IAC-13,E3.4,8x16989

TOWARDS A CYBER-SECURITY POLICY FOR A SUSTAINABLE, SECURE AND SAFE SPACE ENVIRONMENT

Luca del Monte
European Space Agency - Paris, France
Luca.del.monte@esa.int

The space critical infrastructure is an enabler of modern society interconnectivity backbone, but has now become both vehicle and target of cyber-attacks: its disruption would be critical to the whole society and would endanger commercial, institutional and defence activities. Space and Cyberspace are (together with the Air and the High Seas) part of the Global Commons, physical and virtual domains that no states have sovereignty over, and that are available to everyone. Ensuring freedom and access to these areas is a key trade and security challenge of the 21st century, and it is likely that these commons will be an arena where the current and future political, economic and military rivalry will be played out. In the past, 'civil' and/or 'scientific' space missions were unlikely objectives of malicious attackers, differently from military and from commercial telecommunication missions that have traditionally been highly protected. However, this view is now changing, as demonstrated by some serious security incidents which are progressively becoming publicly known. This paper presents the approach and preliminary results of an ESA preparatory study aiming at raising awareness in the space community about the cyber-security issue and at establishing elements of a policy allowing all stakeholders to define their own specific cyber-security requirements.

I. INTRODUCTION

Nearly every aspect of modern society increasingly depends upon information technology systems and networks. This includes computer interconnectivity, particularly through the widespread use of the Internet as a medium of communication and commerce. While providing significant benefits, this increased interconnectivity can also create vulnerabilities to cyber threats. Pervasive and sustained cyber-attacks against European countries could have a potentially devastating impact on national and international systems, disrupting the operations of governments and businesses and the lives of private individuals. Accordingly, in the US, the Government Accountability Office (GAO) has designated federal information security as a government-wide high-risk area since 1997 and, in 2003, expanded it to include protecting systems and assets vital to the nation (referred to as "critical infrastructures")[i]. Critical infrastructures are systems and assets essentials to the nation's security, economy, and public health and safety, some of which may be owned by the private sector. These assets rely on networked computers and systems, thus making them susceptible to cyber-based risks. Such network connectivity – widely enabled through space-based systems and services - is constantly increasing and has become ubiquitous. This is the so-called cyberspace, defined in NATO's Cyber Defence Concept as "*a digital world generated by computer networks in which people and computers co-exist, and which includes all aspects of online activity.*[ii]"

Space has a strong strategic value, as it increasingly allows national and international Institutions as well as the industrial sector to gain independence, scientific and technological prestige, and the capacity to act as a global actor. Space is synonymous of a whole chain of strategic technologies and activities: from launching to the establishment of satellite telecommunications, from meteorology to navigation, space assets appear as a strategic set of infrastructures, meaning that they cannot be backed up by other types of ground networks, and that their disruption would be critical to the whole society. Space assets also should therefore be considered "critical infrastructures", as their disruption would endanger both civilian and defence activities.
The most basic question of what constitutes the space domain, however, is not answered in international law. Although the 1967 Outer Space Treaty and its follow-on agreements do not specify the boundaries that differentiate space from the upper reaches of national airspace, a norm has developed that defines space as the point above the Earth at which satellites stay in orbit[iii].

As it is now clear, space and cyberspace have many similarities and are closely interwoven, yet each has its own distinct properties, and thus they need to be addressed both individually and as a whole. European Countries have highly globalized economies that depend on assured access to these domains, and the free flow of goods, services, people, and information. The commonalities and interlinks between the space and the cyber-space domains have been well described by the doctrine of the Global Commons[iv] providing a useful lens through which to view the world as a complex, globalized whole that depends for its security and prosperity on access to four domains: maritime, air, space and cyber. "Commons" comes from Roman law, which categorized everything in the world according to the rights of ownership[v]. Space and cyberspace are hence regions which do not fall under the jurisdiction of any nation. It is in, through, and from the Global Commons that trade, communications, transportation, and security operations take place.

II . SPACE MISSIONS IN A CONTESTED CYBER-SPACE

One important consequence of what has been exposed in the introductory paragraph is that the concept of cyber-security of space systems should therefore be conceived not only in terms of fighting cyber-threats which are *vehicled* through space systems, but also in terms of security, protection and reliability of space technologies and systems themselves, as potential *targets* of the cyber-threats.

The possibility to operate space mission payloads across networks through public internet connectivity (or through Virtual Private Networks which, although secluded, are mutually interconnected through the net) opens up many threats against space-based assets and services, threats that did not previously existed. As a result, civil space missions must take now into account a wide variety of security menaces. These preoccupations have been substantiated by some serious security incidents which are, only now, progressively becoming publicly known.

On October 20, 2007, a very well-known Earth Observation satellite experienced 12 or more minutes of interference. Again, on July 23, 2008, the same satellite experienced other 12 minutes of interference. The responsible party did not achieve all steps required to command the satellite, but the service was disturbed.

Analogously, on June 20, 2008, another Earth observation satellite experienced two or more minutes of interference. This time, the responsible party achieved all steps required to command the satellite but did not issue commands. Some weeks later, on October 22, 2008, the same system experienced again nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands. The above-mentioned attacks affected satellites used for earth climate and terrain observation. The hackers have used the Internet connection to get into the ground station's information systems.

Access to a satellite's controls could allow an attacker to damage or destroy the satellite. An attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission. Military theorists have developed a holistic view of counterspace operations. They advocate for the use of both "soft" kill (i.e., informational, temporary, or reversible) attacks and "hard" kill (i.e., destructive or permanently disabling) attacks against every aspect of space power: ground-based systems, space-based systems, and communications links.

Partial infiltration could allow the attacker to share data from the compromised satellite, though this would likely be detected given the limited bandwidth of the orbiter (e.g. this is how the current attacks were identified). A high level of access could reveal the satellite's capabilities or information, such as imagery, gained through its sensors. Opportunities may also exist to compromise other terrestrial or space- based networks used by the satellite. Command-and-control infiltration could give more useful capabilities, most notably the ability to trigger some sort of mechanical/electrical overdrive, which could damage critical devices like imaging lenses or the communications antenna. Or they could be used to provide equally damaging misinformation to the victim. If executed successfully, such interference has the potential to pose numerous threats, particularly if achieved against satellites with more sensitive functions. For example, access to a satellite's controls could allow an attacker to damage or destroy the satellite. The attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission.

However, a completely different range of cyber threats is today also menacing our space systems and could results in total loss of mission even far from the boundaries of the Earth orbit, well beyond the attack capability of operational hackers. Unlike previously described cyber-attacks, this new generation of cyber threats (e.g. Stuxnet) does not go after information, but rather after physical infrastructure[vi]. In the space domain, these attacks could exploit weakness/"back doors" in the mission industrial supply chain (e.g. Trojan or latent virus), including customer furnished payloads. As a matter of example, the computer worm called W32.Stuxnet did actual physical damage to Iran's nearly completed Natanz nuclear complex in 2010, by causing the centrifuges used for uranium enrichment to run erratically and, over time, self-destruct. Stuxnet also was able to completely hide any traces of its activity from the systems used by technicians to monitor the centrifuges.

Scientists first learned of vulnerabilities in the Supervisory Control and Data Acquisition (SCADA) system, the same operating system that was targeted by Stuxnet, in 2008. Many critical infrastructure facilities throughout the world, such as dams and electrical grids, run on these same SCADA systems, and there is now concern that they may be vulnerable to attack, possibly from a manipulated or next-generation version of Stuxnet. Even the most sensitive state and commercial facilities rely to some extent on proprietary commercial technologies like SCADA.

Within the context of a space mission supply chain, some spacecraft on-board components available on the market may contain spyware or logic bombs, which, when triggered, will render the system useless or worse, vulnerable to espionage or sabotage, even when far from the Earth orbit. These and other vulnerabilities may not become apparent until the systems are under attack. When that happens, fixing the problem will require coordination between both supplier and user, which raises its own questions regarding the limitations of trade restrictions, or laws that govern potentially dual-use technologies.

III . CYBERSECURITY AT THE EDGE OF THE SOLAR SYSTEM

As explained before, the concept of cyber-security of space systems needs to be conceived not only in terms of fighting cyber-threats which uses the space systems as vehicle, but also in terms of security and reliability of the space technologies themselves (potential target), as key parts of a European critical infrastructure network. In the past, 'civil' and/or 'scientific' space missions were unlikely objectives of malicious attackers, differently from military and from commercial telecommunication missions that have traditionally been highly protected. For many years Space Agencies and commercial operators worldwide have considered themselves to be potential targets of cyber-attacks as any other user of the cyberspace. However, this view (as demonstrated by the serious security incidents briefly described in the above paragraphs) is now changing.

The European Space Agency (ESA) is no exception in this picture. The Agency as an Institution is a target and cyber threats are common in ESA. The most common: viruses, Trojans and worms are distributed by amateur hackers. However some are more serious, sometimes targeted, security attacks. As a matter of fact, ESA's role in programmes such as Galileo, GMES and SSA, has generated interest in a more professional hacker community, seeking to obtain sensitive information. A further threat to ESA is the potential infiltration of critical infrastructures with software that can take over control of the facilities. Many systems are vulnerable as they are not provided with the most recent security patches, or because the employ weak passwords. Once in a system, the attackers hop to others on the same network looking for other similar vulnerabilities. Alternatively, hackers exploit the users of the systems to gain control, for example by sending email that installs key logging software or initiates phishing attacks. In all these cases, a lack of awareness from the owners and users creates conditions that hackers can exploit. All security incidents in ESA are carefully followed up as, in some cases, the impact may be a big one (e.g. loss of productivity or loss of reputation). Continuous watch and liaison by ESACERT[vii], Projects, and Security Office allows fast reaction and continuous monitoring of the potential threats.

Within this contested and aggressive cyber-environment, the European Space Agency's specific Mission adds the complexity of operating infrastructures located so far in the solar system that the electromagnetic pulses need travelling in some cases for over one hour to reach them from the control centre based Earth (e.g. the Huyghens spacecraft landed on Titan, one of Saturn's moons). Obviously, in this context, ESA has the very specific need and obligation to protect also the European tax-payer investments based in space (and sometimes in

deep-space) from cyber menaces, both of operational nature, or hidden and latent in the on-board components of the spacecraft.

The European Institutional response to cyber-threats is progressively becoming more visible and efficient in stimulating awareness within the communities involved in the protection and development of critical infrastructures. With the objective of ensuring a safe and security environment for its institutional missions, the European Space Agency has started an activity supporting the establishment of technical recommendations and of a policy through which ESA missions can define their own specific cyber-security requirements in order to guarantee reaching their mission's-specific objectives and consequently, protecting the image and the interests of the Agency in front of the external world.

The goal of this activity is to let the Agency (i) be better equipped to counter any perceived cyber-threat against its space missions, (ii) raise awareness in the space community about the cyber-security issue, and (iii) be able to establish an Agency-wide policy. Such action is complemented by two parallel studies awarded respectively to GMV (Spain) and THALES (with the support of ThalesAlenia Space France) which have been recently kicked off and which will last for one year. The contractors will compile a set of cyber-security technical and non-technical recommendations (i.e. guidelines or best practices) for the mission planning, design and procurement authorities for all categories of ESA space missions[viii]. The study results will cover the whole life-cycle of space systems including R&D, operations and decommissioning phases. The proposed security measures will be organised as multiple layers of proportionate defence (defence in depth) and shall include: deterrence, prevention, detection, resilience, and recovery. The analysis will also include indications on the projected impacts of the potential cyber-security threats and of the implementation of the proposed risk mitigation measures on the mission implementation schedule and resources (human and financial). The perimeter of the study includes all those elements which may be targeted by ground-to-space, space-to-space or space-to-ground cyber-attacks including:

- User segment equipment
- Space segment, including satellite bus and payload, launcher vehicle on-board equipment, manned spacecraft or stations' on-board equipment for life support and/or scientific experiments.
- Hosted payloads
- Ground segment

Within the scope of this activity, the addressed cyber threats include:

- highjacking/control of the spacecraft
- intentional or unintentional destruction/damage of the spacecraft
- signal interception, jamming or spoofing, eavesdropping
- wiretapping (i.e. "man in the middle")
- Distribute Denial of Service (DDOS)-type of attacks
- attack through the space mission supply chain
- (e.g. Trojan or latent virus), including customer furnished payloads

In technical terms, this study consists of three main tasks, namely (i) Security Threats Analysis, (ii) Security Vulnerability Analysis, (iii) and Security Risks Analysis, with the aim of providing:

1. an exhaustive description of security threats against various categories of ESA space missions and an assessment of such threats in terms of potential impact and probability of the accidental or deliberate occurrence,
2. a description of mission class security vulnerabilities of the various categories of civilian space missions.
3. a security risk analysis and risk mitigation plan of the various categories of civilian space missions based on the identified security threats and vulnerabilities.

The first task concentrates on the analysis of the security threats for the civil institutional systems. Within this task the contractor will first of all propose an appropriate categorisation of the space missions and systems falling in the scope of this study (i.e. taxonomy), which will be adopted as a reference for performing the remaining part of the study. For each space mission class, existing common high-level set of laws, rules, and practices that regulate how information is managed, protected, and distributed[ix] within this particular class of space systems will be briefly described. For each space mission class, a comprehensive examination of the motivations, circumstances and events with the potential to cause harm to a system in the form of destruction, disclosure, adverse modification of data, and/or denial of service will be described and

assessed in terms of potential impact, and probability of occurrence.
The second task focuses on the analysis of the security vulnerabilities for each space mission class previously identified. The weakness in a mission class system, sub-system, component, organisational process (including the supply chain), procedure, information system, or cryptographic system that could be exploited to violate the system security policy shall be identified. The space mission class will be analysed in order to determine the adequacy of existing security measures and to identify the remaining security deficiencies. This task will also include a measurement of vulnerability which includes the susceptibility of a space mission class to a specific attack and the opportunities available to a threat agent to mount that attack.
The third task focuses on the analysis of the cyber-security risks, on the appropriate mitigation security measures and on the countermeasures to address the residual risks identified. The mission manager is the risk responsible, the person who takes care of enacting and funding these measures. The analysis will address the combination of the likelihood of an attack (from a threat source), the likelihood of a threat which could result in an adverse impact (e.g., denial of service, loss of confidentiality or integrity), and the severity of the resulting adverse impact (also in terms of schedule and costs, if applicable).

Based on this risk assessment, the study will (i) determine if existing countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level, (ii) define the portion of risk that remains after security measures have been applied, and (iii) assessing the existing countermeasures in terms of cost/benefits.

A number of technological solutions are expected also to be highlighted in terms of areas where the Agency and its Member States could invest in the next years, including:

- Innovative cyber-secure telemetry, tracking, and commanding (TT&C) techniques,
- Cyber-hard embedded spacecraft flight computers, microprocessors, field programmable gate arrays (FPGAs), and (in general) digital finite state machinery and associated networks, busses, and point-to-point connections, to include architectural, software, and interconnect/interface technologies.
- Robust construction methodologies for building spacecraft, to include the supply chains of components, software, tools, and tool-chains.
- Analytic tools and frameworks that permit enhanced understanding of the concepts behind both the vulnerability of present and better engineering of future systems to cyber-attack.
- Technologies that will allow survivable spacecraft missions under adverse cyber stress.
- Technologies for effectively modelling and reasoning about our on-board space systems that enable them to distinguish among anomalies caused by system failures, adversarial actions, and environmental effects.
- Survivable C3, autonomous self-healing systems, and trusted architectures.
- Advanced engineering techniques that permit mathematical specification of spacecraft functions and formal verification of the security properties of the implementation.
- Methodologies for spacecraft cyber defense-in-depth, focusing primarily on threat avoidance through vulnerability mitigation, and allowing mission survival with graceful degradation under cyber-attack.
- Unique software or procedural approaches for providing protection to deployed / legacy space systems.
- Technologies to provide indications of an active cyber-attack against a spacecraft.

IV. Towards A Cyber-security policy for a sustainable, secure and safe space environment

A wide variety of cyber-security guidance is available from national and international organizations for entities within the critical infrastructure sectors e.g. banking and finance, communications, energy, health care and public health, information technology, nuclear reactors, material, and waste, and water. Much of this guidance is tailored to business needs of entities or provides methods to address unique risks or operations. In addition, entities operating in regulated environments are subject to mandatory standards to meet their regulatory requirements; entities operating outside of a regulatory environment may voluntarily adopt standards and guidance.

Implementation of cyber-security guidance can occur through a variety of mechanisms, including enforcement of regulations and voluntarily in response to business incentives; however, sector-specific agencies could take additional steps to promote the most applicable and effective guidance throughout the sectors. As an example, in the USa number of subsectors[x], such as electricity in the energy sector, are required to meet mandatory cyber-

security standards established by regulation under federal law or face enforcement mechanisms, such as civil monetary penalties. By contrast, entities not subject to regulation may voluntarily implement cyber-security guidance to, among other things, reduce risk, protect intellectual property, and meet customer expectations.

Once governed as separate and distinct areas by treaty frameworks established within the UN system, outer space and cyberspace are emerging nowadays as an increasingly inter-meshed governance regime also beyond conventional legal mechanisms. This evolution was the subject of a famous speech[xi] delivered by the American General James E. Cartwright, Vice- Chairman of the U.S. Joint Chiefs of Staff. In which it was emphasised how the newly established US Cyber Command (USCYBERCOM) resulted from a growing recognition by the U.S. Department of Defence that outer space and cyberspace "together" constitute a unique technologically created domain that is becoming a prominent locus for international strategic, political and economic power competition.

Any policy development geared towards space security and cyber-security should take into account the significance of preserving open access to these two global commons. In the initial reflections about a possible policy development, recently promoted by several think tanks in Europe and in the US, some basic principles appear to be widely accepted. A good starting point is information sharing, within the so-called transparency and confidence building measures, a mechanism that has received particular attention in the cyberspace context through ICANN[xii] and in the space debris context through SDA[xiii]. Information sharing on threats and vulnerabilities should ultimately develop into public-private partnerships preserving access to the commons and managing any risks arising out of it. Any policy approach should also strongly consider the human factor as all technical elements and systems are managed by humans. Lastly, existing institutional partnerships could be expanded starting with a collaborative effort e.g. between the European Union and the North Atlantic Treaty Organization[xiv].
However, many points still remain to be clarified and are currently subject of harsh debate. For instance, vulnerabilities can be related to hazards as well as hostile acts. Assessing the nature of an (space or cyber) incident and attributing it, however, represents a difficult task as it requires a thorough understanding of the incident and the intent behind it. This effort is further complicated by the lack of awareness and information on (space and cyber) incidents. Targeted industries and/or satellite operators are reluctant to publicize numbers on incidents, which hampers an accurate threat assessment necessary for ascertaining and managing risks. Another challenge concerns diverging understandings of "cyberspace". One opinion group identifies cyberspace as a global domain within the interdependent information technology network and infrastructure, while others understand the "information space" as including the additional dimension of the information itself and its effect and influence on individual and social consciousness. This fundamental difference in perspective inhibits the formation of an internationally agreed classification framework of cyber threats[xv].

In this context, practical rules to cope with imminent challenges in the two domains should be adopted at the earliest possible opportunity. Although rule-making in the UN is widely viewed as legitimate, it is also very difficult to achieve. An alternative approach, such as developing norms outside the UN and subsequently expanding the number of supporting countries, could be a pragmatic alternative[xvi].

V. CONCLUSIONS AND WAY FORWARD

ESA intends to take into account the outputs and recommendations resulting from the two on-going studies to develop technological solutions and an ESA-internal set of guidelines on cyber-security aimed at making its institutional missions more secure, safer and more compatible with a sustainable use of the space environment.

Beyond this goal, the ESA guidelines can certainly contribute to the further development of the relevant international standards e.g. CCSDS *Security Threats against Space Missions*[xvii], *Security guide for mission planners*[xviii], *or Guide for secure system interconnection*[xix], as recommended by the ISO *Standards for Information Security Management System*, in order to "develop a balanced and modular set of security measures creating a secure environment in which systems operate"[xx]. The fields of application of these measures shall address physical elements, personnel, non-technical procedures, supply chain control, computer and communications operating procedures.

If necessary and appropriate, already existing inter-institutional cooperation between ESA, the European Commission (EC) and the European Defence Agency (EDA) could even be extended to include reflections

and/or activities to enhance the cyber-security of the European institutional and commercial space missions, taking stocks of the EU Critical Infrastructure Protection programme[xxi], the Code of Conduct for Outer Space Activities[xxii], the recent EU Cyber-security strategy[xxiii], the on-going negotiation of the Transatlantic Trade and Investment Partnership (TTIP) - and its related potential impacts on the European space industrial policy - and the EC/ESA/EDA Joint Task Force on Critical Space Technologies for European Strategic Non-Dependence.

Hence, the key is collaboration: ESA, European and International Institutions, national space agencies worldwide as well as commercial space entities share the same concerns! More coordination efforts among these entities are necessary, in particular:

- The emergency response teams (CERTs) of the stakeholders should be linked by a permanent connection/cooperation
- Technical coordination meetings should be organised to devise common solutions and share experiences (like the ESA International Security Symposium held on March 2012)
- Common protection rules should be enforced
- Mutual support among institutions in possible future technical studies/research activities should be pursued.

Finally, think-tanks and respected international fora world-wide (e.g. the IAF, the European Space Policy Institute, Secure World Foundation, the UN Institute for Disarmament, etc.) should be instrumental in facilitating the dialogue among the stakeholders and international partners, raising the level of awareness about the blurring legal distinctions defining the outer space and cyberspace, and paving the way to the development of a governance needed to guarantee a sustainable use of outer space in an ever more contested, congested and competitive cyber-security environment.

[i] Threats Impacting the Nation, GAO-12-666T , Apr 24, 2012

[ii] http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf

[iii] The Fédération Aéronautique Internationale has proposed an altitude of 100km, called the Karman Line, as a working boundary. UK Military Space Primer, June 2010: pp. 1-1, 1-2, para. 104.

[iv] Major General Mark Barrett, Dick Bedford, Elizabeth Skinner, Eva Vergles, Assured access to the global commons, - Norfolk, Virginia USA - 3 April 2011

[v] Susan J. Buck, The Global Commons: An Introduction (Washington, D.C.: Island Press), p. 6.

[vi] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," v. 1.3, Symantec Security Response, Symantec Corp., November 2010;

[vii] ESA Computer and Communications Emergency Response Team

[viii] The entire spectrum of space missions falling within the remits of the European Space Agency covers: Earth Observation, Launchers, Navigation, Human Space Flight, Science, Exploration, Telecommunication and Space Situational Awareness

[ix] Cyber-threats can arise from any individual with the necessary level of expertise and knowledge of the system and basic access to the system.

[x] GAO, "Cyber-security Guidance Is Available, but More Can Be Done to Promote Its Use", GAO-12-92, Dec 9, 2011

[xi] Delivered on 10 September 2010 at University of Nebraska. 3rd Annual Space and Cyber Conference, 9-10 Sept. 2010, Washington DC.

[xii] Internet Corporation for Assigned Names and Numbers

[xiii] Space Data Association

[xiv] Chatham House in partnership with Finmeccanica UK and Istituto Affari Internazionali, International Security Workshop Summary - Making the Connection: The Future of Cyber and Space, 24 January 2013

[xv] Chatham House in partnership with Finmeccanica UK and Istituto Affari Internazionali, International Security Workshop Summary - Making the Connection: Building Stability in Cyber and Space, 7 May 2013

[xvi] As the multi-stakeholders governance model advocated by Prof. L. Martinez in ESPI Perspective paper n.56, January 2012

[xvii] CCSDS 350.1-G-1, October 2006 edition

[xviii] CCSDS 350.7-G-1, October 2011 edition

[xix] CCSDS 350.4-G-1, November 2007 edition

[xx] International Standards Organization - ISO 27001, 2011 edition

[xxi] COM(2006) 786 final

[xxii] EU Council conclusions n.14455/10, 11/10/2010

[xxiii] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 - JOIN(2013) 1 final