Center for Cyber & Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

Trends in Technology and Digital Security

Space, Satellites, and Critical Infrastructure

Issue Brief 3 in a Series
Based on Fall 2017 Symposium Proceedings

Panelists
Chris DeMay - HawkEye 360
Caitlin Durkovich - Toffler Associates
Nick Eftimiades - Penn State University
Shang Hsiung - Raytheon

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

This publication is the exclusive work product of the Center for Cyber & Homeland Security. It was made possible thanks to the financial support of Razor's Edge Ventures and Raytheon Company.

RAZOR'S EDGE

Raytheon

Issue Brief Series on Trends in Technology and Digital Security
Space, Satellites, and Critical Infrastructure

On September 14, 2017, CCHS convened a Symposium on Trends in Technology and Digital Security. Four panels addressed emerging threats and their implications for security policy, with a focus on digital infrastructure protection and anticipatory analysis. In a series of Issue Briefs, CCHS shares the findings and recommendations that emerged from the Symposium, primarily on a not-for-attribution basis. This third Brief in the series addresses Space, Satellites, and Critical Infrastructure.

Old Space, New Space, and the New Space Economy

In the words of the Department of Defense, space today is congested, competitive, and contested. The last 30 to 35 years have witnessed remarkable change: at the outset of that interval, we did not have the Global Positioning Systems (GPS)[1]; or at least it was not publicly used at that point. There were no smartphones. The World Wide Web was just coming on. There were no laptops, digital cameras, DVDs, hybrid cars, or 3D printing. Artificial Intelligence was in a very nascent form. There was no commercial remote sensing. All of this happened in the space of just one career, as one Symposium participant noted. During that period, the ground itself shifted—relative to society—and that really impacted our understanding of space, how we are able to use it, and how it affects us.

Now, space is a $340-billion industry, every year—and that does not include all the secondary and tertiary uses of space that occur every day (for example, how much FedEx saves when it is using GPS, just-in-time delivery programs, and things of that sort). Seventy nations have assets, significant interests, in space today. Yet, 40 years ago, there were just two: the United States and Russia. Space has become essential, not only to the government and to our ability to project power; but to the American way of life. It is a necessity for disaster mitigation, diplomacy, intelligence, and the economy—it is becoming increasingly commercial.

This is what we are faced with; but we must also add into that mix the changing dynamic of how space is used and how much of a role it plays in society, as well as a threat ramp that is escalating very, very, quickly. It has been for the last 10 years, but the technology is advancing dramatically—the miniaturization technology, our ability to put up small satellites, nanosatellites and such, is advancing tremendously. More and more, space is becoming a commercial endeavor; and then you start adding in the nation-state roles (China and Russia)—and then you have an environment in which we are not really used to dealing.

[1] GPS is a satellite-based system that provides three essential services: position, navigation, and timing. That third piece, timing, is particularly important and enables much of the operational efficiency of our infrastructure and the systems as a whole. It is critical to how we operate as a society and as a people—global commerce, the Internet, mobile technology, and essential services (such as transportation, electricity, banking, and food and agriculture).

When you think about the military's applications in space in particular, it is amazing: in World War II, in order to hit a target that was 60-foot by 100-foot, we averaged 1,500 B-17 sorties dropping nine thousand 250-pound bombs. Fast-forward to current, and we have got one B-2 with sixteen 2,000-pound bombs, able to engage 16 targets. Due to our space communications backbone, we also have automated air re-tasking as well as all-weather flight capabilities. That is an extraordinary change; and that is just in the past decade or two that we have really advanced that type of precision use of space services: blue-force tracking, air/shipping navigation, command and control, drone use—all using space, as the backbone.

In fact, many military simulations, if you start taking out the space-related services of remote sensing and GPS, the casualty rates go up significantly—dramatically so—for U.S. forces. Of course, the Armed Forces exercise these scenarios and try to develop mitigation measures; and change tactics accordingly, as you would hope the military does. But the threat to U.S. forces is still there. We have this issue to contend with in the military; and we have it in civil applications and commercial applications, from weather and urban planning, all the way through to automated autonomous cars and precision agriculture.

All countries in the world that have any interest in space are banking on this new space economy and moving aggressively in that direction. In Tokyo, for instance, the new space economy is much discussed, and the government there is making concerted efforts to move industry into that economy.

So, this is where we live at this point. Is the United States prepared for the future on this, as an issue of policy, and security? One participant, Nicholas Eftimiades of Penn State University, thought not, observing that we still have STRATCOM, which plays the major role in protecting space. Professor Eftimiades questioned whether that is an appropriate paradigm for the future, noting further that the old law of the sea doctrine is a common analogy for space protection. The reality, however, is that this paradigm might not be appropriate for the future. Space is a critical part of this nation's future—it is critical infrastructure—far more critical than a power plant in a given U.S. state. Where are we in dealing with that, in terms of: our policies, our governance of it internationally, and how we are going to identify all the red lines that policy needs to do, to be able to ensure safety and security in space? We are nowhere near the refined level of process and policy that is required.

Satellites, Large and Small: Security Implications

Turning specifically to satellites, one participant in the Symposium, HawkEye 360 co-founder and Chief Operating Officer Chris DeMay, detailed his professional background in government, where he learned much about what it means for large and small spacecraft to be designed with security in mind. After transitioning to the corporate setting, he began learning quite a lot about state of the art in small-satellite technology. Security was not an afterthought in the corporate setting, but certainly the entrepreneurial startup mentality is heavily focused on product development and value delivery.

HawkEye 360 is an analytics company that is developing a novel suite of geo-analytic products and services that utilize radio frequency (RF) data collected from space. The company is launching and operating small satellites in order to get a unique data set that has not been seen commercially before. The company's full constellation of satellites will likely be about thirty satellites in ten clusters. As the company starts to roll out its capability and launch its first satellites next February, it will have something very powerful and very important that is following in the footsteps of what commercial imagery did 20 years ago. Here is a capability that, historically, has been a government capability; that has now been brought commercially, using private funds. Those private funds are invested with the intent of developing capability, in this case, for commercial purposes. But those commercial applications still need security in mind.

HawkEye 360 recognized that to be successful, there must be a day one commitment to systems and operational security. With a startup culture and budget, the company has by design built a team with deep experience in all aspects of security.

The company noted the commercial market is increasingly becoming as demanding as government markets for security. The converging security interests of the private and public sector have led to innovations in cloud technologies that the company works to leverage in combination with its own security practices. Security risks from previously unidentified threats escalate every day. Given that environment, the company hopes the U.S. government community and commercial community will continue to work together to develop and continually evolve best in class security practices. The company is looking to the commercial world and seeing what is being done to leverage proven commercial solutions, including managed cloud solutions. For instance, in the offices of HawkEye 360, you would not see racks and racks of equipment because the company is leveraging the security that Amazon and Google have already built; HawkEye 360 is taking advantage of that. The company seeks to deliver to customers a solution that is transparent, and provides active defense that is seamless.

Another Symposium participant detailed his company's work over the years for the national community in space, emphasizing that security has been a big driver for the company. To this point, a number of different changes have been implemented within the company, including the creation of a cyber group which is primarily trying to bring DOD-level security capabilities into commercial markets.

From a security perspective, loss of assets in space is a concern. Part of the concern, if not a major concern, is that when it takes 15 to 20 years to put that first asset up, the loss of that is critical. But then, you look at a small company (like the previous participant's) which has been in existence for not a very long time, and they have a six-month order-to-orbit model; one then wonders: how does that impact security, because, if I can indeed put up a payload or a capability now, in months instead of years, how can we leverage that model? The participant's company, a large enterprise, is looking at that question in terms of how do we leverage these capabilities in order to help better serve the national security market? By the same token, from the government perspective, what are the capabilities there that could be leveraged as well, directly to the government?

This puts us at an interesting paradigm: what happens to the Defense Industrial Base that is regulated by the Federal Acquisition Regulations (and many other regulations), that appear to go by the wayside when you are dealing with a commercial company? How do we level that playing field? That is something we need discussions about. When a government agency could buy something from a commercial company, maybe there is a competition, maybe there is not; maybe there are all these rules, maybe not.

From a government perspective, there is also risk aversion on the government side. The government tends to want to take 15 years to deploy a program because they want to make sure it is absolutely, positively successful. So, we will spend $10 billion to launch a satellite. Or, one could spend—divide that by 100—and one could launch 100 smaller satellites in significantly less time; is that a better model, if 90% of them fail? Is it better, now, to take the six-month order-to-orbit and say, well, for that kind of money, for that kind of speed, is it worthwhile to fail some, to succeed some?

When you have these short cycles, they actually do improve your security, because you have alternatives to waiting; you have alternatives to the loss now (although, to achieve higher resolution or higher sensitivity, costs more money and takes more time). The smaller satellites may be thought of as a quick replenishment capability, to support as needed, and thereby help deter some threats. There is a potential to do something different; maybe you do not achieve the same effect, but maybe you can achieve an effect that is good enough. The model, whereby the government invests and industry invests, could work—meaning, if the venture is successful, then government is paid back for its investment; or, if the venture is not successful, then both parties lose.

Critical Infrastructure—Positioning, Navigation, and Timing:
Outdated Policy Negatively Impacts Security

Another Symposium participant, Caitlin Durkovich, a director at Toffler Associates and previously the Assistant Secretary for Infrastructure Protection at the Department of Homeland Security, referenced the ubiquity of GPS (Global Positioning System) and PNT (positioning, navigation, and timing), emphasizing the fact that this is a government-provisioned service, it is free, and it is in nearly every critical infrastructure. As such, it underpins our way of life, and certainly our economy—from precision agriculture, to location services, to the efficiency of the electric grid; and, increasingly, as we look at smart cities, the autonomous environment, it is critical to the future. At the same time, it is a single point of failure. We do not have a backup or, at least, a holistic backup to this critical system. There are fragmented solutions that are leveraged across industry; and some of the options that would make it more resilient and more redundant—leveraging other systems like GLONASS and GALILEO—are fraught with their own vulnerabilities as well.

A further problem is that space-based positioning, navigation, and timing is governed by a very outdated policy: NSPD-39, which dates back to 2004. Policy here is largely governed within the space directorate of the National Security Council (NSC). Every now and then other parts of the NSC, such as the Resilience Directorate, or the Office of Science and Technology Policy, get involved; but it is fragmented, within the Executive Office of the President. Equally important, the governing policy gives primacy to the Department of

Defense and the Department of Transportation, with some responsibility to the Department of Homeland Security. Given the ubiquity of GPS and PNT, however, the policy is outdated. Consider: when you convene the interagency on this issue through the National Executive Committee (EXCOM) for Space-Based PNT, Treasury and the Department of Energy do not even have an official seat at the table—which is somewhat ironic, given how much they have come to rely on these services. Even more important, because the EXCOM falls outside of the modern NSC processes, its recommendations have no teeth; they do not end up going to a deputies' committee or principals' committee meeting. This policy needs to be front and center, number one priority, in terms of updating Presidential Policy Directives.

Another challenge is that this area very much embodies what the public/private partnership is, yet it does not leverage some of the principles that have come to define that relationship—primarily, around how we share threat information with, not only manufacturers, but the users of the chips and of the signal itself—to help them understand what is driving government policy, and why maybe we are not making what is in their minds smart business decisions. In turn, this lends itself to the question: should space be another critical infrastructure sector? The idea has certainly been bandied around. Given that, in some ways, it is an outdated framework and an outdated structure that prevails, we do need have to have a serious conversation about this idea—much like we did with election systems and whether they should be designated critical infrastructure. At a minimum, all of the stakeholders should be brought together for discussion. Another Symposium participant proposed that we need not get too hung up on the question of whether space should be designated a critical infrastructure, since government prioritizes its efforts according to the following criteria: is it a system, asset, or network that is so important that its disruption would have a debilitating impact on security, economic security, public health and safety, or a combination thereof? Since many of the assets, systems, and networks in space meet that definition, they will be treated accordingly, regardless of declarative status.

As we increasingly leverage technology and push towards where we are going in new space, we have to keep security in mind, and we have got to have the same kind of risk management approach that we have applied to terrestrial infrastructure. That means appreciating the threats and hazards that exist, and the whole concept of security by design. According to the director of security for a new entrant in the aerospace industry in California, however, innovation still stands in the way of security—just basic practices that we have learned about over time (concerning, for example, the insider threat). We must learn from the lessons of the past; we have to put the security experts next to the coders, developers, and builders, as we move forward. In short, as we rush to adopt technologies in the marketplace, industry needs to better understand the risks that come with it. Security and resilience need to be part of what companies do, too. A breach of security will cause you brand, regulatory, operations, and other problems; and it will cost you money. Yet, security is an afterthought, until it is not there.

The New Space Race Takes Shape

China is leading the play in space. It has poured much into this, and has much coming from foreign sources. Europe has served as an open-source support element for the Chinese

space program. Since most advanced European nations do not have laws regarding just discussion, there is a running stream of European scientists going to and from China, spending 3 or 4 months twice a year (at Beijing University and other places throughout the country), developing China's small-satellite program. As a result, China has moved tremendously quickly in a very short period of time. By comparison, the way our own systems are working is deeply problematic. Consider the Austrian scientist who tried moving his work through the European Space Agency (ESA) for 3 years, and could not get anywhere with the massive bureaucracy, until he went to the Chinese. And now it is China that is doing groundbreaking work in quantum communications.

About Us

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

Website http://cchs.gwu.edu **Email** cchs@email.gwu.edu **Twitter** @gwcchs