SPACE AND CYBERSECURITY
PROJECT GROUP

April 2020

SECOND WEBINAR REPORT

DR. BEYZA UNAL – "CYBERSECURITY OF SPACE-BASED WEAPONS SYSTEMS"
STEFANO ZATTI – "PROTECTING SPACE MISSIONS FROM CYBER THREATS".

Acknowledgments

The organisers wish to express their gratitude to Dr. Beyza Unal and to Mr. Stefano Zatti for their outstanding presentations on "*Cybersecurity of Space-based Weapons Systems*" and "*Protecting Space Missions from Cyber Threats*".

The Webinar immensely benefited from their valuable insights and expertise on cybersecurity and space issues.
Appreciation is also extended to Lucille Roux and Laetitia Zarkan for their support in the organisation of this 2nd webinar, for moderating it and for contributing to this report.
The organizers would like to express their sincere appreciation to Thea Flem Dethlefsen and Antonia Russo for co-leading the Space and Cybersecurity Project Group and for highly supporting the organization of this 2nd 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.
In addition we want to spread the discussions by having the Group create a presentation that can set the basis for members to do cybersecurity presentations around the world themselves. In the longer run, we aim to create a cybersecurity test. At the end of the test participants can download an awareness poster on how to limit exposure to cybersecurity threats, which can enhance SGAC visibility.
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 potential 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 Lucille Roux and Laetitia Zarkan.
It summarizes the presentations and exchanges of the 2nd Webinar organized by the Space and Cybersecurity Project Group, held on April 30, 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 Beyza Unal is a senior research fellow with the International Security programme at Chatham House. She specializes in nuclear policy, cybersecurity, space security, and NATO's defence and security policy at Chatham House.
She formerly worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, taught International Relations, transcribed interviews on Turkish political history, and served as an international election observer during the 2010 Iraqi parliamentary elections.
Dr Unal's current research interest is in emerging technology applications and security in the Middle East. Dr. Unal also conducts research on urban preparedness and city resilience against CBRN threats. She has been given various fellowships for her achievements - most notably she is a William J Fulbright Alumni.

Stefano Zatti is a cybersecurity consultant and Professor of " Risk Management" in the cybersecurity master's program at the University of Rome (La Sapienza).
Mr. Zatti has worked for the European Space Agency for 26 years, covering leading positions within the ESA Information Systems Department and then in the ESA Security Office, that he founded and became the Head of. Previous to that, he worked as a Research Staff member with IBM Research, working on projects on inter-networking, security (KryptoKnight) and security management (Samson).
He holds a Laurea in Mathematics from the University of Pavia and a Master of Science in Electrical Engineering and Computer Science from the University of California at Berkeley.

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 moderators

Lucille Roux is a Trainee at the Council of the European Union, DG Economic Affairs and Competitiveness, Competition, Research, Industry and Space Unit.

Laetitia Zarkan is on the United Nations Institute for Disarmament Research Graduate and Professional Programme and affiliated with UNIDIR's Weapons of Mass Destruction and Other Strategic Weapons Programme.

STEFANO ZATTI

Protecting Space Missions from Cyber Threats

Mr. Zatti started his presentation by stating that space is a basic element for the security of the European Citizens. He identified the elements of security in space and from space, including space situation awareness systems (SSA), satellite tracking, maritime and land surveillance and the protection of critical infrastructure.

Examples of hacking, spoofing, spying in space were presented, such as the damaged caused to the German-US ROSAT space telescope and the interference targeting the satellite Landsat 7 in 2007 and 2008, among others.
Mr. Zatti mentioned the media coverage of these events and how the European Space Agency (ESA) was targeted and how the breach revealed sensitive information related to the agency.

Mr. Zatti described a typical space mission. He explained that space elements are controlled by a network through a link. The network is managed by control centers that telecommand the space segment, receive and process payload data, and carry out house-keeping telemetry. The control centers disseminate data through centers segment to the user community.

He listed the threats to a typical space mission, such as hardware failure and space debris directly affecting space elements, and uplink jamming or payload interception against the

network. He warned the audience about cyberattacks against users and control centers to intercept data.
During the presentation, Mr. Zatti pointed out the motivation behind these threats: financial gain expected, negligence, competitors after information and knowledge, strategic moves from States, hacktivism, and terrorism.

He analysed the potential damages caused by these actions and their consequences for space missions, among which the change of trajectory and deorbit or loss of device, data stealth…

Mr. Zatti revealed some of the countermeasures aiming at safeguarding interests of space operators. He described the functioning of on-board crypto processors based on computer platforms before mentioning the importance of redundancy, SSA, data encryption, key management, authentication, and end-to-end cybersecurity.

He pointed out four key elements about the latter: physical, personnel and information protection as well as information assurance. To mitigate the risks, mission categories are characterized with different security levels applied to each of them.

Mr. Zatti concluded his presentation by declaring that NewSpace will imply new cyber threats since it's a matter a competitiveness, especially for the European space industry and strategic interests.
He underlined the challenged that stem from the increased reliance upon commodity software and hardware for space and ground segments that leaves the door open for cyberattacks.

Zatti Stefano, Space and Cyber Threats, *in* Schrogl Kai-Uwe (eds.), Handbook of Space Security, Springer, Cham, 2019

DR. BEYZA UNAL

Cybersecurity of space-based Weapons Systems

Dr. Unal started her presentation by identifying three parts: the first one concerning space as an enabler for all the mankind and its inevitable interdependency with digital technologies, the second one focusing on the tremendous cyber risks and consequences to which strategic space assets are exposed, and the third one being oriented on the capabilities requirements to tackle this new challenge.

First, Dr. Unal underlined the importance of Space as an enabler for supporting both national and international infrastructure. She illustrated her statement by pointing out all military missions which have been engaged since the end of the 20th century and the beginning of the 21th rely on space capabilities. Dr. Unal stressed the dependency of space capabilities on digital technologies (e.g. cyber technologies), which could undermine confidence in the performance of strategic systems, the loss of trust in technology. She addressed some issues related to integrity, availability, and confidentiality of information. These different aspects impact the credibility of deterrence and strategic stability. She highlighted that mission assurance is disproportionally affected by this vital dependency on space-based assets and the exponential number of cyber risks. Altogether, these issues could increase the risks of misperception in time of crisis and lead to miscalculations in decision-making.

Dr. Unal also pointed out that, in the aftermaths of the previous statements, military staff and cadres (e.g. within NATO) rely on data received through space products and space services to support sensitive missions. More specifically, she laid down the core space services available, namely Position, navigation and timing (PNT), Intelligence, Surveillance and Reconnaissance that provide support to threats assessment or targets identification, among others. Dr. Unal also highlights the importance of space-based assets for communications, environmental monitoring, weather forecasts, and space situational awareness (SSA) for the tracking of space debris and for the detection of threats to space-borne assets.

Second, Dr. Unal flagged that both space products and services could be disrupted due to the reliability of space assets on digital tools. Dr. Unal described cyber risks as follows : on one side the actor-specific threats, on another side, active and passive threats. Such threats target interconnectivity and data, supply chain and design vulnerability as well as two-way communications links.

As consequences, she explained that such cyber risks might hamper products and services assurance required for supporting sensitive activities. For example, cyber risks could undermine PNT services with a loss of contact with troops deployed, a failure of weapon system accuracy, ISR services with a loss of situational awareness, and communications services with the compromised integrity of data. Ultimately, Dr. Unal suggested several measures to implement in order to tackle the risks generated due to the critical interdependency between space and other domains in the exposure to the threat of cyber risks. To that end, Dr. Unal urged the necessity for national and international actors to build up adaptation strategies and to invest into mitigation measures, and in the resilience of space based assets. She highlighted the importance of developing a forward-looking resilience with pro-active design principles, dynamic and flexible considerations and future proofing for space-based assets.

To conclude her presentation, Dr. Unal proposed several resilience measures related either to general or specific space services, among which PNT, communications, reconnaissance satellites.

Unal Beyza, Cybersecurity of NATO’s Space-based Strategic Assets, Chatham House, International Security Department, 2019

QUESTIONS AND ANSWERS

The presentations were followed by discussions.

Between the three infrastructures that support space missions – ground segment, space segment, control segment – which one do you think is the most likely to be targeted?

Stefano Zatti: We initially thought that attacking the space segment is much more difficult than trying to attack the ground segment because of the need to build a ground station to access the uplink, which means basically investing a lot of money in creating the possibility to uplink the data.

Nowadays, with the cyberspace connecting all different networks, it is actually equally possible to access the ground network as well as to access the space network. Space links can be abused. What are the motivations? The most rewarding target is the data. Data is brought to earth so it's accessible on servers, on databases on the ground.

If they intend to damage the spacecraft, the space link can be hacked. Whereas traditionally the ground segment would be more targeted, nowadays via the cyberspace, it is equally possible to target all different components of a space mission.

Dr. Beyza Unal: In the military, if you think of all the crisis or conflict situations, you would probably be seeing that a physical attack might happen against the ground segment or commanding and control systems and so on.

You might see that cyberattacks target the space systems as well. In the space segment, the physical attack is hard. If you want to take out the space products, you might actually want to attack the space segment in the military sphere. That's why all the segments have to work in harmony in a way.

Since cyber threats are 'unfriendly' but not necessarily unlawful operations, do you think we could infer a due diligence obligation upon States when those operations are performed as counterspace capabilities by States themselves?

Stefano Zatti: There is an uncertainty whether you have been hacked or not. After having been hacked, the most important thing is to put measures to prevent similar attacks in the future. If a country is hacked, if a critical infrastructure is hacked and you are aware of it, then you're already working towards putting the actions in.

That's why I believe that countries would not tell each other whether they are going to conduct the cyber operation or not. The whole idea about the deterrence in a way comes in handy for countries to use. I wish there was an operating procedure in a way on the industry but it doesn't exist.

Dr. Beyza Unal: It is important to be able to detect a cyber operation, but it can be difficult. There are not necessarily any clear evidence of an operation taking place. When you steal a car the fact that the car is not where it was left by the owner is a clear example that the car is stolen. But when you steal data this can be done in a stealth form so that the data is still there but somebody else is taking it.

With this kind of knowledge other opponents or competitors could have an advantage. In cyber operations, it is important tracks left after an attack are useful to identify the passage of perpetrators.

For instance, this is the same when you have a dust moved back by the fact that somebody has passed. In cyber space, there is always some kind of cybernetic dust left. The evidence can be built against an action which is perpetrated because the action is not only physical, but also purely logical, and some of the data that needs to be there remains where it was. So I want to underline the importance of having the possibility to build traces and to leave traces of actions performed by other parties to be used as evidence as forensic evidence.

Are space systems and satellites any more vulnerable than other military networks? Is there anything unique about satellites that might make cyber particularly dangerous?

Dr. Beyza Unal: Space has just recently become a new type of military domain just recently. NATO said that space is warfare domain. In space, for decades, they didn't consider much of the cybersecurity measures.

Constellations go up to space and they stay there for decades. If you're talking about weapon systems on the ground, you can modernize those weapon systems, and you can create a modernization process that could be much more easily conducted than for the space installations.

Stefano Zatti: On the protection of civilian, it is important to consider the security of the basic protection of the assets and protection of the data. ICT is a fundamental element for the design of the mission. Once this is done, this becomes basically a discipline related to the design of satellites and the design of space missions.

Security concerns require a proper risk assessment methodology. This is basically what I teach at the University. I can't think of any critical national infrastructure that does not rely on space technology: the energy sector relies on space technology or the financial sector relies on space technology for a time stamps for instance. If you think of any military operation in crisis conflict, most of the time the operations go beyond the weapon systems, their command and control and so on.
The best way to attack critical infrastructure is probably through cyber means. Everything is interconnected in that regard.

What type of mechanisms, if any, have been put in place by NATO member states to identify and respond to a cyber-attack against one of their assets?

Dr. Beyza Unal: NATO has been working on cybersecurity baseline requirements for the space domain. We will see what they're going to come up with. This means that the requirements will be there for countries to consider. NATO cannot actually force a member state to implement any of the cybersecurity requirements that they have discussed. Therefore, it's really critical for Member States to consider this is an important area for their national security.

Quantum communications encryption seems to be the best way to reduce vulnerability, especially in the space segment. What's the level of reliability of quantum communications encryption on current missions?

Stefano Zatti: I have a strong opinion on this: quantum cryptography is very nice theoretically, but in practice, it doesn't work. It is very nice to think that we can distribute keys by using the entanglement of the photons, and to detect if it has been tampered. But if the channel is very noisy, the success of the transmission is very low.

The capacity of the channel is so strongly reduced that it doesn't become practical. The practical use of quantum cryptography for the protection of the space-to-ground communication is still a long way to go, but there are a lot of exercises and a lot of ongoing projects. Maybe this is going to become a reality very fast but this is not a reality yet. Somebody may disagree and I'm happy to discuss.

Dr. Beyza Unal: The way that we have been discussing on quantum communications is really future-looking in our studies as well. In the current missions you wouldn't see quantum encryption technologies to be embedded, but in the future, you need to think about all the options.

Quantum being both the enabler and the problem maker and cause more stress. All of these needs to be identified. I agree with Stefano on saying that it's not yet not yet there but we need to look at the future because the future is more important when it comes to the cybersecurity or cyber threats.

On the other hand, I want to say that the quantum cryptography is for the future but quantum cryptography has been for the future since 20 years because it's not a new idea, but it is a pretty mature idea that has been actually proposed in the 80s'.
So theoretically, it has been there and promising for the future but the future hasn't come yet for 20 years so I don't know how many years we will have to wait.

How do you foresee the prospective relation between ESA, the EU institutions, ENISA and eu-LISA (Large scale IT system in the area of freedom, justice and security) regarding the establishment of a set of rules to frame cybersecurity on space segment, ground and control segments?

Stefano Zatti: The Consultative Committee for Space Data Systems (CCSDS) is a joint effort. It's not only ESA, NASA and all the other space agencies that meet regularly. For more than 10 years, they have put together an effort in order to define standards for the security of the ground link, so the communication between the different ground stations, and the ground to space link, the so-called 'space link extension'. This effort is well underway and it has defined and agreed upon a number of algorithms and solutions to define what can be done in order to provide authenticity, confidentiality, integrity, and availability to the communications. I would say this is something which is not forthcoming but it is quite mature. It can be found on by looking up the CCSDS documents.

In your opinion, what are the most relevant cybersecurity measures for space missions?

Dr. Beyza Unal: If you need to prioritize, I think I would say two things: supply chain security and design security. Those are the critical two points that we need to be focusing on. Supply chain security is highly important and it's really hard to grasp in a way and I know that there has been a lot of focus on this from many countries but I don't think that we are yet there. Most of the time, the focus is done to the big companies.

They are generally the ones who are putting most of the cybersecurity measures because there's a reputational risk for them, as well as monitoring risks. The focus should be also given to the small companies creating space technology. Some companies come and they create a certain level of system that can be used in space.

After a few years, they just disappear and because they are small and niche companies, they do not have this same kind of budget as big companies. Therefore, with the private sector it really is depending on the country regulations themselves. If the country does not put any type of regulations or standards or if they don't consider it in their procurement policies, you can't expect everything from the companies.

Stefano Zatti: Supply chain is particularly challenging because of the very strong drive to reduce costs and when one wants to reduce cost, it will tend or be tempted to choose the cheapest solutions, which are the ones that are less guaranteed in terms of absence of backdoors or potential weaknesses.

For what concerns the design, I think it's much easier because it's only technical – it doesn't touch other subjects – and not procedural. For a secure design, it would be beneficial to devise an architecture which is modular, which allows the activation of different modules depending on the needs that are characterizing each mission.

I describe it in one of my papers. This about the different so-called ‘protection profiles’ that can be enabled depending on the needs of a specific mission, in order to decide on a predefined infrastructure which ones are the levels that the specific missions would have to implement, and to pay for, to finance to get realized depending on what the specific needs of a mission category is.

What can be done to satellites that have been put in space for more than 20 years and don't have quantum crypto available and are at mercy of attacks?

Stefano Zatti: No upgrade of the onboard software can introduce better security in the communications of such an old piece, so the best thing is to use the very last onboard fuel left and use it to deorbit the equipment, thus limiting the amount of debris it can cause. This is what the "code of conduct" for satellite operation mandates nowadays.

How can an operator know when its satellites are being hacked if there is no loss of control ?

Stefano Zatti: I mentioned this in my talk, for lack of suspect behaviour, logs records of all on-board events must be generated and checked to create a trace of all occurrences and react upon it is needed.

In the spirit of the Space-ISAC (which seems rather US-Centric), what info-sharing initiatives are there in Europe/ elsewhere?

Stefano Zatti: A decade ago, there were far less satellites than there are today. Also, assuming hacking activity as well as tools to detect hacking activity have increased in the past decade, why are there only a handful of decade-old examples of real intrusion, why are there no (possibly anonymized) more recent examples of real cases?

There are more and more of these events of course, but in general there is reluctance to share such events for the fear of the loss of image (see my example with Anonymous that is only four years ago).

Personnel from both the ESA and NASA have transitioned to working from home in recent weeks in response to Covid-19. Do you think that this poses an increased risk, given at-home cybersecurity practices might not be at the same level as on-site?

Stefano Zatti: There is an increased risk for sure, but to mitigate it a home connection shall rely on proper VPN solutions to avoid exposure along the way. Ideally also from home a business computer (other than a private computer that stays always at home) connected only via VPM to the home network should be used.

SPACE AND CYBERSECURITY
PROJECT GROUP

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