7-25-2024

Survey of Space Professionals' Perception of Satellite Cybersecurity from 2012 to 2022: Decision-Makers' Thoughts on Satellite Cybersecurity Evolving

Rachel C. Jones
University of North Dakota, rachel.c.jones@und.edu

Open camera or QR reader and scan code to access this article and other resources online.

Survey of Space Professionals' Perception of Satellite Cybersecurity from 2012 to 2022: Decision-Makers' Thoughts on Satellite Cybersecurity Evolving

Rachel C. Jones[1,2]

[1]*Savannah River National Laboratory (SRNL), Aiken, South Carolina.*
[2]*University of North Dakota (UND), Grand Forks, North Dakota.*

ABSTRACT

Cyberattacks on space assets are often portrayed in vague terms of doubt and mystery. Several claims depict satellites being compromised or attacked, but little corroboration has been published or made publicly available. As the commercial space industry grows, increased concern with space cybersecurity will prompt commercial satellite decision-makers to analyze the often-undefined risk of cyberattacks against satellites. This article identifies and characterizes the nature of cybersecurity risks to space assets and postulates why space professionals might not prioritize cybersecurity. Additional information was captured from a decadal survey of space professionals conducted in 2012 and 2022. The results show a rise in the perception of risk to satellites from cybersecurity threats. This increase in the perception of risk is not fully defined or agreed upon leaving room for future studies.

Keywords: space, commercial satellites, cybersecurity, survey, space professionals, perception

INTRODUCTION

In November 2011, sensationalist articles about the hacking of the Earth observation satellite Terra Earth Observation System (Terra EOS) and Landsat-7 trended in the U.S. media, with headlines such as "Real-life Star Wars: US claims Chinese military were behind hackers who seized control of two U.S. satellites" from Daily Mail.com[1] and "Chinese hackers took control of NASA satellite for 11 minutes" from PC Tech.[2] The latter article claimed that "the last hack was so effective that they could have completely taken control of the satellite, but did not do so."[2]

The cyber hacks occurred in 2007 and 2008 but did not make headlines until a 2011 Congressional Economic Report announced them. The attacks on the satellite's command and control systems were featured on page 216 of the 400-plus page Congressional Report entitled *2011 Report to Congress of the U.S.-China Economic and Security Review Commission.*[3] The report outlined four instances of 2––12 min of "interference" from 2007 to 2008.[3] In the case of Terra EOS, "the responsible party achieved all steps required to command the satellite but did not issue commands."[3]

Cybersecurity incidents involving space assets have been referenced in government documents, appeared in news and academic articles, and are publicly discussed at major cybersecurity events such as Blackhat and DEFCON. Several examples of suspected cyberattacks on space assets exist, but

DOI: 10.1089/space.2024.0015

sometimes the details of these attacks are unknown or purposely withheld for security reasons. Academics and the media alike might sensationalize and exacerbate a series of assumed events making it hard to determine the facts of a sitatution.[4] Overall, due to the classification of reports, lack of publicized information, and the possibility of alternative versions of the events, it is often hard to determine what happened and whether cyber was the cause.

In January 2021, the Cyber Defense Project and the Center for Security Studies, ETH Zurich, published the Cyber Defense Report *Terra Calling: Defending and Securing the Space Economy: From Science to Fiction and Back to Reality*. This report claimed that "the most-referenced cyber incidents affecting space system[s] have either not occurred at all, are based on a series of assumptions, or did not occur in the manner they were initially reported."[4] Regarding the Landsat-7 and Terra hacking report, Soesanto outlines that secondary sources do not substantiate the Congressional report due to a limited release of information on the events in question.[4]

Some, such as Soesanto, question the accuracy of cited reports, especially when there is a lack of supporting or collaborating information.[4] Other researchers point out the challenges in determining whether an event is based on a malicious cyber actor or is a natural space environment phenomenon.[5]

As the commercial space industry is growing, it can be hard for decision-makers in the space industry to gauge the risks of cyberattacks to space assets. This article outlines a notable shift in the perspective of space professionals about the cybersecurity of space assets through two separate surveys of space professionals.

This study's research compares survey results from approximately 130 space professionals from a 2012 research project at the International Space University (ISU) and the same survey administered in 2022 as part of an independent research course at the University of North Dakota (UND). The survey results were used to identify shifts in industry perception of satellite cybersecurity. Each survey provides a snapshot of the perspectives of a small sample of space professionals in the respective years. Comparing the decadal results showcases shifts in industry perspective. Questions were centered on perceived threats to satellites and the ability of cyber adversaries. Related subjects included investigation, public declaration of cyberattacks, and support for mandated security minimums. Overall, the surveys attempted to characterize the space industry's perception of the cybersecurity risk posed to satellites.

Section 1 of this article briefly outlines cyber risks to space assets and why space professionals or those making decisions on the building and integration of space technology might not prioritize cybersecurity. Section 2 presents the methods and survey design information. Section 3 describes the results of the survey. Lastly, Section 4 summarizes the conclusions of this decadal study and future areas of research.

WHAT COULD CYBERSECURITY RISK LOOK LIKE TO SPACE ASSETS?

The National Institute of Standards and Technology (NIST) classifies cyber risk by what can be lost through the dependency on a cyber resource or system. This definition of risk can be applied to space systems by removing the word manufacturing from the following quote: A cyber risk is one that produces a "financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system."[6]

The definition of cyber risk can be expanded to all the components of satellite architecture. The typical space architecture of a satellite contains multiple segments to include user, ground, link, and space.[7] The user segment might consist of terminals that interact with the information sent to or received from satellites. The ground segment will host ground stations that can be used to send command and control information to the satellite. The link segment is the medium by which information is sent to the satellite, which is often radio frequency. The space segment can encompass the target satellite and other aspects that interact with the satellite in space, such as satellite-to-satellite communications.

The Aerospace Security Project at the Center for Strategic and International Studies (CSIS) *Space Threat Assessment 2023* describes cyber as a category of a counterspace weapon.[8] CSIS finds that "the barrier to entry is relatively low, and cyberattacks can be contracted out to private groups or individuals."[8] The assessment outlines that space-domain-specific knowledge would be needed to conduct a cyberattack, but not significant financial resources.[8]

WHY MIGHT A SPACE PROFESSIONAL NOT PRIORITIZE CYBERSECURITY?

There is a rising number of new commercial, nongovernmental players in the space industry who are building parts, software, and providing integration and launch services. Commercial companies might have different risk perspectives than governmental actors. Justifying costs, time, and expertise

devoted to the cybersecurity of a satellite can be a hard sell to project managers. This section summarizes some common decision factors commercial space actors might be faced with when determining whether to devote resources toward protecting a space asset or aspect from risks posed by a cyber adversary. Ultimately, when making decisions about satellites, "not all risks can be eliminated, and no decision maker has unlimited budget or enough personnel to combat all risks."[9]

Lack of a Known Risk

Risk generally comes from an active threat and the exploitation of vulnerabilities. A risk doesn't exist if there is not a threat. As Roberta Ewart et al. identified, determining the likelihood of a cyber threat typically aligns with the following three categories: adversary motivation, adversary capabilities, and the difficulty of exploiting a system.[10]

From this, many questions arise:

1) Motivation. Who and why a specific satellite would be attacked? Assuming satellites might be vulnerable to cyberattacks, with almost 4,000 satellites in orbit, why would malicious actors select one particular target over another? What would be a particular attacker's motivation?

Satellites support a growing array of activities. Satellites can provide services that support critical infrastructure of our world. Some satellites are key to providing the backbone for communication, the internet, and position navigation and timing. Other satellites provide sensing or survey information that support imagery, weather predictions, and other applications. In addition, other satellites might be testing new technology or hosting scientific experiments.

Hackers, adversaries, bored teenagers, and the like could have a variety of motivations to target satellites. Usually, there are two types of motivation: targets of purpose and attacks of opportunity. Targets of purpose occur when hackers want to accomplish a specific goal such as to stop a service, gain or manipulate specific data, or cause cascading effects that allow secondary goals to be accomplished. Attacks of opportunity happen when a satellite might have a specific vulnerability, use a specific software, or be positioned in a specific area that makes it easier for an attacker to target. These opportunistic attacks could also be motivated by the simple desire to cause chaos or test a technique to be used against a targeted goal.

2) Capabilities. There are many problems with measuring adversaries' capabilities. First, technology is constantly changing. What was impossible two years ago might not be today. Second, given the security of most space programs and commercial proprietary information used by larger corporations, there is a lack of open-source literature on the details of security tools and defenses used for space assets. This is both good and bad. This means there likely isn't a repository on known successful attacks for satellites, but it also means that there is uncertainty about whether a known type of attack could be used against a space asset. There is a knowledge gap about whether attacks that are currently used against traditional infrastructure would be successful against space targets. Overall, it is difficult to analyze adversaries' ability to compromise space assets, given the lack of resources and materials published on the subject.[4]

In the past, many in the space industry didn't believe satellites could be hacked because they were too sophisticated. Gregory Falco addressed how some satellite systems were built under the concept of "security through obscurity."[11] Falco remarked how the Iridium satellite constellation, despite supporting the Pentagon, had "no special cybersecurity parameters . . . because engineers thought the technology was too advanced for a hacker to compromise."[11]

Industry has dramatically shifted perspectives in possibilities, moving from too complex to attack to inviting individuals to hack the first orbiting cyber range satellite. In August 2023, the first capture the flag event to involve a satellite in orbit, Hack-A-Sat 4, centered on five international teams compromising various aspects of a three-unit CubeSat named Moonlighter. Of those five teams, three were able to use onboard resources to capture a picture from outer space.[12]

3) Difficulties to exploit. Satellites are a system-of-systems that have been growing in networking and complexity without any mandated security requirements. Stakem comments "there are currently no requirements for security of transmissions, or encryption of the uplink of non-DoD [Department of Defense] spacecraft."[13] In addition, the space market is growing to include a variety of new actors and technologies. For example, ground station services have expanded to allow users to use the cloud to send instructions to satellites. This expansion of connectiveness increases the exposed attack surface. In addition, most projects will involve parts and services provided from multiple sources, increasing the complexity and number of possible vulnerabilities.[14]

Cost to Protect

Satellite builders face a "profit-driven," fast-paced, critical market.[7] In his book *Hacking CubeSats, Cybersecurity in Space*, Stakem outlines security costs as "money, speed, and memory."[13] In a market where an extra pound can cost thousands of additional dollars in design and launch costs, there are several reasons suppliers and builders might not prioritize cybersecurity.

Cost of Loss of the Asset versus Cost of Mitigation of Vulnerability

Traditionally, cybersecurity risk calculations are made by analyzing the expected loss or impact resulting from a cyberattack. If a company is at active risk from known attackers who might want to exploit a known vulnerability, a CEO might decide to invest $10,000 to mitigate that vulnerability if it would prevent a likely million-dollar loss from an attack. In that same situation, a CEO could choose not to mitigate a known vulnerability if the impact of the attack would only incur a $2,000 loss versus a million-dollar patch. Calculations should be made between the likelihood of an event occurring measured against the impact of the event in terms of the mission.

Vagueness Between Man-Made and Natural Phenomena

Determining if a satellite has experienced a cyberattack can be challenging as a system loss could be the result of a natural event providing a false positive signal for a cyberattack. Distinguishing between malicious cyber impacts and natural phenomena can be difficult.[5] For example, high energy particle effects can cause loss of power or corruption of a system similar to a cyberattack.[5] The aerospace consulting and training company, Teaching Science and Technology, Inc. (TSTI), suggests that many natural effects of space can mimic the signals that can occur from what might be expected from a cyberattack.[5] Some of these effects are caused by micro-meteoroids, electromagnetic radiation, charged particles, low energy plasma, high energy particles, the Van Allen Radiation belts, the South Atlantic anomaly, and sun events.[5]

Who is at Fault? Evaluating Consequences

If a satellite is hacked, what could the damage or resulting business loss be for the country of registration, the designer, or the builder? Many companies make risk decisions based on the cost to them. If your company built a satellite and that satellite was hacked, how would it impact your business? Would the company be blamed? There are presently a lot of unknowns in the area of cost to business. Without the ability to definitely attribute an attack as a cyberattack, the cost of the loss is not determinable. Furthermore, there are not many case studies in this area.

Continuous Redesign to Match Rapid Technologic Change

Space systems take a long time to develop and can spend an extended time in space. Manufacturers might not have the incentive to continually invest in lifecycle costs. The build, testing, integration, and launch of a satellite could take multiple years to accomplish. In addition, many satellites serve past their expected lifespans. This extended amount of time means that the hardware and software might be several years older than current systems. During this time, many previously unknown vulnerabilities might be discovered. Satellites might not have the capability to upgrade their software or hardware to mitigate newly discovered vulnerabilities.

Other Priorities and Risks

When mitigating risks, multiple factors must be considered. First, a satellite isn't designed just to be secure in space. A satellite has a priority mission or goal. A principle of cybersecurity is that when cybersecurity stops the ability to conduct business, cybersecurity is wrong.

Cybersecurity might not be the biggest risks industry members prioritize. Outer space is a harsh environment that includes solar flares and high energy particle collisions. There are also multiple man-made threats such as space debris or anti-satellite weapons.

The analysis below attempts to assess space professionals' beliefs on the risk posed to space assets from cyberattacks. There are still varying opinions on whether or not a satellite can be hacked. For example, multiple sources still debate today on whether Landsat-7 and Terra EOS were compromised.[3,4] Compounding additional questions follow that if a satellite is compromised, could the individuals accessing the satellite gain the ability to control it? That is, would decision-makers that believed satellites could be attacked invest more in cyberdefense?

METHODS

This study compares the results of two electronic surveys. The first survey, previously unpublished, was completed as part of an independent project at the ISU in the spring of 2012. The second survey, a duplication of the first, was administered at the UND as part of an independent project in the spring of 2022.

The survey consisted of a general consent question, 4 demographic questions (Profession, Industry, Age category, and Geographic association) and 10 questions regarding the perspective of the participants on the cybersecurity of satellites. Survey questions were presented in small groups on separate pages. Participants could not skip ahead to later questions without answering previous questions or choosing to stop taking the survey.

In the 2012 survey, the initial advertisement of the survey was done via socialization at two academic conferences

hosted by ISU and through a targeted email campaign. The survey was hosted on Survey Monkey, and participants were given an electronic link. Designers of the survey used a snowball sampling methodology for broader space industry participation by requesting takers of the survey forward the survey to friends and colleagues in the space discipline. The 2012 survey contained 135 respondents. Results of the initial survey were combined by the survey platform for total percentages.

For the 2022 survey, when possible, the language of the main baseline survey questions was maintained for potential comparison value. The survey was administered via the Qualtrics platform. The survey also went through the UND's Institutional Review Board (IRB) (IRB #IRB0004718). From May to June 2022, advertisement for participation was done via targeted email requests and social media. As this survey was for the support of a student project, the UND Space Studies professional network and the ISU professional network were highly utilized.

In the 2022 survey, 130 respondents initially started the survey. Of those, 128 gave consent to participate in the survey and answered at least one question. Of those who started the survey, 82 respondents completed all questions.

RESULTS

The survey can be divided into three distinct sections: consent, demographics, and main questions. The first section was a consent acknowledgment. This is where participants agreed they met the requirements to participate in the survey and the general information regarding the survey. As the 2022 survey went through the UND IRB, this section was longer and more comprehensive than that of the 2012 survey. All participants were required to consent to participation before proceeding with the remainder of the survey.

Survey Demographic Information

Both surveys contained four demographic questions about the participants' profession, space sector, age, and nationality. The demographic questions focused on how the participants viewed themselves. For the first question, the participant identified themselves as a student, academic, space professional, cyber professional, military, or nonspace-related professional. The next question involved space field the participant had the most experience with, such as commercial space, space agency, international organization, military space-related programs, other, or they did not work in the space field. The third question looked at age categories broken down into one of seven choices. All participants were required to be over 18 years of age.

The final demographic question saw the largest change in wording between the 2012 and 2022 surveys. The intention of the question was to identify the geographic region where the participant lived or worked. The 2012 language asked for nationality, for which the majority of participants answered "other" and typed in individual nationalities such as German, French, *etc*. This question wasn't able to capture the intent of the survey and answers had to be individually categorized by the region after the fact. The 2022 survey rephrased this question to ask for participants' geographic region as North America, Europe, Asia, *etc*.

Overall, the demographics section provides a better insight into the type of individual that responded to the survey. *Table 1* outlines how the average survey participant identified. The respondents between 2012 and 2022 are similar with the exception of age. Participants in the 2022 survey were older and there was a slight increase in commercial space participants.

Survey Questions

Because of limited space, only a few of the survey questions are analyzed here. A full summary of all survey results can be found in the Appendix.

Q1: Highest risk to satellites operating in outer space. One of the thematic foci of these surveys is analyzing whether space professionals perceive satellites as at risk of cyberattacks. The first main question of the survey was asked on an individual page where participants didn't have access to additional questions. This question asked individuals to rank the three options that represented the highest risks to satellites operating in outer space. The list of 15 choices ranged from a combination of satellite system failures, space phenomena, direct/indirect attacks, and a catch-all category for other.

In both the 2012 and 2022 survey, the top two risks identified were space debris collision and space weather. Further, space debris collision was unchanged, whereas the risk posed by space weather decreased slightly. As the risk of space weather has not likely changed, it could be hypothesized that an increase in technology and shielding capabilities has allowed this risk to be lowered. Another option is the increase in competing risks that have removed the focus on space weather. The top-five risks identified in the 2012 and 2022 surveys are shown in Table 2.

In 2012, 5% of participants selected cyberattack in their top-three risks to satellites. Ranking the most selected put

Table 1. Average Demographic of Survey Participants

Average Participant	2012	2022
Category	42% Space Professional	~46% Space Professionals
Space Sector	19% Space Agency 15% Commercial Space	25% Space Agency 17.5% Commercial Space
Between the Ages 18 and 39	69%	~48%
Geographic Location	<50% North American	<60% North American

cyberattacks in fifth place in a three-way tie with accidental collision with another satellite and frequency overload (*i.e.*, jamming). In 2022, 14% of participants included cyberattack in their top-three risks. In the perception of the participants over the past decade, the risk of cyberattack on a satellite had risen 9% or from fifth- to third-ranked highest risk to operating satellites. In addition, other risks such as mechanical failure could have been lowered owing to cheaper satellite launch costs.

Q2: Likelihood of Gaining Unauthorized Access to Satellite Data. The second question used a Likert scale to get participants' opinions on how likely someone could gain unauthorized access to satellite data. This question was modeled on what was proposed by the reported Landsat-7 hack. There is some ambivalence with this question, as satellite data does not always remain on the satellite. There are multiple ways to capture satellite data when the data is not on the satellite, including an unauthorized person setting up a receiver in the downlink footprint of the satellite, hacking into a terrestrial server that holds data collected by a satellite, or accidentally getting emailed a file of collected satellite data by user error. This question does not specify where or how someone gains unauthorized access to the satellite data.

Table 2. Top-Five Risks Identified in the 2012 and 2022 Surveys

Q1	2012	2022
	1) Space Deris Collision—24%	1) Space Debris Collision—24%
	2) Space Weather—20%	2) Space Weather—15%
	3) Mechanical Failure—15%	3) **Cyberattack—14%**
	4) Computer Failure due to User Error—11%	4) 2-way tie: Accidental Collision w/ Another Satellite—8% Mechanical Failure—8%
	5) 3-way tie: Accidental Collision w/Another Satellite—5% **Cyberattack—5%** Frequency Overload (Jamming)—5%	5) 2-way tie: Anti-satellite Weapon (ASAT) from Earth—6% Computer Failure due to User Error—6%

The bold data indicates the highest result.

Table 3. Results of Question Two–Likelihood of Gaining Unauthorized Access to Satellite Data

Q2	2012	2022
Very Likely	13%	15%
Likely	**34%**	**51%**
Neither Likely nor Unlikely	24%	20%
Not Likely	22%	12%
Slim to None	3%	2%

The bold data indicates the highest result.

Table 3 shows participants in both the 2012 and 2022 surveys felt it was likely someone could gain unauthorized access to satellite data. Table 4 visualizes combining the positive responses of *very likely* and *likely*, 47% of participants in 2012 grows to a majority of 66% of participants in 2022. Comparing the change in the surveys, there is a 19% increase in positive response, whereas there is a 11% decrease in the negative opinions of *not likely* and *slim to none*.

The rise of positive responses from 2012 to 2022 could be attributed to multiple factors. First, there has been a rise in publication and articles regarding space cybersecurity and general cybersecurity. Agencies such as NIST and the Aerospace Corporation had multiple publications in this subject area. Second, there was increased public reporting and impact to traditional cyberattacks, such as ransomware and

Table 4. Results of Question Two with Positive and Negative Groupings

Q2	2012	2022
Very Likely and Likely	**47%**	**66%**
Neither Likely nor Unlikely	24%	20%
Not Likely or Slim to None	25%	14%

The bold data indicates the highest result.

Table 5. Results of Question Three–Likelihood of Gaining Unauthorized Control of a Satellite

Q3	2012	2022
Very Likely	4%	7%
Likely	17%	32%
Neither Likely nor Unlikely	15%	23%
Not Likely	**45%**	**33%**
Slim to None	17%	5%

The bold data indicates the highest result.

the 2021 Colonial pipeline attack. The impact of traditional cyberattacks is increasing, which affect a growing number of individuals. Third, many industries are providing increased cyber awareness training, which could influence individual's perspective or belief that cyberattacks are possible.

Q3: Likelihood of Gaining Unauthorized Control of a Satellite. The third question also used a Likert scale to obtain participants' opinions on how likely someone could successfully gain unauthorized ability to control a satellite. This question was modeled on what was proposed by the reported Terra EOS hack. This question has less ambiguity than the previous question.

Table 5 shows the majority of participants in both surveys selected *not likely*. Table 6 visually shows using the previous grouping methodology of positive and negative categories, with positive responses being *very likely* and *likely* and negative responses being *not likely* and *slim to none*, additional perspective can be gained. In 2012, the positive perspective was 21% and the negative concern was 62%. A shift in industry perspective can be forecast when observing 2022, as the positive response is now 39% and the negative response is 38%. This could indicate a shift in perspective of space professionals on the possibility of unauthorized individuals gaining control of a satellite.

Table 6. Results of Question Three with Positive and Negative Groupings

Q3	2012	2022
Very Likely and Likely	21%	**39%**
Neither Likely nor Unlikely	15%	23%
Not Likely or Slim to None	**62%**	38%

The bold data indicates the highest result.

There are multiple reasons a shift in space professionals' opinions changed. Additional research in this area is warranted to answer the following questions. Is there a correlation between increased success of cyberattacks against other industries such as automative, industrial, *etc*. that participants internally compare to satellites? Does the increased access to the satellite market and rise of commercial-off-the-shelf components correlate to attackers' ability to gain control of a satellite? This notional shift has many possibilities for future studies and research.

Q4–5: Who or which entities would want to target satellites. Questions 4 and 5 focused on analyzing the perspective of participants on who or which entities would want to gain unauthorized access to satellite data or control of a satellite (Table 7). These questions asked participants to select up to two groups from a list of eight categories of possible adversaries. As questions 2 and 3 focused on what could or could not be done, questions 4 and 5 involved who would be most likely to perform the action.

There was little change between 2012 and 2022, with both years selecting state-sponsored hacking groups and hacking communities such as Anonymous or Chaos as the most likely actors. Participants did feel that commercial competitors would be more likely to go after unauthorized data than try to take control, whereas terrorists were less likely to attempt gaining unauthorized satellite data and more likely to be suspected of trying to gain unauthorized control of a satellite.

Q8: Mandatory reporting for cyberattacks. Question 8 focused on whether commercial satellite owners should publicly disclose a successful cyberattack on their satellite. There is slight increase in support for this concept with almost a 7% rise in support from 2012 to 2022 (Table 8). This question spells out "a successful attack." A future study might want to modify the question language to a "detected" or "possible" cyberattack.

Q10: Support for security minimums for commercial satellites. Question 10 examines whether security minimums, such as a mandatory encryption level, should be applied to civil and commercial satellites. This concept would involve having more than best practices published for commercial satellites but would imply a baseline minimum standard. Participants supported security minimums in both 2012 and 2022. The 2022 survey shows a 16% increase in support of security minimums (Table 9).

Table 7. Results of Question Four and Five—Who or Which Entities Would Want to Target Satellites?

Q4–5	Data 2012	Data 2022	Control 2012	Control 2022
Commercial Competitors	14.37%	12.32%	6.59%	7.73%
Criminal Groups (illegal arms or drug dealers)	6.32%	4.43%	6.59%	4.64%
Hacking Communities such as Anonymous or Chaos	**22.41%**	**28.08%**	**21.56%**	**23.20%**
Individuals	7.47%	5.42%	4.79%	4.12%
State Sponsored Hacking Groups	**33.34%**	**38.42%**	**38.32%**	**43.30%**
Terrorist	9.77%	5.91%	12.57%	12.37%
I do not know enough about this subject to answer/prefer not to answer[a]	3.45%	4.43%	6.59%	4.412%
Other	2.87%	0.99%	2.99%	0.52%

The bold data indicates the highest result.
[a]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.

It is expected that additional best practices and guidelines for satellite cybersecurity will be published in the upcoming years. Future research is needed to address how the commercial market might want to see security minimums implemented. Would the minimums involve mandatory encryption for the command-and-control links of all satellites or simply require someone sign off on a document acknowledging that the manufacturer has considered cybersecurity risks? The field would benefit from more studies that dive deeper into whether or not a correlation exists between belief in the possibility of a cyberattack against a satellite and support for security minimums. Based on the increased education and awareness between the two studies, it is equally important for the field to understand the underlying factors as to why professionals don't see cyberattacks to satellites as a risk.

CONCLUSION

This article reflected upon what a cybersecurity risk to a space asset could look like and why space professionals might not prioritize cybersecurity. Commercial satellite decision-makers will need to analyze the risk of cyberattacks against satellites and if the cost associated with incorporating cybersecurity is proportional to the perceived threat.

Additional information was obtained from a decadal survey of space professionals conducted in 2012 and again in 2022 (Supplementary Data S1). The decadal results shows an increase in the perceived risk of satellites to cybersecurity threats. From the two sample groups, some additional overarching themes arise:

Table 8. Question Eight—Should Commercial Mandatory Reporting of Satellite Cyberattacks Be Required?

Q8	2012	2022
Yes	45%	51.82%
No	41%	34.55%
I do not know enough about this subject to answer/prefer not to answer	11%	13.64%

Table 9. Question Ten—Should Security Minimums Be Applied to Commercial Satellites?

Q10	2012	2022
Yes	68%	84%
No	20%	13%
I do not know enough about this subject to answer/prefer not to answer	10%	4%

- Space professionals believe that satellites are at an increased risk of cyberattack.
- There is growing belief that unauthorized individuals could likely access satellite data.
- A shift in space professionals' opinions can be seen in the increased support for the notion that unauthorized individuals could gain the ability to control satellites, but a slim majority believe it's still unlikely.
- There is a consistent belief that the unauthorized actors most likely to launch cyberattacks against satellites are state sponsored hacking groups and hacking communities such as Anonymous or Chaos.
- In the commercial market, there is growing support for mandatory reporting of successful cyberattacks against a satellite and requiring minimal cybersecurity standards.

The New Normal

The surveys showed an increased awareness of the cybersecurity aspect of space systems. As the last survey, at least two significant national news events have highlighted the cybersecurity of space assets. A question that future studies might need to address is whether the public attention on the cybersecurity of space assets will lead to long-term increased professional concern.

In Feb 2022, specific modems supported by Viasat's KA-SAT network malfunctioned. This event was later known as the Viasat Hack or by the wiper malware employed AcidRain. The US Department of State released an assessment that "Russia launched cyber attacks in late February against commercial satellite communications networks to disrupt Ukrainian command and control during the invasion, and those actions had spillover impacts into other European countries."[15] This attack was widely known because it impacted areas across Europe and even disabled 5,800 wind turbines Germany.[16]

Another prominent space cybersecurity discussion involves possible Starlink vulnerabilities. Starlink is a commercial satellite constellation owned by SpaceX that provides internet for over 75 countries. This low Earth orbit constellation started in 2019 and, as of April 2024, has over 5,800 satellites in orbit.[17] In August 2022, at the Blackhat and DEFCON conferences, PhD student Lennert Wouters presented on a user terminal Starlink vulnerability that allowed him to get admin or root access to the Starlink Network.[18] SpaceX has a bug bounty page and Lennert's discovered vulnerability was ethically disclosed.

Overall, there is mounting concern by space professionals about the risk to satellites from cyberattack. The observed shift in perspective is not fully defined or agreed upon. Cybersecurity of space assets is a growing area of research that needs additional study. Future studies could investigate information on commercial satellite builders and integrators might be willing to share on cyber vulnerabilities. Also, groups such as NIST or Space Information Sharing and Analysis Center (Space ISAC) might share acknowledged risks and mitigations.

ACKNOWLEDGMENTS

I would like to acknowledge and thank the following advisors for their assistance in these efforts. For the first study, I could not have accomplished the 2012 survey or harnessed such a large space professional network without the International Space University (ISU), the ISU Class of 2012, and Professor Angie Bukley. For the more recent 2022 study, I need to thank the University of North Dakota (UND), my academic advisor Professor Michael Dodge, and my individual advisors for this paper Professors Joseph J. Vacek and Professor Kim Donehower. Overall I cannot emphasize enough my gratitude to the ISU and UND space networks for being able to reach such a wide international and diverse space audience.

AUTHORS' CONTRIBUTIONS

Rachel Jones is the sole author and contributor. She performed all data curation, formal analysis, conceptualization, investigation, and project administration.

AUTHOR DISCLOSURE STATEMENT

No competing financial interests exist.

FUNDING INFORMATION

This work was supported by the Laboratory Directed Research and Development (LDRD) program within the Savannah River National Laboratory (SRNL). This document was prepared in conjunction with work accomplished under Contract No. 89303321CEM000080 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

SUPPLEMENTARY MATERIAL

Supplementary Data S1

REFERENCE

1. Daily Mail Reporter. Real-life Star Wars: US claims Chinese military were behind hackers who seized control of two U.S. satellites. Daily Mail.com. 2011, November 18. Available from: https://www.dailymail.co.uk/news/article-2062755/Real-life-Star-Wars-Were-Chinese-hackers-attacks-U-S-military-satellites.html [Last accessed: February 13, 2024].

2. Tech PC. Chinese hackers took control of NASA satellite for 11 minutes. PC Tech Magazine. 2011, November 21. Available from: https://pctechmag.com/2011/11/chinese-hackers-took-control-of-nasa-satellite-for-11-minutes/ [Last accessed: February 13, 2024].
3. U.S.-China Economic and Security Review Commission. 2011 Report to Congress of the U.S.-China Economic and Security Review Commission. Washington DC, U.S. Government Printing Office; 2011. Available from: https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf [Last accessed: February 13, 2024].
4. Soesanto S. Terra calling: Defending and securing the space economy: From science to fiction and back to reality. CSS Cyberdefense Reports. 2021, January 8. Available from: https://doi.org/10.3929/ethz-b-000460220 [Last accessed: February 13, 2024].
5. ChesleyB, Johnson T, Sellers J. Understanding cybersecurity in the space domain. Workshop presented virtually. Hosted by American Institute of Aeronautics and Astronautics, Teaching Science & Technology, Inc.; 2021 October 6–8; Zoom.
6. Editor CC. cyber risk—Glossary | CSRC. csrc.nist.gov. Available from: https://csrc.nist.gov/glossary/term/cyber_risk
7. Manulis M, Bridges CP, Harrison R, et al. Cyber security in New Space Analysis of threats, key enabling technologies and challenges. Int J Inf Secur 2020;20(3): 287–311; doi: 10.1007/s10207-020-00503-w
8. Bingen KA, Johnson K, Young M, Raymond JW. Space Threat Assessment 2023. Center for Strategic and International Studies. 2023, April 14. Available from: https://aerospace.csis.org/wp-content/uploads/2023/04/230414_Bingen_SpaceThreatAssessment_2023_UPDATED-min.pdf
9. Bailey B, Speelman RJ, Doshi PA, et al. Defending Spacecraft in the Cyber Domain. Aerospace Center for Space Policy and Strategy. 2019, November 5. Available from: https://csps.aerospace.org/papers/defending-spacecraft-cyber-domain [Last accessed: June 26, 2023].
10. EwartR, Wheeler W, Betser J, et al. Cyber enhanced space operations-from frameworks to enterprise evolution. Conference paper of AIAA SPACE 2016; 2016 September 13–16. Reston, Virginia: American Institute of Aeronautics and Astronautics; 2016, September 9. Available from: https://doi.org/10.2514/6.2016-5474
11. Falco G. Cybersecurity principles for space systems. J Aerosp Inf Syst 2019; 16(2):61–70; doi: 10.2514/1.i010693
12. Hack-A-Sat. [place unknown: publisher unknown]; 2023. Available from: https://hackasat.com/ [Last accessed: February 13, 2024].
13. Stakem P. Hacking Cubesats, Cybersecurity in Space. Independently published: Unknown; 2020.
14. Poole C, Bettinger R, Reith M. Shifting satellite control paradigms operational cybersecurity in the age of megaconstellations. Air Space Power J 2021;35(3): 46–56. Available from: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-35_Issue-3/T-Poole.pdf [Last accessed: February 15, 2024].
15. Blinken A. Attribution of Russia's Malicious Cyber Activity Against Ukraine. Department of State Press Statement. 2022 May 10. Available from: https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/
16. Zhadan A. Viasat cyberattack linked to Russian state-sponsored hackers. Cybernews. 2024 January 3. Available from: https://cybernews.com/cyber-war/viasat-cyberattack-linked-to-russian-state-sponsored-hackers/
17. McDowell J. Starlink Statistics. Jonathan's Space Pages. 2024, May 15. Available from: https://planet4589.org/space/con/star/stats.html
18. Wouters L. Glitched on Earth by Humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal. Blackhat You Tube Channel. 2022, November 17. Available from: https://www.youtube.com/watch?v=NXqLMmGwJm0&t=1406s

Address correspondence to:
Rachel C. Jones
Space Scientist
Savannah River National Laboratory (SRNL)
Savannah River Site
Aiken
SC 29808
USA

E-mail: Rachel.Jones@srnl.doe.gov

(Appendix follows →)

APPENDIX

DEMOGRAPHIC INFORMATION

D1-Which of the following categories best describe you?

D1	2012	2022
Student	30%	12.5%
Academic	10%	13.33%
Space Professional (nonmilitary[a], Current, or retired)	42%	45.83%
Cyber Professional (current or retired)	2%	1.67%
Military	2%	5%
Nonspace-Related Profession	7%	15%
Other	2%	6.67%

[a]The nonmilitary designator only appeared in the 2022 survey.

D2-In which sector of the space field does most of your experience lie in?

D2	2012[a]	2022
Commercial Space (Space X, DRL, *etc.*)	15%	17.5%
Space Agency (NASA, ESA, *etc.*)	19%	25%
International Organization (UN)	0%	3.3%
Military Space-related program[a]	N/A	19.17%
Other	7%	15%
I do not work in space-related field[b]	N/A	20%

[a]In the 2012 survey, D2 only asked to the ∼42% participants that indicated they were space professionals.
[b]The "Military space-related program" and "I do not work in space related field" option only appeared in the 2022 survey.

D3-Which of the following age groups would you consider yourself?

D3	2012	2022
Under 19 years old	0%	1.67%
20–29	33%	19.17%
30–39	36%	26.67%
40–49	14%	21.67%
50–59	8%	16.67%
60–69	4%	10%
70 and above	0%	4.17%

D4 (2012)—Please identify your nationality (nationalities)*

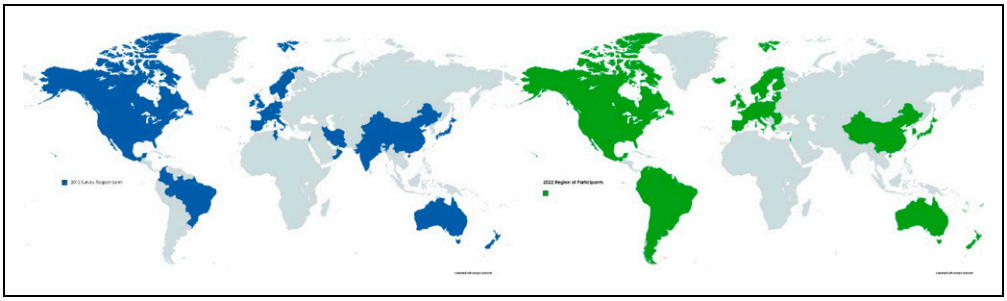
D4	2012[a]	2022
North America (Canada, United Space, Mexico, *etc.*)	–	63.33%
Central America	–	0%
South America	–	4.17%
Europe	–	24.17%
Middle-East	–	0.83%
Africa	–	0%
Asia	–	1.67%
Australia and Oceania countries	–	2.5%
Earthling / Prefer not to answer	–	2.5%
Other	–	0.83%

[a]Individual percentage categories for the 2012 survey would not hold up to scrutiny. Visual analysis of the total typed out "other answer" indicated that more than 50% of respondents identified as North American.

(Appendix continues →)

D4(2022)—Please identify your main geographic location or workplace

Graphical visualization of the survey participants' main geographic location or workplace, question D4.



SURVEY QUESTIONS

Q1-Select the three options that represent the highest risks to satellite operating in outer space.

Q1	2012	2022
Accidental Collision with Another Satellite	5%	8.26%
Anti-Satellite Weapon (ASAT) from Earth	2%	5.9%
Attack from Another Satellite or Spacecraft	>1%	3.24%
Asteroid Collision	2%	1.77%
Computer Failure due to User Error	11%	5.6%
Cyberattack	5%	13.57%
Delayed Ground-Hardware Sabotage	>1%	2.06%
Electromagnetic Field (Jamming)	4%	4.72%
Frequency Overload (Jamming)	5%	2.36%
Ground Control Station Failure	3%	3.24%
Lasers (Ground)	>1%	0.88%
Mechanical Failure	15%	7.96%
Space Debris Collision	24%	23.89%
Space Weather (Radiation, Solar Flare, CME)	20%	15.34%
Other	2%	1.17%[a]

[a]The 2022 survey allowed text input for other answer. Results included: Attitude and/or Orbit Control System Failure, Propellant loss owing to excessive maneuvering to avoid space debris or noncooperative satellites, defunding or bankruptcy of operating agency, incompetent or poorly trained engineers.

Q2-How likely do you think it is that someone would successfully gain unauthorized access to satellite data information?

Q2	2012	2022
Very Likely	13%	15.32%
Likely	34%	51.35%
Neither Likely nor Unlikely	24%	19.82%
Not Likely	22%	11.71%
Slim to None	3%	1.8%

Q3-How likely do you think it is that someone would successfully gain unauthorized ability to control a satellite?

Q3	2012	2022
Very Likely	4%	7.21%
Likely	17%	32.43%
Neither Likely nor Unlikely	15%	22.52%
Not Likely	45%	33.33%
Slim to None	17%	4.5%

(Appendix continues →)

Q4-Which entities (select up to two) would you most likely suspect to try and gain unauthorized access to data (information being collected) of satellites?

Q4	2012	2022
Commercial Competitors	14.37%	12.32%
Criminal Groups (illegal arms or drug dealers)	6.32%	4.43%
Hacking Communities such as Anonymous or Chaos	22.41%	28.08%
Individuals	7.47%	5.42%
State-Sponsored Hacking Groups	33.34%	38.42%
Terrorist	9.77%	5.91%
I do not know enough about this subject to answer/prefer not to answer[a]	3.45%	4.43%
Other	2.87%	0.99%[b]

[a]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.
[b]The 2022 other answers: "Define data. . .the questions are wrong," "State intelligence agencies hacking department (cost this as appropriate)."

Q5-Which entities (select up to two) would you most likely suspect to try and gain unauthorized access control of satellites?

Q5	2012	2022
Commercial Competitors	6.59%	7.73%
Criminal Groups (illegal arms or drug dealers)	6.59%	4.64%
Hacking Communities such as Anonymous or Chaos	21.56%	23.2%
Individuals	4.79%	4.12%
State-Sponsored Hacking Groups	38.32%	43.30%
Terrorist	12.57%	12.37%
I do not know enough about this subject to answer/prefer not to answer[a]	6.59%	4.12%
Other	2.99%	0.52%[b]

[a]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.
[b]The 2022 other answer: "State intelligence agencies hacking department (cost this as appropriate)."

Q6-Do you think a cyberattack against a satellite could be clearly defined as a deliberate attack against an individual country?

Q6	2012[a]	2022
Yes	42%	60.91%
No	45%	32.73%
I do not know enough about this subject/ prefer not to answer[b]	11%	6.36%

[a]The total of the results for 2012 does not equal 100% but these were the scores reported by the survey platform. It's likely that this is based on possible rounding errors or some chose to skip this question.
[b]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.

Q7-Do you think it is possible to prove beyond a doubt that one person/group/state is responsible for an instance of hacking?

Q7	2012[a]	2022
Yes	30%	42.73%
No	49%	40.91%
I do not know enough about this subject/ prefer not to answer[b]	19%	16.36%

[a]The total of the results for 2012 does not equal 100% but these were the scores reported by the survey platform. It's likely that this is based on possible rounding errors or some chose to skip this question.
[b]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.

Q8-Should it be mandatory for commercial satellite owners to publicly announce a successful cyberattack on their satellite/s?

Q8	2012[a]	2022
Yes	45%	51.82%
No	41%	34.55%
I do not know enough about this subject/ prefer not to answer[b]	11%	13.64%

[a]The total of the results for 2012 does not equal 100% but these were the scores reported by the survey platform. It's likely that this is based on possible rounding errors or some chose to skip this question.
[b]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.

(Appendix continues →)

Q9-Who should lead an investigation on a cyberattack directed toward a commercial satellite?

Q9	2012[a]	2022
The Owner of the Satellite	22%	20.91%
The Country of Registration	34%	34.55%
Another or a Different Country/Countries	0%	0%
An International Organization	32%	30.91%
I do not know enough about this subject to answer / prefer not to answer[b]	5%	9.09%
Other	2%	4.55%[c]

[a]The total of the results for 2012 does not equal 100% but these were the scores reported by the survey platform. It's likely that this is based on possible rounding errors or some chose to skip this question.
[b]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.
[c]The 2022 other text inputs were: "The country of registration and the manufacturer of satellite, independent third party, NSA in the US, the countries intelligence service." "This is a national asset like a Nuclear Power Plant, privately owned or not, A collaborative international consortium consisting of ITAR approved countries in cooperation with the commercial or academic satellite originator and manufacturer, Trusted commercial consortium."

Q10-Do you think a security minimum (such as a mandatory encryption level) should be applied to civil and commercial satellites?

Q10	2012[a]	2022
Yes	68%	83.64%
No	20%	12.73%
I do not know enough about this subject / prefer not to answer[b]	10%	3.64%

[a]The total of the results for 2012 does not equal 100% but these were the scores reported by the survey platform. It's likely that this is based on possible rounding errors or some chose to skip this question.
[b]The "prefer not to answer" portion of this choice only appeared in the 2022 survey.