Fall 2021

Shifting Satellite Control Paradigms: Operational Cybersecurity in the Age of Megaconstellations

Carl A. Poole [*]

Robert A. Bettinger

Mark Reith

Shifting Satellite Control Paradigms

Operational Cybersecurity in the Age of Megaconstellations

Carl Poole
Robert Bettinger
Mark Reith

The introduction of automated satellite control systems into a space-mission environment historically dominated by human-in-the-loop operations will require a more focused understanding of cybersecurity measures to ensure space system safety and security. On the ground-segment side of satellite control, the debut of privately owned communication antennas for rent and a move to cloud-based operations or mission centers will bring new requirements for cyber protection for both Department of Defense (DOD) and commercial satellite operations alike. It is no longer a matter of whether automation will be introduced to satellite operations, but how quickly satellite operators can adapt to the onset of control automation and promote cybersecurity in an increasingly competitive, contested, and congested space domain.

Introduction

Control automation has spread from industrial manufacturing and self-driving cars to home and household appliances. Control automation has also moved into

the realm of satellite-control operations, with the focus of satellite-control automation being driven on two fronts. First, the ability to incorporate cost-effective, highly capable equipment in the satellite design allows for an increase in onboard controls processing. Second, the proliferation of space operations in various orbital regimes—this article will focus on low-Earth orbit (LEO)—is pushing complex tasks, such as satellite-link scheduling and conjunction-avoidance maneuvers, beyond the control of human operators.

An additional operational distinction is made between satellite automation—the self-contained system process of conducting repetitive tasks—and satellite autonomy, which gives the satellite the ability to implement changes with limited to no human-in-the-loop actions.[1] This distinction will add a level of complexity to the cybersecurity of satellite control. Placing tasks previously controlled by humans under the control of a computer-executed algorithm may be the only viable way to manage the development of future megaconstellations and enable effective space-traffic management.[2] But the prospect of improved space-traffic safety and collision avoidance via control automation raises several concerns.

While increasing the levels at which LEO constellations can interact and cooperate, the needed hardware infrastructure and data-exchange alterations that will allow for such interoperability will introduce new entry points that, in turn, will likely increase cybersecurity risks. The introduction of software-defined equipment, cloud-based mission-control centers, and Ground Stations as a Service (GSaaS) are prime examples. Space and cybersecurity professionals will need increased interactive cooperation and mission understanding to address new potential cybersecurity issues presented by emerging commercial space applications and automation.

Current Satellite Control Operations

The control architecture for satellites has remained nearly constant since the beginning of the Space Age in the mid-twentieth century. Starting with the launch of the first artificial satellites, each on-orbit system has mostly featured a unique design, function, and mode of operation. This uniqueness has led to self-contained and independent operating procedures controlled by the satellite owner. In the typical satellite-control structure, a satellite downlinks information such as payload data and spacecraft state-of-health information when it is within view of a ground-based receiver. From the receiver, the information is processed and passed to the satellite operations center (SOC), which reviews it for faults and assesses the need for required operating adjustments and/or new system instructions.

In the case of orbital maneuvers to correct for position or to change location (such as slewing, station keeping, or collision avoidance with another object), one member of the operations team scripts the commands for the prescribed maneu-

ver. Several operations team members then review the script before passing it to the human-in-the-loop satellite operator for processing. During the next scheduled uplink opportunity with the satellite, the commands are sent from the SOC to the transceiver and then to the satellite for processing and command execution. This type of hands-on approach developed due to constraints in the onboard systems, specifically, limited computing power and proprietary operating structures.

The emphasis on human control ostensibly meant reduced concerns for cybersecurity and an increased sense of command situational awareness due to the human use of protected ground communications systems and owner-controlled data links. Despite its benefits, this process can be very time-consuming, and task scheduling becomes increasingly complex with the addition of new satellites to the satellite-control architecture. Consequently, this human-in-the-loop satellite-control architecture will be unable, without a substantial increase in infrastructure, manning, and funding, to effectively manage the size of megaconstellations of the near future.

Anatomy of Megaconstellations

The development of constellations consisting of thousands of individual satellites controlled by one operator is no longer a wistful dream of science fiction or avant-garde technologists. With the introduction of LEO constellations such as "Starlink" or "OneWeb," the concept of megaconstellations is becoming a reality, precipitating the rise of megaconstellations as a potential means to provide regional and global telecommunications services.[3]

In Asia, China Telecom reportedly plans to create a 10,000-satellite megaconstellation called "China StarNet" in the next 5–10 years.[4] In late 2020, the European Union revealed plans to initiate a program to develop a telecommunications megaconstellation to establish "European digital sovereignty."[5] The proliferation of LEO with tens of thousands of satellites will require increasing levels of automation to handle intraconstellation operations and to enable future constellation growth and system safety in a given orbital altitude regime.

The creation of megaconstellations is the result of two factors. First, the shift in the commercial space industry to create standardized, rapidly produced, and high-volume space-capable vehicles has caused both the size and cost of individual satellites to decrease drastically.[6] The ability to buy commercial-off-the-shelf components instead of making proprietary hardware lowers the cost of research and development, thus accelerating system production.

The second factor is a function of satellite size. As the satellite form factor decreases, more satellites can fit inside the payload fairing of a single launch vehicle, which, in turn, drives down the cost per satellite to reach orbit. Overall, the costs

of satellite design, production, and space launch are decreasing, thus allowing for the nearly exponential proliferation of near-Earth orbital regimes. Consequently, the increase in satellites will lead to an escalation of costs associated with operations if the current satellite control paradigm does not evolve to meet the challenges of proliferated orbits.

The evolution of satellite control from human-in-the-loop commands to automation will require the megaconstellation, in concert with the ground communications networks, to deconflict satellite pass times over receiver antennas at specified ground stations.[7] By definition, a "pass time" is the time each satellite needs to downlink, or transmit, data to the ground antenna, as well as to uplink, or receive, commands from the ground station. Depending on the mission and amount of information transmitted, timing is critical.

In addition, the orbital altitude of a given satellite determines the access durations to each ground antenna: the lower the satellite altitude, the faster the satellite passes over a given point on the ground. This planning will be increasingly important as the communication bandwidths become more crowded due to more satellites flying within the ground receiver's view.

Since the early twenty-first century, an increase in CPU power has enabled the addition of programmable capabilities to onboard satellite subsystems.[8] A growing number of satellites are now being equipped with onboard systems that resemble a standard personal computer.[9] This design architecture, in turn, increases reliability. A satellite's onboard system can now identify and correct for faults and adapt to changing parameters much faster than a human-in-the-loop system.[10] A human-in-the-loop system is comparatively slower due to data transmission and analysis delays and the need for an extra layer of review to verify the correctness and validity of planned operations before command uplink.

One of the most common satellite-control tasks is that of station keeping or maintaining a satellite's predetermined, mission-centric orbital attitude and position. For megaconstellations, an attitude determination and control system may control all station-keeping operations. Due to an increase in ground-station demand resulting from a vastly greater number of contacts, each satellite will have to determine correct orbital attitude and position deviations autonomously to ensure continued constellation stability and mission functionality and to reduce the likelihood of satellite collisions.[11]

Shifting such attitude and orbit maintenance tasks away from the ground segment, however, will require the introduction of a robust fault- and error-alert architecture to identify and notify the human satellite operators of any anomalous events. Ultimately, raising more house-keeping commands into the purview of control automation will shift the satellite maintenance workload from continuous

hands-on, day-to-day human operations to an on-call, human-response control structure. Greater automation will also remove the likelihood of an incomplete command sent by human operators or the need to check for unsafe commands before data uplink.[12]

Satellite Control Evolution

While automation will play a large role in handling satellite functions, the main changes for cybersecurity will come from the evolutionary shifts made in the ground-control segments and associated security implementation requirements. In the 2020 Space Capstone Publication *Spacepower: Doctrine for Space Forces*, the foundation for cybersecurity is defined in the cyber operations spacepower discipline as the "knowledge to defend the global networks upon which military space power is vitally dependent," the "ability to employ cybersecurity and cyber defense of critical space networks and systems," and the "skill to employ future offensive capabilities."[13]

The future of security implementation is already being felt on the manufacturing side for DOD contracts. The recently introduced Cybersecurity Maturity Model Certification (CMMC) program pushes the level of responsibility for cybersecurity down, starting with the industries providing the components and systems, then to the Department of Defense by requiring it to use the published National Institute of Standards and Technology rating system.[14] The CMMC is also rooted in the Federal Acquisition Regulation, Federal Information Processing Standards, and general industry collaboration.[15]

The CMMC does have several caveats such as not requiring compliance for commercial-off-the-shelf systems.[16] This shift will ensure the hardware and software introduced for future satellite-control needs will be primed for cyberdefense. Another aspect that will play a role in the coming changes focuses on the protection of potential dual-use technologies. "Entrepreneurs with innovative and potentially dual-use technologies must improve the protection of their intellectual property from unintended foreign assimilation, including protecting their networks from cyber exfiltration attempts, and avoiding exit strategies that transfer intellectual property to foreign control hostile to U.S. interests."[17]

Some of these dual-use technologies can come in the form of software-defined components that will allow for greater flexibilities in upgrading the on-orbit and ground-control segments, especially in the area of communication systems.[18] Though software-defined systems will add increased flexibility and allow for faster fixes if damaged (for example, there is no need to replace expensive parts if the component can be simply reprogrammed), it will also introduce a new level of

security requirements and response capabilities due to the inherent vulnerabilities in all software control systems.

Unlike traditional cybersecurity training provided to most Airmen, Guardians may require enhanced cyber skills to manage risk in the space environment. The Space Force chief technology and innovation officer describes USSF as a digital service; accordingly, Guardians will likely need to understand how digital engineering intersects with cybersecurity in order to model complex systems and cyber threats.[19] Guardians will need to be able to conceptualize how existing hardware and evolving software components interact as well as how they may be exploited by threat actors.

Furthermore, they will likely benefit from development, security, and operations training that will help them craft new software components that not only meet mission needs but are continuously hardened in response to evolving threats. Advanced digital twin modeling—a one-for-one virtual model tested in an operationally accurate simulated environment—may provide a feedback loop to inform operators of how well these new software components perform across a risk spectrum.

Another area of evolving satellite control relates to the use of flexible ground control systems, more specifically, the ground antennas used to transmit commands and receive data. Commercial entities such as Microsoft are introducing GSaaS to increase capabilities and offset costs associated with satellite command and control.[20] These systems will need to be diverse in operational software and equipment to cover the wide range of satellite technologies currently used. Alternatively, future satellite designs that intend to use this emerging method of ground control can establish a form of technological standardization. In either case, commercializing the ground segment will help handle the increased volume and bolster networked capabilities.

Despite these benefits, however, current satellite programs base network security on the legacy assumption that ground stations and the associated ground network are program- or owner-controlled, system-specific, and isolated from other networks. A new control structure is only half of the required change—the other half involves changing how and where some of the satellite-control operations and tasks are conducted.

This second change is coming in the form of cloud-based SOCs. As with the software-defined component and commercialized ground stations, cloud-based control will provide a more robust and flexible answer for growing constellations without the need to build costly new mission-specific "brick and mortar" operations centers.[21] This area already has several working examples, such as the "Major Tom" system—produced by the commercial firm Kubos—that is implemented by

the Planet company for use in its Dove constellation consisting of approximately 250 small satellites.[22]

Cloud-based systems will have the added benefit of being accessible from any "secure" networked computer. In concert with the aforementioned commercial ground stations, cloud-based systems could enable megaconstellation control from any location on the globe featuring a proper access point.

In the emerging satellite-control dynamic, an example of potential operations starts with a customer satellite sending spacecraft state-of-health or other data to a configured service receiver. The receiver then uploads the data to a cloud-based SOC that is accessible by satellite operators from any networked computer system. Even with this control flexibility, the use of increasingly networked systems owned by third parties, rather than the satellite or constellation operator, can introduce new entry points and areas for cyber vulnerability.[23] To ensure the cyber protection of all US and Allied space-based assets, satellite programs and control architectures directly in touch with these evolving systems will need to change just as drastically as the systems themselves.[24]

Satellite Survivability Considerations

The goal of any satellite system is to maintain mission functionality for the planned mission lifetime; this requires satellite survivability. Satellite survivability is a function of three time-separated phases: susceptibility, vulnerability, and recoverability. Survivability is promoted if a system's susceptibility and vulnerability to natural and/or manmade threats are minimized while the prospect of recoverability is maximized. From a manmade-threat perspective, susceptibility analysis focuses on the threat system and its ability to successfully detect, be employed, intercept, and finally function as intended vis-à-vis the target satellite system.

Similarly, a satellite's vulnerability relates to its ability to survive the threat's intended weapon effects. Finally, recoverability is the ability of a satellite (and the satellite operators), following damage from a threat system, to take emergency action to prevent the loss of the satellite and/or to regain a level of satellite mission capability.[25] These components of survivability can be extrapolated to megaconstellations as a system-of-systems due to their interconnected internal communications and mission architecture.

The Venn diagram (fig. 1) depicts survivability considerations for megaconstellations, outlining the aspects of susceptibility, vulnerability, and recoverability. Overall, the high number of satellites comprising megaconstellations and the use of emerging autonomy and network technologies represent both primary strengths and weaknesses for megaconstellations. While the risk of satellite collision and debris impact constitute a constant environmental risk to operations, megacon-

stellations are increasingly susceptible to cybersecurity threats due to the use of commercial GSaaS and cloud-based satellite operations.

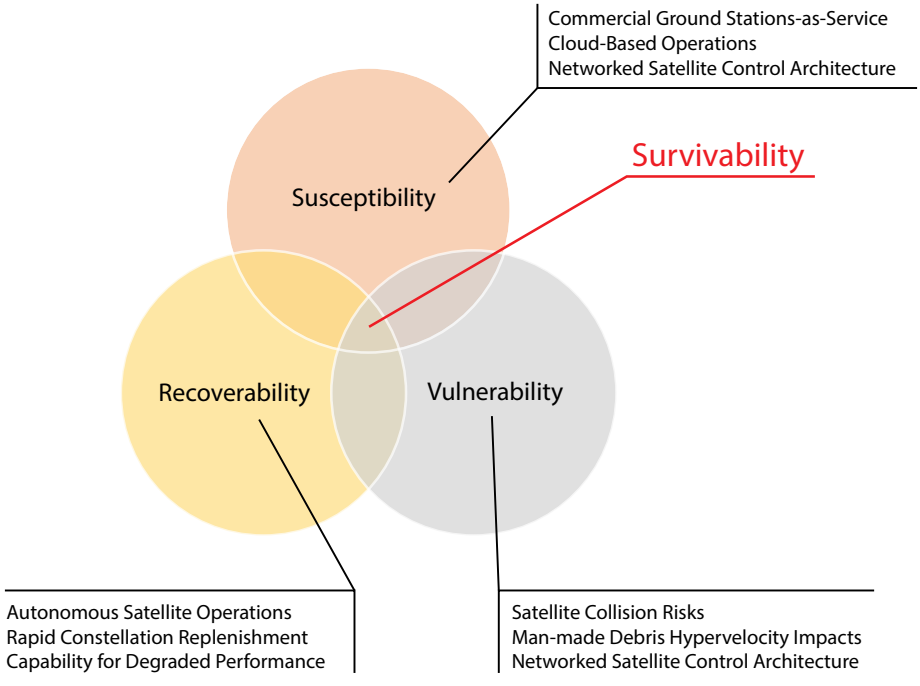

Figure 1. Megaconstellation survivability

Cybersecurity threats are varied based on the source of origin and damage mechanism. Satellite operators must maintain a proper understanding of the cyber-threat landscape and the digital and networked functionality of the mega-constellation in order to secure continued mission effectiveness and survivability.

The Networked Operations Center

With anticipated shifts in both methods and infrastructure for space-control operations, there should be an equal shift in the cadre structure and training for satellite-operation teams in the Department of Defense and commercial sectors. On the satellite-operations floor, operators often reach out to fellow team members when anomalous situations arise with satellite systems. But this consultation only works well if the members on both ends of the conversation talk the same language.

As the transition to increasingly networked centers interfacing with highly automated systems progresses, space operations and cybersecurity professionals should learn and understand more of the other members' skill sets and technical terminology. Ideally, the formal training for satellite-operations team members

will evolve to include a space- and cyber-centric curriculum. This training could be in the form of introductory classes into cyberdefense for space professionals, and satellite mission design and communications for the cyber professionals.

The USSF is in the crucial position to make this happen starting at the ground level. As mentioned in the Space Capstone Publication, increased education will add to the understanding of the "network dimension."[26] Optimally, this education would result in embedding cyberoperations members at key SOCs, in addition to having increased cybersecurity and monitoring training at all levels of satellite operations. This approach will facilitate a highly digitally capable satellite-operations cadre.[27]

Building a cyber-minded and space-proficient space-control foundation will ensure space and cyberspace professionals will have the tools needed to tackle any future growth in satellite capabilities and space mission execution. It will also empower members with the abilities and confidence to react rapidly and even preemptively to future threats.

Conclusion

Satellite systems and controls architectures are in a rapid state of change. Satellite automation could significantly alter the current hands-on satellite-operations mission to one of key-event monitoring, with a consolidated human-in-the-loop team present to react to and resolve issues that cannot be directly handled by the satellite itself or by the megaconstellation. Additionally, the introduction of a more capable and increasingly flexible mission-operations system, one using emerging technologies such as cloud-based networks and services like privately owned and networked ground stations, will make it possible for true 24/7 global access to and control of satellite systems.

To ensure the continued safety and security of on-orbit satellite systems, both the defense and commercial space sectors must adapt to the rapidly changing digital landscape of future space operations. The introduction of the CMMC has already demonstrated such an adaptation, along with the alignment of emergent USSF doctrine and strategy with cyber-mindedness. The final step will be to shape the future of the USSF and USAF space and cyberspace cadre to be better prepared as a digital force synergistically working to remain at the forefront of protection in the increasingly competitive, contested, and congested domain of space.

As LEO becomes more congested and the mission sets for megaconstellations expand beyond telecommunications, the operating altitudes for megaconstellations will also expand. As a result, the space and cyberspace cadre—Airmen and Guardians alike—must be poised to handle considerations of autonomy and cybersecurity in LEO, geosynchronous Earth orbit, and beyond into the cislunar realm. ✪

Carl Poole
Captain Carl Poole, USSF, is an orbital analyst and holds a master of science from the Air Force Institute of Technology.

Robert Bettinger
Dr. Robert Bettinger, Major, USAF, is an assistant professor of astronautical engineering and curriculum chair for the astronautical engineering degree program at the Air Force Institute of Technology.

Mark Reith
Dr. Mark G. Reith, USAF, retired, is an adjunct professor of systems engineering at the Air Force Institute of Technology.

Notes

1. J. B. Hartley and P. M. Hughes, "Automation of Satellite Operations: Experiences and Future Directions at NASA GSFC," in *Space Mission Operations and Ground Data Systems - SpaceOps '96, Proceedings of the Fourth International Symposium held 16-20 September 1996 in Munich, Germany*, ed. T. D. Guyenne (Paris: European Space Agency, 1996): 1262–69.

2. Steven J. Butow et al., *State of the Space Industrial Base 2020: A Time for Action to Sustain US Economic & Military Leadership in Space*, (Washington, DC: USSF, Air Force Research Laboratory, and Defense Innovation Unit, July 2020), http://aerospace.csis.org/.

3. Jonathan C. McDowell, "The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation," *Astrophysical Journal Letters* 892, no. 2 (2020): 1–18, https://iopscience.iop.org/.

4. Dan Swinhoe, "China's Moves into Mega Satellite Constellations Could Add to the Space Debris Problem," Data Center Dynamics, April 20, 2021, https://www.datacenterdynamics.com/.

5. Jonathan O'Callaghan, "Europe Wants to Build Its Own Satellite Mega Constellation to Rival SpaceX's Starlink," *Forbes*, December 23, 2020, https://www.forbes.com/.

6. Mohamed Khalil Ben-Larbi et al., "Towards the Automated Operations of Large Distributed Satellite Systems, Part I: Review and Paradigm Shifts," *Advances in Space Research* 67, no. 1 (June 1, 2021), https://www.sciencedirect.com/; and Ben-Larbi et al., "Towards the Automated Operations of Large Distributed Satellite Systems, Part II: Classification and Tools," *Advances in Space Research* 67, no. 1 (June 1, 2021), https://www.sciencedirect.com/.

7. Ben-Larbi et al., "Paradigm Shifts"; Ben-Larbi et al., "Classification and Tools"; Michael J. Bentley, Alan C. Lin, and Douglas D. Hodson, "Overcoming Challenges to Air Force Satellite Ground Control Automation," in *Proceedings of the IEEE Multi-Disciplinary Conference on Cognitive Methods in Situational Awareness and Decision Support (CogSIMA)* (Curran Associates, June 2017), https://ieeexplore.ieee.org/; and Jun Tominaga, José Demísio Simões da Silva, and Mauricio Goncalves Vieira Ferreira, "A Proposal for Implementing Automation in Satellite Control Planning" (paper, SpaceOps 2008 Conference, Heidelberg, Germany, May 12-16, 2008), https://arc.aiaa.org/.

8. Misa Iovanov et al., "Automation of Daily Tasks Necessary for the Management of a Large Satellite Constellation" (paper, American Institute of Aeronautics and Astronautics (AIAA) Space 2003 Conference & Exposition, Long Beach, CA, September 23-25, 2003), https://arc.aiaa.org/.

9. Ben-Larbi et al., "Paradigm Shifts"; and Ben-Larbi et al., "Classification and Tools."

10. Gilles Kbidy, "Flying Large Constellations Using Automation and Big Data" (paper, SpaceOps 2016 Conference, Daejeon, South Korea, May 13, 2016), https://arc.aiaa.org/.

11. Jérôme Thomassin, Maxime Ecochard, and Guillaume Azema, "Predictive Autonomous Orbit Control Method for Low Earth Orbit Satellites" (paper, International Symposium on Space Flight Dynamics, Matsuyama, Japan, June 6-9, 2017), https://issfd.org/; and Byoung-Sun Lee, Yoola Hwang, and Hae-Yeon Kim, "Automation of the Flight Dynamics Operations for Low Earth Orbit Satellite Mission Control," in *Proceedings of the 2008 International Conference on Control, Automation, and Systems* (Curran Associates, April 2009), https://ieeexplore.ieee.org/.

12. Ben-Larbi et al., "Paradigm Shifts"; and Ben-Larbi et al., "Classification and Tools."

13. John W. Raymond, *Spacepower: Doctrine for Space Forces*, Space Capstone Publication (Washington DC: USSF, June 2020), 52, https://www.spaceforce.mil/.

14. Barry Rosenberg, " 'Start of a New Day': DoD's New Cybersecurity Regs Take Effect Today,'" Breaking Defense, December 1, 2020, https://breakingdefense.com/.

15. "Understanding the CMMC Fundamentals," Cybersecurity Maturity Model Certfication Center of Excellence, November 26, 2020, https://cmmc-coe.org/.

16. Rosenberg, " 'New Day.'"

17. Butow et al., "Space Industrial Base."

18. M. Manulis et al., "Cyber Security in New Space," *International Journal of Information Security* 20 (2020): 287–311, https://link.springer.com/.

19. Space Force Chief Technology and Innovation Office, *U.S. Space Force Vision for a Digital Service*, (Washington, DC: USSF, May 2021), https://media.defense.gov/.

20. Theresa Hitchens, "Microsoft Boosts Space Services, Partnerships," Breaking Defense, October 20, 2020, https://breakingdefense.com/.

21. Ben-Larbi et al., "Paradigm Shifts"; and Ben-Larbi et al., "Classification and Tools."

22. Kubos, "Major Tom"; and Ben-Larbi et al., "Paradigm Shifts."

23. J. D. Scanlan et al., "New Internet Satellite Constellations to Increase Cyber Risk in Ill-Prepared Industries," (paper, 70th International Astronautical Congress, Washington, DC, October 21-25, 2019).

24. Department of Defense (DOD), *Defense Space Strategy Summary* (Washington, DC: DOD, June 2020), https://media.defense.gov/.

25. Andrew J. Lingenfelter, Joshuah A. Hess, and Robert A. Bettinger, "From Sanctuary to Warfighting Domain: A Space System Survivability Framework," *Aircraft Survivability*, Summer 2021, 7–16.

26. Raymond, *Spacepower,* 7.

27. Charles Pope, "Driven by 'a Tectonic Shift in Warfare' Raymond Describes Space Force's Achievements and Future," SpaceForce News, September 15, 2020, https://www.spaceforce.mil/.