IISL Working Group on Cyber Law

Chair: Stephan Hobe
Co-Chairs: Milton 'Skip' Smith and P. J. Blount

I. The undersigned was tasked by the IISL Board to look into the question on whether or not cyber law should be a topic for future IISL Colloquia and something to study more intensively by the International Institute of Space Law.

II. The undersigned called upon all members of the IISL and asked for their interest to participate in this working group. A total of 22 members (in total incl. the Chair and the Co-Chairs) agreed to work. Among those the working group was subdivided into five working groups in order to be able to define questions and separate different areas of interest. This should aim as coming to a thorough assessment on the need and the possibilities for the institute to deal in the future with these questions.
The group was then subdivided into sub-working groups according to the following table:

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	

The sub-working groups were asked to come up with some preliminary results by 1st July 2017. In the following, these results are briefly summarized and some conclusions as well as well as a recommendation are drawn.

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

The sub-group made a thorough assessment of the so-called internet architecture. In the view of the present author this description is so brilliant that it shall be annexed to this report because everybody can profit from it. As to possible questions to be addressed, 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 would 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 is such like diplomatic 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 that the answer to the 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 whether this is done through a self-contained legal regime of cyber law which has the nature of a specific regime of 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 threats for these actors are very alike.

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: Cyber space should not at all be regulated, it should alternatively be considered as one of the global commons, international law being applicable of thirdly, self regulation by satellite manufacturers, software companies and other users could be thinkable as well.

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 very concrete recommendations. Among a few recommendations one could find that cyber enabled space operations should be clarified. 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 concept or through the drafting of new rules specifically regulating cyber enable 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

The need of the sub-working groups, a need for further clarification of cyber law would be thus identified. The need with regard to security aspects through cyber attacks, the mere question of the applicability of space law to cyber activities, the question of the regulator or non-regulation, the question of the specificity of a possible cyber legal regime, the legal cyber regime: all does thus depend on the definition of the technical architecture of cyber space. From that point, some legal consequences can be drawn.

Therefore, the working group comes to a very clear and unanimous recommendation: The International Institute of Space Law should deal with questions of cyber law in the future, include them regularly in its colloquia and arguably task a working group with further questions.

Questions to be tackled could arguably be the ones that were investigated by this working group and in particular by the sub-groups.

The working group thus generally recommends to the Board of Directors to come up with a respective decision.

Cologne, August 2017

Prof. Dr. Stephan Hobe

Annex

What is the technical architecture of Cyberspace?
IISL Cyberspace Working Group/
Sub-working Group on Internet Architecture

Members of Sub-working group :

P.J. Blount, Chair
Roy Balleste
Larry Martinez
Cassandra Steer

I. I. Layers of Internet Architecture

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. For this reason 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. Below, a four layered model is briefly

sketched out, which includes the Physical Layer, the Logical Layer, the Application Layer, and the Content Layer. Using this model for analysis of the Internet helps to reveal the complex legal framework that governs the Internet, since different laws affect different layers. It should be noted that different scholars divide the architecture into different numbers of layers.

A. Physical Layer

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

One of the the important features of the Internet is that it is technology agnostic. The Internet can be accessed through all types of telecommunications systems and most electronic devices. This is because the logical layer, discussed next, serves as a mechanism to interconnect technologies.

B. Logical Layer

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 core of the network architecture established by the TCP/IP is packet switching.

Roughly, the TCP/IP protocol standardizes the following activities by instructing computers on how to divide information in packets, address each packet to another specific device using an IP address, and send those packets along the most efficient path. Importantly, those packets may be routed across the system in a non-consecutive order, in which each packet may take a unique path to reach its assigned destination. The use of these standardized protocols to interconnect devices creates a decentralized, non-hierarchical ‘network of networks’.

Another critical feature of this system is that the transfer of the information is not dependent on the type of information. All that matters is that the information is digitized, thus text, words, photos, videos, and, now, virtual and augmented reality media, among other digital products and services, all travel across the Internet as if the network were "transparent." This means that the limitations on information transfer are substantially bandwidth-related (the physical layer) and whether the end-user's device has the ability to reassemble the packets as the sender intended (the application layer).

C. Application Layer

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 recipient computer, using an email program can receive those packets, reassemble them and display them for the end-user.

This is an important feature of the Internet because it pushes processing power to the ends of the network. Since the TCP/IP is technologically agnostic and is capable of transferring any digital file, the applications running on user devices (as well as the hardware interface devices) define the scope and content of what is available on the Internet.

D. Content or Social Layer

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. The content layer is the human aspect that has expanded the Internet from static websites to fluid social networks into which people integrate and operate. The Internet has done more than just bring efficiency to telecommunications, it has rooted itself into the global social landscape and represents a modern locus for the production and dissemination of culture. It

brings diverse communities and populations into direct contact with each other across borders and this contact can be harmonious or rife with conflict. It is a platform for both politics and pornography, and while society, and the law, often views these types of speech differently, the TCP/IP transfer both indiscriminately. In short, the content layer of the Internet is felt across most facets of society.

II. II. Specific Technical Architectures

The layers model is used to give a general description of certain functions of the Internet. This section will briefly overview three specific architectures that are currently prominent in Internet architecture.

A. WWW

The World Wide Web (WWW) is often what people think of when they think of the Internet, but the WWW is really just another file-sharing application on the Internet. Once again, the WWW's standardized protocols allow web browsers and other applications to exchange information in a wide and expanding range of media and information services. In this way, the WWW is made up of files held by servers around the world that are written in standardized code. Web browsers, a part of the application layer, allow users to visit these servers, using the TCP/IP, and then to download and view these files. The WWW is built on open standardized code that allows users to choose among web browsers to display these files.

B. DNS

As mentioned above, the WWW is essentially files for websites that exist on servers globally. Each of these servers has an IP numerical address that designates it as a unique place on the Internet. These addresses are long strings of numbers that would be difficult for a user to remember. The Domain Name System (DNS) is a system that allows users to rename their server with an Uniform Resource Locator (URL), such as http://www.iislweb.org. This DNS facilitates this functionality by maintaining lists of URLs, and their associated IP addresses. When a user types in a URL, the web browser consults this list and sends the browser to the proper IP address.

C. Encryption and Anonymity

Another effect of the digital TCP/IP is that it facilitates secure communications through computer-aided encryption. Secure transactions on the Internet are a critical feature, as they make commercial activity possible by protecting consumer privacy. Encryption also facilitates anonymous communication, which makes cybercrime possible by allowing virtual bank robbers to hide their identity. Notably, encryption is a function of the application layer, which pushes power to the user.

III. III. The Internet and the Space Segment

As noted earlier, many satellites are part of the physical infrastructure of the Internet. 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.

Satellites that are used for broadband Internet connections serve as transmission devices for the Internet, and increasingly, can also serve as networking devices for inter-connecting Internet end-users. The “bent pipe” transmission function is similar to the traditional role of telecommunication satellites that would transmit voice calls. Newer satellites are now used to facilitate Internet connectivity in geographically remote areas and aboard planes and ships by providing space-based Internet networking between terrestrial end-users.

Satellites can also function as end devices on the Internet. Many satellites have employed IP-based technologies in order to better facilitate not only the uplink and downlink communications between a satellite and ground stations, but also the performance of a multitude of scientific and commercial services in space. For example, earthbound users may instantly access imagery from weather and scientific satellites over the Internet. Astronauts on the International Space Station may send and receive email over the Internet. The Internet capability of satellites also makes it possible for satellites to become networked as back-up communications in cases of cyber security breaches and other infrastructure failures. A user could use application layer technology to communicate through ground stations to other users through

satellite networks. The space segment as a result is deeply implicated not just in ensuring network access to users, but also in the contested cybersecurity environment.

There are also new applications that hope to use satellites to remotely store data for retrieval off the planet. These plans are in part driven by a desire to move data outside the scope of terrestrial control. While some of these ventures have humanitarian intentions, others see this type of data storage as a way to evade terrestrial regulations, and in particular laws that apply to intellectual property.

IV. IV. Possible issues to be addressed by the IISL

The architecture of the Internet brings the space segment into the global network of networks and the issues that this raises are numerous. The working groups identified the following issues, related to architecture, that likely hold promise for investigations by the IISL.

- 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 cybersecurity? Which layers are most vulnerable?
- How might 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 might networked satellites become vulnerable to threats associated with their use as a weapon or affected by cyber weapons?