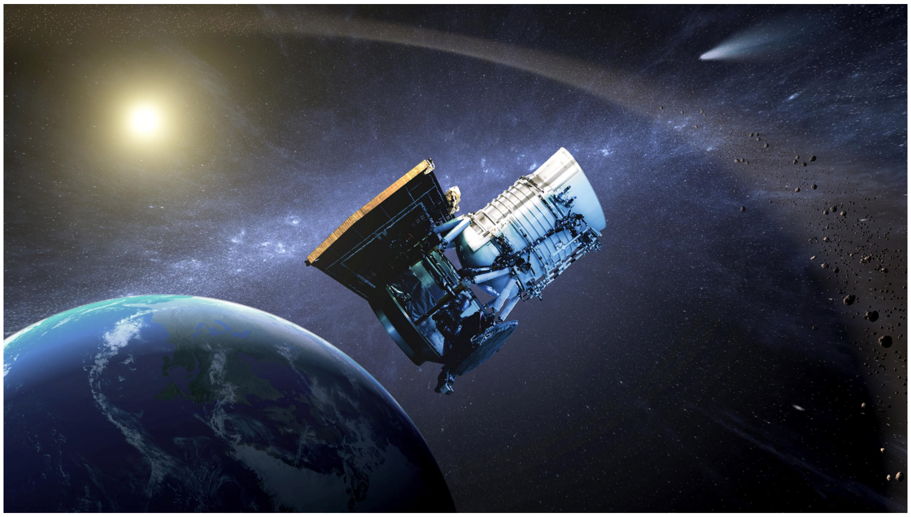
March | 2018

Commercial Companies' Perceptions of Security in Space

A Virtual Think Tank (ViTTa)® Report



Produced in support of the Strategic Multilayer Assessment (SMA) Office (Joint Staff, J39)

Deeper Analyses
Clarifying Insights
Better Decisions

www.NSIteam.com

Author

Nicole Peterson

Please direct inquiries to Nicole Peterson at **npeterson@nsiteam.com**

ViTTa® Project Team

Dr. Allison Astorino-Courtois
Executive VP

Weston Aviles
Analyst

Dr. Belinda Bragg
Principal Research Scientist

Sarah Canna
Principal Analyst

Dr. Larry Kuznar
Chief Cultural Sciences Officer

Dr. Sabrina Pagano
Principal Research Scientist

Nicole Peterson
Analyst

George Popp
Senior Analyst

Dr. John A. Stevenson
Principal Research Scientist

Interview Team[1]

Weston Aviles
Analyst

Sarah Canna
Principal Analyst

Nicole Peterson
Analyst

George Popp
Senior Analyst

What is ViTTa®?

NSI's **Virtual Think Tank (ViTTa®)** provides rapid response to critical information needs by pulsing our global network of subject matter experts (SMEs) to generate a wide range of expert insight. For this SMA Contested Space Operations project, ViTTa was used to address 23 unclassified questions submitted by the Joint Staff and US Air Force project sponsors. The ViTTa team received written and verbal input from over 111 experts from National Security Space, as well as civil, commercial, legal, think tank, and academic communities working space and space policy. Each Space ViTTa report contains two sections: 1) a summary response to the question asked; and 2) the full written and/or transcribed interview input received from each expert contributor organized alphabetically. Biographies for all expert contributors have been collated in a companion document.

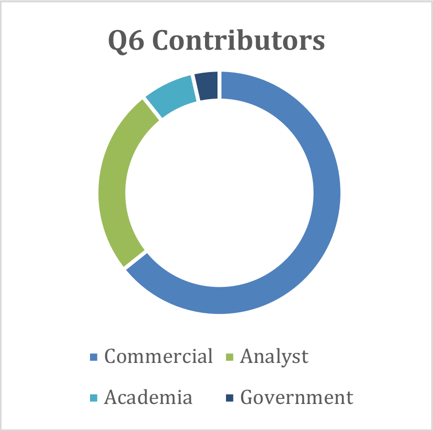
[1] For access to the complete corpus of interview transcripts and written subject matter expert responses hosted on our NSI SharePoint site, please contact **gpopp@nsiteam.com**.

Cover Art: https://www.army.mil/article/152664/future_army_nanosatellites_to_empower_soldiers

Question of Focus

[Q6] How do commercial ventures think about the security of their space assets during peacetime, crisis and conflict? Do industry leaders think about warfare in or through space differently than military leaders? What are their main concerns? How reliant are they on governments for warning or protection of space? What are their threat priorities?

Expert Contributors



Roberto Aceti (OHB Italia, S.p.A. a Subsidiary of OHB, Italy); **Adranos Energetics**; **Brett Alexander** (Blue Origin); **Anonymous Commercial Executives**; **Anonymous Launch Executive**; **Major General (USAF ret.) James Armor**[2] (Orbital ATK); **Marc Berkowitz** (Lockheed Martin); **Bryce Space and Technology**; **Caelus Partners, LLC**; **Elliott Carol**[3] (Ripple Aerospace, Norway); **Chandah Space Technologies**; **Matthew Chwastek** (Orbital Insight); **Faulconer Consulting Group**; **Gilmour Space Technologies**, Australia; **Michael Gold** (Space Systems Loral); **Joshua Hampson** (Niskanen Center); **Harris Corporation**; **Dr. Jason Held** (Saber Astronautics, Australia); **Dr. Moriba Jah** (University of Texas at Austin); **Dr. T.S. Kelso** (Analytical Graphics, Inc.); **Dr. George C. Nield** (Federal Aviation Administration); **Dr. Luca Rossettini** (D-Orbit, Italy); **Spire Global, Inc.**; **Stratolaunch Systems Corporation**; **John Thornton** (Astrobotic Technology); **ViaSat, Inc.**; **Charity Weeden** (Satellite Industry Association, Canada); **Dr. Edythe Weeks** (Webster University) **Deborah Westphal** (Toffler Associates)

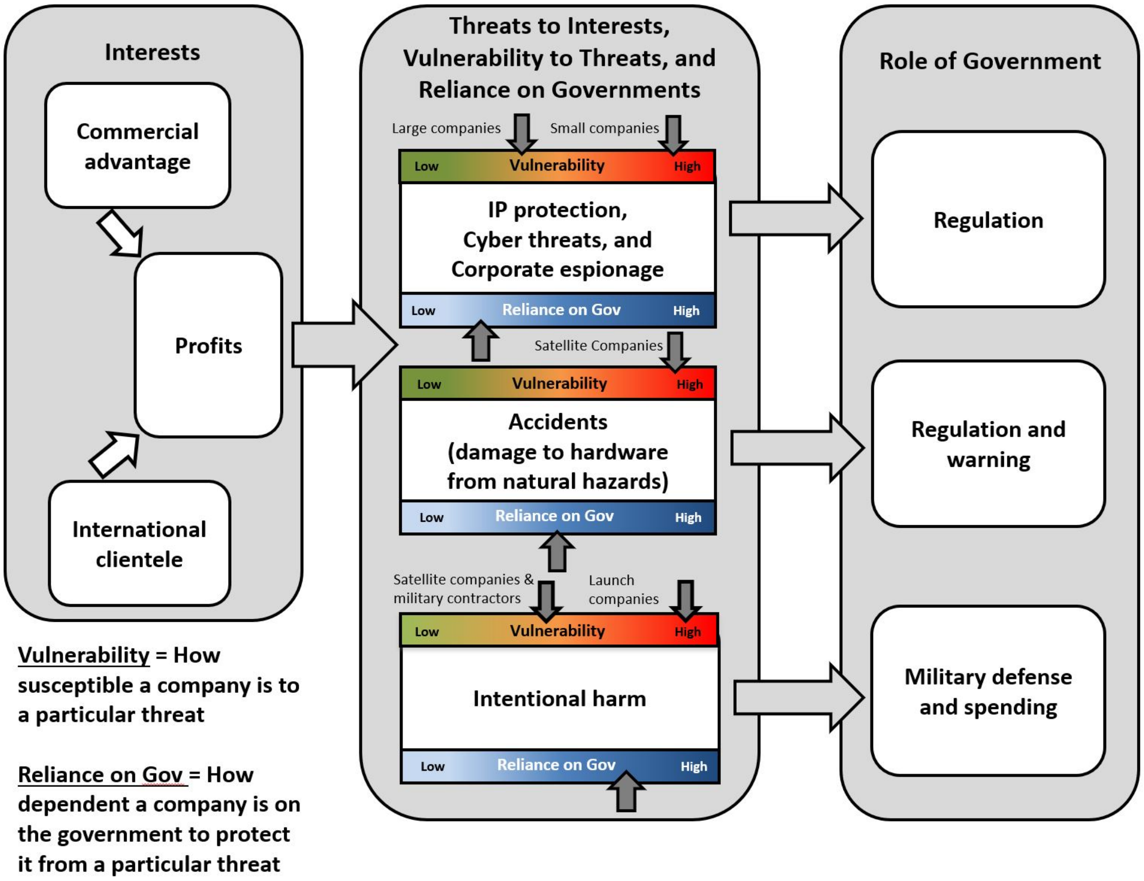
Summary Response

The expert contributors suggest that commercial companies' understanding of security is fundamentally different than that of military leaders. For both, security concerns reflect their primary interests; however, as their primary interests and goals are divergent, so are their perceptions of security and threat. When synthesizing the contributors' responses, it becomes apparent that there is a relationship between commercial actors' key interests, their security concerns and vulnerabilities, and their expectations regarding US government warnings and protection. This relationship is captured in Figure 1 below.

According to the expert contributors, commercial space companies' key interests are maintaining business operations, continuity of revenue, continuity of growth, and continuity of profitability. Their main concerns, therefore, are any and all actions or conditions that may threaten business operations and revenue and profitability—natural, accidental, or intentional. Furthermore, intentional actions can be the result of commercial sabotage or conflict.

[2] Armor's personal views, and not those of his organization, are represented in his contributions to this work.
[3] Carol's personal views, and not those of his organization, are represented in his contributions to this work.

Figure 1: Relationship Between Commercial Companies' Interests, Security Threats, and Need for Government Involvement


Interests
Commercial advantage
Profits
International clientele
Threats to Interests, Vulnerability to Threats, and Reliance on Governments
Large companies
Small companies
Low
Vulnerability
High
IP protection, Cyber threats, and Corporate espionage
Low
Reliance on Gov
High
Satellite Companies
Low
Vulnerability
High
Accidents (damage to hardware from natural hazards)
Low
Reliance on Gov
High
Satellite companies & military contractors
Launch companies
Low
Vulnerability
High
Intentional harm
Low
Reliance on Gov
High
Role of Government
Regulation
Regulation and warning
Military defense and spending
Vulnerability = How susceptible a company is to a particular threat
Reliance on Gov = How dependent a company is on the government to protect it from a particular threat

Interests and Threat Perceptions

The contributors indicate that we cannot think of commercial entities in the same way that we think about the national security space (NSS) community. Commercial space companies are primarily motivated by financial success,[4] whereas NSS is focused on security matters. Consequently, commercial perceptions of "security" are rooted in the potential of any situation or action (intentional or accidental) to threaten profitability.

Commercial companies are also involved in different activities than governments. They often have international customer bases and, consequently, multiple roles and ties to uphold, many of which differ from those of the government (Bryce Space and Technology). Contributors from Bryce Space and Technology explain how companies often adopt an international perspective because of their global clientele:

> Typically, if you're operating a satellite business, you have an international perspective. So, with respect to the consequences of conflict or pre-conflict activities, those industry

[4] Berkowitz; Nield; Thornton; ViaSat, Inc.; and Westphal.

> leaders are going to interpret them differently and bring different and useful perspectives to the table because they will see how those actions or situations will affect their broad business base, which is a global business base.

As several contributors note,[5] commercial space companies are not all the same; they vary in size, in the types of services they provide (i.e., satellite manufacturers, satellite launch companies, etc.), and in the clients to which they provide those services. These three factors, along with commercial companies' specific activities, shape their vulnerabilities. These vulnerabilities, in turn, contribute to their individual threat perceptions and security concerns.

Commercial companies' levels of vulnerability to specific security threats and, consequently, their primary security concerns, vary according to where their assets are located. For example, satellite manufacturers and operators are likely to be most concerned about threats to their assets in space, whereas satellite launch companies are likely to be most concerned about ground-based threats. Vulnerability can also be a function of size. Often, larger commercial companies can more easily afford to provide their own security, whereas smaller companies cannot (Adranos Energetics).

Clientele also affects perceived vulnerability. Many believe that the assets of companies with clients in the national security arena are at relatively greater risk of being targeted than those involved in other types of space ventures.[6] Conversely, contributors note that if a company is not involved with national security affairs, the expectation is that adversaries would have no reason to attack or tamper with that company's assets.[7] As a result, as the Harris Corporation contributors note, "commercial owners, operators, and manufacturers supporting purely commercial capabilities are unlikely to really think about potential threats or prioritize investments for self-protection."

Commercial Companies' Concept of Security

Some of the experts argue that, while commercial companies are concerned about security in space, they do not think about it primarily in terms of intentional kinetic attack.[8] Furthermore, industry leaders generally do not think about space warfare at all,[9] because they consider it to be outside of their domain. In contrast, contributors from ViaSat, Inc. state that kinetic attacks are a concern; and one that it takes "considerable moves to deter or eliminate."[10] The ViaSat, Inc. contributors note that their approach to this is to reduce the vulnerability of their network to attack and loss of continuity by "selling to all sides, [which] keeps us neutral or 'gray,'" and tailoring design techniques to eliminate the possibility of deliberate jamming.

[5] Gilmour Space Technologies; Hampson; Harris Corporation; Stratolaunch Systems Corporation; and Westphal.

[6] Commercial companies that work with the military do have a better understanding of warfare and the mindset of military leaders (Gilmour Space Technologies; Hampson, Harris Corporation; Stratolaunch Systems Corporation; and Westphal). Due to constant contact with these clients as well as their need to be able to understand the customer and their concerns, these companies develop a better idea of what the military's priorities are and how they think (Harris Corporation). However, even if a commercial company has former military personnel on board, commercial companies still do not think about warfare in the same way that military leaders do (Westphal).

[7] Held and Berkowitz.

[8] Anonymous Launch Executive and Bryce Space and Technology.

[9] Berkowitz; Carol; and Nield.

[10] Clarification on this point was provided by ViaSat, Inc. in response to an earlier draft of this report.

There is consensus among the contributors, however, that the primary concerns of commercial space entities involve the assurance of safe day-to-day business operations,[11] including avoidance of natural and accidental threats, spectrum interference, intellectual property (IP) violations, and vulnerabilities in cyber security. They are also focused on their ability to generate revenue, battle competition, and manage space traffic to prevent any sort of interference.[12] To reiterate, tracking potential international conflicts is not typically one of a commercial entity's day-to-day priorities, nor is thinking about protection from an active strike.[13] Furthermore, the contributors indicate that if there was a reason to be concerned about security in the military sense, commercial companies assume that the US government would offer protection.

Commercial Companies' Perception of Risk

As discussed earlier, commercial companies think about risk in terms of loss of profit and commercial advantage rather than national security and defense capabilities.[14] Most companies, particularly those that do not have military clientele, do not perceive their assets as being likely targets of military attacks or threats (Kelso). However, they do recognize that all of their assets are vulnerable to some degree at all times, and that in many cases there is not much that they can do to protect themselves.[15] Commercial space companies recognize that natural hazards, (especially space debris and space weather), cyberattacks, and physical attacks (including sabotage, RF spectrum interference, and spectrum jamming) could all damage their assets at any moment despite conscious efforts to drastically reduce these risks. However, their solutions to these vulnerabilities generally do not include efforts to harden their assets or build in redundancy (a cost-prohibitive approach for most). Instead, they rely on insurance to offset these risks.[16]

Role of Government: What Do Commercial Companies Expect?

Almost all of the contributors agree that commercial companies maintain an almost complete reliance on the US government for protection and space situational awareness (SSA) data from the Joint Space Operations Center (JSPOC). Several contributors[17] argue that this is because commercial leaders believe that the government is best positioned and equipped to provide security against kinetic or other militarized attack against their space assets. In addition, contributors from Adranos Energetics suggest that governments also have better political and legal standing to offer these protections:

> The groups that are in the best position to [regulate and protect assets in space] are governments because they have a greater power to enforce. They have greater incentives among each other, meaning governments have greater incentive to work with other governments than they do with some kind of group located in the US. They also have the resources in this and the desire to enforce it as kind of a public policy manner.

[11] Armor and Held.
[12] Armor; Chwastek; and Carol.
[13] Berkowitz; Carol; and Nield.
[14] Berkowitz and Westphal.
[15] Adranos Energetics; Anonymous Commercial Executives; Berkowitz; Caelus Partners, LLC; Chandah Space Technologies; Kelso; Spire Global, Inc.; and Stratolaunch Systems Corporation.
[16] Berkowitz; Caelus Partners, LLC; and Chandah Space Technologies.
[17] Adranos Energetics and Jah.

Interestingly, some contributors[18] suggest that the government is unaware of the fact that commercial entities expect the US military to protect them in situations of crisis and conflict. If widespread, this lack of communication and common understanding could result in serious government-commercial tensions and vulnerabilities, not only during an intentional attack, but also in response to a natural or accidental space event.

Many of the contributors also mention how inconsistently the government shares data with commercial space entities and how this leads to uncertainty and ambiguity on the commercial side (Jah). Furthermore, some commercial leaders believe that government information is often over-classified, making it difficult for companies to know what is going on in space (Westphal). If governments would provide more information, commercial companies would be able to operate more effectively and be more aware of what is occurring in space.

Despite their dependence on government provision of warnings and protection, some contributors suggest that there is a prevalent mistrust and uncertainty as to whether the government would actually protect companies in a time of crisis or conflict. Dr. Moriba Jah of the University of Texas at Austin even suggests that many companies think that the US government would be "ill-equipped" to adequately protect them from harm during a conflict scenario. This has prompted the establishment of a few private organizations that offer alternative sources of protection and security to commercial space companies.[19] These organizations are currently few in number, but more are emerging due to the growing recognition of the shortcomings in government support. The contributors stress the need for more transparency[20] and communication between the sectors to eliminate some of these misunderstandings, to explain their points of view, and to clarify what commercial companies' expectations are.

The Bottom Line

The experts are unanimous in their assessment that industry leaders do not think about security in the same way that the military does.[21] Commercial contributors argue that this is because they are focused on the health and success of their business ventures (their key interest), while the national security community is more focused on security the case of a conflict or a kinetic attack in space.

Contributors believe that the US government needs to be aware of discrepancy in thinking because the number of commercial space companies and activities are rapidly increasing, as is the probability of natural or manmade threats. Furthermore, as the US government continues to expand its reliance on commercial space capabilities for national security purposes, ensuring that commercial and government actors have a shared understanding of fundamental concepts, such as security, will be critical to avoiding costly misunderstandings and miscommunication.

[18] Gold; Jah; and Kelso.

[19] Anonymous Commercial Executives; Armor; Berkowitz; Caelus Partners, LLC; Kelso; and Spire Global, Inc.

[20] Jah; Kelso; and Weeden.

[21] Armor; Chwastek; and Carol.

Subject Matter Expert Contributions

Roberto Aceti

Managing Director (OHB Italia S.p.A.)
9 September 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during times of crisis and conflict?

R. Aceti: Let's say it would be difficult to respond in very generic terms because commercial ventures are different in nature and architecture and technological solutions, so it comes natural to me to think the kind of commercial venture that we have in mind here in OHB and most specific in OHB Italy and then, based on that, maybe we can try to respond to the question. So, if I can make a little introduction and explain the kind of commercial venture we have in mind, and then answer the question. So, very, very briefly, we have the plan and the idea to deploy a very large constellation of nanosatellites, meaning satellites in the 10, 15 kilograms class that will be put into specific orbits with a set of clear, and I will say ambitious, state of the art performance. The plan is to have a very short revisit time imagery program that is something that you can do with a large constellation, at the price of a resolution which is not exceptional. So, I would say a couple of meter resolution, three-meter resolution with 20 minutes to half an hour of time resolution anywhere in the world anytime. We are doing something that in my view is integrating very well what is already available: space assets which are monolithic large satellites that can provide an exceptional on-ground resolution that is inconceivable for smaller countries, whereas a constellation of this kind is an economically valuable complementary alternative.

So, our idea is to look into this market segment and to do it. But in general terms, I'm looking at the time resolution, as let's say a specific feature that would have a commercial potential, would also have an undeniable security relevance because you can do persistent intelligence with that kind of asset. That is the kind of commercial initiative that we have in mind.

To come back to your question, frankly speaking, if we are really talking about a large constellation of nanosatellites, then I have less of a concern of security of this space asset because we are talking about the constellation with obviously a sort of redundancy intrinsic on the number of spacecrafts that you need to provide a minimum level of service. We are talking about really small satellite, as said before 10 to 15 kilograms so in that sense, looking at my commercial venture, I do not have a major concern in terms of vulnerability of the space asset. Obviously, the security need or concern from my perspective, is really associated than to what we have on the ground because we need a complex ground segment to deliver the kind of service that we have in mind. It would include of course antennas distributed around the world. It would include control centers and also data storage and processing. And of course, that's where I believe the real vulnerability is in terms of for a variety of threats from terrorism to real war situations, we have conflict situation. If the question was what is the security issue in this kind of constellation, I would put the emphasis on the ground segment.

Interviewer: So, if I could summarize through the resiliency of the technology, the large constellation that took Nano satellites more redundancy there in grounds systems, OHB in this regard they're able to provide their own security and sort of disregard any threats through that technology, through just the sheer resiliency of their assets. Is that what you're saying?

R. Aceti: Let's say the architecture that we are going to end up with, descends from reasons which are different than guaranteed security because this is a project with a certain commercial perspective. Even if the commercial perspective is not the only one perspective of course but it's also a security aspect... A security aspect in terms of business, to be honest. But, let's say, we are really talking about hundreds of nanosatellites including spares, including redundancies and so on.

My perception of the vulnerability of the space asset as a whole is relatively low. The different level of vulnerability is if you have one monolithic satellite to work with and of course, in that case you are exposed in a number of threats like space debris that can destroy the satellite. If I have hundreds of tiny satellites, the probability of debris that is impacting simultaneously 100 satellites which are very small is negligible: I think this is not really too concerning anymore. If one or few satellites are impacted they can be easily replaced. The difference lies on the ground segment because on the ground segment we are exposed to any ground segment asset is exposed by definition to a number of threats both in peacetime and in wartime and so that's where the concern, is in my view, for this kind of project.

I don't know if I had answer your question but which way I think about the security of this particular venture because I said that I'm not able to generalize too much. I have to answer thinking about what we review in mind, in terms commercial venture and when I think whether we have in mind terms of commercial venture, I would say that I'm not too concerned about the space asset. I'm concerned about the ground asset.

R. Aceti: We have to introduce a certain number of measure which at the end, just to dwell a bit on this; I think the first level of response to this kind of threat is to introduce a certain redundancy. If we have a threat on the particular piece of the asset let's say one antenna but if we have a certain redundancy so the system is resilient to the loss of one antenna. That will be a way to counteract the problem. Yeah?

Interviewer: Right. Just a few points to that. First of all, speaking specifically as possible to your relevant knowledge and experience on is what we're looking for, so I appreciate that and please continue. Secondly, to follow up on the point, I think that you're saying is by virtue of sheer volume possible of the nanosatellites, the security of space asset is much, much concerning than the vulnerability of ground assets when it comes to be the ways. Is that correct?

R. Aceti: It's absolutely correct, absolutely correct. So, if I have to weigh risk, the risk that I've some major threat in the space assets in some ways that I can really imagine. This to me, is lower than if I have a cyber-attack on my data storage warehouse. That at least, is how I see the biggest threat or the biggest vulnerability on the ground assets.

Interviewer: Would you say threat to ground assets is a common concern for OHB? Really the point of this question is how effective the government is at that communicating threats like that to industry and vice-versa.

R. Aceti: OHB is a group of national assets all over Europe. OHB in general is not really so much directly concerned with ground segments. They are more of a space segment development entity, but in this particular case for this particular commercial venture, we are going to take responsibility for the overall system when we will build it. So space and ground and processing of data and so on. In this case again, I'm kind of generalizing, there is a concern about the ground segment safety and security and again my first level of response to it is to introduce a certain level of redundancy in that aspect as well.

Interviewer: How reliant is OHB on government warning with protection of space or today have successful with calculus that they utilized already?

R. Aceti: Honestly, we are totally reliant on government for warning and protection of space in terms of service, yes. I am not aware of any internal system to provide this kind of warning or protection that's here. This is something that to our mind, the government has to provide.

Adranos Energetics

Chris Stoker
Chief Executive Officer

Dr. Brandon Terry
Founder and Chief Technology Officer

11 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during peacetime or crisis?

C. Stoker: Yeah, sure. I'm just kind going to kind of use some examples. Like if I owned a satellite or had a bunch of satellites in space, I think it would be kind of to different threat form. One would be more of a cyber-threat and the other would be more of a physical kind of destructive kind of threat, when someone wants to destroy my satellite. I think as you're watching this on peacetime, crisis and, conflict, I think our elevation of concern increases and the peacetime I was always concerned that someone is going to take out your satellite or take control of it if they can using their cyber weapons. But in times of war that's going to go up, right? But other than that I don't know. Brandon, do you have anything to add?

B. Terry: No add. That was what I was thinking.

C. Stoker: They're not secure because you can't build any kind of… it's not like we're protected by global force fields here. So everything's open and it can be attacked at any time.

Interviewer: Okay. So, I have a few follow-up questions for that. Is intellectual property a concern, and is that a particular concern that you think is unique to the space industry, particularly in your space, or is this just a normal concern that you can find across any business that does international business.

C. Stoker: I think it's always a concern in companies like ours that are highly reliant on protection of IP at any time.

Interviewer: Okay. Then the second thing I'd like to add is about the security of space assets, so you can speak specifically about satellites in this case. As the safety of those assets becomes more and more of a concern, would you look to industry or some sort of institution or organization for protection of that? So, something like the Commercial Space Federation or the Satellite Industry Association, or would you specifically look to the government for some sort of mechanism to regulate and protect assets in space?

C. Stoker: I think that the groups that are in the best position to do that are governments because they have a greater power to enforce. They have greater incentives among each other, meaning governments have greater incentive to work with other governments than they do with some kind of group located in the US. They also have the resources in this and the desire to enforce it as kind of a public policy manner. So for those reasons I think, maybe I'm wrong, but I think by far I think the government.

Interviewer: With respect to companies in your space that you're familiar with as far as their threat priorities, does this enter the business calculus from day to day or is it just simply not a daily concern?

C. Stoker: I think it's a huge concern. I mean for us, I'll take IP for example. I mean IP trade secrets like we have…we're basically trying to play certain strategies to keep our IP safe even though we're following some pattern. We're highly sensitive to even nations in our own competition taking advantage of our IP and that's a huge issue. We don't do much about security in space, but we would have… we do a lot of cyber security concerns, we have a lot of those. We just don't as a small company have the money to really put into practice cyber security controls. So, all we do is all our sensitive stuff is basically left on computers or drives that aren't connected to anything. So yeah, we're really sensitive to that. Brandon, anything else do you think?

B. Terry: No. That's about covers it. Another thing that I think we worry about, especially probably even more during peacetime is always the fear and I've been seeing this as we go to some of these conferences especially in the small sat community, is as this micro-sat community enlarges and get more and more launches up there. This concept of I don't know if you want to call it orbital responsibility or whatnot, but I a big peacetime threat is what happens if somebody messes up and started getting space debris problems, collisions, inadvertent mishaps in space. Again, down the road, it's going to have to be something that's more strictly managed by either a government entity or a commercial group that comes in, just because the amount of objects that are 10 cm and above are going to be rapidly expanding here in the next couple of years.

Brett Alexander

Director of Business Development and Strategy (Blue Origin)
14 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of space assets during peace time, crisis, and conflict? Do industry leaders think about warfare and our current space differently than military leaders? What are their main concerns? How reliant are they on governmental warning or protection of space and what are their threat priorities?

B. Alexander: Yeah, I think from a Blue Origin perspective, you know, we are a launch company first and foremost and that's what we've been working on. My broader experience has been with commercial satellite companies and operators as well as [with] the government-hat on [there has been] increased awareness over the last 20 years about, you know, unfriendly actors doing jamming and other things as well as things that can happen to your spacecraft in space without being able to be able to tell exactly what happened to it. There is increased awareness about that -- about the need for situational awareness as well as possibly protection for assets.

Interviewer: Speaking specifically more the nature of Blue Origin as a launch company, would you say that your counterparts in the military and the government are aware of the specific concerns that a launch service may have? Is there a miscommunication between Blue Origin and the government, specifically on this issue?

B. Alexander: I don't think there's been lot of conversation between Blue Origin and the government about the security aspect for launch. I know that from a, on the government side, that there's, you know, there is concern or, you know, awareness of the single-point failure nature of launch. You know, of having fixed assets in a few locations that are vulnerable or at least could be vulnerable but that is not a conversation Blue Origin's had very much with the government.

Anonymous Commercial Executives

24 August 2017

WRITTEN RESPONSE

How do commercial ventures think about the security of their space assets during peacetime, crisis and conflict?

Space companies in general are familiar with the risk-base of their equipment, technology and data the moment an itme is launched into space. Space assets are a source of revenue and are typically considered sunk cost once on-orbit**.** Non-peacetime assured missions require additional capabilities, increasing cost. Commercial entities typically only expend such funds if costs are expected to be recovered, making sense from a strict business standpoint.

Once an asset goes into space, even in peacetime, there is always an assumption of atmospheric or space weather-related events that can occur. A technical malfunction is also always a possibility, derailing a mission.

Do industry leaders think about warfare in or through space differently than military leaders?

Yes, since space is used as heavily as a military intelligence gathering and holds assets, the industry is in tune with warefare uses. In addition, many companies are working in conjunction with the military, providing parts or services. There is a degree of unknown for companies when it comes to certain classified intelligence matters. Commercial space expects protection by the U.S. governmnet, much like inter-state commercial truckers don't arm themselves, but expect protection for state and federal authorities.

What are their main concerns?

Loss of revenue, no matter what the cause. Space companies expect protection .

How reliant are they on governments for warning or protection of space?

Historically, very reliant. Due to lack of adequate warning, however, commerical space is becoming more self-reliant.

What are their threat priorities?

RF interference, space weather, debris collission, and man-made intentional harm.

Anonymous Launch Executive

17 July 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during peacetime, crisis, and conflict? Do industry leaders think about warfare and or through space differently than military leaders? What are the main concern and how reliant are they on government forewarning protection of space? What are their priorities?

Anonymous: Well, so there's a couple of perspective differences between me and probably everybody else. The first answer I give you is we don't think about it. It's just not a concern to us because we're not specifically dealing with government activities and that sort of thing. So you know if we get attacked it's sort of a proxy on the US commercial asset, which I recognize could happen. But the second thing is the first part of our business is we launch vehicles so it really doesn't even fall into this category. You're thinking more generally I think about geo-assets that are up there and I'm quite aware on the classified level what's going on in terms of threats and things like that. But even when I was working with those guys, they just don't think about it, it's just not in their sphere of thought and I know with a lot of what the military does is that they try to educate these folks and on the fact that hey, if you're running military data through it, then that's considered a legitimate asset to be threatened in a wartime scenario. So now as far as we're concerned, we still think about it. And I think most people, their initial reaction was just what we were talking about

So the second part of our business is within the galactic sky and I think what we are going to be more concerned with in our galactic sky capability is actually cyber threats than we are for physical counter threats that we might be worried about with that. I'm thinking when you say threats, I'm thinking kinetic threats against it, I'm thinking ground-based threats. I won't be specific for obvious reasons about that. I just don't think people think of this. I think they think of think of cyber threats. That's probably in the way I look at things the more likely counter threat I would be concerned with a the commercial launch provider would get attacked by say a third nation like terror nation like Iran or North Korea or something like that, probably a cyber-attack anyhow. That's their easiest way to reach us. So yeah I don't mean to beat the air out of your question but we just don't think about it much. We would be completely relying on the government to tell us who's attacking and then we probably wouldn't trust what they told us anyhow.

Major General (USAF ret.) James B. Armor, Jr.[22]

Staff Vice President, Washington Operations (Orbital ATK)
7 August 2017

WRITTEN RESPONSE

To commercial ventures security means protection of IP and assurance of safe operations throughout the span of global geopolitics (peace-crisis-conflict).

Peace: industry expects & supports

- unpolluted environment (debris, spectrum), and
- "norms of behavior", that can be monitored and enforced, especially with non-US activities. (Space traffic management would be good), and
- limited rules/licensing for public protection (e.g., FAA/AST for launch, FCC orbit/spectrum registration). Basically support "fairness" & level playing field for commercial activities

[22] Armor's personal views, and not those of his organization, are represented in his contributions to this work.

Of course, industry leaders think differently than military leaders. Industry needs to think about safety of employees and owners'/shareholders' interests (value of firm – IP, assets, infrastructure, business relationship, etc.) Military needs to think about political & military objectives.

Industry now is very reliant on USG for space warning & protection (i.e., SSA). Commercial capabilities are emerging, however, due to shortcomings in USG support (timeliness, accuracy, liability). (Associations like SDA; service providers like AGI, SSC, etc.)

Marc Berkowitz

Vice President, Space Security (Lockheed Martin)
25 August 2017

WRITTEN RESPONSE

How do commercial ventures think about the security of their space assets during peacetime, crisis, and conflict?

Commercial ventures think about the security of their assets differently than the US Government national security and civil sectors think about the security of their assets. They are concerned about security in the context of their profit motive to generate revenue to obtain a return on investment, compete effectively in their commercial market segment(s), and extend and grow their sales, orders, and profits to provide value to shareholders.

Consequently, commercial ventures provide security and protection of their mission critical employees, information, infrastructure, and assets only to the extent required as part of their business plan to protect their investment and generate returns. This typically entails cyber, information, and physical security practices primarily to protect against natural hazards in the space environment, unintentional human-made threats, and the likeliest intentional threats during peacetime.

The private sector, in general, does not see its assets as likely targets in crisis or wartime and has no incentive to provide passive or active countermeasures to protect and defend its assets against the spectrum of threats beyond cyber security, electronic protection, and physical security. To the extent commercial ventures think about the security of their assets in crisis and wartime, they expect their governments to provide for their protection and defense.

Do industry leaders think about warfare in or through space differently than military leaders?

Industry leaders generally do not think about space warfare at all. While some US/allied military leaders also may not think much or at all about space warfare, there are at least some military leaders whose job it is to do so part or full time. Industry leaders are in business to make money. They do not see their businesses or assets as likely targets in the event of crisis or conflict. Industry leaders typically have a risk management mindset that takes into account geopolitical circumstances and other factors that could impact their business environment. They buy insurance to offset the likeliest risks (e.g., launch failure) for peacetime operations.

Only a small subset of commercial satellite communications and remote sensing enterprises, however, have business plans that lead them to seek to be integrated into the US national security space architecture. In the case of those enterprises, they typically are seeking additional compensation in the form of indemnification from liability, war damages, advanced funding, and access to classified information and/or technology to do business with the government and support national security operations because they have a profit motive and business case to do so.

While many privately owned and publicly traded US companies have boards of directors and corporate officers who are patriotic and most likely would respond favorably to requests for support from the US Government in crisis or conflict, there are many who do not believe it is in their best interest (i.e., believe their business case will suffer) if they are perceived to be aligned with the US national security apparatus.

What are their main concerns?

Commercial space businesses are primarily concerned competition in their market. With respect to security, their main concerns are natural hazards and unintentional human-made threats to their assets and operations (e.g., electronic interference, orbital debris, and conjunctions with other spacecraft). Secondary concerns are protection of their intellectual property against insider threats and (corporate or foreign) espionage; protection of their mission critical services and products against cyber and electronic threats; and protection of corporate officers and critical infrastructure and property against low intensity physical threats. As noted above, many commercial businesses do not want to be seen as aligned with the US Government because of the risk of losing customers and revenue because of privacy, civil liberties, and other issues that would adversely impact their financial bottom line.

How reliant are they on governments for warning or protection of space?

Commercial enterprises are very reliant on governments for warning of natural hazards, (e.g., space weather events), warning and assessment of conjunctions risks with resident space objects, support for resolution of electromagnetic interference events, support for anomaly resolution, and indications and warning of deliberate hostile actions. Their reliance on governments for conjunction risks and electromagnetic interference resolution, however, is diminishing as commercial entities such as the Space Data Association and ExoAnalytic, for example, are emerging to provide commercial space situational awareness data, products, and services to support space operations. In addition, aside from enterprises that have provided a degree of personnel, cyber, electronic, and physical protection, the majority of the commercial sector is vulnerable to attack and would expect their government to provide for their protection and defense in the event of crisis or conflict involving the space domain.

What are their threat priorities?

As discussed above, commercial ventures' threat priorities are: natural hazard; unintentional human-made electronic and physical threats; and intentional cyber, electronic, and low intensity physical threats (e.g., sabotage, terrorism). Some remote sensing space owners/operators are also concerned with directed energy threats (primarily low power laser illumination of optical sensors).

Bryce Space and Technology

Carissa Bryce Christensen
Chief Executive Officer

Brigadier General (ret.) Ian Dickinson
Chief Operating Officer

Phil Smith
Senior Space Analyst and Artist

26 July 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space access during peacetime, crisis, and conflict?

C. Christensen: Speaking primarily to the attitude of satellite operators, who launch or operate large satellites providing enterprise services to commercial customers and government customers. Just to give you context, Bryce works with many of those companies. We are an objective analytic resource, so, I'm going to provide you our insights and their insights based on what we hear from those companies and what we've learned about what they do.

Satellite operators deal with persistent jamming, spectrum interference, sometimes unintentional or accidental. Those concerns are a daily matter for those satellite operators. The idea that there is a clear dividing line between peacetime behaviors in which you operate your satellite and deliver your services in a manner that is unobstructed by others and a conflict situation in which you have to cope with obstruction, that's to some extent a false dichotomy, because those companies are identifying and responding to, managing attacks and disruption on a regular basis.

Companies that provide services to the U.S. Government (so that's either U.S. companies or the proxy companies, companies that are headquartered internationally, companies like SES and IntelSat) frequently articulate the perspective that they are like any other company working in the U.S. There's a desire to support, expectation of supporting the nation in wartime, that is normal. What I've heard these companies say is that comes with being an American company. I think that that's a serious statement.

This question has multiple parts. You want to go to each part individually or just kind of speak to them all?

Interviewer: Whatever you would prefer.

C. Christensen: The question of if industry leaders think about warfare in or through space differently than military leaders? Absolutely. Industry leaders tend to think about… I think there's an obvious answer that an industry leader is responsible for his or her business and has got to think about the effects of any given situation on that business. And that's not such an interesting insight, it's sort of obvious. To me, there are some other ways that industry leaders tend to think differently that I think are very interesting.

One is that industry leaders, particularly now thinking about satellite operators, tend to think internationally to a very great extent. Their customer base is often international, they may have distribution partners. Typically if you're operating a satellite business, you have an international perspective. So, the consequences of conflict or pre-conflict activities, those industry leaders are going to interpret them differently and bring different and useful perspectives to the table, because they will see how those actions or situations will affect their broad business base, which is a global business base.

Interviewer: How often does politics affect the decision-making practices of industry leaders and how concerned are they with the politics of their host nation?

C. Christensen: So…a few layers to that, and that's a really interesting question. First, there is the difference between a host nation as opposed to a customer nation. Consider a company like SES, which is headquartered in Luxembourg, which has a proxy company that is dedicated to providing service to the U.S. government, with its own board in the U.S. and using assets owned by the SES parent, which has global assets. The next layer is what do we mean by politics? One of the significant elements for those companies is the regulatory environment in which they're operating. We see that in the U.S., we see that globally in the protection of spectrum, terrorists and thieves, their ability to operate, their need to engage or partner with local companies. All those considerations are absolutely built into the process of managing a global business.

Politics in the sense of geopolitical dynamics of nation states as they ally and/or approach conflict, those kinds of considerations, I think, are certainly a part of decision making. They are part of the risk calculus of any large company and tracking those dynamics and their potential outcomes from the business' standpoint is part of the risk management job of corporate leadership.

Interviewer: Yeah, absolutely. So, would you say that occurrences like that, more centered around politics or the threat of conflict and the consequences of that, such as regulation, that is much more of a concern for the commercial sector rather than actually protecting space assets from a military strike, for example?

C. Christensen: I would say that there are a few things that you just listed. One is political dynamics around conflict, another is the regulatory environment of countries in which those businesses operate and deliver services, and the third was protecting assets from active strike--from a military strike as opposed to jamming or they could be commercially driven.

I would say that from a day-to-day standpoint, the most significant business issue of those three is the regulatory environment. I would say that the considerations of tracking potential conflicts is a less day-to-day consideration and protecting from active strike is certainly a consideration. Any company that operates infrastructure worries about ensuring that infrastructure continues to operate. Historically, that risk has not been a particularly large risk.

So, as our view of the space environment and the risks in the space environment evolves, and it's evolving rapidly… I can envision that as changing. The degree to which companies' corporate leadership pay attention to that explicitly, may change and evolve. But at the moment, I don't see it in daily conversations. It's not off the table, but it's not a daily focus.

Interviewer: Sure. And that's what we've been hearing from commercial companies so far. It's that as far as protection goes and warning, they're almost completely reliant on the government and it can affect their day to day decision making that much, if at all.

C. Christensen: If you define it as a kinetic attack as opposed to… as I said, they deal with jamming and lasing all the time.

Interviewer: Would the threat of that be from a foreign nation or another commercial company?

C. Christensen: To the extent that I have insight into this, and I have a little bit, but not comprehensive… the answer to that either/or question is yes. It may be a competitor in a foreign nation, it may be a government -backed competitor, it may be a hidden government activity for some other reason. The operator can typically identify or can often identify where the attack is coming from and will reach out to national leadership and say, "Hey, some actor in your space is not behaving properly and appropriately. We need this to stop."

Caelus Partners, LLC

Jose Ocasio-Christian
Chief Executive Officer

24 August 2017

WRITTEN RESPONSE

Commercial ventures look at the security of space assets as a significant risk to the investment into a technology. There are only two ways for a commercial venture to "protect" or "derisk" the deal: 1. Become a nation-state contractor to increase the probability that the government will protect your interests or 2. Get insurance to underwrite the risk. The easier of the two varies depending on the technology.

Because of the traditional dependence on nation-state support for space, many (if not most) commercial industry leaders in the space sector either have served in a government organization or have employees that have served in the military with appropriate security clearances. Space industry leaders' primary concern is a cyber-attack or a communication interference scenario between the technology they are invested in and the ground station / NETOPS that guides, controls, and gains information from the technology. Almost all industry players are significantly dependent on the National Space Defense Center. There are some international players and large industry who use other means to track debris and satellites to avoid collision or interference, but they are small in number.

Elliot Carol[23]

Chief Financial Officer (Ripple Aerospace)
7 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during peacetime, crisis, and conflict? Do industry leaders think about warfare and view space differently than military leaders? What are their main concerns? How reliant are they on governments through warnings and protection of space? What are their threat priorities?

E. Carol: Regarding security of our space assets, when we're assessing the risk of putting satellites into space or launching them, we're more concerned about natural threats. Threats such as meteors, asteroids, space junk, solar flares and not so much kinetic warfare. I have yet to experience either, through internal meetings or external meetings, a commercial company developing systems - at least a new space commercial company developing systems - specifically for space warfare, but with that said it's an easy way to justify a business model. I think a lot of new space

[23] The responses here represent the sole views of Carol and are not intended to represent the position of Ripple Aerospace.

startups, Ripple Aerospace included, see a potential market through military acquisition of our technology, in addition to development funding as well. What do we see as the biggest threat during peace time? Space Junk. I think the biggest threat without a doubt would be the aftermath of space junk flying in space and causing major damages to the satellites already up there and future satellites, in addition to the launch vehicles that we'll have to bring them up into space with.

Regarding the next question, do industry leaders think about warfare in or through space differently than most military leaders? Commercial space leaders, I do not think so.

Most of the people that I work with do not deal with the military and are focused on the commercial aspect of space. And I believe, based on my experiences, it is fair to say commercial space does not think about military conflict. So what are our main concerns? Personally, during conflict and or crisis, one of my biggest concerns is if satellites are taken out or damaged during a military warfare, what's the plan to get them back up there? Because, at least where I'm sitting, probably one of the most important assets for our nation is launch pads and yet, they're probably one of the most difficult to protect. I've asked this question with military officials. What is the plan if during warfare if the launch pads get bombed or taken out for any reason? I have tried to have those conversations because the technology at Ripple Aerospace is developing is a launch vehicle which is launched, semi-submerged from the ocean. We see our technology as a potential solution. I have yet to hear a convincing argument what the plan is. Any questions so far?

Interviewer: So, I would like to follow-up on that. As far as intellectual property goes, at least proliferation of innovation that a company like Ripple Aerospace is forging, is that a concern to commercial actors, that they expect government their government counterparts to protect them and their intellectual property in the event of corporate espionage or brought on either by in-country actors or foreign political actors?

E. Carol: At Ripple we have serious concern of demonstrating our technology outside the US and Europe. To be clear, we're a Norwegian company and am really the only US individual involved. There are always concerns about showing what we're doing to countries that are hostile to US, and especially demonstrating our technologies to countries like China because they have this reputation of using technology that were developed elsewhere and making their own, so to answer your question, yes. In regard to corporate espionage most of that is covered through NDAs. I was in finance before joining the aerospace world. I cannot believe there's an industry more strict with signing Non-Disclosure Agreements than aerospace. There is a concern about corporate espionage. I think there are only two or three instances where ex-employees started new companies. There hasn't been a scenario where a large corporation that I know of has gone after another corporation for stealing their information. Mostly it comes from internal sources that start their new company.

Chandah Space Technologies

Dr. Helen Reed
Co-Founder & Chief Technology Officer

Adil Jafry
Co-Founder & Chief Executive Officer

Lee Graham
Senior Research Engineer (NASA)

Christian Fadul
Co-Founder & Business Development

Andrew Tucker
Co-Founder & System Engineering

17 August 2017

WRITTEN RESPONSE

How do commercial ventures think about the security of their space assets during peacetime, crisis and conflict?

During **peacetime**, commercial ventures assume that the only risk to their asset is from faulty operations (including ground handling, launch, and on-orbit) or design/manufacturing component (or subsystem) failure or space weather/environmental effects. Debris in LEO could potentially be a challenge as well, but is not as widely thought to impact in GEO. In these scenarios, it would be feasible for a commercial venture to purchase insurances necessary to cover the operations, manufacturing, component, or potentially even risks emanating from debris (assuming there was high confidence in the model). During peacetime, commercial sensors can help complement US government sensors to help complete the picture in the area of situational awareness.

During a **crisis** however, it would be difficult to say if the malfunction in a commercial asset is a result of the asset being targeted by an adversary. The more important an asset is perceived to be (either economically and/or politically), the greater its susceptibility during crises. Depending on how the insurance policy for the asset is written and what events are insured, asset anomalies (when the cause is not clearly determined, or likely to be a result of tampering) could very well be excluded from payout to the owner until the investigation has been completed and all open items answered.

During a **conflict**, very likely, the commercial asset owner would move their asset to safety, away from the conflict zone. Further, it is very likely for owners/operators of assets (that may not be performing per expectation) to point to the conflict as the root cause of any satellite anomaly (there is of course "moral hazard" involved here as well, and underwriting firms routinely assess this risk as part of their pricing risk exercise). Very likely, an insurance policy would not cover damage to an asset during conflict, either because of clauses related to "act of war" or "force majeure".

Do industry leaders think about warfare in or through space differently than military leaders?

In general, industry leaders probably don't want to operate commercial assets in the middle of a war zone (to the extent that is possible), since an impaired asset would become an economic liability, possibly with no insurance payout due to "act of war" exclusions.

However, given the finite life of the asset, the owner may want to repurpose the asset for use in support of government activities.

Military leaders on the other hand have a duty to protect their country's assets and priorities, and may correctly view warfare as inevitable for sustaining their country's strategic interests and needs.

Military leaders may further view industry assets as a potentially useful complement (or not), depending on the ability of these commercial assets to complement USG goals (and architectures) during warfare.

What are their main concerns?

An industry leader's main concern would be that warfare could potentially limit the economic use of their assets currently placed in orbit.

Additionally, they would also be worried that results of a conflict might stall the growth of their organization (e.g., because of debris) due to inability to safely place and operate additional assets in-orbit.

An additional fear could be surrounding long-term reduction in demand of their product, either because of the inherent migration of demand to a superior product (in terms of price and/or capabilities) resulting from war activities, or because the outcome of the conflict favors a commercial competitor from a different region (who may perhaps even be a war adversary).

Overall, this could have an adverse impact on the company's stakeholders (employees, communities in which they live, suppliers, and shareholders).

The very likely request from the industry in such a circumstance would be to repurpose their asset for USG use at a value similar to their foregone commercial (economic) opportunity.

However, very likely this dialogue would remain a work in progress since the original assessment of any impact may prove to be incorrect, and may require a follow-up review as well.

How reliant are they on governments for warning or protection of space?

The industry leaders (in space) would tend to rely upon their own government for warning or protection of space just as for example industry leaders operating internationally do for warnings and protection during warfare.

The precedent for this already exists as JSPOC performs and provides conjunction warnings and analysis for industry as it deems essential.

What are their threat priorities?

The key priority for commercial sector operating in orbit would be to find out ahead of time if their asset has the potential of being targeted.

This would allow the asset owners to mitigate the circumstance by moving their asset to safety.

Next, the company's priority would be to find out as soon as possible if their asset has already been targeted, so that it can then mitigate its impacts (financial, technical, operational, etc.) by notifying the key regulatory and commercial stakeholders, and assessing the impacts of asset impairment on the firm's long-term economic valuation.

It would be important for the firm to know the exact nature and likelihood of a space threat so that it can make the necessary operating and asset decisions (from moving the asset to its replenishment) following the severity and likelihood of adverse conditions resulting from the threat.

Matthew Chwastek

Director of Product Management, Public Sector (Orbital Insight)
22 July 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during peacetime, crisis, and conflict? Do industry leaders think about warfare in or through space differently than military leaders? What are their main concerns? How reliant are they on governments for warning, protection of space and what are their threat priorities?

M. Chwastek: Sure. Just to be clear, Orbital Insight does not build, operate or own space assets. We're a little bit removed from concerns about our own space assets. We would say that we watch what is going on in the market and the world to understand risks to our supply chain, to understand our supply chain's security and ability to continue delivering data to us. I would say industry leaders do not think about warfare in the same way that military leaders do for the simple reason that we're focused on the business of being a business. But the operations of the military and government rely on preventing conflict. The industry relies heavily on the government to provide warning and protection in space. The biggest thing that industry relies on themselves is working with government, like in the US, to do collision avoidance, as well as working with international organizations. Their priorities really are making sure that their platforms continue to operate more than anything else … in the orbit where they're most effective and most efficient.

Interviewer: Yeah. This is something we have heard from a lot of the commercial space people we've talked to: there's an expectation for the government to provide security. It seems that the issue of security, broadly speaking, doesn't really affect the decision-making processes of many commercial space actors. Would you agree with that?

M. Chwastek: I would agree to some extent. I think it's becoming a more visible concern for the industry. I would say one of the bigger challenges you're seeing in the past decade is the disruption you're seeing in space. Historically, it took billions of dollars to put a satellite in space whereas now there could be millions of dollars including launch, which is a drastic change in the price point. Now, you're seeing ubiquitous growth of the space of space. The security is something that I think government should provide.

Interviewer: Okay. Moving beyond security in as far as legal issues and other cooperation in space in the international setting, does the commercial sector look to the government to take the lead on this or does the commercial sector look to themselves to pioneer their way through that?

M. Chwastek: I would say it's collaboration between both, I think the private sector really drives the government to try to move faster. The topic of regulation in space is often a friction point that can slow companies down either with licensing for actual launch or licensing for the kind of data that they are going to bring down from orbit. That's a bigger challenge. I've been party to a number of conversations in the last two to three years with the industry and also government representatives about export control laws. Also the impact of ITAR regulations and also licensing across the various organizations, and that the US government has the onus for licensing states.

Internationally, I think it works faster because markets in the industry outside of the US are generally not as well built. So, the US probably has the most robust and most advanced state industry. We've seen countries like India, Russia, and others really extending their accessibility to commercial space companies, which is driving some launch of satellites out of the US and into those countries because their price points are lower and companies can reach space more quickly. It's really the regulations that are the bigger hindrances in Space, largely because it's not always clear if those organizations are using the resources that they could be when the companies engage them for approval, as well as what the reasoning for existing regulations are. Some of them date back decades to when technology was different, the level was different, the industry was different and cost was different. So when you're putting up one satellite for a billion dollars, the regulations involved there have a smaller but heavily invested community of interest, but if you have tens of thousands of satellites for millions of dollars, it becomes a much broader pool of people within the space.

Faulconer Consulting Group

Walt Faulconer
President

Mike Bowker
Associate

Mark Bitterman
Associate

Dan Dumbacher
Associate

15 August 2017

WRITTEN RESPONSE

They don't. Companies in most cases are beholden to their shareholders and are fiscally obligated to provide sound management judgement including risk management of assets. We find that they don't think differently but rather recognize a different risk posture and ensure and insure against those risks. This doesn't seem to be much of a risk in their minds, at least at this point. The risk they are most worried about is space debris, and what could cause the space debris. Everyone in the US is totally reliant on the US Air Force for warning on space debris. Other areas of somewhat interest is RF interference (i.e. natural for solar activity or unnatural). We find that leaders of companies like Boeing, Northrup Grumman, Raytheon and Lockheed Martin view this similar to military leaders whereas companies like One Web, SpaceX and Blue Origin look at the risk differently than military leaders. Main concerns are space debris, cyber security, effects from solar activity and potential sabotage. They are totally reliant on the government.

Gilmour Space Technologies

Adam Gilmour
Chief Executive Officer

James Gilmour
Director

13 July 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during peacetime, crisis and conflict? Do industry leaders think about warfare in or through space differently than military leaders? What are their main concerns? How reliant are they on governments for warning or protection of space? What are their threat priorities?

A. Gilmour: We don't really think too much about security of our space assets during peacetime crisis or conflict because we got launch people who spend a lot of time in space. I guess I'd be a little bit concerned if the Chinese or the Russians started knocking down anything that's starting to fly, but, I think, we'd have bigger fish to fry if that happened.

I think we look at warfare very similarly to military leaders, mainly because we bring in a lot of discussions with them. We think our views are similar to what we hear these defense people say in about what are the risks in space, what happens if GPS satellites get knocked out and other communication satellites get knocked out. That is what I think is their main concern. The military, I think it's communication and PNT, when weapons are guided from GPS. If that gets knocked out, we're in a world of hurt.

It's one thing to conduct warfare on countries that can't shoot your satellite down at the sky, but very different when you do go against the country that can.

J. Gilmour: And we're talking from a commercial perspective. Obviously, the different landscapes, we'd be intimately involved with defense. But, in terms of an Australian perspective, we believe that there is a need for access or space capability within the decade. It works to have that opportunity of providing the leaders of those capabilities.

A. Gilmour: We will be very reliant on government for warning or protection in space. But, right now, I don't see a big stretch. I don't think it's going to be a space war in a hurry.

Interviewer: So, considering the commercial perspective and business calculi, there's not too much thought given to, "Okay. Do we need to protect anything we're sending up to space or worry about losing assets?"

A. Gilmour: No.

Interviewer: Space, I think at this time, is relatively secure, right?

J. Gilmour: Yeah.

A. Gilmour: Yes. I will concur with that.

Michael Gold

Vice President of Washington Operations and Business Development (Space Systems Loral)
4 September 2017

WRITTEN RESPONSE

The space environment is becoming increasingly crowded and contested, forcing commercial ventures to focus on both physical and cybersecurity. Even during peacetime, there are any number of natural and man-made threats that commercial customers want protection from. Future architectures and capabilities such as satellite servicing and constellations of small satellites, are examples of private sector solutions that are being developed to enhance the capabilities and resilience of space systems during peacetime and will also help bolster satellite security during periods of crisis and conflict.

Due to the benign orbital environment that commercial satellites have operated in for over 50 years, and the inherent nature of their civilian roles, many industry leaders in the commercial satellite world have not dedicated a great deal of time and effort to considering the implications of space-based warfare. Most if not all satellite operators are very interested in supporting defense-related communications traffic, but insufficient attention (with the caveat of private sector participation in war-gaming exercises) has been given to the repercussions of a full-scale conflict in space and how to cope with electromagnetic and kinetic attacks. The commercial satellite industry does devote time and attention to the potential for debris strikes and other forms of conjunctions. However, even in this area, the private sector relies primarily on the U.S. Government for threat warnings, and beyond maneuvering capabilities, industry is also entirely reliant on government for protection against hostile actions.

For all of these reasons, the Department of Defense, the Intelligence Community, and the U.S. Government generally should engage in a more robust fashion with the private sector to discuss and explore responses to space-based warfare. This government and industry engagement can occur through federal advisory committees, such as the National Space Council's Users' Advisory Group and/or the FAA Office of Commercial Space Transportation's Commercial Space Transportation Advisory Committee ("COMSTAC"), targeted events and retreats hosted by the U.S. Government, or a combination of both. Industry is willing to dedicate additional resources to thinking more and differently about space-based warfare and the security of orbital assets to meet emerging threats, but the U.S. Government needs to play a catalytic role to support and encourage such discussions.

Joshua Hampson

Security Studies Fellow (Niskanen Center)
26 July 2017

WRITTEN RESPONSE

As of yet, there has not been direct conflict in space. While there have been crises, such as the 2007 Chinese anti-satellite weapon (ASAT) test, space capabilities are still primarily used for terrestrial force enhancement. In addition to the relative remoteness of the orbital environment from conflict, there is a sense that a war in space would be an escalation that would benefit no one involved.[24] As such, the risks of conflict *in* space may not yet be fully internalized by commercial ventures.

[24] Clark, Colin, "Exclusive: War in Space 'Not a Fight Anybody Wins' – Gen. Raymond," *BreakingDefense*, April 6, 2017 [accessed July 18, 2017] http://breakingdefense.com/2017/04/exclusive-war-in-space-not-a-fight-anybody-wins-gen-raymond/.

Space companies that produce assets directly for the military are more specifically focused on the threats military leaders see in space; they have to ensure that the capabilities they produce are hardened against those threats. The wider commercial space community, however, has been more focused on related, but separate concerns: space debris and cybersecurity. Debris and cyber intrusions can result from conflict, but are also not necessarily direct attacks.

The danger of orbital debris is probably the largest concern for commercial ventures. Debris fields can stay in orbit for years (even decades or centuries). While China's 2007 ASAT test only directly affected its own weather satellite,[25] the debris field placed the International Space Station, as well as other low-earth orbit satellites, in danger.[26] While the military lesson from that ASAT test was that China was capable of threatening U.S. assets in orbit, the commercial lesson was that a conflict between two nations in space could quickly spread to unrelated satellites and architectures.

Cyber-vulnerability is the other threat to commercial space activities that is gaining attention. While the U.S. military is responding to potential vulnerabilities in its space architecture,[27] commercial space ventures may be unable to properly defend themselves against cyber intrusions.[28] Similarly to the space debris problem, the risks to commercial ventures could stem from deteriorating relationships between countries. A potential adversary of the United States may find it easier to degrade American commercial space architecture than attempt to engage the U.S. military. The difficulty of cyber-attribution increases the risks.

Commercial space companies are then focused on these environmental risks to their architectures, and less on direct threats. Military leaders work to mitigate these environmental risks as well, but also have to ensure protection of assets that may be directly threatened.

Commercial space ventures are highly reliant on government warning and protection in space. The U.S. Air Force is the primary provider of global space situational awareness (SSA), for example.[29] There is a commercial conglomerate that provides some SSA data, but it is limited in its capabilities. While companies are developing the ability to provide commercial SSA more fully, the viability of these services will depend on whether governments determine SSA to be a public good. If the U.S. Air Force, or a civil agency, provides SSA for free, there will be limits on demand for commercial SSA. Since physical protection of space assets rests on SSA, commercial space ventures are reliant on governments for protection of space as well.

Commercial ventures may be able to address some cyber-vulnerabilities in space architectures independent of governments, but it depends on the threat. If a country deploys state cyber-capabilities against a space company, or funds private groups to degrade commercial space capabilities, space companies may need government support to defend against attacks, restore capabilities after attacks, or attribute the source of the attacks. This is not unique to the space sector, however, as evidenced by the recent ransomeware attack on hospitals, airlines, banks, and utilities.[30] Because countries use these attacks as a form of coercive bargaining,[31] commercial companies are

[25] David, Leonard, "China's Anti-Satellite Test: Worrisome Debris Cloud Circles Earth," *Space.com*, Feb. 2, 2007 [accessed July 18, 2017] https://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html.

[26] Ibid, https://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html.

[27] Werner, Debra, "Air Force Knocking Down Stovepipes to Shore up Space Cybersecurity," *SpaceNews*, May 3, 2017 [accessed July 18, 2017] http://spacenews.com/air-force-knocking-down-stovepipes-to-shore-up-space-cybersecurity/.

[28] Burgess, Matt, "Hackers targeting satellites could cause 'catastrophic' damage," *Wired*, Sept. 22, 2016 [accessed July 18, 2017] http://www.wired.co.uk/article/satellites-vulnerable-hacking-chatham-house.

[29] Weeden, Brian, "Time for the U.S. military to let go of the civil space situational awareness mission," *SpaceNews*, Sept. 20, 2016 [accessed July 18, 2017] http://spacenews.com/time-for-the-u-s-military-to-let-go-of-the-civil-space-situational-awareness-mission/.

[30] Brandon, Russell, "A new ransomware attack is infecting airlines, banks, and utilities across Europe," *The Verge*, Jun 27, 2017 [accessed July 18, 2017] https://www.theverge.com/2017/6/27/15879480/petrwrap-virus-ukraine-ransomware-attack-europe-wannacry.

[31] Valeriano, Maness, Jensen, "Cyberwarfare has taken a new turn. Yes, it's time to worry," *The Washington Post*, July 13, 2017 [accessed July 18, 2017] https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/?utm_term=.cd9d8e25bc51.

at risk of being caught up in international politics. While this has not yet been used against commercial space architectures, it may be in the future, and commercial space ventures will be reliant on the U.S. government's ability to deter or counter such attacks.

Harris Corporation

Brigadier General (USAF ret.) Thomas F. Gould
Vice President, Business Development, Air Force Programs

Colonel (USAF ret.) Jennifer L. Moore
Senior Manager, Strategy and Business Development, Space Superiority

Gil Klinger
Vice President; Senior Executive Account Manager for National Security Future Architectures

15 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of the space assets during peace time crisis and conflict?

T. Gould: In the commercial sector, the answer likely depends on the relationship between the users and the owner operators of space systems and services. Commercial Owner/operators and manufacturers supporting purely commercially capabilities are unlikely to really think about potential threats or prioritize investments for self-protection. They are also less likely to have much space situational awareness on space threats. Although there is increasingly more information available on the subject. Commercial owner/operators are almost wholly dependent on the US government and other governments for flight safety and collision-avoidance information and notification. Although Harris has substantial commercial business and many commercial customers, our space business focus is primarily with the US government. As a result, our information, thinking, planning, and activity is largely shared with DOD and the ICs from the mindset of a warfighting domain.

J. Moore: I think that really addresses the second question, "Do industry leaders think about warfare or approach things differently than military leaders." I think the important consideration… and we're looking at these questions… and particularly from a perspective of Harris… our business really is predominantly government-based. We think about it in much the same way that the government does or our customer does but that's not necessarily true if you have a truly commercial space venture. It's not a matter of where you stand it's where you sit. You understand that what your customers concerns are and in our case, that's predominately US government and in many cases the DOD.

T. Gould: You know, to piggy back on that, we talk about most commercial entities rely on either the US government or other governments for their flight safety and collision avoidance, and assumed they did have to factor in hostile acts. I think the Chinese test in 2007 clearly changed that calculus. but the answer varies significantly between the users and the operators. At the end of the day, the question will be whether there is a business case for changing how they do business during times of conflict. An example is commercial shipping. Commercial shipping assumes there are effective Navies or international law to protect them, their cargo, and revenue stream. It wasn't until the pirates of off Somalia started hijacking their ships that some companies start to think through the business case for either… one, arming their own ships or, or two, avoiding the area all together. While we would like to think commercial entities will stay in space, the business case might not be there for them to defend themselves and if the US government cannot, they may find a different way to deliver their product or service.

Dr. Jason Held

Chief Executive Officer (Saber Astronautics)
17 August 2017

WRITTEN RESPONSE

Bottom line is that commercial ventures don't think about physical threats a lot. Risk assessments will increasingly consider cybersecurity and mostly in the context of competitive differentiations. We are seeing more examples of IP theft for downstream services, especially in saturated markets such as GPS. The highly public Dominos Pizza vs Precision Tracking case is an interesting example on the downstream. Upstream space component there are competitive pressures relating to frequency spectrum, which, I think, can easily spill into commercial actions which are a bit more aggressive. Keep in mind that a commercial "threat" can look very different than a military action and are usually leverage legal/regulatory mechanisms ranging from IP control to spectrum control.

I have not seen any cases where commercial entities show concern about military conflict. None of our customers either in "BigSpace" or "NewSpace" show a concern of jamming or spoofing, for example. Physical threats would be environmental, for example space radiation and other conventional peacetime operational service interruptions. Although there are some tie-ins to consider. Most companies have to deal with fallout from space debris and pay attention when space based weapon systems are made public. But this doesn't translate to protective measures. Crisis or wartime actually becomes a commercial opportunity for space companies, especially for data providers in imagery and SATCOM markets.

However I see no evidence of these companies preparing for aggressive response from a military adversary, even in cases where they are active suppliers. Most companies see protection of assets as a military duty and outside of their responsibility. Only cybersecurity will be protected because that has far more visibility and awareness, and has better historical heritage. As mico/nano satellites, in particular large constellations gain traction, we might see an increase in both the frequency/creativity/diversity of threats from commercial actors as the field becomes more competitive. Nation states in conflict will also have a larger number of easy-to-kill targets and some of these targets do not have the sophistication in their day-to-day operations to even know they were hit in the first place.

Dr. Moriba Jah

Associate Professor (University of Texas at Austin)
3 October 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets or in peacetime, crisis, and conflict? Do industry leaders think about warfare in or through space differently than military leaders do?

M. Jah: By and large military leaders tend to think of this as problems that they have to deal with. They view things like "threat" and "conflict" as being very defense-centric, and think that commercial operators don't necessarily have these same kinds of concern. However, after speaking to quite a few commercial operators, I beg to differ. Moreover, right now, given that there's a growing number of actors in space, I'd say that commercial operators, more so than ever, are worried about people affecting their bottom lines, tampering with their systems, space piracy, etc.—not necessarily somebody taking over their satellite, although that is probably one concern, but more of somebody interfering with their space services and capabilities, because they have a profit to make and customers and stakeholders to report to.

In general, the commercial community is very intolerant to anything that's less than perfection. If their customers are watching TV and all of a sudden the signal starts degrading once an hour, then these customers might start thinking about changing to another provider. People in the commercial sector are worried about these kinds of things.

Interviewer: It seems logical that as more and more commercial entities get involved in space and put more and more stuff into space, some of the more traditional military concerns regarding threats and indications and warnings would start to blend over into the commercial side. So, I'm wondering, is the commercial side dependent on the military side for the identification of those threat indicators and warnings, or is that something that the commercial side is starting to take more of an initiative with?

M. Jah: To date, commercial entities are very reliant on government and expect the government to take care of these kinds of things. However, at the same time, the commercial side sees government as being ill-equipped to do so. The gamut and variety of space activities are outpacing any given government's ability to really monitor or enforce everything that could be constituted as harmful behavior, intentional behavior, or a threat. I've heard rhetoric from commercial entities saying, "Well, we should just be able to self-regulate," which I think is a horrible idea for a variety of reasons.

Interviewer: Do you want to talk a little bit about why you think commercial entities self-regulating is a horrible idea?

M. Jah: Sure. First of all, companies that are already in space won't want to share orbits with anybody else. So, in terms of self-regulation, they'll just form monopolies and prevent other people from getting on orbit. There are already signs of this happening now. Secondly, this would allow them to be the judge, jury, and executioner all at once. So, I think self-regulation is a bad idea when it comes to the commercial sector and what goes on in space. I think government needs to step in and provide legal frameworks that help commerce thrive and keep everybody safe.

Interviewer: Okay. That's interesting. We haven't heard too much about the idea of commercial entities self-regulating themselves. But to transition to the next question, and you have touched upon this a little bit, does substantial investment and heavier commitment by both governments and commercial interests provide an avenue of approach for space security and disincentive for kinetic military action?

M. Jah: I think so. The thing that disincentivizes any sort of military action is transparency, and I think that's where the space community wants to go. Right now, only a few countries monitor stuff and the data aren't shared, so a lot of the times you run in to a "he said, she said" kind of situation.

I think a good example is what happened with the AMC-9 satellite. What happened was ExoAnalytic posted a video online in which they were tracking AMC-9. The video seems to show—let me underscore "seems to show"—what appears to be pieces separating from the satellite. ExoAnalytic said that there was some sort of explosion or a collision or something like that, which resulted in what appeared in the video; however, the AMC-9 operators claimed that they remained in full control of the satellite and that there were no indications that anything anomalous happened. Because data isn't appropriately shared and there isn't full transparency or ubiquity, these types of situations basically become a "he said, she said" situation. Even though ExoAnalytic might have video evidence, the AMC-9 operators say, "Well, who cares about the video. That's just one piece of data. There could have been clouds or other things that influenced the video. We didn't collect the data. Who verified and validated that that's actually true? Somebody could have doctored this stuff up."

So, as long as there's uncertainty, ambiguity, and a lack of transparency, it's an environment that's rife for some sort of military action. However, if data is shared more ubiquitously (i.e., creating a global system of globally-shared data that can be accessed throughout the globe) and things become more transparent, then I think that military conflict behavior in space will be disincentivized.

Interviewer: So, is the idea that as more actors get more infrastructure in space they'll be less likely to be aggressive because of that investment? Or, is the idea that as more actors have more infrastructure in space there will be better monitoring and awareness of activity and potential aggression, which will help decrease the likelihood of unintended conflictual action? Or, is it a little bit of both of those?

M. Jah: I'd go more towards the latter.

Dr. T.S. Kelso

Senior Research Astrodynamicist (Analytical Graphics, Inc.)
4 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: Got it. So, now let's move on to the next question that I sent over to you, which is about how commercial space entities think about security in space. Given your government experience and commercial experience, I think you'll provide interesting perspective to this question. So, I'm wondering if you can talk a little bit about how commercial space ventures think about the security of their space assets in peace time, crisis, and conflict, and whether or not industry leaders think about warfare in or through space differently than military leaders.

T.S. Kelso: Well, I've been thinking a fair amount about this, and obviously the DoD focus is going to be more on things like warfare, prevention of warfare, etc. The operators we deal with, when it comes to security concerns, are probably more focused on day-to-day kinds of things, which can clearly have implications for national security as well. But, the operators we deal with are concerned with things like "am I going to be jammed by somebody on the ground or in space or whatever" and "am I going to be potentially impacted by operations of another satellite—impacted not just in terms of might I have to move, but might I be subjected to potential for collision and loss of that asset and that kind of thing." And, obviously, since the US military relies heavily on a lot of these satellites, particularly the communication satellites, or what they're doing, it obviously has national security implications as well.

So, when it comes to thinking beyond the day-to-day operations and thinking about some kind of a conflict that would somehow reach out into space, I think most of our operators are not so much concerned about what they can do to avoid being attacked (i.e., some kind of a blatant attack on those satellites, beyond just jamming for example) but more of the reliance that they have right now on the US for space surveillance information to do those tasks that we were just talking about. More specifically, are those tasks going to be preempted by the military because they're focused on these other activities? Every day we're out there trying to figure out what data we have and what it's telling us about things that might get too close to one of our satellites, and we do occasionally see issues where the data flow may slow down or the processes don't seem to be run on the schedules that they should normally be run on. So, we have a lack of transparency there.

This lack of transparency can become increasingly problematic if our focus at a given time is committed elsewhere (i.e., if we're off working some other higher-priority task or with some kind of computer glitch). So, we're left wondering how vulnerable what we're doing to try to just maintain normal operations might be in the event of some kind of a military activity that requires a JSPOC, for example, to be focused on it instead of focused on providing information for commercial or civil operators. That's been one of our big concerns. It's not so much that we're worried about what we could do if somebody decided they wanted to blow up a satellite in extreme case, but rather what we would do in probably a more realistic case where all of a sudden the attention of the organizations that we rely on for the information that we do get about what's going on up there gets diverted away because of some other activity.

Interviewer: Okay. So, you mentioned a situation where commercial entities seem to be somewhat reliant on the government for surveillance activities. This segues into the second part of our question, which has to do with the reliance of commercial entities on the government for indicators and warnings of threats and for the protection of space. So, I'm wondering, how reliant are commercial entities on the government for warnings and/or protection in space? Is this something that commercial entities started to do themselves (i.e., do commercial entities try to survey for indicators and warnings of threats in space?), or is it something that is fully in control of the government right now?

T.S. Kelso: So, I think there are things that we're doing that really kind of undermine the effective way to approach these problems. In particular, the SSA data that we get in large part up until recently has been solely provided by the US government. So, there's been a reliance on the USG for this SSA information—and I saw this when I was in the military working at the Air Force Space Command, where I was the head of analysis—but the release of that information is overly constrained because of a concern that it will reveal capabilities or limitations or the other typical kinds of things that you would be concerned about from that perspective. But this gives operators a perspective where there's a lack of transparency and a lack of dependability on the data that's available.

So, from my perspective, it has looked like we've tried to protect capabilities that haven't changed literally in decades with the false notion that somehow nobody else is going to figure out how to do that, and when they do, they'll figure out how to do it better and just basically bypass what our military is doing. So, I have always tried to push for the idea that "if we're going to stay ahead of the enemy, we have to be constantly innovating, not classifying everything and trying to make sure they can't figure it out on their own or figure it out from what we're doing. So, we basically forfeited a lot of that control because, in the meantime, the commercial sector has now started going off on its own because they feel that they can't depend on some of these assets from the US government, so the commercial sector is trying to come up with their own capabilities on the side.

I work for AGI, and the Commercial Space Operations Center (ComSpOC) is one of the activities at AGI in which we are developing networks. As part of ComSpOC, we have incorporated telescopes, passive RF, etc.—essentially, capabilities that we don't easily have access to from the DoD or aren't easily shared by the DoD with commercial and civil operators currently. So, commercial entities have clearly started looking to other non-government sources to get this type of information that they can easily use for the kinds of things that they need to do to protect their satellites on a day-to-day basis. I think, to a large extent, this is a loss for the USG because the USG is now left with a system that is years behind the time, and, because of the government procurement process, doesn't seem to be able to implement some of these capabilities into their systems. Hopefully what will happen is that the commercial stuff will be developed and then validated, and then eventually the USG will get to the point where they realize that the task of basic catalogue maintenance doesn't need to be a military mission—the USG should work with these partners to do the majority of the background kind of stuff and then use their assets, and the exquisite amount of assets and time that are currently being dedicated to catalogue maintenance, to focus on the assets in space that might be a threat to our national security interests.

Dr. George C. Nield

Associate Administrator for Commercial Space Transportation (Federal Aviation Administration)
1 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their assets during peacetime, crisis, and conflict?"

G. Nield: I feel like this is clearly a question that industry needs to answer for themselves, but you did ask it, and so I would say most companies probably don't think about military threats to their space systems, and so in that sense, it's different than for military leaders. Their concerns are really focused on the bottom line, what is going to impact their commercial operations, their profitability and so forth. I think most of them are wholly reliant on government for wartime protection, but they probably incorrectly assume that the government is actually going to protect them from military threats. I do not think that is necessarily the case. In terms of priorities, I don't believe that they view this in the same way the military community does. Again, they are focused principally on events that could interrupt or negatively impact their commercial operations and profitability.

Dr. Luca Rossettini[32]

CEO and Founder (D-Orbit)
16 August 2017

WRITTEN RESPONSE

At D-Orbit we consider three main threats:

1) Space debris. A potential collision with a defunct satellite or a fragment of a space asset could compromise our mission and put at risk other satellites – ours or someone else's – in the same orbital plane.

[32] Rossettini's response to this question reflects the point of view of D-Orbit, which operates across the space domain, focused on the new commercial approach to space as its main driver, but taking account of considerations related to our business with the more consolidated "standard" space industry practices.

2) Cyberattack. It is evident that measures to increase satellite reliability are also increasing the accessibility for potential malevolent actions performed by hackers. A hacked satellite could easily become a weapon: it could be redirected towards another satellite target or pointed towards Earth along a predetermined trajectory to the ground.

3) Missile attack, either from Earth or space. Although current warning and alert mechanisms are becoming more and more reliable and fast[33], current propulsion means adopted in satellites and space assets in general may not be reactive enough to counter act and perform avoidance maneuvers. Electric propulsion systems, chosen by most of the new satellite operators to save on mass, and launch and operations costs, are orders of magnitude less controllable than chemical propulsion systems, exposing satellites to a higher risk of collision and destruction.

For a commercial entity operating in space, although the aforementioned threats are considered, it is important to note that business KPIs are the drivers for selecting the hardware and investing in operations of the satellite. In particular, while defense hardware and products in general are known for their high reliability proportional to their costs, commercial satellites prefer tradeoffs that favor cost over reliability. Also, the overall perception among "newspace" firms of potential malicious attacks on space assets is low or very low. Not only is space debris not yet perceived as a real threat, but being hacked or hit kinetically with intent is hardly mentioned in the risk analyses I've read from our customers and suppliers.

I believe an efficient warning methodology, taking into account a wide source of inputs accurately analyzed and filtered to avoid false positive situations, would be widely accepted by existing and developing space industry players. This is a necessary step, but an insufficient solution to the conjunction or attack problems because, even with a very reliable warning, a slow space asset is weak and completely unprotected, and lacks maneuverability.

Spire Global, Inc.

Peter Platzer
Chief Executive Officer

Dr. Alexander E. (Sandy) Macdonald
Director of Global Validation ModBD

Jonathan Rosenblatt
General Counsel

15 August 2017

WRITTEN RESPONSE

Commercial space ventures focus on both security and resiliency. With regards to security of space assets, the two main topics to be addressed are data security and physical vulnerability of the satellites themselves.

While the approach to data security can be highly variable, established companies such as Spire that are subject to security requirements (such as 15 CFR Part 960) take the protection of data very seriously. Spire has a comprehensive data protection plan, which includes utilizing AES-256 encryption on satellite data and transmitting in bent pipe mode through our ground station network. This protection plan also includes physical access

[33] Alert and warning mechanisms could be seriously affected by enhancement of space debris data provided by new ground and space infrastructure detecting very small – mm-range – pieces of debris. The "space fence" project in US, and similarly the big radars and telescopes infrastructure being built under the SSA program within the European Union, will generate a very large quantity of potential conjunctions alerts. If not proper analyzed and filtered, a confusing situation could lead to "space panic", opening the way for malicious physical attacks on relevant satellites and space assets to become less detectable.

limitations and controls on access to our ground stations and mission control centers. Our concerns related to data security would principally be if our systems were compromised, and thus either compromising the availability of our services, or the perceived security of our services to our customers (either commercial and government).

The physical security of satellites is also very important, and relates to the broader concept of resiliency. For example, with regards to collision avoidance, many organizations and companies rely on the Joint Special Operations Command (JSpOC) for orbital conjunction alerts. Spire, however, has GPS receivers onboard that provides hyper-precise location data that allows our satellites to have extreme precision in the prediction of their orbits. This capability will greatly reduce the number of false positive conjunction alerts, thus providing better information for collision avoidance measures.

Another aspect of this resiliency is physical security from attack. The principal threats can be from missiles launched into space, other satellites, or man-made objects. In the case of one large satellite platform, an adversary could utilize a single anti-satellite weapon to destroy or disable a single platform. With a constellation of small satellites, it would be extremely difficult to destroy or disable many hundreds of satellites, as it would require a significant amount of resources and anti-satellite weapons.

Stratolaunch Systems Corporation

Steve Nixon
Vice President for Strategic Development

Melanie Preisser
National Systems Director

18 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during peacetime, crisis, and conflict?

S. Nixon: Yeah. Here I have to make a distinction again, on how we're doing versus my impression of how most of the industry is thinking about this. I think in most of the industry, security and contested space are concerns that don't really help them with their business cases. They're trying to get products into doing commercial stuff as quickly as they can. They don't do a whole lot about security stuff because that doesn't help their bottom line much. Now, I think we are a little different because we position ourselves on some issues as interested in helping the DOD and so we're thinking about it pretty significantly. But even we in terms of investment are limited in terms of how much we can spend of our own money hardening our systems for warfare in the future. We think that's probably something we need help from the DOD on, if we need to augment things to make us more resilient...

The inherent thing about our system is that we're air launch and we use solid rockets. So, there are inherent things about our system that could be very beneficial and interesting for the DOD. Stuff like cyber protection in particular is a huge issue. We probably need some sort of DOD help to harden ourselves for that. I think other companies are probably not even thinking about it for the most part.

One other point I'll make is, most launch is from fixed sites which are incredibly vulnerable to disruption from an adversary. It's a pretty fragile infrastructure that has more and easy access to an adversary. Most launches are still coming from those fixed sites. I think DOD for the most part doesn't know how to grapple with that. The vulnerability is clear, and it seems they feel that there's not much they can do about it, and so they haven't done much about it.

To the extent that other companies plan to launch that way makes them vulnerable to the same issues. One of the things that we provide is since we're air launch, we can just move to other airports that might be more secure. Just being mobile makes you more secure and having flexibility in a variety of different launch points makes you more secure. That's another thing about our particular system that makes us better suited for that stuff. I think by and large, the commercial industry is not really thinking about it, and particularly if you're launching from Vandenberg or the Cape, that's just inherently a very dangerous climate in a contested environment.

John Thornton

Chief Executive Officer (Astrobotic Technology)
11 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their space assets during peacetime, crisis, and conflict?

J. Thornton: I'll speak to our experience and our thinking around creating a delivery system for the Moon. Our goal is to make the Moon accessible to the world and delivering payloads to build a DHL-like delivery service up to the surface. Then once we're there, we become the local utility providing power and communication. Much of this will be in that context the way I answer these questions. In terms of security of space assets, the Moon is obviously not yet a highly trafficked area, but in the medium to long term, we are thinking increasingly about the additional applications that will be occurring on the moon including mining, potential settlement, potential resource utilization for sales on the moon and in lunar vicinity. In those contexts, security and rights to minerals and the certainty that you can use that and then sell that, becomes of greater and greater importance. Especially as you have more and more nations vying for similar kinds of activities on the surface of the Moon.

Interviewer: Now, would you say that your company and others like yours specifically look to the government for security? In other words, does it enter in the business calculus of your day to day operations at all?

J. Thornton: It hasn't yet, but we see that as a very clear issue on the horizon. Let me just give you for example. We think that one of the first commodities in space will be water. Much like oil is powering the Earth and it's our source of fuel and a lot of different kind of products, we think water will be the first commodity in space because of how valuable it is. On the Moon, there's vast quantities of water that can be turned into rocket fuel. So, there's your oil comparison. If you've got water in the form of rocket fuel, it's the same fuel that the shuttles use so you can fly around the Moon, around space going to deeper space destinations and potentially even provide fuel for in-space operations much cheaper than here on Earth. You could imagine that there are going to be some hot spots for water on the Moon. Namely, they'll be in polar regions. Namely, they'll be in permanently shadowed craters. Whoever is operating in there and able to control those areas could potentially have huge, huge resource values that other nations might not be able to have. So, in thinking about the long term, that's definitely something we're thinking about. When we're operating or mining on the surface of the Moon and China comes in and lands next to us, what do we do there? Or any variation of. It's not an immediate right now, but it is very much on the horizon that we're keeping an eye on.

ViaSat, Inc.

Richard A. VanderMeulen
Vice President of Space and Satellite Broadband

Ken Peterman
President, Government Systems

Shannon O'Meara Smith
Executive Director of Strategic Initiatives

Fred Taylor
Vice President, Space and Cyber Applications

Bruce Cathell
Vice President of Government Operations

15 August 2017

INTERVIEW TRANSCRIPT EXCERPTS

VanderMeulen: From a satellite service provider perspective, there are numerous threats to our continued business operations. These threats can come from essentially any direction, external or even internal.

As an example of an internal threat, what happens when the broadband network gets filled up? When we started our Satellite Broadband service, a company called WildBlue, we quickly grew to have over 400,000 subscribers. This was back in the 2005/2008 period of time, when broadband was considered 5 megabits, by 1 megabit or even less. The threat to the business came from our own success and customers desiring to use more and more data. The result was a network in congestion, or a network with slower speeds at busy times. As you would expect, as the speeds would get slower at busy times, the customers were motivated to find new sources and leave the network. They would churn off the network and switch to DSL or some other service.

Even this mishandled over-success is a threat to continued business operations. Failure to provide a network that remains pertinent by the standards of your customers and market alternatives can cause a loss of customers, which causes a loss of revenue, which causes a business to be less pertinent in the marketplace and maybe even lead the business to fail.

Interviewer: I'm making an assumption here, so correct me if I'm wrong, but it's probably easier to communicate a concern like space debris or any other kinetic action up in space, versus the kind of concern you just described (i.e., the feasibility of the network), would you agree with that?

VanderMeulen: Yes, we believe the government considers space debris as a real threat. But oversubscription of your network is also a real threat. If you oversubscribe your network and something bad happens, your customers' ability to communicate can be negatively impacted.

It seems the government perspective of space threats focus on very, very big threats that are against the space infrastructure. Our view focuses on threats to the network, and those threats can come from any direction and domain of the network. Threats include cuts or outages of your fiber; take-down of your ground station(s); thunderstorms over your antenna degrading RF performance; even overselling your capacity to too many subscribers and therefore not being able to meet your service level agreement regardless of the cause. All of these threats are of importance considering the outcome of outages and business interruption. Applying this network view of threats to the war-fighter scenario, we would believe that an adversary will select the path of, let's say most effective damage for lowest cost and least attribution. Thus, space threats might not actually be against infrastructure space in the first place.

Interviewer: This is an example of a technologically specific concern that industry/commercial actors are more apt to be aware of than their counterparts in the DOD, right?

VanderMeulen: Right. I think that's because we look at it from this holistic or enterprise perspective and the government considers their Satcom systems, both purpose-built and leased commercial networks from the product or element perspective. Anything that causes our business to fail is something that we have to be worried about. Whereas, if you just asked a general officer if they would consider adverse weather as a threat to their space system, they'd probably say no. Or if the system oversubscribed WGS so that it wasn't available when military needed it, do they view that as a threat? They'd probably say no. Without an end-to-end network or enterprise perspective, they wouldn't even consider the network's performance baseline.

Interviewer: That seems concerning. Moving forward to thinking about a solution to this problem, from your perspective as commercial actors, what do you think is the best way to overcome this gap in communication? Is the DOD in a need of systemic reform, or is it just in need a better leadership? Or do they just need to spend more time listening to the commercial counterparts, or providing a new institution for concerns like this? What do you think would be the best solution to this current problem?

VanderMeulen: In summary, the DOD needs to take an enterprise focused perspective. This means the space, ground entry, fiber backhaul, user terminals, and space, network, and cyber operations need to be managed as a whole and not a set of individual products operational commands. We have some ideas on this but it would be presumptuous of us to talk about how the DOD or the government should be organized, other than to discuss the need for enterprise or holistic perspective. We definitely observe the various constructs in the current draft NDAAs, one construct from the House side through Chairman Rogers…Space Force. There's another construct in the Senate and their NDAA…Chief Warfare Officer. From our perspective, neither of those constructs address the full enterprise spanning services, commands, and budget authorities. Which leads to our thought, are these constructs any better or worse than anything else? We think you must have a holistic view. When your view is only from the domain that you live in (i.e., "I live in the cyber domain," or "I live in the space domain," or "I live in the ground domain," etc.), you do not have a holistic view.

If you think about it the government way: Airforce Space Command through SMC builds the satellites; DISA builds the ground segment; and the Air Force or the Army or the Navy will integrate the terminals onboard ships, airplanes, or for a deployed unit. All those things have to work together. The history is that they haven't done that very well. We think it's not just from the development or operational perspective; you have to think holistically if you want to protect it. It has to operate as a holistic ecosystem and it has to be defended as a holistic ecosystem.

[…]

Interviewer: It seems that many commercial actors don't take the short- to medium-term emerging threats and other security risks into consideration. It's interesting that ViaSat gives serious consideration to these things but other commercial space actors do not.

F. Taylor: It is a competitive market and other companies are entering the market place, any threats to performance or mission assurance also pose a threat to business success. For instance, let's take cyber as an example. As our network becomes filled, which is where we're at right now with the ViaSat-1 network, we need ViaSat-2 to add the essential capacity to meet customer demand and growth. In this state, you certainly notice things like malware. Malware is a nonpaying customer. Malware on PCs in a home consumes traffic over our network and they're not the paying customer. If we can squash that malware, then we have more capacity to sell to our customers.

So our ability to detect malware and to control it becomes something that we're going to make an investment in. This is an example of our market demand driving us to counter cyber threats. We're making investments to block denial of service attacks; we're making investments to block malware. We're essentially making investments to block any of these things that would tend to run over our network which would make our network run less effectively.

WRITTEN RESPONSE

Commercial and private sector ventures are keenly focused on the security and preservation of their entire ecosystems including the security and preservation of their space based assets. Interruption of service delivery in peacetime, crisis or conflict, either intentional or unintentional, all lead to negative strategic effects on commercial brand. These effects may include potentially enduring impacts on revenue and the ability to achieve the necessary return on investment capital to remain a viable commercial or private sector business entity.

Business failure is no more an option for a commercial or private sector company than losing National Security Space leadership is to the US Military and government. While the failure of a commercial system may not lead to the loss of lives or failure of military missions, if a commercial service is unreliable or unavailable for an extended period of time, it damages the commercial brand and eventually leads to the ultimate failure of the business. A business failure can easily lead to the loss of millions of dollars in assets and capital for the business and its shareholders, as well as the loss of employment for thousands of workers and their families across a broad geographic area.

Therefore, commercial and private sector companies think of warfare or any intentional or unintentional threat to our space ecosystems in much the same way as the government and the Department of Defense. Any threat realized could impose negative impact on service delivery, revenues and business continuity. Some subtle differences may exist however in our assessment of a various threats and their likelihood of occurrence or severity of effect. For example, from a Satcom perspective, we consider weather as a highly frequent adversary. Weather effects at ground stations or gateways can occur frequently and in the past would have caused outages. To deter this adversary, commercial or private sector systems have replicated or augmented ground stations or gateways to enable continuity operations routing services around effects of weather, fiber outages, power outages, etc. While these capabilities were built to deal with weather threats they are also translatable to provide mitigation of any number of other more intentional threats.

We are fully supportive of all commercial/private sector and government source indications and warnings (I&W) for protection of space elements, and also seek similar I&W for all elements of our ecosystems. We believe that a thoughtful US Space Policy that addresses the US government's role in the protection of commercial and private sector space assets and the associated extended ecosystem is overdue.

Our threat priorities are aligned with those of the military/government sector. We are concerned with threats from/to weather, power, fiber, blockage, interference (intentional jamming or unintentional) and regardless of its source (ground, sea, air, or space), cyber, kinetic or destruction regardless of it location (ground, sea, air, or space), PNT, scintillated atmosphere, etc.

Due to policy and licensing restrictions, commercial and private sector assets do rely on government for both warnings and protections in space. Private sector assets are restricted in the amount and types of Space

Situational Awareness they can collect and distribute and the protective measures they can employ. Policy changes that reduce the restrictions on commercial and private sector assets collection and distribution of Space Situational Awareness could benefit both the private sector and the government as the proliferation of advanced private sector SSA could be used to both parties' benefit.

Our concerns include any impact to our service delivery network or ecosystem that negatively affects the customer experience and/or overall business performance and revenue generation.

Charity Weeden

Senior Director of Policy (Satellite Industry Association)
Former Assistant Attaché, Air & Space Operations (Canadian Defence Liaison Staff, Washington, DC)
24 July 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security of their assets during peacetime, crisis, and conflicts?

C. Weeden: The physical environment is of utmost importance and you might already be aware, many of the commercial satellite operators share ephemeris data with each other through a non-profit called Space Data Association (SDA). Another thing that SDA does is provide RF interference indicators as well. Understanding both the physical and electromagnetic environments are during either peacetime or wartime. There's also an acute understanding knowing commercial assets will be critical to the fight. I believe our members would agree that while they may understand the space environment, they likely want to understand more of the threat environments to better prepare and to be a good partner for the US DoD. I didn't talk much about cyber security, but it is of course critical to space operators as well. Additionally, satellite operators are involved in the commercial integration cell at the Joint Space Operations Center to share information and better understand the threat environment. They're also involved in war games … it has become a really good engagement in partnership between the commercial and DoD to make sure there is transparency so commercial operators understand what's going on.

Dr. Edythe Weeks

Adjunct Full Professor (Webster University)
16 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: What are the biggest hindrances to a successful relationship between the private and government space sectors, and how can these be minimized?

E. Weeks: Okay. So, what are the biggest hindrances to a successful relationship between the private and government space sectors, and how can these be minimized? I would say that any hindrances between private sector actors of space and the US government are likely to stem from the existence of a deeply seated ideological ongoing passionate tension, which began shortly after the end of the Cold War. So, from around 1991 until today, this assumption that I just made is evident by numerous documents and discourses, various published articles and hearing transcripts before the House and Senate, and verbal articulations made by key private actors steering public discussion at space conferences.

Now, at the core of this tension is the idea that private actors know how to move forward with the outer space agenda, beyond satellite telecommunications and other established and critically essential, but often viewed as being somehow at stake, commercial industries. The sentiment fueling this tension, I believe, is rooted in the very idea of what America means. So, you have discourses evidencing the tensions, and the private actors tend to say that they know how to speed up development and that can do it more efficiently and effectively than the government. And, for many people, that seems to represent the very freedom that makes Americans proud, and makes us the envy of the world, so it feels right and true even to the very government actors caught in the middle of this ideological struggle. So, there's this an invisible, dormant, unaddressed dilemma.

Okay, so this tension tends to pivot around the issue of who knows the best way—the key actors within the private sector versus the US government—and who knows the best way to push the outer space development agenda forward to next step. So, it is within this paradigm that I just described, the US government and NASA are often said to be too slow or too bureaucratic or too unreliable in comparison to the private sector, and this is an ideological debate that seems real to most people. To many, this seems like it is a real description of the reality. For the key actors involved in this process, both the US government and the private sector, this is consistent with how we're all socialized to view the history of business enterprise and innovation. So, it seems right—it seems like, "yeah, yeah, that is right. The government is slow, and we want our freedom."

But the invisible social and psychological structure that I just described is a fabric upon which these hindrances are molded to play out. So, historically, it is a myth that the private sector usually gets its way and usually has the upper hand against the government. Now, the problem with this scenario is that the assertions launched against the government ignore the extensive history of the US government being the way in which we get the funds for research and development for space technology. The US government has been very successful in providing billions of dollars over decades for space, and I think this gets forgotten in the process. The US government has been very successful in securing funds for research and development space technology. NASA has been extremely successful if you look at its history. So, this is why space technology exists. People get excited about the commercial sector, but where does this technology come from? Elon Musk could not have created his space vehicles without the government, without NASA.

So, for decades, the private sector has been receiving grants, loans, contracts, technology transfers, etc. from the US government and from NASA, and this pattern has enabled the private space sector and commercial space operations to happen. Ignoring this reality is problematic, especially when it comes to elected officials every year having to approve NASA's budget. I've been a part of the blitzes that usually involve about 30-40 hand-picked individuals representing space to go around meeting with elected officials in Congress and the Senate. Usually, these teams meet with interns, sometimes with the elected official directly, and pretty much have to beg for them to renew NASA's budget every year. And, listening to what elected officials say, makes perfect sense to me. Some elected officials are in districts where the people say, "We are not being paid. We need education, we need government, we need food, and we need jobs." This makes it unstable, and makes advances in space unstable because every year we're not sure whether or not NASA is going to have their budget.

Many members of Congress and the Senate feel obliged to pay homage to the expressed feelings of their constituents. That's understandable. And these constituents have often indicated that space activities are usually meaningless to them. So, the private sector's ability to put innovation to work is mostly funded by the American taxpayers. Most Americans like the idea of NASA and having a space program, and view it as an asset; however, many are completely unable to interpret any real value or personal realizable benefit for themselves and their families and people they know. Unwittingly, the private sector discourses, which attack NASA and attack the government, help to fuel emotions—people are seeing this stuff on the Internet and they're getting upset because they're paying for the space program. So, these discourses tend to fuel these emotions of suspicion and disdain for elites, and these are the people who are truly funding space activities—the taxpayer, the constituents of elected officials who vote on NASA's budget.

If something catastrophic happened out there in space (e.g., some private actor does something that causes a chain of events to cause a catastrophic incident), private sector actors are likely to look to NASA or the USG or US military for the solution. The US government and the American public remain legally responsible for private activities in space, according to the Outer Space Treaty of 1967 Article 6. This is the reality, and it seems that the US government is buckled down by the private sector's ability to consummate an ideological, philosophical win, and the USG is adhering. For example, there was a 2001 joint hearing between the Congress and the Senate, and during these hearings, one after another member of the space community came out advocating for private space and articulated an argument against the USG and against NASA, arguing that these government institutions are slow and bureaucratic.

So, it seems that the US government is buckled down by the private sector efforts to constantly make this ideological, philosophical win—because it sounds right. But this is causing a barrier that both parties need to realize. The private sector can do nothing substantial in the long-term without the US government, US military, and NASA. So, the hindrances that you asked about, come from an unwillingness to see the human aspect of this dynamic. This is how I would suggest the hindrances be looked at. It's only once we can see these hindrances and what causes them and what is fueling them, that we can really step back and ask that question of, "what can we do to ensure successful relationship between the private and government space sectors?"

Interviewer: Okay. So, it sounds like you are again highlighting the idea of cooperation and working together for mutual benefit, but in this case between the government and commercial space sectors.

E. Weeks: Yeah, but when you say it like that it reminds me of debates in international relations courses. What I'm saying is that cooperation is always preferred, but we can't ignore the effect of this realizable conflict. So, I'm not just simply hanging my hat on cooperation because sometimes you can't get people to cooperate. So, I guess what I'm saying is that cooperation can't happen until the key players realize what's real, what's not real, what's happening, etc. So, yeah, I guess it would boil back down to letting them see that there's no need not to cooperate because the "conflict" was filled by imaginary phenomena. I just don't like the word "cooperation" because it too often leads to certain thoughts and ideas that we should shy away from. But, ultimately, I just want to say that hindrances between private and government actors are caused by the myth that the private sector can do space better than the US government and better than NASA and better than the military, because I think that's a myth. If anything, it has been true that, historically, the US government has initiated the commercial activities and has granted the private sector laws, contracts, technology transfers, etc.

But, there is something special about our country. There is entrepreneurship. There are people who come up with ideas and they are ready to roll, and they might be more creative than the people who are contracted by government. There certainly is that. But, I think the all or nothing debates that tend to operate in the space community, needs to be looked at realistically, because I don't think it centers on anything real. The US government doesn't need to fight with the private sector. There's a history of the US government providing the private sector with whatever it's asked for, and, in my mind, why bite the hand that has fed you and that may have to protect you down the road?

Deborah Westphal

Chief Executive Officer (Toffler Associates)
17 August 2017

INTERVIEW TRANSCRIPT EXCERPT

Interviewer: How do commercial ventures think about the security, their space assets during peacetime, crisis, and conflict?

D. Westphal: To be honest, they really don't. That is very much a national security perspective; commercial ventures aren't thinking that way. Commercial ventures are thinking about revenue generation and life expectancy. The commercial ventures have customers and are mindful of their customers requirements with regard to maximizing profit. Depending on what the business model is, they're trying to maximize capacity and performance, extend life expectancy, and they're trying to decrease cost and weight, etc. They are focused on securing their assets to ensure reliability for their customers' needs, but not necessarily security, with regard to safekeeping assets in times of peace, crisis and conflict.

Granted, I come from a background in national security, so I may be reacting to "security of space assets" differently. But it's not at the forefront of their mind. That said, the commercial ventures within a Lockheed Martin or a Boeing, there is some part of the equation as they are building a satellite that they consider what it will take to secure the asset. But their focus is their customer and how they can drive capacity and capability at the lowest cost.

Interviewer: Okay. So, I'm guessing industry leaders do think about warfare in or through space differently than military leaders, correct?

D. Westphal: Absolutely. Industry business leaders don't think about warfare like the military does. Some commercial industry companies have military veterans in their ranks or on their board, and they work to respect each others' perspective. But if you expect an industry leader to think about warfare in a way that military leaders do, well, they're not going to do that. Theirs are two separate and very different missions or perspectives: one wants to make money and to grow a business.; the other's objective is to protect national security. Their risk and reward equations are very, very different. There are industry leaders that get involved with the discussion with the military and bring that learning into the company. For example, Kay Sears -- when she led Inmarsat she knew and worked with the military on space security and protection issues. She brought that learning back into Inmarsat, but Inmarsat was a commercial company that was being driven by commercial objectives.

Warfare is the military's purview, not industry's.

Interviewer: Absolutely. If, hypothetically speaking, we could assume that there's a growing threat in this space domain in the next five to ten years, then what would be the best way for the government to communicate that risk for the commercial sector to help make them more aware?

D. Westphal: The first challenge is the government can't even talk about the growing threat due to so much classification at so many different levels and in so many different compartments within the government. The first thing the government needs to figure out is if all classifications are necessary and if the information can be streamlined across the different groups and departments so it can be more clearly and effectively communicated outside the government. Secondly, the commercial sector doesn't have access to the information due to the security requirements. And by the time it's been watered down into an unclassified report, the industry has to determine whether or not it's worth the cost to act on the information. Is it worth the cost to change the design of their satellites or modify their operations? For a lot of these companies, their capabilities are insured as well. So, as part of your study, you'll want to look at how elements are insured. In some cases, if the satellites get lost, insurance will cover it. The insurance side of the business needs to be considered. But as far as communicating the growing threat, the first priority is to improve the processes inside the government.

As part of the security space protection panel, the commissions that we've done with Marty Faga and Gen. Ellis featured additional levels of clearance even though it was supposed to be a TS/SCI cleared panel. We had people who would come in that couldn't access all the information, making it difficult for everyone to achieve the same level of understanding. And, as an example, this was a very small group. Which is simply to illustrate how critical it is to address process improvement inside the government in order to effectively communicate risk with external parties who have a role to play in ensuring the security of space.