Session E7.4 contained nine presentations dealing with the legal issues arising from the intersection of space activities and the use of cyberspace.

Hamid Kazemi focused on the challenges posed by cyber activities on state responsibility in space law. The author pointed out that while action taking place in cyberspace has become one of the biggest challenges for space technology and space activities in recent years, cyberspace and outer space are interlinked and can be both an opportunity and a threat to each other. At present, the determination of state responsibility in both spaces is not clear. And international law has so far been slow to react to cyberspace. The only multilateral treaty dealing directly with cyberspace – the 2011 Budapest Convention on Cybercrime, does not directly address state responsibility. The challenges to prove attributability, however, especially with regard to increasing private space activities, result from numerous difficulties such as fragmentation and different national approaches, lack of uniform international rules, and the transnational cyberspace intensifies these issues. If cyber activity takes place without the use of space technologies or somewhere outside outer space, such activity cannot be considered a space activity. In case cyber operations are carried out using space technologies or by human beings in outer space, such actions are subject of the rules and legal principles governing state responsibility in outer space. Cybercrime, if it is an aggressive and damaging act, such as the destruction of a space object or interference, must be placed under the jurisdiction of states that are responsible for controlling and supervising space technology. It seems that technology is so advanced that it is possible to identify the responsible state based on documented information. On the other hand, space law restricts responsibility to the launching State and the State of Registry. In the end of the presentation, Kazemi concluded that State responsibility for cyber space activities requires new binding regulations, whereby possible solutions may be found in intensified international cooperation, and/or in the adoption of new laws and regulation to address possible liability for cyber activities affecting outer space.

Stefan Kaiser's presentation entitled “When Cyber Activities are Space Activities: Definitions are Key” started with the reasoning, on the basis of Art. VI OST, behind the need for definitional clarity, and the issues resulting from the lack of an international definition of ‘space activities’. He submitted that certain elements of a space activity can, however, be identified. They are included, for example, in the OST Preamble, in Art. I, Art. III, Art. VIII and At. IX OST. Kaiser observed that while the national laws of some States focus on the purpose of space activities, others refer to the substance – e.g. the launching of space objects, the return of OS to Earth, operations in outer space, incl. guidance, command, control. Typically, as a general wording, the use of outer space is included within the scope of a space activity. The linking element to cyber activities is the fact that space objects are commanded and controlled from the Earth by remote control radio links. Also with regard to cyber activities, no international definition has been accepted so far. Three elements can, nevertheless, be identified: first, cyber activities are performed using digital information and execute logical functions through self-executing code. Second, they depend on a physical infrastructure consisting of networks, and on wireless links. Third, cyber activities have effects on: digital data in cyberspace; physical domains through the IoT; possibly on space objects or somewhere in outer space in connection with space activities. Not any kind of interference (e.g. physical cable disruption, jamming) is a cyber activity, while spoofing may qualify also as a cyber activity under the three abovementioned elements. In
analysing the question on when a cyber activity is also a space activity, Kaiser pointed out that this is the case when an authorized or unauthorized cyber activity produces an effect on a space object or somewhere else in outer space. Examples include the launch, the operation and the return of a space object, including the command and control of payload, and physical effects. In contrast, transmitted information that merely traverses outer space, should not qualify as a space activity. Examples include information that is channeled through the transponder of a communication satellite or remote sensing image information that is further processed on the ground. Kaiser concluded the presentation by arguing that in general, definitional clarity in differentiating between cyber activities and space activities can help in establishing state responsibility under Art. VI OST.

Sarah de Heer focused in her presentation on the need for a legal regime to react to cyberattacks. Such may be performed also in outer space – either by private individuals, or by governments, subdivided in attacks during peacetime and war. With the scope of the presentation, the main question to be analysed was the extent to which cyberattacks can be performed with a ‘peaceful’ purpose under the OST and be regulated by Art. VI OST. De Heer argued that the OST is undoubtedly applicable to cyber activities in outer space, regardless of the actor performing them. Thus, no adaptations of the OST should be proposed. With regard to the term ‘peaceful purposes’, non-aggressive cyberattacks fall within the remit of OST and general international law. The author thus proposed to follow the school of thought according to which cyberattacks from Earth directed to outer space and vice versa should be considered space activities. In order to overcome the unclarities however, including the lack of clarity as to how to define outer space, it is suggested that a new document and soft law measures should be adopted to clarify these relevant notions.

Ishita Das tackled the topic “Outer Space and Cyberattacks: Attributing Responsibility Under International Space Law.” Underlining the enormous impact of cyber activities to the space sector, she explored, first, the interrelation between outer space and cyberspace, and second, the available legal instruments in the OST and the Liability Convention, before offering some solutions. Das argued that cyber activities in outer space may take place through cyber interference with the flight control and the payload control, offering inlets both to the ground-based, the peripheral systems and the space system components. For example, the operator of the flight control may, possibly, be liable for damage caused by actions it has never authorized. After looking into Arts. VI, VII and IX OST, and into Art. II and Art. III Liability Convention, Das concluded her presentation with the standpoint that the legal framework is currently not adequate to deal with the threats resulting from unauthorized cyber activities and argued that a multilateral agreement under the supervision of UNCOPUOS is the need of the hour.

Chimnoy Roy presented the perils posed to cybersecurity in outer space as a very pressing issue. After illustrating the possible impacts of offensive cyberattacks, including such used by terrorists, hackers and politically-motivated perpetrators, and arguing that such activities may lead to the generation of space debris, the author explored the potential motivations for cyber and electronic attacks against space systems and the various links that can be employed by intruders. Roy came to the conclusion that the existing legal framework of space law is silent on cyberattacks and their effects and proposed seven main elements of a future international framework for the cybersecurity of satellites, including: forensic mechanisms to attribute cyberattacks in outer space; mandatory de-orbiting of satellites; the establishment if-of an international regulatory authority for satellite hardware and software; regulation of COTS; engaging all interested groups; formulating cybersecurity standards in a clear manner. The author went as far as to suggest the removal and destruction of unregistered space objects conducting questionable space activities as one possible solution within such a future framework. In conclusion, the author underlined the importance of prioritizing cybersecurity of space assets at par with cybersecurity of critical infrastructure in general.
Daryia Bohdan’s presentation focused on cyber inflicted damage which can be addressed at the ground segment, the space segment and the communications between them and thereby influence the functionality of space objects and additionally result in infliction or damage on the surface of the Earth, to aircraft in flight or to other space objects. Bohdan looked also at damage to the space environment, in the form of space debris caused as a consequence of cyber events. Next, the author outlined the relevant legal framework applicable in peacetime and in times in conflict and suggested that cyber damage inflicted by space objects without kinetic collision shall be considered direct damage under the Liability Convention. This could be done under an evolutionary interpretation in light of current technological developments, whereby damage caused to the environment must be considered for the purposes of compensation. The author further suggested that Arts. VIII and IX OST can be applied accordingly to recover cyber damage. Within the scope of due diligence as a duty of conduct, it was moreover suggested that protection units, firewalls, etc. are employed to protect space objects. During conflict, all damage caused by cyber activities to an illegitimate target (such as a space object used for peaceful purposes by at least one launching State) should be covered under international law.

Ingo Baumann and Eric Pellander’s presentation on “GNSS jamming and spoofing under national and international law” started with an overview on the growing dependence of the global economy on reliable positioning, navigation and timing services provided by GNSS and regional GNSS-augmentation systems. Sectors such as communications, financial services, energy, transport, food and farming rely on GNSS data. This dependence leads to various risks for economy and infrastructure, also in the military sector. The two methods to disrupt GNSS services (jamming and spoofing) may take place both locally, regionally, or have global impact. Under the ITU legal framework, jamming and spoofing fall in the category of harmful interference which is prohibited under the ITU Radio Regulations. However, enforcement of the prohibition is a weakness within the ITU system as ITU bodies lack appropriate enforcement measures against intentional jamming and spoofing. Next, a look into the ICAO legal framework shows that dedicated SARPs have been developed to determine maximum interference levels. Moreover, the ICAO GNSS Manual provides an Interference Mitigation Plan. Another international organization relevant in this context is the International Maritime Organisation (IMO) which oversees GNSS implementation in the global maritime navigation, thereby setting performance standards as important tools for preventing and mitigating the effects of GNSS jamming and spoofing. Next in the presentation, an outlook on the application of the international legal framework to jamming and spoofing was given. As international law is not binding upon private persons, States have to introduce respective national laws in order to ensure conformity with international rules. The presentation ended with a recap of its main findings and a recommendation of adoption of preventive and mitigation measures for GNSS jamming and spoofing.

George Anthony Long presented his paper entitled “Terrestrial Cyber Activity of Non-Governmental Actors and State Responsibility under Art. VI OST”. He pointed out that Art. VI OST does not apply to national persons, but requires that States authorize and continuously supervise the space activities of their national persons. Based on a plain language interpretation of Art. VI OST, the author argued that not any terrestrial act facilitating interference with a satellite or with satellite services, equates with a space activity and provided some illustrative examples. Long suggested that the most practical course for classifying a terrestrial cyber activity as space activity under Art. VI OST is to base the determination on the status of the owner or operator of the space object rather than on the effects and purpose of the terrestrial activity on a space object. He argued that as such owners/operators are subject to the duty of authorization and supervision, this would allow States, in fulfilling their duties under Art. VI OST, to monitor the terrestrial cyber activity only of some, and not of all nationals. The presentation was concluded with a caution to avoid an unwarranted expansion of the duty to authorize and continuously supervise space activities on terrestrial activities.