Launch Pad Seminars: Episode II
Cyber Warfare in Space
May 27, 2020
Virtual Seminar

Cyber Warfare in Space

Panelists:

- Moderator: John Borrie (UNIDIR)
- Presenter: Beyza Unal (Chatham House)
- Respondent: Raji Rajagopalan (Observer Research Foundation)

John Borrie: Good afternoon, everybody. My name is John Borrie and kia ora, as we say in New Zealand. I am the Program Lead for WMD and Other Strategic Weapons at the United Nations Institute for Disarmament Research. I'm really pleased to welcome you today to this second in the series of Launch Pad Seminars that UNIDIR has organized with our partners...

The Secure World Foundation and the Fondation pour la Recherche Stratégique, FRS, Paris. People are connected all over the world to this virtual seminar and it's something of an experiment for us. Hopefully, we'll have smooth sailing today in terms of our technical things.

Of course something like this event is only made possible by global satellite communications, and in particular digital transmission of data through cyber and real space, but there were risks to this. Today we'll be discussing "Cyber Warfare in Space." What it is, what it means, and what might be done about it?

Before we move on to introducing our speaker and our respondents today, I like to make a couple of announcements, which will make the meeting go more smoothly. The purpose of this meeting is to provide and form a virtual platform, to keep discussing space security issues. Event is being reported. Event will be in English only.

To all of you who are coming in as participants in this meeting, if you can, please make sure that you keep your microphones muted and your cameras switched off. There are literally hundreds of people joining this meeting. If you're all making a tiny bit of noise, it's going to quickly become quite overwhelming.

If you want to find those controls, just move your mouse, if you're using a computer, you'll see a row of round buttons show up at the bottom-center of your screen. You'll see on the left-hand side, you have a microphone and sort of moody camera icons. If you hover over those, it will tell you whether you're muted or unmuted, or not. If you can make use of those, that would be really good.

We also have the ability to ask our questions and to gather your responses through a multimedia viewer. Some of you may have already participated in a poll that we've had running for the last few minutes. If you aren't aware of how to use that, again, go to the round buttons on your screen. Then, second from the right, you'll see a round button with three red thumbs on it.

If you click on that, a window will come up and at the top-left, you'll see probably in blue something that says, "Multimedia Viewer." If you click on that, that will bring up another window where you'll see more information and you could submit your answers.

That will be quite useful because we're going to be using this a couple of times in the course of today's one-hour [inaudible 3:11] .

Just a couple of other things. We'll be sending out a link for evaluations of this meeting in the next day or two. You'll be able to share your thoughts on what we've done right, what we've done wrong, and maybe how we can improve before the meetings.

It gives me great pleasure to welcome you to this event on cyber warfare in space. I'm pleased today that we have two great panelists. We have Dr. Beyza Unal, who's a senior research fellow with the International Security Department at Chatham House.

She's also the author of a very interesting report on cybersecurity of NATO's Space-based Strategic Assets. It was published last year. She's also done a lot of work looking at cyber and nuclear monitoring control.

The other panelists today is Dr. Raji Rajagopalan from the Observer Research Foundation in New Delhi. Raji is very knowledgeable in this area. In fact, just last year for UNIDIR, we published a paper on electronic cyber warfare in outer space. You can find that on UNIDIR's website at www.unidir.org.

Now I'm going to pass over to Beyza for a few minutes to talk to us. "What is a cyber-attack, and how does that translate to the space? Do these have unique features?" as somebody asked from China before the meeting, and "Why do strategic military systems depend on space-based assets?" Beyza, over to you.

Dr. Beyza Unal: Thank you very much, John. Just before getting into it that what does a cyber-attack, it's important to start with the understanding of the idea of space warfare, then I'll just take the audience to decipher part if you don't mind.

The whole idea of space warfare when we look at it has been in a way romanticized, I call it, for decades now. Both in the film industry and also in political decision-making, we see that romanticization.

Please, move to image one. The focus in that regard has always been given on the physical elements of space warfare, and not much attention was given to the cyber elements up until recently, I would say.

The reason why cyber became an important element of the discussion is, I believe in three folds. We can move to the second image.

The first reason I would say is that space technology if you look at it, relies on digitalization, and that the digitalization also is at the heart of the cyber technology. When you talk about digitalization, digitalization always comes with certain potential cyber vulnerabilities.

By exploiting cyber vulnerabilities, an adversary can be able to take remote control over satellite, for instance. I see that one of the members of the audience put that into the question that you've asked. They can jam satellite signals, they can spoof associated data to those satellites, and so on.

What we're really fearing of is the integrity, the reliability, and the confidentiality of data to be lost due to cyber interferences.

The second important part of this is that space technology is, when you look at it is integrated through the critical national infrastructure. That dependency, I think, is critical.

We can move to the third image, please. In the third image, you can see that I pointed out a number of critical national infrastructure that uses space and space technologies. Take energy sector, for example, space data is fundamental. It's critical for oil and gas pipeline monitoring purposes.

Or if you look at the financial sector, you will see that the GNS services are important for timestamps that record the timing of the completion of a transaction.

Why critical national infrastructure is linked to the weapon systems, in my mind is that in conflict time, the critical national infrastructure will be vulnerable as well. When we talk about warfare in space, we do not actually think only about what's happening in space. We also need to think about the whole ground segment, the Earth. What's going to happen on the Earth segment as well?

Moreover, I would say that the third point is that strategic weapon systems depend on the space technology. Defense sector for instance, heavily relies on all aspects of space services. I would say is that most of the dependency probably relies on the PNT service. The PNT service is the service mainly. The application comes from the GPS and the GNSS utilization.

If you think about strategic weapons systems and how they depend on the space technology for your question, John, weapon system generally use space technology for the space services that are highlighted in this slide.

As I mentioned, PNT is one of them. PNT provides, for instance, synchronization of military operations, or they support targeting operations to track forces and assets.

Environmental monitoring, for instance, is generally the one that most of the time is forgotten. Submarines rely on weather information, which is the environmental monitoring. All weather information is actually important in any military operation.

You need to know the speed of the wind, you need to know whether it's a cloudy day or a rainy day or a sunny day, and so on. All of these services, we rely on space.

We can move to image four. In fact, there is growing dependency of the use of space technology in military operations. In this image, you can see that during the first Gulf War, the space dependency was around 10 percent. When you look at the war in Afghanistan and Iraq War, you will see that this has increased fundamentally to 60 percent to the 65 percent respectively.

What I mean by space dependency is the utilization, the reliance on precision-guided munitions in military operations. These numbers come from official sources, UK Parliamentary Studies, and so on.

What I can say is that then, the reliance on space technology is only going to increase in the future. It would be naive to expect the type of decrease that will happen in here.

We need to realize that the future warfare is going to be hybrid in nature. This probably doesn't mean that warfare will take place in space in physical sense. It means in my mind that space services and products will be fundamental in any military operation, and for assuring that mission assurance in a way in national security.

In the last part that I would like to raise, please, move to image six, it is important actually to protect space assets from cyber attacks. It is fundamental to do so, and there are ways to achieve this.

The way that I look at it is threefold. We need to think about mitigation measures. In my mind, these are cultural and technical measures that could be addressed. We need to think about adaptation measures, which involves in a way adapting to the new contested or denied operating environment for the military.

Thirdly, and most importantly, we need to think about resilience measures, which probably is more about what type of future proof solutions that we need to rely on to protect space assets.

Only when I think we're able to provide resilience in the space segment against cyber attacks, the adversary will be deterred at the very beginning. That's how I would put it, John, in five minutes.

John: Thanks very much, Beyza. There's a lot in what you've just said and it'd be interesting just unpack some of these ideas.

Raji, how do cyber means of attack differ from electronic means of attack just quickly, because that may not be altogether clear to everyone and, I guess, who's got these capabilities? Have we seen many openly acknowledged or verified incidents of cyber operations, headlines of space object.

I know that you've been following these things and you've written about them. You want to share with us what you know.

Dr. Raji Rajagopalan: Thank you, John, and thank you, Beyza. That is a fascinating overview of the cyber warfare that takes place in outer space. Giving out a lot of facts and numbers to say how dependent the militaries around the world are on cyber and space, the interlink and interface, so on and so forth. That's terrific.

It's also important to see where we are heading. I think that's where it's also important to look at the differentiation between, for instance, John asked the question, "What's the difference between the electronic warfare and the cyber attack," so to say.

Electronic warfares essentially uses the radiofrequency energy to interfere with or jam communications to and from satellites, but they do not cause physical damage, whereas cyber technologies use an entire range of software network techniques to compromise, control, interfere with or destroy certain systems since lead to satellite operations.

I think it's again, the more these our space systems are linked to cyber nodes, the greater the vulnerabilities and gaps there are in a sense.

There have been many openly acknowledged and some incidents that have been verified. I think there are a number of countries that are developing these capabilities generally to engage in cyber capabilities, cyber warfare against non-space objects and targets as of now.

Against outer space access, there have been a few incidents that have been verified so far, because that's a critical aspect in terms of how reliable are some of the information available in open sources in essence.

In one of the earlier incidents, I think sometime in 2007 and 2008, there were two US satellites that were compromised to a ground station in Norway. This again was done via Internet was traced to China.

The severity of the attack particularly in the case of the 2008 attack was particularly alarming, because the hackers were able to achieve all the steps required to command a satellite, although there was no harm done to it.

That is, I do think and I argue that many countries have been testing out their capabilities to see the feasibility of engaging in the cyber operations and in-space assets.

Then in 2014, there was US National Oceanic and Atmospheric Administration, NOAA, satellite that was hacked. Again, no data was compromised. Again, the published news reports talked about the origin of this particular attack in China.

In October 2018, NASA was hacked where again, Social Security numbers as well as personal data of former as well as current NASA employees, were found compromising.

There have also been a group of Russian speaking hackers with possible links to Russian government, who have been reported to be using malware named Turla for attacks on communication satellites.

There have been a number of incidents that have come to light. Some of these have been verified. At least these few have been verified, but there are a number of incidents that have been reported to be happening on the cyber outer space front.

A whole range of other countries including Russia, China, Iran, and North Korea, have developed significant cyber warfare capabilities, but they have been mostly tested against non-space assets at this point in time.

John: Thanks, Raji. That's really interesting. It signals that we're not dealing with science fiction here. This stuff is going on and it's been going on for some time.

What's also been going on for some time, I see is we have quite a lot of questions flowing in from the audience, which is fantastic. I'm going to send a few of them your way Raji and Beyza.

To the audience, I have to be completely honest with you, I don't think we'll get through all the questions that we're being asked in today. We only have an hour, but we'll try to get through many as we can. If you do feel like including your name or where you're from in your question, we're happy to read that out, too.

Just a couple of quick questions for you, Beyza. One person was asking, you were talking about levels of space dependency in your presentation. Somebody was just asking where that data came from.

Also, though, there was a question about commercial space actors whether these actors are more vulnerable to hacking and militaries. I guess that links to something else, which I think would be really interesting to hear from you based on your work looking at NATO.

You pointed out in your report on NATO that NATO doesn't own any space assets of its own, it uses the assets of its member alliance date, but then that can create issues of its own in terms of the coordination between those different actors. Does that create any strategic vulnerabilities? Or, is that a good thing that increased resilience?

While you answer that, I'll ask Raji to mull over a question. Good cyber operations in space contribute to conflict escalation. Beyza, over to you first.

Dr. Unal: Thank you very much, John. I think I mentioned on the first question about the space dependency numbers. If you studies, one of them is the UK Parliamentary Study. They are all cited in the report that you've also pointed out into 2019 report that we published. They can find those numbers there as well if they're interested in it.

The second question on commercial space actors whether they're more vulnerable to hacking. That's an interesting and an important question. It really depends on, probably, whether the commercial sector or the organizations are actually being on top with their cyber maturity, I would say.

Partially, it also links back to how much military relies on commercial companies, and space products and services from commercial companies. The numbers are increasing every year even in the wars in Iraq and Afghanistan. I can't remember off the top of my head right now, but I know that the United States relied on commercial companies during the operations.

Now, saying that in my discussions with NATO officials on this is that even when NATO uses and relies on commercial companies, there are certain checks that they need to do before commissioning the company to go ahead and give the data or any type of services to them.

Also, they talk about certain level of hardening of the commercial systems and making them in a way coming to the military terms, but of course, this depends on who. If it is a company that completely works on space technologies, invest on space technologies, and have the budget to implement cyber requirements and baseline requirements that need to ask, that's perfect.

Sometimes, what we see in the commercial sector is that there's a small company that they just come for one specific objective. Once that objective is done in two, three years' time, they just either go away or they start to focus on something else.

If the company closes off, then the question is, who is accountable for any type of fall, breach that might happen during the longer duration of that service that need to or any other country is going to use that service for? I think that's partially important to realize.

I wouldn't say whether commercial companies are more vulnerable or not. I wouldn't answer yes directly, but I would say countries at least are trying to create some baseline requirements when they use commercial sector. In the last point that you raised on The Alliance, you said The Alliance does not have their own satellites and this create additional vulnerabilities in terms of cyber hacking.

That's an important interesting question as well because we debated on the subject a lot with some, again, officials. The officials are rightly pointing out saying that NATO does not have many capabilities. It's not only the set of lies in other areas. Also, that NATO doesn't have capabilities.

It's not actually fair. They say that it's not fair to say NATO space capability comes at the discretion of its member states. Probably, it's true, but the problem with the space assets is that when that discretion comes from the member states, you rely on the implementation procedures, the baseline requirements that that member state is putting on.

As NATO, you do not have much saying in that regard, whether those services or the products are secure or not. That is probably going to be a big problem in the long run if not right now. Because NATO right now, probably we're talking about eight to nine countries that have high space capability and a role in space.

But, the whole structures, 30 states, in the long run, that is going to probably affect. I'll turn to you, Raji, perhaps.

Dr. Rajagopalan: Hi. Thank you, John, for the question, for those cyber operations in space, whether it contributes to conflict escalation. That's a very interesting question, but it's also a difficult question to answer because it's not very clear as to how things accelerate and pick up the pace.

There are a couple of important questions to be answered before one can get to the conflict escalation point. For instance, what should be the criteria for deciding that a cyber attack has taken place in the first instance?

Because you also need to build consensus among states on this particular question, and that's not going to be easy. It's also likely that most states would agree that an attack has happened if it leads to physical destruction for them to see or even [inaudible 24:35] cause by a fatality of individuals and so on and so forth.

It's going to be a lot more difficult to reach an agreement on this question when there is nothing that you can see in clear terms as to what kind of damage has happened, and especially, if it becomes even more challenging when a state or private industry that has been engaged in this endeavor has used cyber measures only for tampering or testing other feasibility, or even for stealing data.

That particular interference has not resulted in any physical destruction of assets. It becomes a lot more difficult. Clearly, there are bases to do it. For instance, unauthorized access, generally, is considered a crime. But again, whether it would amount to international aggression, that's somewhat problematic and possibly a point of disagreement among the number of states.

That, in fact, is a sign of the larger problem that you see in the outer space domain, which is to build consensus among states. Finding that agreement among all the different states in terms of what has happened, how do we go about it, and so on and so forth, I think that's going to be extremely challenging in a sense.

It's unclear as to how you can determine that first and foremost an attack has happened. How do you respond to it? Can you call for a conflict escalation? Can you foresee conflict escalation? That's a separate challenge because of the agreement that you need to build among different states.

John: Thanks very much, Raji. What we're going to try to do under the discussion over the next few minutes is to put another question out to the audience using Mentimeter feature of the multimedia viewer. You'll see a slide on your screen, "Does a hack qualify as an attack on a satellite?" Yes, no or maybe.

Again, if you go to the round button on your screen with [inaudible 26:36] , you'll find your multimedia viewer there, and you can bring up a window which will be able to see around.

Results, we can already see. Maybe and yes. Yes is doing very well. We will continue to keep that open for a few minutes, but I want to ask a couple more questions to our panelists.

We're getting a lot of questions coming in. A lot of them are relating to broader strategic things such as nuclear deterrence and so forth. These are probably quite difficult questions to answer.

A very interesting question here, though, from one of our colleagues from Demetrius Ivanovich. He's asking, "Are there any capabilities for cyber and electronic warfare attacks using space assets against ground infrastructure?" Maybe that's one for you, Raji. You want to take that on?

Dr. Rajagopalan: Sure.

John: I got some question. I'll just queue up a question here for Beyza to think about as well. We're seeing these new technologies like AI and machine learning, and huge satellites, for example, cheap, small satellites that can be launched in large constellations.

What kind of impact to these likely to have? Will they increase resilience [inaudible 27:55] against cyber attacks? Will they make cyber attacks easier in the case of AI and machine learning? Is there been any thought about that? That'd be really interesting to hear what you have to say. Raji, over to you first.

Dr. Rajagopalan: Sure. Thank you. Thank you, Demetri, for the question. I don't think we have too many incidents where we have seen attacks on ground infrastructure. Mostly, this has been on satellites. In a sense, for instance, I can give you how the ground operations have been affected.

There are a number of incidents to show that. For instance, in 2010-12 period, North Korea was using GPS spoofing of the South Korea's GPS signals for days at a stretch thereby affecting their flights, ships, and even personal devices.

I haven't come across really situations or if there have been several number of other incidents, but again, none of them have been, in a sense attacking, the ground stations as it. Mostly, these have been in those communication satellites or GPS, and so on and so forth.

GPS have been particularly the most attractive option target for a number of countries or private individuals, hackers who have been engaged with this [inaudible 29:21] .

None so far that have targeted ground. At least, none new confirmed reports to suggest hacking of grounds stations, for instance, but number of incidents involving the attack on satellites that have in turn affected ground operations.

John: Raji, can I just ask a quick follow-up to that from Tom Hickey, one of our colleagues at UNIDIR?

He asked -- It's a good question because it's not necessarily obvious to our audience - "What are the advantages or disadvantages of using cyber capabilities against satellite compared with other counter space capabilities?" Can you just shoot them down with ASAT detectors, or use lasers or something like that? Why use cyber?

Dr. Rajagopalan: That's a great question. In fact, Daniel Porras from UNIDIR and I did a paper long ago on looking at the cyber outer space interface, in a sense, for the Observer Research Foundation. Again, we're looking at that particular point to see that.

There have not been despite...For instance, the return of the ASAT are with the Chinese. They conducted their one of the first successful satellite that just in 2007. You still did not see too many other countries following that path.

That was a good thing because anti-satellites are -- One, they are inherently destabilizing in many ways. Second, the amount of long-lasting space debris that they produce, that's a much larger problem when you look at the space security, but also the long-term sustainability of our space. Those are much bigger challenges.

Whereas, cyber is a much more attractive option because anybody who can jamming a device or hacking option, you don't need a whole lot of expertise. These things are available for a couple of hundred bucks on the Internet. You can buy these things.

It's much easier to use the cyber option as against...Even lasers, lasers again, things are available, but we have not seen too many countries, too many places going down this path. We haven't seen too many different [inaudible 31:43] , too many states, or even other place using lasers at this point of time.

There are instances of abuse, but it's been still limited. Using cyber, it's cheaper, it's easier to produce, easier to procure. The biggest attraction with regard to cyber option is that it gives you the deniability option.

You can conduct in cyber option, getting engaged in a cyber attack, and [inaudible 32:12] deny that of your role and responsibility in that particular attack in a sense. It does give you a huge amount of advantages when it comes to cyber options, which are not necessarily available with other kinetic, or even other lasers and other such options.

John: Thanks, Raji. That's really a nice segue into the question for Beyza. Beyza, while you're answering, I'm just going to ask our producers if they might be able to bring up the slide again with the results of poll while you're talking. Over to you.

[pause]

Dr. Unal: What I would probably say that the emerging technologies are an opportunity and a curse at the same time when you think about protecting space assets. There are a number of opportunities that comes with emerging technology that I think it's important to focus on dimension on artificial intelligence and machine learning.

Cyber intrusions. Detections can be done through artificial intelligence and machine learning applications. There has been some work going on in that regards, not in the space sector that I know of, but in other sectors that probably the space sector would get on board as well at some point.

There are also robotics-related applications that's out there to be discussed for cleaning space debris, which is fundamental. Also, I would say for resilience purposes, I'm also looking a little bit on the quantum technology side of the issues, mostly on quantum communications, as well as quantum sensors and sensing technology.

Of course, the quantum technology, we're not yet there. But, what I'm trying to understand is can we create a certain level of future proof understanding on resilience by relying on these technologies? Or, would these technologies be a problem by themselves or not?

I would say in that regard to a new technology, you need to do a risk assessment, whether that emerging technology can create an opportunity or a risk.

John: Thanks, Beyza. Let's just look at this slide for a moment. Our respondents are here. This is super interesting. What you guys are telling me is that there are already hacks of satellites going on, and they have been for some time.

66 percent of our respondents think that a hack qualifies as an attack on a satellite. Very few of them say it doesn't, and we've got about a third of people who are undecided. That's interesting because this is going on all the time. It's pretty serious.

We don't see states reacting in a way they would say if they had a ship or an airplane attacked by somebody else. It is interesting, isn't it? What do you guys make of this? Raji?

Dr. Rajagopalan: Absolutely. The numbers are very interesting and a clear demonstration of the fact that much of the strategic community believes that this is a serious problem and this is not going to go away. I think that also ties it to the fact that an earlier question that you had put to Beyza. For instance commercial actors, whether they are more vulnerable in a sense.

I think that is both yes and no. In one sense, I would say that private sector may have more stringent guidelines and best practices in play. They may actually invest a great deal more in financial and technical terms to remove some of the vulnerabilities from hacking or any such kind of acts of cyber warfare.

At the same time, we are increasingly seeing a trend where private sector is launching satellites with mixed payloads and mixed stakeholderships and so on and so forth, which makes them equally vulnerable or even more in that sense.

This may not be the case so much in Asia because most of the Asian states still have the states running their space program, but it comes to a lot of Western countries private sector has been an active player even in the security and military space programs in a sense. Therefore, the vulnerability of the private sector in that sense is a lot more, I would think.

But the cyber, whether it's hacking, jamming, all of those things are only going to go up because given the current state of the play in terms of the major power relations and the changing balance of power dynamics at play, I would think the competition is only going to intensify. You will see a lot many more incidents in the coming years.

John: Thanks, Raji. Beyza, do you have anything to add?

Dr. Unal: Yes, I guess so. This is an interesting slide. I'm more focusing on the 32 percent of the maybes, [laughs] and the 3 percent nos than the 65 percent yeses. The 3 percent nos, it means that we couldn't convince them with our speech.

The maybes is really interesting because I think what they're saying is that it depends on the hack itself, and I agree with that. It's a yes and a maybe at the same time, I would say. Some hack for instances like traditional espionage type activities, do you qualify them as an attack?

How can you qualify something as an attack if it did not have, let's say any kind of cause of injury, or a death, or it didn't damage any infrastructure, it didn't cause any damage in any place? This is really a hard question in that sense, in that small question you were asking a lot [laughs] from the audience.

Coming back to your question, what is cyber attack? I didn't actually fairly give the definition to you. There is a definition that the Tallinn Manual makes. That definition would answer your questions in here as well. The Tallinn Manual says that a cyber attack is an attack as a type of operation in a way. It could be defensive or offensive in nature.

Then in that operation, it should either cause an injury or a death to a person, or it should cause damage or destruction to the objects. I think that's important to qualify. Thanks, John.

John: Thanks, Beyza. That's a really useful point. Maybe we should have rephrased that question somewhat and said, "If a hack causes physical damage or destruction to the satellite, is it an attack?" or something like that. That would be an interesting question to answer another time.

We've got a lot of questions coming in. There isn't going to be time to answer many more of them. Quite a few of these questions seem to be about the sorts of responses. What do you do about this?

Raji, in the Unity of Space Dossier that you wrote for us last year, you noted that existing multilateral regulatory frameworks seem to be insufficient to cope with the threat of space systems posed by both cyber and electronic capabilities. You said that new measures defining norms of behavior and rules of engagement [inaudible 40:30] are required.

What would be some possible ways forward, in your view? Would there be transparency measures or something else? Where could these kind of things be viewed? I notice, for instance, we've had a question from someone in Venezuela asking about those sorts of issues.

Beyza, for you, I wondered in view of your thinking about NATO, and some of the Alliance and the arms racing dimensions of this was because, of course, NATO has a big interest in this, the leading space powers including the US, China, Russia, and India.

What other things that we might envisage on those states agreeing on to try to reduce this problem, but at a time where there's quite a lot of strategic tension, competition, and rivalry [inaudible 41:28] . This is a big question. I know maybe you want to take a shot at that. Raji, you want to go first?

Dr. Rajagopalan: Yeah, sure. Thank you. Thanks, John. It's absolutely clear. Anyone who has been working in this domain would know how contentious the debate has become when it comes to the global governance of outer space, and the new and emerging challenges, how do we deal with them.

You have had some of their very good comprehensive measures like the Outer Space Treaty, but there are certain important gaps, which is, for instance, Outer Space Treaty does not ban the weapons other than weapons of mass destruction. It does not prohibit states from placing weapons in outer space -- conventional weapons or any other weapons.

In a sense, states have also come around to interpreting this in a very, very broader fashion to say that [inaudible 42:25] weapons placement is not a violation of any of their commitments. We are reaching a very, very dangerous turn with those expansions or a very broad base debate in a sense.

We need to find very innovative ways to deal with these particular new sets of challenges, whether it is electronic cyber warfare, and also other types of challenges that are coming about. One of the first ways to recognize is that states have ultimately the responsibility when it comes to any challenges, any attacks that stem from within their territory.

One of the best ways to tackle this particular aspect is to look at the UN Security Council Resolution 1540, which is a good measure. I would say that it might be a good useful thing to look at in the context of cyber warfare as well because it mandates each state to control the actions of citizens and individuals within its borders.

Cyber is a domain where individuals can hack or jam a particular satellite, and so on and so forth, and states can come out and say, "Oh, we don't have any control over this particular sector. This is not a state entity or she's not a state entity. It's up to me. It's just an individual."

Here is where mechanisms like the UN Security Council Resolution 1540 can also be looked at as a model to develop something along those lines for cyber means. It's also important to look at where do you debate some of these issues because, traditionally, we have discussed security and strategic aspects of outer space within the city in the Conference on Disarmament in Geneva.

Given the state of the affairs -- The stalemate situation for more than two decades -- that's not really going to take us very far. Again, we need to look at other options. UN Disarmament

Commission could be one where we could get the process of introducing future possible regulations about it.

That could hopefully lead to better understanding more policy convergence at a slightly later date. I have my suspicions about how things might pan out there because given the recent conduct of the UNDC in the last couple of years, the prospects of effective deliberations are slim.

I would say that we need to try all the different avenues. Again, if at all we get to the UNDC and other such platforms to debate some of these questions, there's a broader way to look at cyber electronic warfare under one basket and/or otherwise follow a much narrower approach to define what an armed attack against outer space object is all about.

The requirements for verification and monitoring mechanism in a future instrument, or even a mapping exercise to identify the national technical capabilities, and to avail a means for verification and monitoring. In this regard, UNIDIR has an excellent paper to look at, but these are some of the ways to get the debate started. This is not going to be easy.

Once you have these debates, [inaudible 45:50] the UN Disarmament Commission level, you can take them later to the General Assembly First Committee or the UN Security Council for further action.

I wouldn't say that any of these are going to be easy, especially in the last few years, we have seen how even some of the multilateral processes such as the UN Group of Governmental Experts initiatives have suffered in that sense.

It's the inability of the major powers to come together or develop consensus on some of the critical issues have been a major impediment in creating future pathways, but we need to try every possible avenue and every possible initiative. There is a group of states which believe that voluntary mechanisms are the best way even the current contentious nature of industry traditions.

There is another group of states which believe that our TCBM or transparency and confidence-building measures are only supplementary measures, but it cannot replace the importance of legal instrument. We need to find the midway. I believe there was even a debate about having legally binding TCBMs. That might be something for us to look in terms of further taking that process forward. Thank you, John.

John: Thanks, Raji. It's really useful and it is interesting in bodies like the Conference on Disarmament, and the discussions on PAROS or the Prevention of an Arms Race in Outer Space. It's interesting, isn't it?

There's a chicken and egg problem that I've been talking about PAROS and the importance of it 40 years or more. That they don't negotiate any legally binding agreements because they have these very, very different conceptions of what PAROS is, whether you're, for example, a Western country, whether you're from another part of the world.

I guess today's strategic environment in which you're seeing more and more rivalry, in particular between the United States, Russia, and China, this is complicating things. In that sense, over to you guys, what are your thoughts on those other things that might be possible?

Dr. Unal: I think it links really well with your question on NATO and the arms race, and how NATO countries should be thinking about these issues. One of the challenges on that is the legal challenges.

What has really allowed in space for NATO and member states is they need to be agreed from there end as well, and it needs to fit into the international law and the norms that exist in the space already. When you have 30 member states, it's hard to get an agreement on these things.

That's going to be an important point of reference that we need to be tackling in the next round. As you know, space became a policy as a space policy within NATO. It's an operational domain right now. As cyber [inaudible 48:57] , and land and maritime domain is, is the same way that NATO is seeing it. There are certain elements that they will still continue to work on.

For instance, they need to focus on the acquisition policies that need to be sorted out. They need to focus on enhancing resilience requirements. They need to focus on the baseline requirements or all the best practices.

There are also of course considerations that need to be done on interoperability of the forces because NATO forces rely on space assets, and that really thinks to the interoperability of them. In the next three or four years or so, these are the focus areas that the NATO member states are going to be working more on. Thanks, John.

John: Thanks very much, Beyza. That's really interesting. One of the questions that we have had today...I'm not sure we have time to answer it, but somebody was asking and it relates back to what you were saying about resilience. What if there was a cyber attack that knocked out the Global Positioning System all around the world?

At one level, that's the military system, but in another, it's a very widely used civilian system, and if suddenly knock it out, they could have quite a humanitarian cost because it's so widely used for navigation and all other functions in the modern age. I guess it goes back to the question that you guys were discussing before, which is what really constitutes a cyber attack?

What is that threshold? There does seem to be quite a key question. What I'd like to do now is if our producers can bring up the next question that we have for our audience, who hopefully have been absorbing and digesting everything that you've been saying today, what can be done to make space-based systems more secure?

You guys have thrown out some ideas and become interesting to see what our audience thinks, too. Hopefully, people will find the multimedia viewer, and then will start putting their answers in and we can start populating the slide and seeing what people are thinking out there.

[pause]

John: I see precisely what new [laughs] idea increase understanding among stakeholders. How do you think that this can be done? Do you have ideas, guys?

Dr. Unal: How this can be done?

[laughter]

Dr. Unal: One of the points that's raised us...

[crosstalk]

Dr. Unal: Go ahead, John. Sorry.

John: No, up to you.

Dr. Unal: One of the points that's been raised actually is on the standards. It's an area that we've been focusing on as well. I know that there are some commercial work that's going on with regards to standards. Can we think about space standards just the same way as we were thinking about cyberspace standards?

We have been doing some work on that, and I think it would be a good way of thinking about how to make it more secure, how to make the space-based systems more secure. That's a really good idea. There was a comment on the GPS and GNSS systems. If you want to make something more secure or more resilient, I think there are a few characteristics that you need.

One thing that you need is the system to be robust. The other thing that you would need is redundancy in the system. If it is only the GPS/GNSS that we're relying on, and at NATO at the moment we do, then you need to think about alternative PNT applications that could be applied in operations.

For communications, I saw a question that came out on 5G, for instance, would it create vulnerability, or so on? I look at it on the other way. I think 5G actually would be helpful, because the communication systems today relies on two things, either the ground segment information or from the space segment.

5G can create decentralized communication networks for military operations. We need to think about redundancy, I think that's really key on making space-based systems more secure.

The last thing I would point out is that, when you're thinking about redundancy when it comes to cyber, you also need to think about not to copy-paste the same software that has the same bugs to the next redundant system.

Because while you're thinking that you create redundancy, what you end up doing is actually you're repeating the vulnerability in the redundant system. Designing it from designing stage is really important to consider cybersecurity. Raji, do you want to add anything else?

Dr. Rajagopalan: Yeah. It's an excellent point. First on the number of stakeholders and how do you get them, too. I think that's an interesting dynamic that's been the part of the conversation in some ways in the outer space domain, but how willing are stakes in a sense to engage for instance, the private sector has. They do come up with security standards.

They do come up with various protocols as part, because they are making significant financial and technology investments. They want to make sure that the vulnerabilities to those technologies are removed in the sense.

At the same time, to make them an active stakeholder when it comes to developing norms of responsible behavior or even have them as an active stakeholder in the room. You are still seeing some resistance when it comes to private sector engagement. That's part of the problem in that sense.

Cyber may be slightly different, but when it comes to outer space, which is somewhat more a traditional sector in that sense. You are seeing a lot more sustained government to government engagement as the principal driver of the government's debates. I would argue for a bigger role for the private sector, because that can change the dynamics in some sense.

The other aspect is we need to call out irresponsible behavior. There have been a lot of debates, a code of conduct for instance, whether they change the behavior of a particular state. It does not guarantee good behavior from states.

At the same time, if you endorse a code of conduct, it does bring in certain amount of peer pressure onto you to adhere, to certain standards, to certain responsible behavior.

Therefore, when you see there is a bad behavior, there's has been an attack, those so on and so forth, coming in from a particular state, we need to call out irresponsible behavior, bad behavior and so on and so forth. There are issues that we need to deal with.

My larger point is to have an expanded stakeholder base, so that you drag the number of people who have a stake in ensuring the global governance to reach some progress is that many more. I think that is the only way, too. The private sector should be given a greater say.

John: Thanks, Raji. That's really important, and thanks to both of you and to Beyza. There are a lot of interesting answers coming through on the slide.

One point that seems relevant to me, is that in space it also means the major protagonists thinking through some of the sites of these attacks and their potential consequences, and focusing on areas of cooperation where there are these tragedies of the common situations that should be avoided.

It seems to me resilience works to a degree, but if you have cyber attacks cause satellites to slam into each other and cause loads of debris, then everybody loses. There must be areas of cooperation where that would be possible.

Also, tried to hit off wasteful arms-racing where there's a mess of [inaudible 57:38] type solution. What we're going to do now is we're going to wrap up because it's been almost an hour. I want it to thank our presenters today.

Raji Rajagopalan and Beyza Unal, you've been fantastic panelists. I want to thank you. I hope our audience has enjoyed the session today. I am sorry that we couldn't take more than a few of your questions, but loads of interesting stuff here.

I encourage you to read Raji's paper and to read Beyza's work on the CRA as well. There's a lot of good food for thought there.

We will be sending out evaluation forms, as I mentioned by email over the next day or two. Please fill these in. It helps us improve, helps us learn how we can deliver on what you out there want to learn about.

I would also invite you to join us next Wednesday for Episode 3 at the same time of The Launch Pad Seminars. It's going to be on rockets, missiles, and space lessons from the Hague Code of Conduct and beyond. There's going to be really an interesting meeting.

I also want to, as well as thanking our presenters, I'd like to thank the many people behind these themes who are working on this event. It is a huge amount of work, believe it or not, to do an event like this, particularly on a platform like WebEx.

Thanks to our colleagues at Reese McCann who helped to produce this event, and also my colleagues at UNIDIR, in particular, Daniel Perez and Leticia Zac Ken who has done a huge amount of work behind the scenes.

There on the slide, you can see the information about our next seminars. I want to thank you once again, and I hope you have a wonderful rest of the week. Thank you, and from us, goodbye.

Dr. Rajagopalan: Thank you, John.

Dr. Unal: Jonathan, thank you.

Transcription by CastingWords