This suggests that measures as simple as encouraging a greater number of countries to issue national policy documents or further clarify their existing policies can play an important role in mitigating the effects of the escalatory cycle.

Another example is that the lack or insufficiency of clear definitions of key terminology contributes to the lack of international agreements, which in turn fosters the ambiguity of intent and perceived threat that drive the escalatory cycle. One potential solution might be in ensuring better, agreed definitions. However, the presence of dual-use technology has revealed that unambiguous definitions are particularly difficult to achieve. The flowchart therefore shows that another consequence of the paucity of key definitions is that it contributes to a lack of international cooperation, which also leads to the ambiguity of internet and perceived threat that reinforce the escalatory cycle. An alternative solution might be to take steps to promote international cooperation, which would act to decrease ambiguity of intent and the perceived threat fuelling the escalatory cycle, thereby counterbalancing the escalatory momentum generated by the lack of definitions of key terminology. The flowchart therefore also helps to convey how remedial actions in one area might be used to offset escalatory pressures in another area.

There is growing concern within the cyber and space communities that both sectors are heading not only towards increasing militarization but a step beyond, towards increasing *weaponization*. It is therefore vital to take steps to break the escalatory cycle now, before it is too late.

Figure 1: Flowchart depicting common factors impacting the growing militarization of the cyber and the space sectors


Militarization of a small number of countries
'Perceived threat'
Prompts other countries to militarize
'Escalatory cycle' of militarization
'Ambiguity of intent'
Lack of national policy documents
Lack of international cooperation
Lack of definitions of key terms
Dual use technology/ blurred line between non-military and military use
Lack of treaties and international agreements
'Offence is easier and cheaper than defence'
Blurred line between offence and defence

Part I
Country Perspectives

China’s Information and Space Security Policies

Dr Guoyu Wang

President Hu Jintao’s Work Report to the 18th National Congress of the Communist Party in 2012 was the first time that either cyber security or space security was highlighted at such a high level. The Work Report recognizes that China faces a series of interlinked challenges that threaten not only its security and development interests but also its very survival; and it explicitly identified both cyber security and space security as part of those challenges, stating that China ‘should attach great importance to maritime, space and cyberspace security’.

Information security policy

China has not published a *cyber security strategy* to date. However, it has issued a number of *information security policies*. The Chinese approach goes beyond cyber security to encompass the broader concept of information security, which China defines as the ‘protect[ion of] information, information systems and internet security from any unauthorized access, usage, leak, damage, modification and destruction in order to assure the[ir] integrity, confidentiality and availability’. A strategy document would need to be issued at the national level, either by President Xi Jinping or by the National Congress of the Communist Party, while policy documents are issued at the ministry level. To this end, the relevant statements of President Xi have been taken as guidance in the formulation of ministry-level policies. The present lead document is the Ministry of Industry and Information Technology’s 12th Five-Year Development Plan of the Information Security Industry (2011–15),[10] which sets forth objectives and targets and guides the development of the country’s information security industry. However, the document is more of an *industry development* policy than a comprehensive *information security* policy.

The policies set out in the Five-Year Development Plans governing the information security industry have promoted China’s economic growth, proving especially conducive to the rapid development of the information security industry. The issuance of a more comprehensive information security policy (or of a strategy) could therefore provide even more benefits. First, it would allow China to engage in international cooperation more effectively. For example, a more comprehensive policy could clarify the connections between information security and cyber security, contributing to greater international understanding.

Second, it could better highlight the relevance of information security to national security, thereby increasing public and industry awareness. While China’s current information security policy focuses on industrial development, a more comprehensive policy should encompass national security as well, emphasizing it as a key goal.

[10] See http://wenku.baidu.com/link?url=K6pc3LeJxffKN7Ii0ti1VMbqJxYbaJShnDtXtUqj9QlwFQR9wItJeUJWPWAgtDHhwK3mi9M4mwqKV5lnOAxL7ahbb5X3AH_GNGMY4nrx723.

Third, it would 'enable a more proactive rather than reactive foreign policy'.[11] For instance, although China's Ministry of Foreign Affairs created an office to deal with cyber security issues in 2013,[12] the absence of specific policies guiding how it might respond to international situations impedes long-term planning.

Fourth, it could also form an important part of the country's declaratory policy. More specifically, by outlining what China would consider a cyber attack, and how it would respond, a more comprehensive policy could have a deterrent effect.

In a promising recent development, China may be preparing to issue a more comprehensive information security policy or a strategy. In February 2014 the Chinese government established the Central Internet Security and Informatization Leading Group. Headed by President Xi, the group is tasked with 'lead[ing] and coordinat[ing] internet security and informatization[13] work among different sectors, as well as draft[ing] national strategies, development plans and major policies in this field'.[14]

Space policy

China has issued neither a national space *strategy* nor a national space *policy*. The Information Office of the State Council has released three white papers on China's space activities, in 2000, 2006 and 2011,[15] which were presented to the press by the China National Space Administration. They play an irreplaceable role in guiding the development of the space industry and achieving economic development goals, and many commentators have taken them to constitute the country's national space policy. However, they are primarily programme documents on China's space activities issued at five-year intervals. Thus, as in the information security domain, they represent a space *industry development* policy rather than a dedicated space policy.

The development of an official space policy (or strategy) would bring China many advantages. First, as in the information security sphere, a space policy would enable China to take part in international cooperation more effectively. Increasing China's transparency in this regard would bolster the country's international reputation and increase other countries' willingness to collaborate with it.

Second, in another parallel with the information security domain, a space policy could further emphasize the importance of space to national security, particularly among the public and industry in China.[16] For example, a better understanding of space's national security role would contribute to the greater political legitimacy of space activities relevant to national security.

Third, it would further spur the economic growth of China's space sector, as China's information security policies have done in the information security sector. For example, by providing more clarity on the country's security priorities, a space policy would help to further delineate the respective roles of various space actors and would help industry to better prioritize the allocation of resources.

[11] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO Cooperative Cyber Defence Center of Excellence Publication, 2012, p. 46.
[12] China's Foreign Ministry sets up cyber security office, *China Daily*, 14 June 2013; http://usa.chinadaily.com.cn/china/2013-06/14/content_16623576.htm.
[13] The term 'informatization' refers to the extent to which a geographical area, an economy or a society is becoming information-based.
[14] Xi looks to a nation of cyberpower, *China Daily*, 28 February 2014; http://europe.chinadaily.com.cn/china/2014-02/28/content_17311471.htm.
[15] The English-language text of the 2011 white paper is available at http://www.gov.cn/english/official/2011-12/29/content_2033200.htm.
[16] Countries such as the United States and Russia, which have advanced national space policies, are well aware of this. The United States, which has the most developed space policy and the most advanced space technology in the world, recognizes the importance of its space activities to national security. Similarly, Russia has emphasized the importance of space to national security in its several proposal papers submitted to the Long-term Sustainability of Outer Space Activities Working Group of the Scientific and Technical Subcommittee of the UN Committee on the Peaceful Uses of Outer Space from 2013 to 2014.

The Chinese government has recently taken steps that may contribute to the development of such a space policy. In April, President Xi underscored the national security importance of space, citing the need 'to speed up air and space integration and sharpen their offensive and defensive capabilities'.[17] This might be an ideal time for China to consider advancing its national security and other relevant interests in outer space through an official space policy.

Conclusions

Issuing policy (or strategy) documents at the national level brings a host of benefits ranging from greater prospects for international cooperation to an opportunity to better highlight the national security relevance of certain sectors. The Chinese government appears to have recognized this, and may be considering developing a more comprehensive information security policy and issuing a space security policy. Moreover, it seems to be preparing to issue an overall national security strategy as well that would include both information security and space security. In 2013 China established the Central National Security Commission, a high-level interagency coordination group for security, headed by President Xi, in which cyber security, space security and other relevant issues can be addressed as part of an overarching national security policy or strategy.

[17] China's President Xi urges greater military use of space, Reuters, 15 April 2014; http://uk.reuters.com/article/2014/04/15/uk-china-defence-idUKBREA3E03G20140415.

France’s Cyber and Space Security Policies

Dr Xavier Pasco, Vincent Joubert

Cyber security policy

Background

France’s national cyber security policy is the result of an ongoing institutionalization process. This began with the French government’s 2008 White Paper on Defence and National Security (Livre blanc sur la défense et la sécurité nationale),[18] which called for the establishment of a national agency responsible for the security of the country’s information systems. Accordingly the French Network and Information Security Agency (ANSSI, Agence nationale de la sécurité des systèmes d’information) was established in 2009. ANSSI issued a national cyber security strategy in 2011.[19] This was followed by the French government’s 2013 white paper on defence and national security, which highlighted cyber security and cyberdefence as one of France’s top priorities.[20] France increased its cyber security budget in response. And recently, the defence ministry presented its Cyber Defence Pact (Pacte Défense Cyber) establishing a cyberdefence action plan for 2014–16. This corresponds to the first phase of the Military Programming Law (Loi de Programmation Militaire) that allocates the country’s military spending for the next six years.

Analysis

France is continuing to improve its cyber capabilities: ANSSI is expanding its capacity. In addition, the national cyber security strategy has identified essential areas of action to meet the country’s strategic objectives, demonstrating a comprehensive vision of the issues. Furthermore, the Cyber Defence Pact is setting out a number of measures that will reinforce France’s capacity to respond to cyber attacks, in line with the national cyber security strategy’s objectives and within the budget allocated. The Pact will also strengthen research and development by financing universities as well as innovation projects in the private sector, including those of small and medium enterprises. The primary goal is to ensure that France has the capability to defend its critical assets and national interests in the face of rapid technological innovation and the large number of cyber attack techniques.

In the light of Edward Snowden’s revelations about the US National Security Agency’s cyber espionage capabilities, France has further emphasized the importance of securing and preserving the sovereignty of its national critical information systems. The French government is actively developing public policies intended to promote the development of national cyber security products. ANSSI has also issued a set of technical guidance measures designed to strengthen and increase the implementation of security provisions in the private sector. The main objective of these measures is to promote the ‘digital trust’ (confiance numérique), concept and label, which provides internet users with certified, secure internet access according to their cyber security needs.

[18] See http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341/0000.pdf.

[19] Information Systems Defence and Security: France’s Strategy (Défense et sécurité des systèmes d’information: Stratégie de la France); http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

[20] An English-language version of the 2013 white paper is available at http://www.livreblancdefenseetsecurite.gouv.fr/pdf/the_white_paper_defence_2013.pdf.

France can be considered a major international actor in cyberspace and it has strong industrial, engineering and intellectual expertise in the domain. Despite relatively late political involvement in the sector, the current institutionalization process as well as the associated policies and Cyber Defence Pact has accelerated the evolution of French cyber security and cyberdefence capabilities. But France, like many of its peers, will need to develop an attractive recruitment policy in order to meet its human resources requirements for cyber security experts. The continued success of its efforts to strengthen cyber security will depend largely on the effective implementation of these new policies and the Pact.

Space security policy

Background

France has a long history of public investment in space activities, covering key domains such as Earth observation, telecommunications, launchers and science, as well as having corresponding expertise in defence and security. It established its space agency, the National Centre for Space Studies (CNES, Centre National d'Etudes Spatiales, in 1961. CNES launched France's first satellite in 1965 and today it operates some 20 institutional satellites. Space operators such as EUTELSAT (in satellite telecommunications) and Spotimage (in commercial Earth observation) have reinforced the industrial and economic dimension of the country's space activities.

Analysis

In view of their increasing role in France's national security and economic well-being, space systems constitute part of the country's critical infrastructure and thus must be protected against all types of threat, including cyber attacks. The increasing importance of space systems was reaffirmed in the 2008 and 2013 White Papers on Defence and National Security. The latest version also emphasizes the need to protect these assets, stating that 'the protection of outer space is now a major challenge given the importance of the services and missions carried out by spacecraft'.[21]

France has decided to strengthen the security of its space systems in response to the increasing threats to the sector. A key aspect of this involves efforts begun a few years ago to develop the first elements of a space situational awareness system. France has opted for a nationally developed programme, primarily managed by the military, to ensure that space system operations have a high level of security at all levels. This includes the main ground stations, enabling platform services and payload data transmission.

The country considers its highest-resolution space imagery to be 'military intelligence', and thus all elements forming part of the space 'intelligence chain' must be processed according to rigorous classified protection rules. France is one of a small number of countries to possess military-grade telecommunications satellites, again managed by the military, which provide highly secure communication links. Its main space surveillance radar, the Major Adapted Network to Watch Space (Grand Réseau Adapté à la Veille Spatiale), is run by the French air force, and the data generated are classified at the 'defence confidential' level.

[21] Ibid., p. 98.

It is important to remember that the French military space programme arose from strategic needs linked to the country's nuclear strike force (force de frappe), notably in the field of military Earth observation. This has obvious consequences in terms of the programme's organization and level of security. In this respect, France's security principles are notably stricter than the procedures designed for dual-use or civilian systems, which have generally been adopted by most of its European partners.[22] The French approach has been closer to that of the United States or Russia when it comes to ensuring the security of its critical space infrastructure.

Cyber and space policy

The cyber security of space-based platforms, ground stations and related space assets is now emerging as a particularly important issue in France. The country has a strong industrial base that can handle this challenge through innovative research and development. Educating and training personnel through appropriate simulation exercises is vital to ensure that proper reaction and responsive measures are implemented in case of attack. Both the French government and the private sector are aware of the sensitivity of cyber security issues involving space assets and they have adopted risk management-based policies to ensure that the technology, security norms and standards designed for space assets are strongly protected.

[22] Germany has also adopted military-grade protective rules for its more recent military radar satellites.

India’s Cyber and Space Security Policies

Dr Rajeswari Pillai Rajagopalan

While many countries still regard cyber security and space security as ‘future challenges’, or issues that will need to be dealt with in the coming years, India is already tackling them today. Unlike in the more traditional security realm, where a global architecture exists to handle problems as they arise, the cyber security and space security domains are characterized by limited understanding, few accepted global definitions and a lack of clearly articulated norms and regulations. These issues must be addressed in order to articulate sound policy, including at the national level.

The space domain is slightly more advanced than the cyber domain: It has some broad agreements in place, although they lack a number of elements, including definitions of key concepts in space security. There is a clear need for new architectures that will fix these anomalies and establish new parameters of responsible behaviour for the long-term sustainable use of these domains.

Cyber security policy

Strengths

A large pool of available talent and capabilities. India’s significant talent and capabilities in cyber security is one of its biggest strengths. With a highly educated, technologically skilled workforce, the country possesses one of the largest talent pools in the world.

An ideal blend of Western and Eastern approaches. One can argue that India has found an ideal blend of Western and Eastern approaches to cyber security. Its approach to cyber security is driven by two factors: national security and social harmony. At the global level, there are two schools of thought regarding cyber security. The Western approach, led by the United States, looks at cyber security through a national security prism. The Eastern approach, driven by China and Russia, emphasizes social cohesion. Until several years ago, India viewed cyber security predominantly from a national security perspective, with its primary concern being the protection of critical infrastructure. Lately, however, it has increasingly emphasized social harmony and cohesion. Thus the Indian view today combines the Western and Eastern approaches.

Challenges

Lack of a comprehensive policy. The lack of a clear and comprehensive cyber security policy is one of India’s major weaknesses. The Indian government issued a National Cyber Security Policy (NCSP) in July 2013, but the document came under sharp criticism because it did not clearly articulate the policy’s objectives.

Government policy that has been slow in exploiting the available talent pool. The government’s inability to exploit the large pool of available talent in the country is another key challenge. The NCSP’s lack of clarity reflects the inadequacy of talent and innovation in the Ministry of Communications and Information Technology, which was responsible for producing the document.

Lack of a holistic approach. The country also lacks a holistic approach to cyber security. In order to develop a comprehensive policy, it would be important to involve experts from the information and communications technology field as a whole rather than information technology experts alone. India has not done so.

Insufficient private sector input, including public-private partnerships (PPPs) that involve only large corporations. The policy-formation process in India does not allow for sufficient private sector input into cyber security policy. The NCSP was also criticized because the government made a minimal effort to obtain input and expertise from other sectors. Although it engaged with industry groups such as the Federation of Indian Chambers of Commerce and Industry, the process was half-hearted at best. In addition, Indian PPPs tend to involve only big corporations. This excludes an entire pool of talent that is available from India's many start-up firms, as well as individuals. A true PPP would go a long way towards bringing strengths and talents from across the spectrum to create a comprehensive approach towards cyber security.

Insufficient public input. The policy-making process in India also does not provide for sufficient public input into cyber security policy. The NCSP was also criticized for its lack of public input. Analysts described the Indian government's proclamation of seeking 'public comments and suggestions' for the NCSP as a farce, calling the exercise a mere formality. The participation of civil society groups has been weak as well. An open and transparent process, and gaining the support of the public are essential to creating a successful cyber security policy.

Lack of a strong security culture. India lacks a strong security culture. A country's security culture should permeate all those who are actively engaged in security-related sectors. This is especially important in the cyber security domain, where every individual has the potential to be both a defender and a victim. India must therefore increase the priority it accords security issues in general.

Lack of an institutional and legal framework. India's institutional framework for dealing with cyber security challenges is at a nascent stage. The lack of a legal framework is one of the biggest gaps in India's cyber security approach today. As yet, it has no overarching cyber security law to address incidents of cybercrime, cyber attacks and cyber breaches.[23]

Space security policy

Strengths

A large pool of available talent and capabilities, including a great capacity for innovation and indigenization. As in the cyber domain, India has a large pool of talent and capabilities in the space domain, including a highly educated and skilled labour force. Its capacity for innovation and indigenization is the biggest strength of India's space programme.

[23] For an overview of initiatives and challenges, as recognized by the government, see Integrated Defence Staff, Ministry of Defence, Government of India, 'Cyber Security in India's Counter Terrorism Strategy', available at http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf. For counter-viewpoints by analysts and experts, see Cyber Security in India blog, available at http://cybersecurityforindia.blogspot.in/, and International Legal Issues of Cyber Attacks, Cyber Terrorism, Cyber Espionage, Cyber Warfare and Cyber Crimes: International and Indian Legal Issues of Cyber Security blog, available at http://perry4law.co.in/cyber_security/.

Challenges

Lack of a comprehensive policy. As in the cyber security domain, the absence of a comprehensive, declared policy concerning space may be India's biggest weakness in the field. Its space policy has to be pieced together from the statements of Indian officials in Parliament and in multilateral forums such the Conference on Disarmament and elsewhere at the UN. In the past, when the Indian space programme was being challenged by the international community, there may have been benefits to not having a declared policy. Today, however, the situation is drastically different, and the advantages of a declared policy far outweigh the disadvantages: an open policy could alleviate the fears of other states, build confidence in India's objectives and prevent ambiguity about its intentions. Such a policy could also be an effective tool to send messages to both friends and foes. Most important, a declared policy would bring about greater clarity, improved allocation of resources and better prioritization, enabling an optimal use of resources.

Government policy that has been slow in exploiting the available talent pool, including policy that is driven by technocrats and the scientific bureaucracy. As in the cyber domain, India's approach to space is driven entirely by the government. Within this, it is driven by technocrats and the scientific bureaucracy instead of by a political leadership that articulates priorities and directions. Despite the huge technological progress that India has made, successive governments have adopted an ad hoc approach to its approach to space. India should realize that it does not have to match every capability that China may develop and that it should prioritize both from a commercial and a national security perspective. It has to change its casual approach if it wants to emerge as a dynamic player with a strong programme.

Insufficient private sector input. As in the cyber sphere, the Indian space sector is characterized by limited private sector input. The Indian private sector participates in the country's space programme in that it manufactures almost 80 per cent of key parts and components, but its voice is limited in shaping space policy. It is a source of strength that India has sizeable industry participation in its space programme, and this could be further enhanced if India were to have a dedicated military space programme.

Lack of a strong security culture. As in the cyber domain, the lack of a strong security culture, applicable to both the cyber and the space domains, is something that India must take note of and take steps to improve.

Financial resources that are stretched between shared civilian and military assets. Much as India has emphasized its desire for a peaceful space programme, the security imperatives in its neighbourhood may push it to adopt a more assertive military space policy. Under these circumstances, it would be particularly beneficial to have separate civilian and military assets. This would also mean a clearer institutional architecture that could better cater to growing demand from both the civilian and the military sectors. This in turn could result in better financial allocation as currently, the institutional architecture and financial and human resources are stretched between competing civilian and military needs.

Cyber and space security

The convergence of the cyber security and space security domains presents a complex challenge, yet the severity of the challenge is rarely acknowledged in India. The country has sufficient talent in both the public and the private sector, but the sluggish nature of the Indian bureaucracy and poor synergization have meant that its full potential has yet to be realized. Given the cross-domain nature of challenges in the cyber and space domains, states such as India have to invest in regional and global efforts in order to understand these environments. But this requires significant political direction, which has so far been lacking.

Italy’s Cyber and Space Security Policies

Dr Claudio Catalano

Cyber security policy

Background: the development of Italy’s cyber security policy

Italy first became concerned about cyber security issues in response to internet crime: In the mid-1990s, the growth of the internet raised the Italian police’s awareness of cybercrime. This led to the creation of a telecommunications unit in 1996 and of the Postal and Communications Police Service in 1998. The financial and border police (Guardia di Finanza) established a task force in 2001.

The 9/11 attacks on the United States in 2001 raised awareness of terrorism in Italy and around the world. This included the possibility of terrorists launching cyber attacks against critical national infrastructure (CNI). A special branch of the Postal and Communications Police, the National Center for Infrastructure Protection, is responsible for protecting CNI. In 2012 a new law also tasked the intelligence services with preventing terrorist attacks against CNI, including cyber attacks.[24]

For their part, the Italian military has developed computer network operations. The Defence General Staff’s Centre for Defence Innovation issued documents on military computer incident response in 2008, on computer network operations in 2009 and on joint cyberdefence policy in 2012.[25] As part of its network enabled capability objective, the military intends to integrate all systems into a net-centric area of operations.

The Italian government’s first official public report on national cyber security threats was issued by the Parliamentary Committee on Intelligence and Security Services in 2010. The report introduced the concept of asymmetric cyber threats, viewing cyberspace as the ‘next battlefield and the scenario of geopolitical competition in the 21st century’. It identified four key threats: cybercrime, cyber terrorism, cyber espionage and cyberwarfare. The report also set forth the notion that cyber security is not only a public security threat but also a strategic issue.

Subsequently, the prime minister’s decree of 24 January 2013 tasked a working group of national stakeholders with drafting a cyber security doctrine. This resulted in the publication of the National Strategic Framework for Cyberspace Security (Strategic Framework) in December 2013. It included the National Plan for Cyberspace Protection and ICT Security (National Plan). The Strategic Framework identified six guidelines to implement: enhancing the capabilities of national institutions dealing with cyber security; strengthening capabilities to protect critical infrastructure from cyber attacks, including national transport systems, the power grid and command-and-control centres; facilitating private-public partnerships; promoting a culture of cyber security; reinforcing online crime-fighting capabilities; and strengthening international cooperation. Interestingly the Strategic Framework includes a definition of a cyber weapon,

[24] Law no. 133 of 7 August 2012 amending Law no. 124 of 3 August 2007 on ‘Intelligence system for the security of the Republic and new provisions governing secrecy’, which introduced the protection of CNI in national intelligence service tasks.
[25] SMD-I-013 on the computer incident response procedure of defence networks (2008), SMD-JIC-011 on computer network operations (2009) and SMD-G-032 on joint cyberdefence policy (2012). These documents are not publicly available.

a widely debated topic in cyber security literature. The National Plan identifies priorities and provides specific guidelines and procedures for implementing the Strategic Framework.

Strengths

A strength of Italy's cyber security policy is its police structures for fighting cybercrime. The Postal and Communications Police Service's work focuses on tackling online child pornography, hacking, computer piracy and e-commerce scams as well as on enforcing copyright protection. The Guardia di Finanza task force focuses on cyber-related fraud. The Carabinieri have an ICT security unit and special investigation branches for cybercrime.

Another strength is the country's computer-incident response centres, which include the cyber security centres of excellence of the Ministry of Defence and of Selex ES, a division of Finmeccanica. Selex ES, in partnership with Northrop Grumman, also provides NATO with a computer-incident response capability.

Space security policy

Background: the development of Italy's space assets

Italy's space programme dates back to the early 1960s with the San Marco Project, which boosted the creation of the national space industry. This project made Italy the third country in the world to launch a satellite (after the United States and the Soviet Union), in 1964.

Between 2007 and 2010, Italy launched Cosmo-SkyMed (COnstellation of small Satellites for Mediterranean basin Observation), a constellation of four Earth observation and imaging satellites. The satellites are used for both civilian and military applications, including civil protection. They were also employed for disaster relief in Asia, in the Caribbean and following the Abruzzi earthquake in Italy. The country has also developed Sicral (Italian system for confidential communications and alerts), which provides secure communications to the Italian military and NATO countries. Launched in 2001, Sicral 1 has played an important role in Middle East operations, particularly in Iraq and Afghanistan. Sicral 2 will be operational by the end of 2014. In February 2014 Italy launched Athena-Fidus (Access on THeatres for European allied forces NAtions-French Italian Dual Use Satellite), a next-generation communications satellite.

Strengths

A strength of Italy's space policy is its scientific-industrial partnerships for R&D. The San Marco Project was created as a partnership between the Italian National Research Centre, the Italian air force, and the University of Rome in collaboration with NASA in the United States. It resulted in the creation of the Via Tiburtina space industrial cluster. Located in a suburb of Rome, it is an innovation hub similar to Silicon Valley and the Cambridge Cluster. The close proximity of space companies, academic institutions such as the University of Rome's aerospace engineering school and small and medium-sized enterprises has enhanced cooperation and created a dynamic space industrial base.

Another strength is the country's international cooperative initiatives. Finmeccanica and the French firm Thales have two joint ventures: Thales Alenia Space and Telespazio. Both Sicral and Athena-Fidus arose from these joint ventures. Italy also participates in major European programmes such as the Earth observation programme Copernicus and in satellite navigation programmes such as Galileo and the European Geostationary Navigation Overlay Service.

Italy's strength also lies in the joint management of military and dual-use satellites by PPPs. Athena-Fidus is managed by a bilateral scientific–industrial PPP that includes the Italian and French ministries of defence and the Italian and French national space agencies. Sicral is managed by a PPP consisting of the Italian Ministry of Defence and Thales Alenia Space. Cosmo-SkyMed is managed by a scientific-industrial public-private partnership that includes the Italian defence ministry. These management models increase flexibility in the design, operation and support of space assets.

Italy has also invested in developing ground control stations. Originally built in 1963, the Fucino Space Centre remains the largest civilian ground station in the world.

Cyber and space policy

Italian institutions and industry place a high priority on the protection of both cyber and space infrastructure from emerging threats, including advanced persistent threats. The cyber protection of space assets implies the protection of data transmission links between satellites and ground stations. The data transmission links of Italian military telecommunications satellites are secured from jamming, spoofing, tampering and cyber attacks. As the military applications of dual-use satellites must meet the same rigorous security requirements as military satellites, the military applications of dual-use satellites such as Cosmo-SkyMed also have defences against cyber attacks.

The country also emphasizes the protection of ground control stations. Military ground control stations are guarded against both physical and cyber attack. The Fucino Space Centre contains a securitized ground segment for the management of Cosmo-SkyMed's military applications. This is interoperable with the civilian teleport.

The Italian armed forces consider cyberspace to be a critical element of a multidimensional battlefield. They have developed cyberdefence doctrines for the air, sea, space, cyberspace and electromagnetic domains. The Italian air force views cyber protection of data links between satellites and unmanned aerial vehicles (UAVs, or drones) as vital. It frequently uses UAVs for strategic reconnaissance during operations abroad. The combined use satellites and UAVs is an emerging model for area monitoring and maritime patrolling. This implies the extensive use of a mix of imaging satellites and UAVs to complement satellites' operational endurance. This gives command-and-control centres greater shared situational awareness and a more effective operational picture. The Italian military is also leading the way to the emergence of a new combined air, space and cyber doctrine.

Japan’s Cyber and Space Security Policies

Dr Kazuto Suzuki

Cyber security policy

A major strength of Japan’s cyber security policy is its public-private partnerships. Japan views cyber security not only as important for defence but also as an opportunity for its industry to improve its international competitiveness. The Japanese electronics industry, which has faced strong foreign competition, has found that it needs to develop more advanced security technologies and products in order to compete in the international market. With the emergence of the ‘internet of things’, it predicts an explosive growth in the necessity of incorporating cyber security protection into everyday physical objects as they become increasingly internet-connected over the coming years. The Japanese government also understands the industrial implications of cyber security: its latest Cybersecurity Strategy,[26] adopted in June 2013, emphasizes the country’s goal of becoming the world’s most advanced IT country.[27] Its aim is to construct a ‘world-leading’, ‘resilient’ and ‘vigorous’ cyberspace that leads to a cyber society that is ‘full of innovations.’ It also underlines the importance of a risk-based approach, developing capabilities to meet various kinds of risk by partnering with other stakeholders to share responsibilities.

A weakness of Japan’s cyber security policy is its lack of focus on national security risks. Its Cybersecurity Strategy underscores commercial and industrial aspects but the national security implications remain vague and undefined. The document defines ‘cyber attacks’ in a narrow sense, viewing them as attacks on commercial or government IT infrastructure. However, it does not emphasize the potential consequences of such attacks. In other words, Japan views cyber security as an issue that concerns primarily the security of IT systems but not the underlying critical infrastructure such as power plants and the electricity grid, telecommunications, railway systems and so forth, which depend on those IT systems. Although the Cybersecurity Strategy addressed the importance of protecting critical infrastructure, it provides guidelines and action plans only for governmental agencies, not for the operators of that critical infrastructure.

Space security policy

The strengths of Japan’s space policy include a combination of high technological standards and political commitment. For many years, Japan’s space policy focused on technological development, on catching up with other advanced countries. Japanese launchers are, technologically, more sophisticated than those of Europe and the United States. Japanese satellites provide high-quality services with complex technologies. But this technological sophistication has not made Japanese industry competitive because market demand is for cheaper spacecraft that have a proven track record. Because the high cost of R&D makes Japanese spacecraft so expensive, they have not been proven to be reliable owing to a lack of launching opportunities. To address this and other challenges,

[26] A provisional English-language translation of the document is available at http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf.

[27] Ibid., p. 3.

the Diet passed the Basic Space Law in 2008, which established the Office of National Space Policy in the Cabinet Office, tasked with coordinating Japan's overall space policy, and created a ministerial portfolio in the cabinet to oversee it. (Previously, various government ministries had developed elements of space policy independently.) This aims to make Japanese space policy and industry more competitive and reliable.

A weakness of Japan's space policy is its lack of focus on security and defence aspects. Japan abided by a self-imposed restriction on the use of space for military purposes for many years. Conforming to Article 9 of its Constitution (renouncing war as a means of settling international disputes), it limited the military applications of space technology from the onset. The country's space programme is centred on the principle of 'peaceful' use, which it considered to mean 'non-military' use until recently.

However, the 2008 Basic Space Law stated that one objective of Japan's space activities is to contribute to the country's national security. It also reinterpreted 'peaceful' use to mean 'non-aggressive' use, which is more closely in line with international community norms. This has opened the way for the possible use of space for defensive purposes. Indeed, the Ministry of Defence is gradually recognizing the importance of having space assets. This is particularly true in view of the nuclear and missile threat from North Korea as well as recent disputes with China. Moreover, the country is increasingly taking part in international peacekeeping operations worldwide, and the United States is applying political pressure on Japan to contribute to space situational awareness activities as part of these operations. But as the defence ministry does not have the technical capability to engage in space programmes, space at present has a limited role in defence policy.

Cyber security and space security

The Japanese public and private sectors have a limited capability for dealing with cyber security challenges to space-based platforms. There is no institutional linkage between the cyber and space communities, and key decision-makers in each community do not realize that they need to communicate with one another. In most cases, the cyber security threat to space-based assets is thought to be preventable if the system is robust enough. The Japanese Aerospace Exploration Agency requires all spacecraft to incorporate cyberdefence systems into their hardware, but this is the extent of its efforts to promote cyber security. There is some security awareness of the need to protect ground stations but this is not focused on defence against cyber attack. Thus awareness of cyber and space security risks and the capability to handle them are quite primitive at this time.

Russia’s Information Security Policy

Oleg Demidov

Russia’s information security concept

Russia’s cyber security policies have several specific features that constitute both its key advantages and its weak points. Its whole approach, especially its foreign policy dimension, is built on the concept of information security. This encompasses a broad range of content issues, including propaganda and psychological operations conducted through information networks. In fact, the term ‘cyber security’ does not exist in Russian legislation or in any adopted doctrines. The Russian government used the term for the first time in a draft document, the Concept of Russia’s Cyber Security Strategy, which was circulated in January 2014.

Impact on Russia’s organizational structure

Russia’s focus on information security has far-reaching consequences not only at the doctrinal level but also for the policy-making process and the distribution of powers within the government. Owing to information security’s broad scope, responsibility for these issues is divided among a number of government agencies and ministries. The major ones are the Federal Security Service (FSB) and the Federal Protective Service (FSO), other civil regulators (the Ministry of the Interior, the Ministry of Communications and Mass Media, the Ministry of Energy and the Federal Service for Technical and Export Control) and the military (the Ministry of Defence and the General Staff of the Armed Forces’ Main Intelligence Directorate). In addition, the Security Council and the Ministry of Foreign Affairs are responsible for the development and promotion of international information security, i.e. for the national approach to global legal regulation of the information space.

The variety of government bodies involved in regulation allows Russia to distribute competencies and to allocate specialized resources to achieve its information security goals. A drawback of this organizational framework is that Russia lacks a single coordinating body that oversees all major information security issues. This can result in ambiguity and an overlap of responsibilities. For example, Russia is currently establishing an information operations force (‘information troops’) and capabilities under the command of the General Staff of the Armed Forces in the Ministry of Defence. But other bodies, such as the FSB or the FSO, may believe that the troops should come under their authority.

A more general implication of the diversified structure of policy-making bodies in charge of information security affairs is the lack of single, comprehensive legal policies in some segments of information security. Thus far, this has not resulted in any serious failures of foreign policy issues and initiatives. On the other hand, it has at times introduced non-compliance and contradictions among domestic laws, orders, strategies and other forms of regulation. One example is Russia’s legislation on critical information infrastructure (CII).[28] At least three pieces of legislation have been proposed and

[28] Executive Order of the Government of the Russian Federation, dated 23 March 2006, No. 411-pc, ‘The list of critical infrastructure objects of the Russian Federation’. Access to the document is limited but is available to the author.

debated by different bodies since 2006,[29, 30] including the recently proposed legislation of 2014,[31] but there is still neither a single set of legal definitions nor a comprehensive legal regime to protect CII from information and other threats. And the Conception of Russia's National Cybersecurity Strategy, drafted in 2013, has also introduced some new definitions for CII and measures for its protection.[32] Moreover, the list of federal bodies in charge of protecting CII is broad and not always definitive; this can lead to clashes of jurisdiction and the duplication of functions.

Cyberdefence capabilities

One of the strengths of Russia's information security policy is the greater protection of a broader range of critical infrastructure from cyber threats than in other countries. In particular, it is well guarded against internet-enabled attacks on critical infrastructure pertaining to information systems and industrial facilities: only 3–5 per cent of Supervisory Control and Data Acquisition (SCADA) systems in Russia can be accessed through the internet; and even then, the majority of these systems are air-gapped, or completely isolated from the public internet. This is a direct result of a general regulation policy that follows a conservative approach to connecting SCADA systems and other information systems of industrial facilitates to the internet. By contrast, the share of SCADA connected to the internet in the United States, South Korea, the United Kingdom and a number of other developed countries may reach 35–40 per cent, resulting in a corresponding increase in the number of vulnerabilities and the level of risk.

Russia is still significantly behind the US in terms of its cyber-attack capabilities. But the situation is changing rapidly: Russia announced in May 2014 the creation of its 'information troops', which will become operational in the coming months. Although this force, which will consist of several hundred troops, cannot rival the size of the US Cyber Command – which has more than 3,000 operatives – it nonetheless creates and provides proactive potential in the information space that is new to the Russian military. The armed forces also have a clear advantage over most of their Western counterparts, such as those in the United States, the United Kingdom and France in terms of dependence on information systems. In the longer term, Russia's development of its information operations force may reduce the gap between it and other major 'cyber powers' such as the United States in offensive capabilities.

GLONASS satellite navigation system

Russia's national assets in outer space, including its global navigation satellite system (GNSS), are more vulnerable. Russia owns one of the two major GNSS services in the world, GLONASS (Globalnaya Navigatsionnaya Sputnikovaya Sistema). The other, GPS (Global Positioning System),

[29] General Guidelines of the state policy in the field of security protection of automated industrial and technological process control systems at critical infrastructure objects of the Russian Federation,. Security Council of the Russian Federation, 4 July 2012; http://www.scrf.gov.ru/documents/6/113.html (last accessed 13 August 2014).

[30] Decree of the Government of the Russian Federation, dated 2 October 2013, No. 861, Moscow. On confirmation of the Rules of informing by the actors of the fuel and energy complex about the threats and committed acts of unlawful interference at the objects of fuel and energy complex. Rossiyskaya Gazeta, 3 October 2013; http://www.rg.ru/2013/10/03/tek-reyderstvo-site-dok.html (last accessed 13 August 2014).

[31] Departmental Order on confirmation of requirements to the protection of data in automated industrial and technological process control systems at critical infrastructure objects, potentially hazardous objects and objects posing special hazards to people's health and safety and the environment. Project Passport. United portal for the information on elaboration of projects of legislative and regulatory acts by the Federal agencies of executive authority and on the results of their public discussions, 14 February 2014; http://regulation.gov.ru/project/12434.html (last accessed 13 August 2014).

[32] Conception of the National Cybersecurity Strategy of the Russian Federation (Project), 30 January 2014, official website of the Council of Federation of the Federal Assembly of the Russian Federation; http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (last accessed 13 August 2014).

is owned by the United States. GLONASS includes a group of 24 satellites that transmit two types of signals:[33] an open signal for civilian use, which is less precise and a protected signal for military use, which has increased precision. The protected signal[34] can contain up to 36 kilobytes of data and require up to 12 minutes for transmission. As with GPS, GLONASS is vulnerable to jamming, which is a major information security risk to Russia's global navigation system.

Moreover, the Russian armed forces' increasing reliance on GLONASS-enabled systems may partially erode the advantage that a lower dependency on information systems currently gives them over the West. In 2010, the Russian armed forces introduced GALS-M1 equipment, which are navigation devices that use GLONASS technology and can be operated on numerous models of military vehicle and weapon system. This increases the armed forces' combat potential but also brings vulnerabilities from jamming and other electromagnetic countermeasures to these vehicles and systems.

Geographic reach

The biggest obstacle to the further development of GLONASS is not its cyber vulnerabilities but its geographic reach. GLONASS itself is global but it still does not provide adequate precision (especially for military purposes) in a number of geographic locations (near the equator etc.) owing to an insufficient quantity of Earth monitoring and augmentation stations outside Russia. At present, there are 46 GLONASS ground stations on Russian territory, eight in neighbouring countries, three in Antarctica and one in Brazil. This is not sufficient for a global network and cannot compete with GPS, which has more than 100 stations around the world. Russia plans to build seven more stations abroad in 2014. But in order to provide a uniform global signal quality, it also needs stations in North America, South Asia, Africa and beyond.

This is becoming more difficult to achieve today given the continuing deterioration of Russia's relations with the West. As a result, the industry that produces combined GPS/GLONASS devices may fall victim to diplomatic battles and 'sanction wars'. This industry is led by IT giants such as Explay and Lenovo and is aimed primarily at end-user dual-system devices for civilian users. The combination of these two systems makes sense, as each system has different 'strong points' in terms of coverage and quality of signal (e.g. GLONASS is better than GPS near the poles). If Russia and the United States continue to clash, and perhaps more intensely still, and to apply sanctions to each other's satellite navigation infrastructure, the industry based on combined GPS/GLONASS devices may stagnate or eventually disappear – a disadvantage for civilian Russian users as well as for users in many other countries.

Russia–West relations

The impact of increasing tensions between Russia and the West is also being felt in the information security sector. In March 2014 the United States suspended the work of the 21st Working Group on Threats to and in the Use of ICTs in the Context of International Security, established under the US-Russia Bilateral Presidential Commission. The Working Group was established in 2013 as a step in implementing a series of bilateral agreements with Russia that had been signed in June 2013 by President Obama and President Putin. The agreements involved the implementation

[33] FDMA (Frequency Division Multiple Access) and CDMA (Code Division Multiple Access) signals.
[34] L1, L2 configurations.

of confidence-building measures in cyberspace and promoted an unprecedented level of active collaboration between the two Cold War-era rivals. Concretely these agreements would have put in place an information exchange hotline between the Kremlin and the White House, a bilateral group of experts to discuss cyber security issues, a mechanism for direct communication and cooperation between national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), and direct communication links between the national Nuclear Risk Reduction Centers.

The general freezing of these agreements, which might follow from a further deterioration of US–Russia bilateral relations, would show how the general political environment imperils encouraging prospects for collaboration. This is to be avoided if we want to build a global framework to counter threats in cyberspace and to overcome security challenges in outer space.

Conclusions

In a broader perspective, one of the major challenges facing Russia is the effective synchronization and integration of its efforts in information security on the levels of domestic regulation and global initiatives. Owing to the transborder nature of the ICT and global connectivity of the internet, any specific model of domestic IT regulation would be genuinely efficient and advantageous only if it were incorporated into global practices and approaches. This is why the foreign policy dimension, its future now highly controversial, remains vitally important for Russia’s information security policy.

On the one hand, political clashes with the West and continuing contradictions over legal regulation concepts and governance practices in the IT sector threaten to undermine global perspectives of Russia’s ICT-security paradigms. On the other hand, Russia’s leadership among the countries calling for more responsible internet governance (i.e. its internationalization) raises its chance to seize the post-Snowden moment and finally promote many of the initiatives that it has been proposing since 1998. Joining forces in this effort with the BRIC states (Brazil, Russia, India, and China) and other countries and stakeholders irritated and spurred to action by the Snowden case might bring it strong support.

Changing the rules of the game globally would also enable the realization of nationwide projects such as the hybrid digital sovereignty model (from hardware to software applications level), the localization of data and content regulation. In the move towards these goals, the win-lose confrontation logic with the West and other stakeholders must be avoided, as must a digital arms race, which might result in cyber conflicts.

The United Kingdom's Cyber and Space Security Policies

David Livingstone

Background

The cyber security of the United Kingdom is a national policy priority, with 'cyber' one of the top four issues identified in the National Risk Assessment. Maturing steadily since the first formal iteration of the National Cyber Security Strategy in 2009 and benefiting from a sizeable public investment of £860 million between 2011 and 2016, the UK approach to cyber seeks to balance the need to provide internet-based platforms for economic growth and innovation with the need for increased protection against a sophisticated and well-resourced set of threats. On the international stage, the UK has taken a leading role in developing the global debate on cyber issues, underpinned by confidence in its own approach to the cyber insecurity phenomenon that emphasizes the protection of both national and international business domains. Between 2011 and 2013 some £14 million (5.4 per cent) of cyber security spending was allocated to engaging with the private sector and to underpinning new initiatives in education and awareness. An authoritative study places the UK as a leading country among the G20 in preparedness for cyber attacks while also developing a strong digital economy.[35]

In contrast to cyber security, the UK government's complementary policies relating to the safeguarding of assets in the space sector are less well developed. The government published its first Space Security Policy (SSP) in April 2014.[36] The document points to the UK's increasing national dependency on satellite services and the need for a coordinated approach in order to increase resilience in the sector, which would once again help the UK to play a leading role in European space security. Here too, the UK sets out to lead the security debate at the international level by setting appropriate performance standards within its own jurisdiction.

However, the SSP contains scant detail on addressing the cyber problem in relation to space, particularly regarding the security of space vehicles themselves and their data/control links. In this, we assume that the cyber security of the various satellite missions' ground elements would be addressed by the well-understood instruments relating to the security of CNI. What is less clear is whether there are special considerations for extending those guidelines to space-borne elements. They pose distinct problems, particularly the inability to change a vehicle's hardware if it becomes disabled by cyber attack.

Cyber threats to satellites

The international aspect of cyber and space security is both a critical area and one that is probably most vulnerable to exploitation in the context of very complex supply chains and space-related

[35] Booz Allen Hamilton and the Economist Intelligence Unit, *The Cyber Power Index 2012*.

[36] National Space Security Policy, UKSA/13/1292; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307346/National_Space_Security_Policy.pdf.

operational infrastructure. Satellite services are key targets for a number of cyber threats, as they support a critical level, growing year by year, of functionality within a country's national infrastructure. This means that a single successful attack on a critical node can affect a large number of important national and international capabilities.

Much work would be required to define each and every segment of a typical space mission and to develop strategies to mitigate threats. In the 'upstream' sector, that is, the manufacture, preparation, launch and operation of a space vehicle, many thousands of components are sourced from around the world, and an operational satellite controlled (and its data communicated) through its potentially 30-year life cycle via a communications infrastructure has a unique global footprint. In the 'downstream' sector, the exploitation of satellite-derived services, a good example is data centres: they have a two-way connection to a plethora of stakeholders based in any number of countries, all of which will be working under their own national security guidelines.

The confines of this submission do not allow an analysis of the broad ambit of cyber and space security threats, but we can raise some individual points, simply to illustrate the complexity of the issues involved. We need to look at the integrity of space vehicle systems themselves. What would the consequences be, for example, if a reasonably common piece of software that controls solar panels (and there are only a select number of solar panel manufacturers in the world) were exploited and a significant number of satellites were simply switched off in a single attack? Although new satellites may have configurable control systems, older ones may not, and will thus be less resistant to modern methods of attack.

And if a modern vehicle does have configurable software, how can we future-proof the embedded electronics against emerging or over-the-horizon threats, such as quantum computing gone bad? Do satellite systems have sufficient failover modes to override malicious attacks and at least keep the vehicle functioning while restorative actions are taken? Is there a need to test our satellites for cyber resilience before we launch them? How do systems integrators assess vulnerabilities when suppliers for each mission are based in jurisdictions with less developed approaches to cyber security? Has the International Space Station ever been virus-checked?

Safety measures

The UK National Cyber Security Strategy emphasizes reducing cyber risk by 'getting the basics right',[37] and the UK government has instigated a number of public communications initiatives to reinforce this message. A new strategy, the Cyber Essentials Scheme,[38] identifies the security controls that organizations must have in place in their IT systems in order to be confident that they are mitigating the risk from internet-based threats. Suitably adapted, these can be a cyber security baseline for a truly internationalized space ecosystem:

- Secure configuration for space vehicles and their components, for ground-based infrastructure and for data systems, to reduce current and future vulnerabilities
- Boundary firewalls and internet gateways to provide, at minimum, a basic level of protection where an organization connects to the space-based electronic domain

[37] CESG – 10 Steps to Cyber Security, updated 15 January 2014.

[38] Cyber Essentials Scheme, Summary, BIS 14/698, April 2014; http://insidecybersecurity.com/iwpfile.html?file=apr2014%2Fcs2014_0084.pdf.

- Control of access and administrative privilege management: protecting user accounts and helping to prevent the misuse of privileged access
- ‘Patch’ management, to ensure that the software used in satellites and in associated ground segments is kept up to date
- Malware protection against a broad range of threats and the capability to carry out virus removal

These would be reasonable standards to adopt at the international level in the cyberspace and space domains. They would be the basis for end-to-end system due diligence in the complexity of the global upstream–downstream user–supplier ecosystem. This ecosystem itself is becoming intrinsic to society, and thus more critical and, unfortunately, more prone to attack by those who wish to inflict harm.

The United States' Space Security Policy: Cyber Security Vulnerabilities

Dr Joan Johnson-Freese

The United States has the largest number of satellites in orbit,[39] arguably the most technically advanced assets in orbit and ostensibly garners the most from these assets in terms of military advantages and civilian applications. It is also the country that relies most on these systems. Thus, although space assets are a valuable enabler of the information age and a powerful force-enhancement tool, the United States' dependence on these assets has also created a potential Achilles heel, making the country vulnerable to asymmetric attacks. Both the private sector and the public sector must therefore be proactive in protecting these assets. The question is how.

Cyberdefence of satellites

As bright objects in predictable orbits against a dark sky, satellites are vulnerable to kinetic attack. Moreover, several countries have demonstrated the capability to reach these satellites for potentially hostile purposes. The idea of protecting space hardware, especially satellites, with hardware has elicited much support in recent years in the United States. But the technological difficulties involved have shown that defensive options are limited. Offence is easier and cheaper than defence, as is demonstrated by countermeasures that can be used to thwart missile defence. Furthermore, the potential for debris created by kinetic impacts in space, including defensive ones, would have harmful consequences for all countries with activities in space. As a result, countries are growing increasingly concerned over cyber attacks on satellites and are attaching greater importance to cyberdefence.

Cyber attacks on satellites are on the rise. The US-China Economic and Security Review Commission alleged in 2011 that cyber attacks on US satellites had taken place, citing incidents in 2007 and 2008. According to its report, hackers had achieved 'all steps required to command' a NASA satellite and had interfered with other satellites too. More recently, the military is recognizing the vulnerability of military satellite communications terminals and very small aperture terminals (VSATs) used by military units. US vulnerability is considered high owing to heavy reliance on satellites by both the civilian and military sectors. Both sectors are actively involved in addressing these vulnerabilities.

Civilian/private sector activities. Private companies provide cyber protection for ground stations, satellite testing equipment and satellite operations. Hacking can include industrial espionage, stealing trade secrets and general economic espionage. The US charged five Chinese military officers with such crimes in May 2014. Private companies are working to thwart these attacks by countering not only known issues but also 'zero-day' exploits. These exploits make use of 'zero-day' vulnerabilities, which are vulnerabilities that have not yet been identified, so no patches or defences exist against them. The most effective way to combat threats from both inside and outside the network is by 'tamper-proofing' the algorithms, an approach that the military is increasingly using as well.

[39] 502 satellites of 1,167, according to the Union of Concerned Scientists database, updated as of 31 January 2014; see http://www.ucsusa.org/nuclear_weapons_and_global_security/solutions/space-weapons/ucs-satellite-database.html.

Military/public sector activities. Military officials have emphasized that building defences into space systems is the preferred way to approach the problem, rather than trying to retrofit or to react after the fact. But acquisition regulations are cumbersome and have already proven a hindrance, at times impeding the maximization of design choices. Officials have complained that the acquisition process for military satellites is not sufficiently responsive to keep up with the latest threats. Many cyber analysts believe that the US civilian/private sector can innovate more quickly to response to the cyber threat.

Blurring of the distinction between offensive and defensive cyber capabilities

The United States' policy is to employ 'active cyber defense' capabilities to defend military networks and systems and to conduct 'full-spectrum military cyberspace operations' when directed to assist in this regard. The term 'active cyber defense' is commonly understood to include offensive actions in cyberspace taken with defensive purposes in mind. These actions are tactical operations with the limited goal of mitigating an immediate hostile act. The US Cyber Command, the military's combatant command tasked with cyber operations, announced an increase in personnel from 900 to more than 4,000 in 2013.[40] One of its tasks is to protect the computer systems undergirding 'electrical grids, power plants and other infrastructure deemed critical to national and economic security'.

Recognition of the widening reach of cyber threats across the public and private spectrum has led to several governmental initiatives to address the threats. The National Defense Authorization Act for Fiscal Year 2014 called for 'control of the proliferation of cyber weapons'.[41] According to the Act, 'The President shall establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate.' This followed the Comprehensive National Security Initiative, signed into law by President George W. Bush in 2008, to defend proactively against network intrusion, guard against the full spectrum of threats through counterintelligence and strengthen the future cyber security environment through education, coordination and research. The National Security Agency has begun to build data centres pursuant to the programme, including a $1.5 billion centre in Utah.

Conclusions

The rising profile of cyber activities related to space hardware, threats to those activities and consequent countering efforts guarantees increased attention to these topics in the US. The first step for both government agencies and the private sector is to sort through the complex problems involved and to identify and implement an approach that balances security with revenue, as the most secure networks can be extremely expensive. The government will probably be hindered by interagency turf battles and intra-agency allocation of resources; while in the private sector, security requirements can slow down operations, costing money and generating resistance.

[40] Pentagon to boost cybersecurity force, *Washington Post*, 27 January 2013; http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.
[41] See http://www.gpo.gov/fdsys/pkg/CPRT-113HPRT86280/pdf/CPRT-113HPRT86280.pdf (Section 940).

There is no choice regarding whether to deal with these issues; it is merely a matter of how to do so. As Mark Maybury, Chief Technology Officer at MITRE Corporation and a former US Air Force Chief Scientist, said in January 2014, 'The single largest vulnerability of space systems today is cyber.'[42] If cyber is indeed the Achilles heel of space systems security, then it is ignored at peril.

[42] Dave Majumdar, 'Space Cyber Attacks: A Wake Up Call', AIAA, 14 January 2014; http://www.aiaa.org/SecondaryTwoColumn.aspx?id=21097.

Part II
Perspectives from International Institutions

An EU View: Comparisons and Establishing Norms in the Cyber and Space Domains

Frank Asbeck

A comparison of the cyber and space domains

The cyber and space domains are both global capabilities. Understanding their common features is therefore paramount. Both domains are omnipresent, and their related applications affect people's everyday lives and countries' economies in a fundamental way. They are connected operationally and share common threats: each depends on the electromagnetic spectrum and on IT infrastructure and they are also exposed to asymmetric vulnerabilities caused by a reduction in barriers to entry.

Naturally not all challenges to the cyber domain apply to the space domain, and vice versa. Space has evolved over the past 60 years from being an exclusive domain of governments to one that also includes commercial satellite owners and operators. An international legal framework governing space activities also exists: The Outer Space Treaty of 1967 establishes states and international intergovernmental organizations as the primary actors in the domain.[43] Furthermore, the UN has a dedicated body, the Committee on the Peaceful Uses of Outer Space, in which member states can engage in dialogue. A number of countries have also enacted national space legislation.

Cyberspace broke free from government control from the outset, accompanied by openness and interoperability. Internet infrastructure is predominantly in the hands of private enterprise; and although governments use the internet for a multitude of purposes, the majority of users are individuals and private companies. It is often difficult, if not impossible, to identify the source of malicious activity in cyberspace. Hostile acts against public infrastructure and economic entities, as well as cybercrime, have become a serious challenge to all governments.

The dual-use nature of the cyber and space domains: establishing norms

As both the cyber and the space domains employ dual-use capabilities, traditional arms control instruments that focus on banning certain technologies are difficult, if not impossible, to apply, not least owing to the problem of effective verification. Accordingly it is important to emphasize norms, guidelines and responsible behaviour for both domains. Best practices can go a long way in advancing the safety, security and sustainability of outer space activities. The EU, for example, has proposed an International Code of Conduct for Outer Space Activities in order to strengthen behavioural norms in this sphere. Over the past two years it has held three rounds of multilateral, open-ended consultations with the aim of securing, in an inclusive and transparent way, broad international support for this voluntary, politically binding instrument. The initiative has benefited greatly from work conducted in a number of relevant forums, especially under UN auspices. In fact, the idea for a code of conduct emerged in response to a 2006 UN General Assembly Resolution. The

[43] According to Article VI of the Outer Space Treaty, 'the activities of non-governmental entities in outer space … shall require authorization and continuing supervision by the appropriate State Party to the Treaty'.

EU believes that such a code is an important contribution to transparency and confidence-building measures (TCBMs) in outer space.

Similarly, international norms and principles for cyberspace can enhance interoperability, openness, reliability and security in this domain. The Cybersecurity Strategy of the European Union, issued by the EU High Representative for Foreign Affairs and Security Policy and the European Commission in February 2013, is the first comprehensive policy document that the EU has produced in this area. However, the EU does not support the creation of new international legal instruments to promote cyber security. It focuses instead on ensuring the enforcement of existing legal norms – such as the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights – in the realm of cyberspace. The EU supports the Budapest Convention on Cybercrime[44] as the model for global acceptance, which, if implemented and applied, promotes international cooperation and thus contributes to cyber security on a wider scale.

If armed conflict were to extend into cyberspace, international humanitarian law and, as appropriate, human rights law would apply. As in space, the EU attributes great importance to TCBMs in the cyber field, including establishing contacts between national cyber authorities, setting up hotlines to react to cyber incidents, engaging in dialogue over cyber security policies and doctrines, and holding regular discussions among policy-makers. The EU therefore welcomes the efforts of the Organization for Security and Co-operation in Europe (OSCE), which in December 2013 agreed a set of confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. It also supports the ongoing discussion on TCBMs in other political frameworks such as the ASEAN Regional Forum.

Without doubt, both domains require the involvement of a combination of government and private actors in order to address common threats. In this connection, situational awareness is the key to maintaining and enhancing capabilities in both domains.

Conclusions

Although cyber and space technologies have stark differences, both domains interact and complement one another and both require similar approaches. They are key war-fighting domains with critical vulnerabilities, both unintentional and intentional, and their national security importance makes them a vital target in a military altercation. Furthermore, hostile acts or acts that are perceived as being hostile in either domain could jeopardize international relations and stability and even lead to conflict. Yet a conflict in either of these domains, and what should be a proportionate response to it, is not well understood today. This could lead to misperceptions, miscalculations and misinterpretations if there is ambiguity about the nature or the originator of a presumed attack. Policy-makers thus need to see the cross-domain similarities in order to address the growing challenges facing the cyber and space fields.

[44] The Convention on Cybercrime was opened for signature by the member states of the Council of Europe, and by non-member states that participated in its elaboration, in November 2001; it entered into force on 1 July 2004; see http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185.

An OECD View: The Growing Risks of Satellite Signal Interference

Claire Jolly

In examining the economic significance of space infrastructure and its potential impact on the global economy, the Organisation for Economic Cooperation and Development's (OECD) Space Forum has identified a number of risks to satellite systems and their users, with interference to satellite signals being an especially important issue. In the wider context of increasing awareness of cyber security threats, governments and the private sector need to develop efficient policies and instruments to handle these growing challenges.

The challenges: increasing jamming of satellite communication links and satellite navigation signals, and the blinding of Earth observation satellites

Signal interference is not a new phenomenon. As early as the 1980s, when commercial satellite broadcasts became available, some interference, intentional and often unintentional, was already taking place. The difference today is that interference can affect the function and reliability of services in many different segments of the orbital infrastructure, i.e. broadcasting, communication links, navigation and positioning, and civilian Earth observation.

Commercial satellite communication broadcasts have suffered the most from various types of 'jamming' over the years. Jamming is also increasingly affecting global navigation satellite systems signals, used in products ranging from smartphones to cars. The 'blinding' of Earth observation satellites' instruments (optical and radar) is a relatively new phenomenon and it is affecting a growing number of scientific satellites over large areas. The different types of signal and data flow failure are often not confirmed until significantly after the event has occurred. The causes may vary: software glitches, natural obstructions that block signals and jamming, whether deliberate or not.

Intentional jamming is increasingly causing problems. In 2009 satellite-positioning receivers using a new air navigation aid at Newark Airport in New Jersey experienced daily data reception breaks. The culprit was a lorry driver who drove by on the nearby New Jersey Turnpike each day and had a cheap GPS jammer to avoid being tracked by his company. It took several months for Federal Aviation Administration investigators to identify the problem and find the culprit.

The way forward: the need for both technical developments and improved governance to deal with signal interference

As reliance on information tools comes to pervade every facet of modern society, a number of OECD and non-OECD countries have developed or are developing national policies to deal with cyber security threats. However, the specificities of satellite signal interference are frequently still not dealt with at this level. National cyber security and space security policies rarely intersect. Nevertheless some countries are already adapting their legal and regulatory frameworks to such threats, putting new instruments in place to deal specifically with satellite signal jammers, e.g. those in the United States and the United Kingdom. Both the private sector and governments must be involved in order to counter these growing threats. Technical developments are needed from industry in order to prevent illicit disruptions, and improved governance mechanisms are required at the national and international levels.

Technical developments. Over the past decade, technical developments to alleviate conflicts over bandwidth allocation and to improve signal protection have been made, at least for satellite telecommunications. They include shielding, frequency hopping, lower power output, digital signal processing, frequency-agile transceivers and software-managed spectrum use. To circumvent intentional and unintentional interference from third parties, most satellite operators and ground-based equipment providers are better informing their users and looking at diverse technical solutions with their networks of customers. These solutions do not resolve all problems – policy and regulatory approaches are needed in parallel – but they contribute to a better awareness of the risks. However, regarding threats to satellite navigation signals and Earth observation data flows, much remains to be done.

Improved governance. Negotiations at both the national and international levels are essential for improving governance, as very different systems must coexist and deal with cyber security threats. As the scope for wireless communication increases, efficient spectrum-allocation will become a more important policy and economic issue. The International Telecommunication Union (ITU) continues to play a major political and regulatory role in arbitrating conflicts about radio signal interference (as demonstrated by the 2012 satellite communications disputes in the Persian Gulf) and to provide best practices. Although governments cannot be forced to apply ITU regulations strictly, most countries do abide by the rules that they set themselves. Without resolving all interference issues, regular improvements in the international regulatory process should nonetheless contribute to a more efficient use of the spectrum. The same issues apply at the national level with competition for the spectrum heating up and as more cybercrime is reported. Recent examples of GPS and GLONASS signal failures and disruption demonstrate that innovative legal responses will need to be reconciled in many countries in order to deal with new forms of jamming.

The UN Structure: The Intersection of Cyber Security and Outer Space Security

Ben Baseley-Walker

This piece is written in a personal capacity and does not necessarily reflect the views of the UN Institute for Disarmament Research or the UN.

The UN cyber regime

The UN system is struggling to develop a comprehensive multilateral cyber policy. Cyber security is a very broad concept, and the various UN organizations have a limited understanding of the issues related to it and their own relevant responsibilities. As cyber policy touches on everything from development policy and economics to warfare and sovereignty, there is no specific organization in the current UN apparatus for coordinating cyber issues.[45]

From a cyber stability and strategy perspective, the UN system has three main components responsible for the creation and implementation of cyber security-related policy:

1. **The International Telecommunication Union (ITU).** As a specialized agency of the UN, the ITU has a clear mandate to support the building of cyber capabilities in UN member states, particularly in developing countries. The ITU carries out wide-ranging work to support cyber resilience, responsible cyber practices, and the need for national and regional cyber policy development. The ITU's Cyber Security Agenda is an important contribution to defining technical and policy baselines for states when approaching the development of cyber policies.
2. **The UN Office on Drugs and Crime (UNODC).** The work of UNODC focuses on cybercrime and its law enforcement applications, especially across boundaries. Its work also encompasses promulgating the tenets of the Budapest Convention on Cybercrime and capacity-building on cybercrime issues at the national and regional levels.
3. **The UN General Assembly First Committee.** The First Committee of the UN General Assembly and related disarmament machinery have touched briefly on the peace and security issues of cyber policy by way of a series of resolutions and Groups of Governmental Experts on Information Security. Although member states consider the topic important, it has not been a major subject of discussions more generally. Several member states have proposed a draft code of conduct on information security for consideration by the UN Secretary-General.

Strengths and weaknesses of existing UN cyber stability and security policy mechanisms

The UN cyber regime is in its infancy. Like many governments and other institutions, the UN system is struggling to adapt to the quickly evolving realities of the cyber domain. The traditional policy creation mechanisms of multilateralism, i.e. a siloed issue or a domain-based approach, cannot

[45] Given this lack of appropriate structures, internet governance mechanisms, such as the Internet Governance Forum and the governance work of the ITU, as well as human rights and privacy aspects of cyber policy, are not included in this assessment. These aspects of cyber policy are of course critical, and clearly they affect traditional security questions. However, they often cloud discussions of cyber strategy.

accommodate the extremely complex and multilateral policy considerations that arise when examining cyber policy development. The UN system is, at its root, a product of the will and interests of its member states, and the fact that governments are having to develop national, regional and multilateral policies simultaneously does not support clear-eyed, inclusive policy development in a UN context.

Another challenge the UN, as an inter-governmental organization, is to allow for the effective participation of the cyber commercial sector, which owns, operates and manages the vast majority of the cyber domain. In addition to the length of time it often takes to secure agreement in a UN forum, there is a concern as to whether UN processes on cyber policy development can remain timely and relevant.

The cyber domain is indeed a globalized environment – a ‘cyber border’ is no more than an intellectual construction. As one of the few truly representative international bodies, the UN is a forum that must be used if a globally relevant cyber policy is to be developed.

The UN space regime

The UN is the major forum for debate about many of the key aspects of multilateral relations to do with outer space. It is also the body under which the five outer space treaties, which form the basis of the outer space legal and policy regime, originated: the Outer Space Treaty (1967), the Rescue Agreement (1968), the Registration Convention (1976), the Liability Convention (1972) and the Moon Agreement (1984).

The UN system has three main components responsible for the creation and implementation of space-related policy:

1. **The Committee on the Peaceful Uses of Outer Space (COPUOS).** Set up in 1959 by the UN General Assembly, COPUOS is the main body dealing with peaceful uses of outer space. Broadly defined, these consist of civil space activities, including remote sensing, launching, space debris and satellite power sources, and space activities for development. COPUOS is supported by the UN Office of Outer Space Affairs (UNOOSA). In addition to its duties as the secretariat of the committee, it is tasked with assisting developing countries to use space technology to meet development objectives under the UN Programme on Space Applications.
2. **The Conference on Disarmament (CD).** As the only standing multilateral disarmament negotiating forum, the CD has had a longstanding item on its agenda dealing with the Prevention of an Arms Race in Outer Space, or PAROS. It is broadly considered to be responsible for discussions and negotiations on the weaponization of space. Several initiatives have been presented in the CD, including a Russian–Chinese draft treaty on preventing the placement of weapons in outer space. The CD, however, has been in deadlock for nearly two decades, limiting the potential for progress. As for wider UN disarmament machinery, the CD is supported by the UN Office for Disarmament Affairs (UNODA). UNODA also works on policy and processes related to disarmament, which includes outer space, but currently it carries out no substantive work on space policy issues apart from secretariat support to the UN General Assembly-mandated 1993 and 2012 Groups of Governmental Experts dealing with transparency and confidence-building in outer space activities.
3. **The Space Services Division of the ITU.** The ITU’s Space Services Division carries out an implementation/coordination role as regards frequency allocation for space systems. This is a

critical component of space activities but it is somewhat isolated from the wider context of space policy development.

Strengths and weaknesses of existing UN space policy mechanisms

The UN space regime is, in many ways, unique. The reality of space activity today is that there is a limited margin, if any, for accepting irresponsible space actors who do not conform to the accepted international norms of space behaviour. The growing dependence of all countries of the world on space services, and the increasing threats to those services such as possible collisions in crowded orbits and the proliferation of space debris, means that the actions of the individual space actor can quickly affect the global community at large. Thus there is really no other option but to develop agreements between *all* space actors if the long-term viability of orbital resources is to be safeguarded. In view of the multilateral nature of the UN forum, it is perhaps the only extant body that can play that role.

However, the UN regime faces several legacy challenges that impede its ability to address future space policy development effectively. The most significant of these hurdles is the dichotomy between 'peaceful' uses of outer space and non-peaceful uses. The reality of today's space environment is that many of the key issues cut across the civil-military spectrum. For example, the question of space debris involves improving launch standards and responsible end-of-life disposal of satellites as well as dealing with the risk of debris being produced as a by-product of the intentional kinetic destruction of space assets. These issues cannot be compartmentalized. The fact that the EU chose to introduce its proposal for an International Code of Conduct for Outer Space Activities – a document that attempts to address space security concerns holistically – in a process outside the UN framework clearly shows that current UN policy mechanisms may be inadequate to serve the evolving needs of the international community.

Linkages

To date, the UN system has not been significantly engaged in making linkages between the outer space and cyber sectors. UN organizations such as the UN Institute for Disarmament Research (UNIDIR) have carried out substantive analysis of and held conferences on the potential interactions and their implications; but at the policy-making level, few connections have been made. But as satellites are, in many respects, simply 'servers in the sky' that are increasingly critical to the daily life of any global citizen, the technical aspects of forming international policy regarding how to safeguard data flow and the utility of linked space and cyber services needs to be addressed in more depth.

Acronyms

ASAT	Anti-satellite weapon
ASEAN	Association of Southeast Asian Nations
CD	[UN] Conference on Disarmament
CERT	Computer Emergency Response Team
CII	Critical information infrastructure
CNI	Critical national infrastructure
COPUOS	[UN] Committee on the Peaceful Uses of Outer Space
CSIRT	Computer Security Incident Response Team
DDoS	Distributed denial of service
EU	European Union
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema (Global Navigation Satellite System)
GPS	Global Positioning System
ICT	Information and communications technology
ITU	International Telecommunication Union
NCSP	National Cyber Security Policy
OECD	Organisation for Economic Cooperation and Development
OSCE	Organization for Security and Co-operation in Europe
PAROS	Prevention of an Arms Race in Outer Space
PPP	Public-private partnership
PPWT	Prevention of the Placement of Weapons in Outer Space
R&D	Research and development
SCADA	Supervisory Control and Data Acquisition
TCBM	Transparency and confidence-building measure
UAV	Unmanned aerial vehicle
UNIDIR	UN Institute for Disarmament Research
UNODA	UN Office for Disarmament Affairs
UNODC	UN Office on Drugs and Crime
UNOOSA	UN Office for Outer Space Affairs
VSAT	Very small aperture terminal

About the Authors

Lead author

Caroline Baylon is Research Associate in Science, Technology and Cyber Security in the International Security Department at Chatham House, where she specializes in cyber security, internet governance, and the science and technology aspects of international security. Caroline holds an MSc in Social Science of the Internet from Balliol College, University of Oxford.

Contributing author

Dr Patricia Lewis is Research Director of the International Security Department at Chatham House, where she founded the Project on Cyber Security and Space Security. Her former posts include Deputy Director and Scientist-in-Residence at the Center for Nonproliferation Studies at the Monterey Institute of International Studies, and Director of the UN Institute for Disarmament Research (UNIDIR).

Contributors

- Frank Asbeck, Principal Adviser for Space and Security Policy, European External Action Service, European Commission
- Ben Baseley-Walker, Programme Lead, Emerging Security Threats Programme, UN Institute for Disarmament Research
- Dr Claudio Catalano, Senior Analyst, Research Department, Finmeccanica
- Oleg Demidov, Research Manager, Cybersecurity and Internet Governance, PIR Center
- Dr Joan Johnson-Freese, Professor, National Security Affairs, US Naval War College
- Claire Jolly, Head, OECD Space Forum
- Vincent Joubert, Research Fellow, Fondation pour la Recherche Stratégique
- David Livingstone, Consultant, Satellite Applications Catapult, and Associate Fellow, Chatham House
- Dr Xavier Pasco, Senior Research Fellow, Fondation pour la Recherche Stratégique
- Dr Rajeswari Pillai Rajagopalan, Senior Fellow in Security Studies, Observer Research Foundation
- Professor Kazuto Suzuki, International Politics, Graduate School of Law, Hokkaido University
- Dr Guoyu Wang, Deputy Director, Institute of Space Law, Beijing Institute of Technology, and Academy Senior Fellow, International Security Department, Chatham House

Acknowledgments

The authors would like to thank Finmeccanica UK for its generous funding and support of this research project. In particular, the active engagement of Peter Young, Chief Executive Officer of Telespazio Vega UK, as well as Dr Carlo Musso, Head of the Research Department at Finmeccanica, has been instrumental in its success. We are also grateful to Prof. Richard Crowther, Chief Engineer at the UK Space Agency, for his valuable comments during the preparation of this report. In addition, David Livingstone, Associate Fellow at Chatham House, played a key role in the development of the research project seminars. Finally, we should like to thank all of the contributors to this report, as well as the participants who took part in the seminar discussions. Any errors of fact in this paper are our own.