January 2020

FIRST WEBINAR REPORT

DR. PJ BLOUNT – “CYBERSECURITY AND SPACE LAW”
RAM LEVI – “CYBERSECURITY AND SPACE ASSETS”

Acknowledgments

The organisers wish to express their gratitude to Dr. PJ Blount and to Mr. Ram Levi for their outstanding presentations on "*Cybersecurity and Space Law*" and "*Cybersecurity and Space Assets*".

The Webinar immensely benefited from their valuable insights and expertise on cybersecurity and space issues.
Appreciation is also extended to Thea Flem Dethlefsen for her support in the organisation of this 1st webinar, for moderating it and for contributing to this report.

The organizers would like to express their sincere appreciation to Hannah Lindberg for co-leading the Space and Cybersecurity Project Group and for highly supporting the organization of this 1st Webinar.

Also, the organisers would like to express their appreciation to the attendees for their participation, time and input. Finally, many thanks are expressed to the members of the Project Group for contributing to the organization of the Webinar.

About the organisers

Project Overview

The Space and Cybersecurity Project Group follows the outcomes of the Space & Cybersecurity working group at the European Space Generation Workshop 2018, hosted in Bucharest, to emphasize the need to reflect on the nature of space and cybersecurity, what the priorities of governments and international institution should be, whether data should remain open source or limited in its availability, possible technical solutions to the challenges posed above, and the shape and origin of threats to cybersecurity in space.

Objectives

The Project Group aims to create an international forum to further the discussions we had in Bucharest, which we aspire to lead to papers being published.
The Group is supporting SGAC's goals to providing a dynamic forum, where members can share their thoughts, views and opinions on international space policy issues, and raise awareness among the next generation of space professionals about the global scale of space activities.

The United Nations has also shown interest in the topic of cybersecurity, through resolutions and reports. We wish to push the cybersecurity agenda at UN Committee on the Peaceful Uses of Outer Space. The Project Group has 9 advisors, which supports SGAC's strategy to strengthen relationships and partnerships with academia and industry.

More information about the Space and Cybersecurity Project Group are available at:

https://spacegeneration.org/projects/space-cybersecurity

Additional note

The report was drawn up by Thea Flem Dethlefsen, Lucille Roux, Antonia Russo, and Laetitia Zarkan.
It summarizes the presentations and exchanges of the 1st Webinar organized by the Space and Cybersecurity Project Group, held on January 27, 2020.

The views and opinions expressed in this document are the sole responsibility of the Space and Cybersecurity Project Group.

The report aims to reproduce — to the greatest extent practicable and in a comprehensive manner — the content of the presentations and of the debates that followed the webinar.
Where this document reports or refers to statements made by panellists, every effort has been made to provide a fair representation of their views.

About the speakers

Dr. PJ Blount is a post-doctoral researcher at the University of Luxembourg in the Faculty of Law, Economics, and Finance and a Research Fellow in Cybersecurity Governance and Regulation at SES.
His teaching includes courses on Space Security Law, International Telecoms Law, Cyberlaw, International Law, Human Rights Law, Intellectual Property, and US Foreign Policy.
Previously he worked as a Research Counsel and Instructor at the University of Mississippi School of Law; was a Visiting Scholar at the Beijing Institute of Technology, School of Law; and an Adjunct Professor at Montclair State University, Department of Political Science and Law.
He holds a B.A. in English and an A.B.J. in Print Journalism from the University of Georgia; a J.D. from the University of Mississippi School of Law; an LL.M. in Public International Law from King’s College London; and an M.S. and Ph.D. in Global Affairs from Rutgers University.
He has recently published the book “*Reprogramming the World, Cyberspace and the Geography of Global Order*”.

Ram Levi is the Founder and CEO of Konfidas, a leading Israeli cybersecurity company. He is a cybersecurity expert, and an advisor for global organizations with extensive knowledge in policy, technology and hands-on experience. Ram served as the secretary for the PM of Israel National Cyber Initiative.
He is currently the cyber advisor to the National Council for R&D and Senior Fellow at Tel Aviv University. Ram holds an MA (Cum Laude) from the Tel Aviv University, is a graduate of the International Space University, holds a degree in Computer Science and trained in the elite IDF Mamram Programming School.

About the webinar

SGAC organizes free webinars open to all and giving the participants the opportunity to engage with experts on space-related topics.

About the moderator

Thea Flem Dethlefsen is a Young Graduate Trainee in procurement for Human Spaceflight, Robotic Exploration and Science at the European Space Agency. She holds a Bachelor and Master in Law from University of Copenhagen and an Advanced LLM in Air and Space Law from Leiden University.

DR. PJ BLOUNT

Cybersecurity and Space Law

Dr Blount discussed the intersection of cybersecurity and space law and focused on commercial actors rather than on state actors, specifying that there is a lot of overlap between them. There is no mention of cybersecurity in space law at all because the treaty regime really predated the concept of cybersecurity. The relationship between cybersecurity and space law is mainly built on some national policies. Looking at how the UK space policy talk about cybersecurity without having been addressed formally in domestic legal regimes. The other important thing to remember about space law is that it's addressed to States, who are the subjects of international law Space law doesn’t govern space but space objects in space.

Few standards exist but nothing comprehensive, and a lot of those standards have to do more with data transmission and data portability than with cybersecurity. Thinking about how ubiquitous cybersecurity as a concept is, and how it has no standard definition, cybersecurity rules come from law and regulation but also from policy, technical standards, and what is called good practices. The rules often come from the code itself. All the code that underlies the programs that is running and the hardware that is used change our ability to do things and not do things. If space law is addressed to space objects and cybersecurity is addressed to networks and systems, then these two regimes intersect to the extent of how a satellite and a space system functions or is capable of functioning on a digital network using an on-board computer. Cyberspace and cybersecurity are everywhere now. If you can digitally connect something, you're on cyberspace, so cybersecurity is a concern: they can be hacked.

For commercial actors in space, a lot of the intersection between space and cybersecurity comes at the liability level. A nation might be on the hook for damage caused by a space actor, under liability in the international space law regime. Pursuant to the Outer Space Treaty, States are responsible for the activities of their own state actor. Under the liability convention, launching States are liable for damage done. When a damage occurs against an object in outer space, then liability is fault-based.

Consider a situation where a cyberattack occurs and takes over the command and control of a communications satellite A in the geosynchronous orbit, and the attacker uses satellite A to collide with and to incapacitate satellite B. The question is: is the State owner of satellite A liable for the collision? Has there been fault? Actually, the fact that there has been a breach of the cybersecurity is not necessarily indicative of fault. The solution is a solid law and the fault is based on what a reasonable, a prudent satellite operator would do in this situation.

Here an example of faults: did the owner of satellite company A employ state-of-the-art information security protections applicable to critical infrastructure? Did they employ security standards for an IOT device? Between those two questions, where does fault lie? A satellite operator might not be at fault for this cyberattack if they are using state-of-the-art information security protections, if they are treating the satellite in geosynchronous orbit as if it is critical infrastructure, and if they have documented evidence of it. However, if the operator has treated the highly valuable geosynchronous orbit satellite like it is a networked housing object, they might be more likely to be at fault because they haven't done the things that a reasonable prudent satellite operator would do to secure their operations. The interplay of cybersecurity and space law is the extent to which a space player employs the requisite amount of security based on the risk to the system.

No one is cyber secure and that a system is never secure. There are always entry holes and ways in, and some people are looking for them.
A system can be resilient, which means that an operator has the ability to counter attacks and to mitigate attacks when they happen. The absolute security is really unattainable and therefore cybersecurity is about risk mitigation, assessing possible threats and looking at the cost for the mitigation of those threats, taking into account the value of the data, the value of the information system, and the resources that you have to put towards that. The other thing to remember is the more complex the system, the less resilient it is.

Space is a strategic domain, so some satellites likely qualify as critical infrastructure. For commercial actors, the question is how we maintain a requisite level of cybersecurity, especially when they are functioning in the strategic domain. Cyberattacks and cyber threats to the satellite have national security implications, and commercial actors therefore have to think about how their satellite might affect national security.
These national security implications mean that the actors have to take risk assessment and risk management into account when they are assessing cybersecurity risks. Some satellites are more likely to be targets of entities that are looking to disrupt national security objectives of another state.

Cybersecurity from an enterprise perspective is very much about compliance with laws, regulations, and policies. These are often general and usually concerned with individual data is not possible to put down specific technological standards, or to say that cybersecurity is going to require a certain type of encryption, because two months later, two days later, all of that can change as technology advances really quickly.

Laws, regulations and policies often have to do with individual data. The first one is the HIPAA regulation in the US, the GDPR in the EU, and the CCPA which is the new one in California. The next thing for a company is to show they are compliant with industry standards on how to do cybersecurity. For instance, the National Institute of Standards and Technology (NIST) framework for critical infrastructure cybersecurity, the ISO/EIC 27000 family of standards, and in particular 27001, on information security management systems. These texts are not stating a specific way to be cyber secure but tells how to do compliance. There is a need to make sure that this data is secure by checking certain boxes. Each enterprise, each company might choose different technical implementations of security.

Considering all of these points the idea that underlies cybersecurity is that you are paying attention continuously. Currently there are not a ton of space specific cybersecurity standards. Some industry and government initiatives are underway to develop these, but development has been slow, because it used to be really difficult to perform a cyberattack against a satellite. It is possible to jam and spoof, but actually affecting the command and control of a satellite was seen to be tough. Because satellites are physically remote so as a result, we didn't protect them in this way and we didn't really think that we had to. Suddenly, we're recognizing that cybersecurity threats are everywhere, and that space is not immune from that. Therefore, the space industry is sort of playing catch-up right now and trying to figure out how to do this and compliance.

In both technical and legal fields, it is really important to have a written policy describing how to comply with the different obstacles and the different standards. Those policies have to be backed up with actual technical implementation. .ISO 27001 certification is sort of a gold standard for information security. However, if the employees of a company don’t know the policies, there's no technical implementation. Cybersecurity is both being technically secure and being able to show how and why the security is done. The goal is to show that the company is a reasonably secure space operator in case of a breach. This idea of a reasonably prudent cyber operator is a legal term. In the common law world, a succession of cases is slowly building up what this idea of a reasonable prudent person is. If it's just tort law, it's a reasonable prudent individual. If it is a mining company, there would be practice over time that shows what reasonable prudent mining companies do in certain situations.

This concept doesn’t exist in the space world yet. It is very unclear what a reasonable prudent space actor is. A reasonable prudent space actor doesn't just apply that to space security, it’s a question on the issue of debris mitigation and end-of-life, or what is a reasonable prudent space operator when it comes to mega constellations. Cybersecurity plays into that and there is no background on how space is secure enough.

Hopefully, as the space sector is moving forward, more laws, guidelines, or best practices will emerge so we will be having a better idea of what constitutes a reasonably prudent actor. Referring to Dr. Blount article ‘A Satellite is Just a Thing on the Internet of Things’ written in

2017, a space actor needs to be concerned about cybersecurity because satellites and sensors are just more connected devices and it is important to figure out how to secure them. Finally, Dr Blount presented his most recent book about how cyberspace is changing the way that we think about international and global governance.

Blount PJ, Reprogramming the World: Cyberspace and the Geography of Global Order, E-International Relations Publishing, 2019

Blount PJ, A Satellite is Just a Thing on the Internet of Things, Air and Space Law 42, 2017

RAM LEVI

Cybersecurity and Space Assets

The first important thing to note is that a cyber risk is coming from an adversary that can be located in any part of the world without a limitation of geography. This adversary can operate at the speed of light, and can create some kind of a damage, whether it's for financial purposes economic purposes, activism to negate some kind of system. Furthermore, space is vulnerable because of the way it's built. Some attacks can enable adversaries to achieve strategic results without paying a high price. It is also possible to negate a satellite service without negating the satellite itself. One of the biggest advantages of cyberattacks is that even if a nation knows who was behind the attack, they will most likely not disclose it. That gives a very interesting opportunity for adversaries to conduct attacks which are actually almost cost-free, because if there is no law enforcement and no punishment, adversaries can do whatever they want.

When it comes to cyberspace, it's not enough to look at the cyber space or at the satellite itself. It would be more useful to look at an attack from a service perspective and to protect entire satellite systems, including the ground stations that receive the downlink, the supply chain, and all the service providers around those ground stations, as well as the infrastructure of the launchers.

The regulation around the space industry has not been developed enough to drive the satellite operators and manufacturers to consider cybersecurity. Because cybersecurity is slowly becoming an enabler for innovation, and because of the commercialization of space, the next step should be to standardize, regulate and create a culture of security of cybersecurity within the space industry. Operators tend to think that cyberattacks are a relatively new phenomena, but they're actually as old as computers, and computers have been around since the 1960s.

Referring to the movie “Underground: The Julian Assange Story”, released in 2012, rumours spread that NASA wanted to launch a plutonium-based satellite to space. At the time, there were protests outside the Kennedy Space Center in Florida by anti-nuclear groups regarding the use of such plutonium-based power modules in Galileo. The shuttle was supposed to be launched in 1986, the same year Challenger exploded. The protesters claimed that if this shuttle blew up “like Challenger did”, the plutonium spill would cause widespread death to residents of Florida. A worm called “WANK” appeared on a DECnet computer network shared between NASA and the US Department of Energy (DOE), days before the launch of a NASA space shuttle carrying the Galileo spacecraft. On infected computer's screen, the WANK worm displayed a political message and a file deletion dialogue that tricked users into believing that files were being deleted.

Today, it looks like everything is flowing in bits and bytes, and that criminals are hard to understand. Quoting Michael Rodger: “conflict in the cyber domain is not simply a continuation of kinetic operation by digital means, it’s unfolding according to its own logic which we are continuing to better understand”. For experts the understanding of this new phenomena is a challenge.

One of the problems is that companies have to defend themselves with their hands tied behind their backs, because they cannot hack back: this is the role of the government. Companies’ chief information security officers don’t know what they need to protect. Networks are so complex, and the threat landscape changes almost on a daily basis that it's almost impossible to know what they are defending. “If you don't know what you're protecting, how do you protect it?”

A lecture given by Rob Joyce during USENIX Enigma Event, on January 27, 2016 about ‘Disrupting Nation State Hackers’ is recommended. In this lecture, Mr. Joyce identifies the intrusion phases: reconnaissance, initial exploitation, establish persistence, install tools, move laterally, collect exfil and exploit. He explains how adversaries think.

Almost 17,000 vulnerabilities are discovered every year. Out of that, about 1/4 are high vulnerabilities which means they can be used to take control of a device without any interaction from the user. Usually, a cyberattack can be done remotely. This explains why chief information security officers have to deal with a great amount of high-risk vulnerabilities.

This phenomenon creates a management problem almost impossible to fix and that it is very tough to recreate proper defence. For example, the European Space Agency (ESA) officially recognized in 1998 that someone took control of the ground station operating the German-US

Rosetta satellite and changed the direction of the satellite towards the sun to damage it. This attack created new irreversible damage to the optical sensor. This is one of the few examples that there are physical attacks against satellites and that operators don’t have any ability to do something about it.

A Der Spiegel journalist came to a ground station called Stellar Communications Systems in Germany, and showed the employees the amount of information regarding the network architecture of the ground station, including a map of the ground station networks. He explained that this is what adversaries know, that they collect information, so they know what they're attacking. To this, the engineers answered that the adversaries know the network probably better than them: they know most of the routers, and the map was constituted of the deep network between the company’s clients and the ground station. It means that adversaries can listen and eavesdrop to every communication coming from and to the ground station. Attacks against ground stations and satellite systems are happening all the time, even if we don't hear about most of them.

The theory of system transformation is helpful to understand how a satellite system can be disrupted without any attack against the satellite itself. According to this theory, in order to get a system to collapse, you have to eliminate only a partial amount of nodes in the system. A partial amount of nodes is around 10 percent of the system of the nodes. With this amount, there is a probability of 50 percent that the system will collapse without prior knowledge. If it is possible to reach 50 percent of the system, then there is 100 percent probability that the whole system will collapse.

For a space system, the components of a system include the ground station, the satellite itself, the antennas, the public switched telephone network controlling the antennas, and the computers used to do the invoicing for the ground station. Considering the supply chain, the employees, the workers, and their phone, if an adversary target 50 percent of them at the same time, there's a hundred percent chance that the ground station will not be able to function. If the ground station is not able to function, the satellite will not be able to provide the service, because the ground station doesn't function.

As an example, consider the destructive worm that started propagating in 2017 from Ukraine to companies operating from Ukraine and then to about a hundred countries in the world. Think about how the attack was built and how high the financial loss was: there were very little consequences, only mainly sanctions, and that they didn’t make a big difference in the ability to restrain adversaries. Attacks against space-based assets will come from a nation-state. This is a big issue because it will be hard to find insurance covering nation-state attacks against space systems.

GPS jamming occurring in the Middle East and coming from different sources in the area of the Black Sea, eventually to prevent guided missiles from receiving the GPS signals. This is a case of an attack against space-based system which has become critical for our daily life because ships are using GPS to calculate their course over ground. Therefore, jamming it is not only a safety issue but an operational issue with consequences on maritime business and on airlines companies. However, it is very hard to assure an efficient defence against these attacks because of the dual geopolitical tensions if nation-states are involved.

Quoting Albert Einstein: “we cannot solve our problems with the same thinking we used when we created them”. Applied to cybersecurity, Mr. Levi offered the audience four laws to implement every time they approach a cybersecurity problem. First, cybersecurity is an art, it's not a science. It needs to be adapted to the company, its culture, people, structure, IT architecture, and so on and so forth. Each cybersecurity strategy policy procedure is different. Second, context is important when talking about a system, an environment or a company. It is impossible to copy one protection, one strategy from another company.

Third, focusing on risk management the question is: how much money companies are willing to spend to close exposures. They need to achieve the time to market quickly so they need to save costs. They cannot spend too much money eliminating a security risk, even more for a company whose ability is to transfer the risk to a third party which is usually an insurance company.

Fourth, a cyber risk is a human-made risk and cyberattacks are human-made risks and not only a technical issue.

Underground: The Julian Assange Story, Robert Connolly, 2012

Rob Joyce, ‘Disrupting Nation State Hackers’, USENIX Enigma Event, January 27, 2016 – https://www.usenix.org/node/194636

The Space & Cybersecurity Project Group, under the SGAC, provides a platform for students and young professionals to contribute to technical and policy debates on the nature of space and cybersecurity.
https://spacegeneration.org/projects/space-cybersecurity