IISL Working Group on Cyber Law

I. In 2017, the Chair of the IISL Directorate of Studies (DoS) Prof. Dr. Stephan Hobe was tasked by the IISL Board of Directors to look into the question on whether cyber law should become a topic for future IISL Colloquia and something to be studied more intensively by the International Institute of Space Law.

II. In order to come to an assessment of the need and the possibilities for the Institute to deal with questions on cyberspace and cyber law pertaining to the regulation of space activities, the DoS Chair invited the IISL Members to participate in an IISL Working Group on Cyber Law. A total of 22 Institute members (including the DoS Chair and the Co-Chairs of the five sub-working groups listed below) expressed their interest to do so. The working group was divided into five sub-working groups to define specific questions and separate areas of interest.
The work of the working group was then divided into five topics as follows:

1. What is the technical architecture of cyber space?	**2. Is there a (self-contained) specific legal regime for cyber space?**	**3. Who is supposed to regulate cyberspace?**	**4. Is the law on outer space applicable to cyber activities in outer space?**	**5. What are the legal aspects of cyber security for space assets?**
Headed by: P.J. Blount	Headed by: Stephan Hobe	Headed by: Rada Popova	Headed by: Fabio Tronchetti	Headed by: Skip Smith and Olga Stelmakh
Larry Martinez	Maureen Williams	George Kyriakopoulos	Lesley-Jane Smith	Jack Beard
Cassandra Steer	George Anthony	Jenni Tapio	Neta Palkovitz	Ranjana Kaul
Roy Balleste	Jairo Becerra	Rita Lauria *(resigned due to work committments)*	Rao Tejas	Ingo Baumann
			Erdem Merve	

In the following, the results of the work of the sub-working groups are briefly summarized.

1. Sub-working Group 1, headed by P.J. Blount dealt with two questions: **What is the technical architecture of cyber space? Which legal questions can be derived therefrom?**

The members of the sub-working group came with a detailed report stating that the architecture of the Internet is key to understanding how it disrupts conventional telecommunications infrastructures and the legal issues associated with its operation and regulation. This is because the Internet's revolutionary digital architecture is endemic to how law can regulate and which law can regulate. It has been argued that 'architecture' represents a 'law' of sorts because it sets the limitations of what a user may and may not do. This theory is often referred to as "code is law," first posited by Lawrence Lessig. As a result, it is useful to have an understanding of how the Internet works in order to judge its legal impact because architecture and regulation are intrinsically linked in what is sometimes referred to as the "lex informatica".

The Internet is more properly understood as a 'network of networks', meaning that the "Internet" is a diverse set of networks and devices that are all able to communicate via a standardized software protocol. One of the clearest ways to explain how this works is to employ a layered model of Internet architecture. The layered model divides the architecture into various components and protocols that all work together to allow computer networking. It should be noted that different scholars divide the architecture into different numbers of layers. For an analysis of the Internet, a four-layered model which includes the Physical Layer, the Logical Layer, the Application Layer, and the Content Layer helps to reveal the complex legal framework that governs the Internet, since different laws affect different layers.

The physical layer contains the infrastructure that the Internet runs on. This includes copper wire, fiber optic cable, radio transponders, as well as the various devices and servers that are connected to a telecommunication network.

The logical layer is the heart of the Internet. It is made of open protocols, namely the Transfer Control Protocol and the Internet Protocol (TCP/IP), which establish a standardized system for transferring information from digital machine to digital machine.

The application layer is made up of the programs that run on end-user devices. The Internet is an end-to-end network, which means that it connects devices together. These devices run programs that can reassemble and output data sent across the Internet. For example, an email program takes text and attachments, divides it into packets and sends it across the Internet using the TCP/IP.

The final layer is the content on the Internet as well as the social, economic, and cultural phenomenon of cyberspace. The TCP/IP allows the Internet to be widely available by ignoring technological stovepipes, and the applications define the type of content that can be digitized and transferred.

As to the Internet and the space segment, it must be noted that satellites are part of the physical layer of the Internet, with the possibility of acting as both a means of transmission and as a device on the network. This does not mean that all satellites are necessarily integrated into network operations of the global Internet. However, any satellite that employs IP-based communications technology can potentially be connected to the Internet. Satellites have two primary functions in relation to Internet technologies: as a transmission/networking device and as an end device.

As to possible questions to be addressed by the IISL, the group came down to the following seven points:

- Does the Internet architecture, by defining the technical environment of satellite operations, also define the legal environment of satellite operations?
- If so, which layers are the most legally defined and which are more difficult or resistant to define?
- How should the space community address the growing law and policy issues connected to cyber security?
- How could networked satellites change the national and international security environment in space?
- Are there intellectual property issues that arise from satellites being networked, especially in light of the potential for off planet data storage and retrieval?

- The Internet is often characterized as a platform for innovation. What innovative opportunities does it create for the space segment, and how should the law facilitate these opportunities?
- How can networked satellites become vulnerable to threats associated with their use as a weapon or affected by cyber weapons?

From this it can be concluded that the architecture of the Internet must be thoroughly understood before legal conclusions can be drawn. There are indeed really open questions with regard to the legal definition, with regard to cyber security and its legal issues involved as well as to intellectual property issues from satellites networking and in terms of legal security - issues of threats associated with the use of satellites used as weapon or affected by cyber weapons.

2. Sub-working group 2 was headed by Stephan Hobe and dealt with the question: **Is there a (self-contained) specific legal regime for cyber space?**

In essence, the working group was split in answering the question whether there is and should be a specific and self-contained regime for cyber space. As is well known, in the jurisprudence of the International Court of Justice a self-contained regime *per se* (such as diplomatic law or WTO law) contains all legal regulations in itself and does not allow for any recourse to general international law.

In this respect, a preliminary conclusion was drawn according to which the answer to this question would very much depend on a thorough assessment and of the nature of cyber space. It should therefore be clarified whether cyber space is regulated at all by rules of public international law and if this question can be answered in the affirmative, it follows to find out whether this is done through general norms or by a self-contained legal regime of cyber law as a specific regime within public international law.

3. The third sub-working group headed by Rada Popova was entitled: **Who is supposed to regulate cyberspace?**

The sub-working group identified the variety of actors involved in cyber space such as states in a military and non-military context, international intergovernmental organizations and non-state actors, whereby the threats caused by the (malicious) use of cyberspace for all these actors are very alike, unfolding multiple issues related to attributability and jurisprudence. While already some self-regulation initiatives exist, currently, only states would be in a position to legally regulate cyber space on the international and national level.

The group ended with three possible alternatives: (1) Cyber space should not at all be regulated; (2) It should alternatively be considered as one of the global spaces to which international law is applicable and (3) Cyber space in relation to space activities must be left to self-regulation by satellite manufacturers, software companies and other users.

4. Sub-working group 4, headed by Fabio Tronchetti dealt with the following question: **Is the law on outer space applicable to cyber activities in outer space?**

This group ended up with a few very concrete recommendations. Among them is the plea to clarify the nature of cyber-enabled space operations. Such process of clarification could go via the interpretation of existing space law terminology and concept, through the expansion of the scope of existing space law terminology and concepts or through the drafting of new rules specifically regulating cyber-enabled space operations.

5. Sub-working group 5, headed by Skip Smith and Olga Stelmakh dealt with the question: **What are the legal aspects of cyber security for space assets?**

The sub-working group felt it necessary to come up with a legal definition of cyber security, space assets and its constituent elements. Moreover, cyber threats against space assets like satellite jamming, spoofing, hacking, etc. should be identified and legally classified. Moreover, there should be an overall assessment of cyber threats in the context of international law and space law particularly with regard to *jus in bello* and *jus contra bellum*.

III. Overall assessment

In the work of the sub-working groups, a need for further clarification of cyber law as an element of various regulatory subjects of law was identified. The need to analyse the security aspects of cyber attacks, the question on the applicability of space law to cyber activities in outer space, the question on the need for regulation or non-regulation, the question of the elements of a possible cyber legal regime: all these issues depend on the definition of the technical features of cyber space. From that point, some legal consequences can be drawn.

Therefore, the IISL Working Group on Cyber Law came to a very clear and unanimous recommendation in 2017: The IISL should deal with questions of cyber law in the future, include them regularly in the IISL colloquia and, if such a need is identified, task a working group with more specific further questions.

As a result of these deliberations, the IISL Board of Directors took a decision to dedicate technical sessions to questions pertaining to cyber aspects in its annual colloquia from 2018 on.

Cologne, 2018

Prof. Dr. Stephan Hobe